Státnicový okruh 1: Matematické metody

26. dubna 2022

Obsah

Množiny, operace s množinami, kartézský součin množin, konečné, spočetné a nespočetné množiny. Číselné množiny. Princip indukce. Relace a jejich vlastnosti, operace s relacemi, reprezentace relací. Binární relace na množině, uzávěry relací, ekvivalence, rozklad na množině, uspořádané množiny. Zobrazení a jejich vlastnosti.

1 Množiny

Množina je objekt, který se skládá z jiných objektů tzv. **prvků** té množiny. Množiny zpravidla značíme velkými písmeny (A, B, ..., Z), jejich prvky pak malými písmeny (a, b, ..., z). Fakt, že x je prvkem množiny A značíme $x \in A$. Není-li prvkem A značíme $x \notin A$.

Množina je jednoznačné dána svými prvky. Prvek do množiny buď patní nebo ne. Nemá tedy smysl hovořit o pořadí prvků a také nemá smysl zabývat se tím kolikrát se daný prvek v množině nachází. Speciální množinou je tzv. **prázdná množina** značíme $\emptyset$. Tato množina neobsahuje žádné prvky tedy pro všechna x platí, že $x \notin \emptyset$.

1.1 Dělení množin

Množiny dělíme na **konečné** a **nekonečné**. Množina A se nazývá konečná právě když existuje přirozené číslo n tak že prvky této množiny můžeme očíslovat čísly 1, 2, ..., n. Číslo n nazveme počet prvků množiny a značíme jej $|A|$ Pokud $|A| = \infty$ nazveme množinu nekonečnou a říkáme, že má nekonečně mnoho prvků.

Spočetná množina znamená zjednodušeně řečeno „množina, jejíž prvky lze spočítat“. Spočítáním se zde rozumí očíslování prvků množiny přirozenými čísly - přitom je jedno, zda použiji konečný nebo nekonečný počet přirozených čísel.

1.2 Zapisování množin

Množiny můžeme zapisovat následujícími způsoby:

1. **Výčtem prvků** - Množinu která obsahuje prvky $a_1, a_2, \dots, a_n$ zapíšeme následovně $\{a_1, a_2, \dots, a_n\}$.
2. **Pomocí charakteristické vlastnosti** - Množina obsahuje právě ty prvky, které splňují vlastnost $\varphi(x)$ zapisujeme $\{x|\varphi(x)\}$. Vlastnost $\varphi(x)$ může být popsána i slovně. Příklad $\varphi(x)$: číslo x je sudé.

1.3 Vztahy mezi množinami

Základními vztahy mezi množinami jsou **rovnost** $(=)$ a **inkluze** $(\subseteq)$

$A = B$ znamená, že pro každé $x : x \in A$ právě když $x \in B$

$A \subseteq B$ znamená, že pro každé x : jestliže $x \in A$ pak $x \in B$

$A \neq B$ znamená že neplatí $A = B$

$A \not\subseteq B$ znamená, že neplatí $A \subseteq B$

Množina jejichž prvky jsou právě všechny podmnožiny dané množiny X, nazýváme **potenční množina** množiny X značí se $\mathscr{P}(X)$ nebo také 2^X. Tedy $2^X = \{A|A \subseteq X\}$.

1.4 Operace s množinami

Mezi základní operace s množinami patří průnik (značí se $\cap$), sjednocení (značí se $\cup$), rozdíl (značí se $\setminus$).

Jsou-li A, B množiny, definujeme množiny $A \cup B, A \cap B, A \setminus B$ následovně:

$A \cap B = \{x|x \in A \text{ a } x \in B\}$

$A \cup B = \{x|x \in A \text{ nebo } x \in B\}$

$A \setminus B = \{x|x \in A \text{ a } x \notin B\}$

Množiny nazýváme navzájem disjunktní právě když $A \cap B = \emptyset$.

1.4.1 Vlastnosti operací

- $A \cap \emptyset = \emptyset, \quad A \cup \emptyset = A, \quad A \cap A = A$
- $A \cup B = B \cup A, \quad A \cap B = B \cap A$
- $(A \cup B) \cup C = A \cup (B \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $A \cup (A \cap B) = A, \quad A \cap (A \cup B) = A$

2 Princip indukce

Princip matematické indukce umožňuje dokazovat tvrzení ve tvaru „pro každé přirozené číslo n platí $V(n)$“, kde $V(n)$ je nějaké tvrzení, které závisí na n (např. $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$).

Věta 1. *Nechť je pro každé $n \in \mathbb{N}$ dáno tvrzení $V(n)$. Předpokládejme že platí*

- *V(1) (indukční předpoklad)*

- *pro každé $n \in \mathbb{N}$: z V(n) plyne V(n + 1) (indukční krok).*

Pak platí V(n) pro každé $n \in \mathbb{N}$.

Princip indukce je jednou ze základních vlastností přirozených čísel, Z předpokladu, že každá neprázdná podmnožina $K \subseteq \mathbb{N}$má nejmenší prvek (což je pravdivý a intuitivně jasný předpoklad) lze princip indukce dokázat.

Příklad 1. *Dokažte už uvedený vztah $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. Tedy V(n) je tvrzení $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$. Podle principu indukce stačí ověřit indukční předpoklad a indukční krok.*

Indukční předpoklad: V(1) je tvrzení $1 = \frac{1\cdot(1+1)}{2}$ a to evidentně platí.

Indukční krok: Předpokládejme, že platí V(n) a dokažme V(n + 1). $1 + \cdots + n + n + 1$ se rovná $(1 + \cdots + n) + n + 1$, což se dle předpokladu rovná $\frac{n(n+1)}{2} + n + 1$. Dále je $\frac{n(n+1)}{2} + n + 1 = \frac{n(n+1)+2(n+1)}{2} = \frac{n^2+3n+2}{2} = \frac{(n+1)\cdot(n+2)}{2}$. Celkem tedy $1 + \cdots + n + n + 1 = \frac{(n+1)\cdot(n+2)}{2}$, což je právě tvrzení V(n + 1).

Podle principu indukce je tedy tvrzení dokázané.

3 Relace

Pojem relace je matematickým protějškem pojmu *vztah*. Různé objekty jsou nebo nejsou v různých vztazích. Například číslo 3 je ve vztahu „být menší“ s číslem 5. Vztah je také určen aritou tj. počtem objektů které do vztahu vstupují, výše uvedený příklad má aritu 2 protože porovnáváme 2 čísla. Takovou relaci nazveme binární. Dále máme unární (jeden prvek), ternární (tři prvky), ...

Definice 1. *Kartézský součin množin $X_1, X_2, \ldots, X_n$ je množina $X_1 \times X_2 \times \cdots \times X_n$ definovaná předpisem*

$$X_1 \times \cdots \times X_n = \{\langle x_1, \ldots x_n\rangle | x_1 \in X_1, \ldots, x_n \in X_n\}$$

Kartézský součin n množin je množina všech uspořádaných n-tic prvků z těchto množin. Je-li $X_1 = \cdots = X_n = X$ pak $X_1 \times \cdots \times X_n$ značíme také X^n (n-tá kartézská mocnina množiny X)

Definice 2. *Nechť $X_1, \ldots, X_n$ jsou množiny. Relace mezi $X_1, \ldots, X_n$ je libovolná podmnožina kartézského součinu $X_1 \times \cdots \times X_n$.*

Příklad 2. *Mějme množinu $A = \{1, 2, 3, 4\}$ a množinu $B = \{a, b, c, d\}$. Relace $R, S \subseteq A \times B$ mohou vypadat následovně.*

$$R = \{\langle 1, a\rangle, \langle 1, b\rangle, \langle 3, d\rangle, \langle 4, a\rangle\}$$

$$S = \{\langle 3, a\rangle, \langle 1, c\rangle, \langle 4, c\rangle\}\}$$

3.1 Operace s (binárními) relacemi

Relace jsou množiny n-tic. Proto s nimi jde provádět množinové operace ($\cap, \cup, \setminus$) a lze na ně aplikovat rovnost a inkluzi ($=, \subseteq$). S binárními relacemi můžeme provádět další operace. Začněme tzv. inverzní relací k relaci $R \subseteq X \times Y$ je relace R^{-1} definovaná předpisem:

$$R^{-1} = \{\langle y, x\rangle | \langle x, y\rangle \in R\}$$

Další operací je tzv. skládání Je-li R relací mezi množinami X a Y a S relací mezi množinami Y a Z, pak složením relací R a S je relace $R \circ S$ mezi X a Z definovaná předpisem:

$$R \circ S = \{\langle x, z\rangle | \exists y \in Y : \langle x, y\rangle \in R \text{ a } \langle y, z\rangle \in S\}$$

Věta 2. *Pro relace $R \subseteq X \times Y, S \subseteq Y \times Z, T \subseteq Z \times U$ platí:*

a) $(R^{-1})^{-1} = R$

b) $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$

c) $R \circ (S \circ T) = (R \circ S) \circ T$

3.2 Reprezentace relací

3.2.1 Tabulkou

Binární relace lze znázorňovat tabulkami. Například relace
$R = \{\langle 1, \alpha\rangle, \langle 2, \gamma\rangle, \langle 1, \delta\rangle, \langle 2, \beta\rangle, \langle 3, \alpha\rangle\}$ mezi množinami
$X = \{1, 2, 3\}$ a $Y = \{\alpha, \beta, \gamma, \delta, \epsilon\}$ je znázorněna následující tabulkou.

R	α	β	γ	δ	ε
1	$\times$			$\times$	
2		$\times$	$\times$		
3	$\times$				

Tedy je-li $\langle x, y\rangle \in R$, je v průsečíku řádku x a sloupce y symbol $\times$, jinak tam není nic.

3.2.2 Maticí

Matice typu $m \times n$ je obdélníkové schéma o m řádcích a n sloupcích, ve kterém se na každém místě odpovídajícím nějakému řádku a nějakému sloupci nachází nějaká (nejčastěji číselná) hodnota. Označme tuto matici M, pro každé $i \in \{1, \ldots, m\}$ a $j \in \{1, \ldots, n\}$

Nechť R je relace mezi množinami $X = \{x_1, \ldots, x_m\}$ a $Y = \{y_1, \ldots, y_n\}$. Potom relaci R reprezentujeme maticí tak, že pokud:

$$\langle x_i, y_j \rangle \in R \text{ pak } m_{ij} = 1$$

$$\langle x_i, y_j \rangle \notin R \text{ pak } m_{ij} = 0$$

Tuto matici nazveme **matice relace** R a značíme ji M_R. Matice M_R relace $R = \{\langle 1, \alpha \rangle, \langle 2, \gamma \rangle, \langle 1, \delta \rangle, \langle 2, \beta$
mezi množinami
$X = \{1, 2, 3\}$ a $Y = \{\alpha, \beta, \gamma, \delta, \epsilon\}$ bude vypadat následovně.

$$\mathbf{M_R} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Nevýhodou této metody je její paměťová složitost. Pokud budeme mít matici 1000×1000, tak musíme v paměti uchovat milión prvků a pokud z nich bude jen 3000 rovno 1 potom zbytek uchováváme zbytečně protože víme, že na ostatních pozicích musí být 0.

Pro binární relace můžeme zavést operace, které odpovídají operacím s relacemi. Mějme binární matice M, N typu $m \times n$ a matici K typu $n \times k$. Definujeme následující operace:

$$M \vee N = P, \qquad p_{ij} = max\{m_{ij}, n_{ij}\};$$

$$M \wedge N = P, \qquad min\{m_{ij}, n_{ij}\};$$

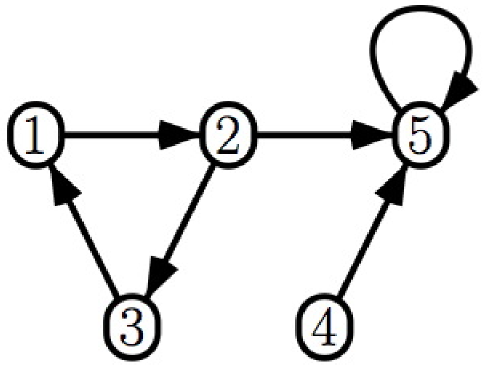
$$M - N = P, \qquad max\{0, m_{ij} - n_{ij}\};$$

$$M \cdot K = P, \qquad max\{m_{ij} \cdot k_{ij}; I = 1, \ldots, n\};$$

$$M^T, \qquad m^T_{ij} = m_{ji}$$

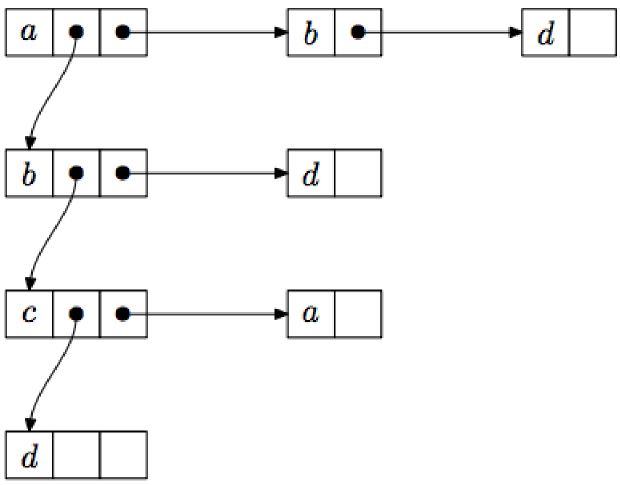
3.2.3 Grafem

Grafy představují další způsob reprezentace binárních relací, který je názorný. Graf binární relace R na množině X dostaneme tak, že každý prvek $x \in X$ znázorníme v rovině jako kroužek s označením daného prvku. Pokud $\langle x, y \rangle \in R$, nakreslíme z uzlu x do uzlu y orientovanou hranu.



3.2.4 Seznamem seznamů

Další způsob reprezentace pro uložení binární relace R na množině X (pro uložení binární relace v paměti počítače) je reprezentace seznamem seznamů. Tuto reprezentaci tvoří hlavní (spojový) seznam, ve kterém jsou uloženy všechny prvky množiny X. Z každého prvku $x \in X$ hlavního seznamu vede seznam obsahující právě ty $y \in X$, pro které platí $\langle x, y \rangle \in R$. Mějme relaci $R = \{\langle a, b \rangle, \langle a, d \rangle, \langle c, a \rangle, \langle b, d \rangle\}$ na množině $X = \{a, b, c, d\}$ potom reprezentace seznamem seznamů vypadá následovně.



3.3 Zobrazení (funkce)

Zobrazení (funkce) je matematickým protějškem běžně používaného pojmu přiřazení.

Definice 3. *Relace R mezi X a Y se nazývá zobrazení (funkce) množiny X do množiny Y, právě když pro každé $x \in X$ existuje právě jedno $y \in Y$ tak že $\langle x, y \rangle \in R$.*

Definice 4. *Zobrazení $f : X \to Y$ se nazývá* *a)* ***prosté (injektivní)****, právě když pro každé* $x_1, x_2 \in X$*, pro* $x_1 \neq x_2$ *plyne* $f(x_1) \neq f(x_2)$*,*

b) ***surjektivní*** *nebo-li zobrazení* X ***na*** Y*, právě když pro každé* $y \in Y$ *existuje* $x \in X$ *tak, že* $f(x) = y$*,*

c) ***vzájemně jednoznačné (bijektivní)****, právě když je prosté a na (je tedy injektivní a současně surjektivní).*

Věta 3. *Pro zobrazení* $f : X \to Y, g : Y \to Z$ *platí*

a) $f \circ g$ *je zobrazení,*

b) jsou-li f,g injekce, je $f \circ g$ *injekce,*

c) jsou-li f,g surjekce, je $f \circ g$ *surjekce.*

Věta 4. *Nechť* $f : A \to B$ *je zobrazení. Inverzní relace* f^{-1} *je zobrazením* $B \to A$ *tehdy a jen tehdy, je-li* f *bijekce.*

Důsledek 1. *Nechť* $f : A \to B,\ g : B \to C$ *jsou bijekce. Pak*

a) $f^{-1} : B \to A$ *je bijekce*

b) $g^{-1} \circ f^{-1}$ *je bijekce* C *na* A *a platí* $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Definice 5. *Nechť* $A \neq \emptyset$ *je množina. Zobrazení* $id_A : A \to A$ *dané předpisem* $id_A(x) = x$ *pro každé* $x \in A$ *se nazývá* ***identické zobrazení****.*

Věta 5. *Nechť* $f : A \to B$ *je zobrazení. Pak*

a) $f = f \circ id_B = id_A \circ f$

b) f *je bijekce tehdy a jen tehdy, když existuje zobrazení* $g : B \to A$ *tak, že* $f \circ g = id_A, g \circ f = id_B$

3.3.1 Poznámka k nekonečným množinám

Definice 6. *Množina* A *se nazývá* ***spočetná*** *, právě když existuje bijekce* $f : A \to \mathbb{N}$*. Množina se nazývá* ***nespočetná****, právě když je nekonečná a není spočetná.*

3.4 Binární relace na množině

Binární relace na množině jsou matematickým protějškem vztahů mezi dvěma prvky množiny například: „x je menší než y“. Speciálními relacemi jsou **prázdná relace** $\emptyset$**,** **relace identity** $\omega_X = \{\langle x, x\rangle \mid x \in X\}$, a **kartézský čtverec** $\tau_X = X \times X$.

Definice 7. *Nechť* R *je binární relace na* X*. Řekněme že* R *je*

- ***reflexivní**, pokud pro každé $x \in X$ platí $\langle x, x \rangle \in R$*
- ***symetrická**, pokud pro každé $x, y \in X$ platí $\langle x, y \rangle \in R \Rightarrow \langle y, x \rangle \in R$*
- ***antisymetrická**, pokud pro každé $x, y \in X$ platí $(\langle x, y \rangle \in R \wedge \langle y, x \rangle \in R) \Rightarrow x = y$*
- ***tranzitivní**, pokud pro každé $x, y, z \in X$ platí $(\langle x, y \rangle \in R \wedge \langle y, z \rangle \in R) \Rightarrow \langle x, z \rangle \in R$*
- ***irreflexivní**, pokud pro každé $x \in X$ platí $\langle x, x \rangle \notin R$*
- ***asymetrická**, pokud pro každé $x, y \in X$ platí $\langle x, y \rangle \in R \Rightarrow \langle y, x \rangle \notin R$*
- ***úplná**, pokud pro každé $x, y \in X$ platí $\langle x, y \rangle \in R \vee \langle y, x \rangle \in R$*

Relace R je **(relace) ekvivalence**, jestliže je reflexivní, symetrická, a tranzitivní. Relace R je **(relace) uspořádání**, jestliže je reflexivní, antisymetrická a tranzitivní.

Reflexivita relace R vyjadřuje, že každý prvek $x \in X$ je v relace „sám se sebou“. V matici takovou relaci poznáme že má na diagonále samé 1, v orientovaném grafu je u každého uzlu smyčka.

Symetrie relace R vyjadřuje, že $\langle x, y \rangle \in R$ právě když $\langle y, x \rangle \in R$ Tedy relace R je symetrická pokud pro $\forall x, y \in X$ máme buď současně $\langle x, y \rangle \in R$ a $\langle y, x \rangle \in R$, nebo současně $\langle x, y \rangle \notin R$ a $\langle y, x \rangle \notin R$. Symetrickou relaci v matici M_R poznáme tak, že je symetrická podle hlavní podle hlavní diagonály. V grafu se tato relace pozná tak že pokud vede orientovaná hrana z x do y pak musí vést i z y do x, nebo z x do y nevede žádná hrana.

Antisymetrie relace R vyjadřuje,že pro každé dav různé prvky $x, y \in X$ neplatí současně $\langle x, y \rangle \in R$ a $\langle y, x \rangle \in R$. V matici M_R poznáme antisymetrii tak, že dvě různá pole, která jsou souměrná podle diagonály neobsahují dvě jedničky. V grafu se antisymetrie projevuje tak, že meze dvěma různými vrcholy x, y je buď jedna hrana nebo žádná.

Tranzitivita relace R vyjadřuje, že pro pokud $\langle x, y \rangle \in R$ a pokud $\langle y, z \rangle \in R$, pak také $\langle y, z \rangle \in R$. V grafu je tranzitivita projevuje tak, že pokud vede hrana z x do y a zároveň z y do z potom také x do z.

Irreflexivita relace R vyjadřuje, že žádný prvek $x \in X$ není v relaci „sám se sebou“.

Asymetrie relace R vyjadřuje, že do R nepadnou $\langle x, y \rangle$ a $\langle y, x \rangle$ současně.

Úplnost relace R vyjadřuje, že aspoň jedna z dvojic $\langle x, y \rangle$, $\langle y, x \rangle$ padne do R.

3.5 Uzávěry relací

Ke každé binární relaci můžeme stanovit její reflexivní, symetrický a tranzitivní uzávěr, to je nejmenší reflexivní, symetrickou a tranzitivní relaci na dané množině, která obsahuje výchozí relaci.

Věta 6. *Nechť R je binární relace na X. Pak*

- *Ref(R)* $= R \cup \omega_X$
- *Sym(R)* $= R \cup R^{-1}$
- *Tra(R)* $= \bigcup_{n=1}^{\infty} R^n$, *kde* $R^1 = R$ *a* $R^n = R \circ R^{n-1}$

3.6 Ekvivalence

Je binární relace, kterou lze interpretovat jako matematický protějšek nerozlišitelnosti. Pro ekvivalenci E na množině X definujeme pro každý $x \in X$ množinu $[x]_E = \{y \in X \mid \langle x, y\rangle \in E\}$, kterou nazýváme **třída ekvivalence prvku** x. Zřejmě $[x]_E$ obsahuje právě ty prvky z X, které nelze od x rozlišit ekvivalencí E.

3.7 Rozklad

Rozklad na množině je matematický protějšek shluků nerozlišitelných prvků. Rozklad na X je **disjuktní pokrytí** X.

Definice 8. *Nechť $X \neq \emptyset$. Systém množin $\sqcap \subseteq 2^X$ splňující*

1. $Y \neq \emptyset$ *pro každou* $Y \in \sqcap$,
2. *pro každé* $Y_1, Y_2 \in \sqcap$ *platí: pokud* $Y_1 \cap Y_1 \neq \emptyset$, *pak* $Y_1 = Y_2$,
3. $\bigcup \sqcap = X$,

*se nazývá **rozklad na množině** X. Množiny $Y \in \sqcap$ nazýváme **třídy rozkladu** $\sqcap$. Pro prvek $x \in X$ označíme $[x]_\sqcap$ tu třídu rozkladu $\sqcap$, která obsahuje x.*

Na množině X existuji dva mezní rozklady.Prvním z nic je rozklad $\sqcap$, kde $[x]_\sqcap = \{x\}$ pro každé $x \in X$, tj všechny třídy rozkladu $\sqcap$ jsou jednoprvkové. Druhým mezním případem je rozklad $\sqcap = \{X\}$, tj. $\sqcap$ obsahuje jedinou třídu, která je rovna celé X, tedy $[x]_\sqcap = X$ pro každé $x \in X$.

Věta 7. *Nechť $\sqcap$ je rozklad na X. Pak binární relace $E_\sqcap$ na X definovaná $\langle x, y\rangle \in E_\sqcap$, právě když $[x]_\sqcap = [y]_\sqcap$ je ekvivalence.*

Kromě ekvivalencí a rozkladů existují další přirozené pohledy na to „jak zjednodušit nazírání“ na výchozí množinu. Jedním z nich je **surjektivní zobrazení**. Pokud je zobrazení $f : X \to Y$ surjektivní, pak lez chápat obraz $f(x)$ prvku x jako vyjádření „prvek x nahradíme prvkem $f(x)$“. Ukážeme, že surjektivní zobrazení a ekvivalence mají zvláštní vztah. Pro zobrazení $f : X \to Y$ definujeme binární relaci E_f na X předpisem

$$\langle x, y\rangle \in E_f \qquad \text{právě když} \qquad f(x) = f(y)$$

Zřejmě E_f je ekvivalence, tzv. **ekvivalence indukovaná zobrazením** f.

3.8 Uspořádání

Uspořádání je v informatice zcela zásadní ačkoliv si to někdy neuvědomujeme, Mezi základní každého informatika patří znalost problému třídění a typických třídicích algoritmů. Problém třídění jako takový však de facto nemá smysl uvažovat pokud bychom na množině klíčů, podle kterých třídíme, nezavedli nějakou smysluplnou relaci uspořádání – obvykle ji však chápeme jako „určenou daným kontextem“ a explicitně ji nezdůrazňujeme. Uspořádání množin může výrazně zvýšit efektivitu některých algoritmů, například vyhledávání.

Definice 9. *Reflexivní, antisymetrická a tranzitivní binární relace R na X se nazývá* ***uspořádání****. Úplné uspořádání se nazývá* ***lineární uspořádání*** *neboli* ***řetězec****. Pokud je R uspořádání na X, pak se $\langle X, R\rangle$ nazývá* ***upořádáná množina****.*

Relace uspořádání na X obvykle značíme $\leq$ v souladu s intuitivním chápáním uspořádání a místo $\langle x, y\rangle \in \leq$. Zdůrazněme ale, že označení $\leq$ v tuto chvíli nemá (obecně) nic společného se srovnáváním čísel, na které jsme zvyklí. Uspořádání pořád ještě není formálním protějškem „upořádání“ na které jsme zvyklí při porovnávání čísel. Je-li $\langle X, \leq\rangle$ uspořádaná množina, pak mohou existovat $x, y \in X$,pro které neplatí $x \leq y$ ani $y \leq x$ (definice to nevylučuje). V tom případě říkáme, že prvky jsou **nesrovnatelné** což někdy značíme $x \parallel y$. V opačném případě prvky nazýváme **srovnatelné**. Je-li $\leq$ lineární uspořádání na X, pak je $\leq$ úplná relace, což znamená, že každé prvky jsou srovnatelné. Lineární uspořádání lze tedy chápat jako matematický protějšek „tradičního srovnávání čísel“. Každá relace identity ω_X je uspořádání které nazýváme **antiřetězec**

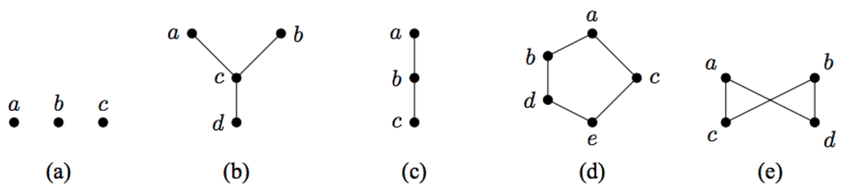
Věta 8. *Princip duality. Nechť $\leq$ je uspořádání na X. Pak $\leq^{-1}$ je uspořádání na X, které označujeme $\geq$.*

Konečné uspořádání $\leq$ na X je relace, mžeme ji tedy reprezentovat binární maticí nebo příslušným orientovaným grafem. Díky speciálním vlastnostem konečných uspořádání je však můžeme znázorňovat mnohem přehledněji pomocí speciálních diagramů. Ke každému uspořádání $\leq$ na X lze uvažovat odvozenou relaci $\prec$ definovanou předpisem

$$x \prec y, \text{ právě když } x \leq y \text{ a } \forall z \in X \text{ platí:}$$

$$\text{pokud } x \leq z \leq y, \text{ pak } z \in \{x, y\}$$

Relaci $\prec$ nazýváme pokrytí příslušné $\leq$, a výraz $x \prec y$ čteme „x je pokryt y“ nebo „x pokrývá y“. Na relaci pokrytí je založena jedna z metod jak znázornit konečnou uspořádanou množinu, tak zvané **Hasseovy diagramy** uspořádaných množin.



Definice 10. *Nechť $\langle X, \leq \rangle$ je uspořádaná množina. Prvek $x \in X$ se nazývá*

- ***minimální**, jestliže $\forall y \in X$ platí: pokud $y \leq x$, pak $x = y$,*
- ***nejmenší**, jestliže $x \leq y$ pro každá $y \in X$,*
- ***maximální**, jestliže $\forall y \in X$ platí: pokud $y \geq x$ pak $x = y$,*
- ***nejmenší**, jestliže $x \geq y$ pro každý $y \in X$.*

Věta 9. *Nechť $\langle X, \leq \rangle$ je uspořádaná množina. Pak platí*

1. *v $\langle X, \leq \rangle$ existuje nejvýše jeden největší a nejvýše jeden nejmenší prvek;*
2. *je-li $x \in X$ největší (nejmenší) prvek, pak je také maximální (minimální);*
3. *pokud je $\leq$ lineární uspořádání, pak je $x \in X$ největší (nejmenší) prvek, právě když je maximální (minimální).*

Definice 11. *Nechť $\langle X, \leq \rangle$ je uspořádaná množina a nechť $Y \subseteq X$. Definujeme množiny*

$$L(Y) = \{x \in X \mid x \leq y \text{ platí pro každé } y \in Y\}$$

$$U(Y) = \{x \in X \mid x \geq y \text{ platí pro každé } y \in Y\}$$

*L(Y) se nazývá **dolní kužel množiny** Y v $\langle X, \leq \rangle$. U(Y) se nazývá **horní kužel množiny** Y v $\langle X, \leq \rangle$.*

Jinými slovy dolní kužel množiny Y v $\langle X, \leq \rangle$ obsahuje tedy právě ty prvky z X, které jsou menší nebo rovny všem prvkům obsaženým v Y, analogicky pro horní kužel.

Definice 12. *Nechť $\langle X, \leq \rangle$ je uspořádaná množina a nechť $Y \subseteq X$. Pokud má $L(Y)$ největší prvek, pak se nazývá **infimum** Y a označuje se $inf(Y)$. Pokud má $U(Y)$ nejmenší prvek, pak se nazývá **supremum** Y a označuje se $sup(Y)$.*

Definice 13. *Nechť $\langle X, \leq \rangle$ je uspořádaná množina. Pokud pro každé $x, y \in X$ existuje $inf(x, y)$, pak $\langle X, \leq \rangle$ nazveme **průsekový polosvaz**. Pokud pro každé $x, y \in X$ existuje $sup(x, y)$ pak $\langle X, \leq \rangle$ nazveme **spojový polosvaz**. Je-li $\langle X, \leq \rangle$ průsekový i spojový polosvaz, pak $\langle X, \leq \rangle$ nazveme **svaz**.*

Vektorové prostory, lineární závislost a nezávislost, báze a dimenze vektorového prostoru. Eukleidovské vektorové prostory. Matice, determinanty: vlastnosti, operace s nimi. Řešení soustav lineárních rovnic. Algebraické struktury: grupa, okruh, obor integrity, těleso. Svazy: modulární, distributivní, komplementární.

4 Algebraické struktury

4.1 Grupoid

Definice 14. *Nechť $A \neq \emptyset$. Binární operací na množině A nazveme každé zobrazení $f : A \times A \to A$.*

Příklad 3. *Nechť $\mathbb{Z}$ je množina všech celých čísel, $+$ přiřadí každé dvojici čísel $a, b \in \mathbb{Z}$ číslo $a + b \in \mathbb{Z}$. Je tedy binární operace.*

Definice 15. *Nechť $A \neq \emptyset$ a $\circ$ je binární operace na A. Dvojici $\mathscr{A} = (A, \circ)$ budeme nazývat grupoid. Jeli operace $\circ$ asociativní, tj. jestliže $\forall a, b, c \in A$ platí $a \circ (b \circ c) = (a \circ b) \circ c$, nazývá se grupoid $(A, \circ)$ pologrupa. Operace $\circ$ se nazývá komutativní jestliže $a \circ b = b \circ a$ pro každé $a, b \in A$.*

Budeme-li operaci v grupoidu zapisovat symbolem $+$, nazýváme grupoid $(A, +)$ **aditivní**, budeme-li operaci zapisovat $\circ$ (nebo vynechávat), nazývá se grupoid $(A, \circ)$ **multiplikativní**.

Definice 16. *Jestliže v grupoidu $(A, \circ)$ existuje prvek e takový, že $a \circ e = e \circ a = a$ pro každé $a \in A$, nazývá se e **jednotkou** $(A, \circ)$. Jestliže v A existuje prvek n takový, že $a \circ n = n \circ a = n$, nazývá se n **nula** grupoidu $(A, \circ)$.*

Definice 17. *Nechť $\mathscr{A} = (A, \circ)$ je grupoid, nechť $\emptyset \neq B \subseteq A$.Jestliže $\forall a, b \in B$ platí $a \circ b \in B$, nazývá se $(B, \circ)$ **podgrupoid** grupoidu $\mathscr{A}$.*

4.2 Grupa

Definice 18. *Nechť $(A, \circ)$ je pologrupa. Jestliže pro každé dva prvky $a, b \in A$ existují $x, y \in A$ tak, že platí $a \circ x = b, y \circ a = b$, pak se $(A, \circ)$ se nazývá **grupa**.*

Další možností jak definovat to, že je grupoid $\mathscr{G}$ grupa říká následující definice.

Definice 19. *$\mathscr{G} = (G, \circ)$ nazveme grupou pokud platí*

1. *$\forall a, b, \in G : a \circ b \in G$ (uzavřenost)*
2. *$\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$ (asociativita)*
3. *$\exists e \in G \quad \forall a \in G : a \circ e = e \circ a = a$ (jednotkový prvek)*

4. $\forall a \in G \quad \exists a^{-1} \in G : a \circ a^{-1} = a^{-1} \circ a = e$ *(inverzní prvek)*

*Grupa se nazývá **abelovská** právě když platí komutativita:*

$$\forall a, b, \in G : a \circ b = b \circ a$$

Definice 20. *Nechť* $\mathscr{G} = (G, \circ)$ *je grupa. Podgrupoid* $(A, \circ)$ *grupoidu* $(G, \circ)$ *se nazývá **podgrupa grupy*** $\mathscr{G}$*, je-li* $(A, \circ)$ *grupou.*

Příklad 4. *Grupa* $(\mathbb{Z}, +)$ *je podgrupou grupy* $(\mathbb{R}, +)$ *všech reálných čísel.*

4.3 Okruh

Definice 21. ***Okruhem*** *nazveme trojici* $\mathscr{R} = (R, +, \cdot)$ *takovou, že* $R \neq \emptyset$ *je množina,* $+$ *a* $\cdot$ *jsou binární operace na* R *a*

1. $(R, +)$ *je abelovská grupa (0 její jednotka)*
2. $(R, \cdot)$ *je pologrupa*
3. *Platí **distributivní zákony**, tj. pro každé* $a, b, c \in R$ *platí*

$$a \cdot (b + c) = a \cdot b + a \cdot + c, \qquad (b + c) \cdot a = b \cdot a + c \cdot a$$

Okruh $\mathscr{R}$ *se nazývá **komutativní**, jestliže* $a \cdot b = b \cdot a$ *pro každé* $a, b \in R$*. Okruh* $\mathscr{R}$ *se nazývá **unitární**, má-li pologrupa* $(R \setminus \{0\}, \cdot)$ *jednotku. Je-li* $\mathscr{R}$ *unitární, budeme jeho jednotku označovat 1. Prvek 0 (jednotka* $(R, +)$*) se nazývá **nulou okruhu*** $\mathscr{R}$*.*

Příklad 5. *Komutativní unitární okruhy jsou například: okruh celých čísel* $(\mathbb{Z}, +, \cdot)$*, okruh reálných čísel* $(\mathbb{R}, +, \cdot)$*, okruh komplexních čísel* $(\mathbb{C}, +, \cdot)$ *a okruh racionálních čísel* $(\mathbb{Q}, +, \cdot)$*.*

Definice 22. *Prvek a okruhu* $\mathscr{R} = (R, +, \cdot)$ *se nazývá **dělitel nuly**, jestliže* $a \neq 0$ *existuje* $b \neq 0, b \in R$ *tak, že* $a \cdot b = 0$*.*

4.4 Obor integrity

Definice 23. *Okruh* $\mathscr{R} = (R, +, \cdot)$ *se nazývá **obor integrity**, je-li komutativní, unitární a neobsahuje dělitele nuly.*

Příklad 6. *Každý z okruhů* $(\mathbb{Z}, +, \cdot)$*,* $(\mathbb{R}, +, \cdot)$*,* $(\mathbb{C}, +, \cdot)$*,* $(\mathbb{Q}, +, \cdot)$ *je obor integrity.*

4.5 Těleso

Definice 24. *Okruh* $\mathscr{R} = (R, +, \cdot)$ *se nazývá **těleso**, je-li množina jeho nenulových prvků grupou vzhledem k operaci* $\cdot$*. Těleso* $\mathscr{R}$ *se nazývá **komutativní**, je-li* $(R \setminus \{0\}, \cdot)$ *abelovská grupa.*

Příklad 7. *Okruhy* $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ *jsou komutativní tělesa. Okruh* $(\mathbb{Z}, +, \cdot)$ *není těleso.*

Věta 10. *Každé komutativní těleso je obor integrity.*

Definice 25. *Je-li* $\mathscr{R} = (R, +, \cdot)$ *okruh,* $A \subseteq R$ *taková že* $(A, +, \cdot)$ *je opět okruh, pak se* $(A, +, \cdot)$ *nazývá* ***podokruh okruhu*** $\mathscr{R}$*. Je-li* $\mathscr{R} = (R, +, \cdot)$ *těleso,* $A \subseteq R$ *taková že* $(A, +, \cdot)$ *je opět těleso, pak se* $(A, +, \cdot)$ *nazývá* ***podtěleso tělesa*** $\mathscr{R}$*. Každé podtěleso tělesa* $\mathscr{C} = (C, +, \cdot)$ *komplexních čísel nazveme* ***číselné těleso****. Každý podokruh okruhu* $\mathscr{C}$ *nazveme* ***číselný okruh****.*

Příklad 8. $\mathscr{R} = (\mathbb{R}, +, \cdot)$, $\mathscr{C} = (\mathbb{C}, +, \cdot)$, $\mathscr{Q} = (\mathbb{Q}, +, \cdot)$ *jsou číselná tělesa.* $\mathscr{Z} = (\mathbb{Z}, +, \cdot)$ *je číselný okruh, který není tělesem.*

5 Vektorové prostory

Definice 26. *Nechť* $A \neq \emptyset \neq B$ *jsou množiny. Zobrazení* $\circ : A \times B \to B$ *nazveme* ***levá vnější operace nad množinami*** *A,B (v tomto pořadí). Jsou-li* $a \in A, b \in B$*, pak prvek* $\circ(a, b)$ *budeme zapisovat* $a \circ b$*.*

Definice 27. *Nechť* $(V, +)$ *je abelovská grupa, nechť T je číselné těleso, nechť* $\circ : T \times V \to V$ *je levá vnější operace nad* T, V*. Pak čtveřici* $\mathscr{V} = (V, +, T, \circ)$ *nazveme* ***vektorový prostor nad*** *T, platí-li* $\forall u, v \in V, \forall c, d, \in T$

1. $c \circ (u + v) = c \circ u + c \circ v$
2. $(c + d) \circ u = c \circ u + d \circ u$
3. $(c \cdot d) \circ u = c \circ (d \circ u)$
4. $1 \circ u = u$

Prvky v V budeme nazývat ***vektory****, čísla z tělesa T* ***skaláry****. Množinu V nazveme* ***pole*** *vektorového prostoru* $\mathscr{V}$*.*

Definice 28. *Nechť* $\mathscr{V}$ *je vektorový prostor nad tělesem T, nechť* $v, u_1, \ldots, u_k \in V$*. Řekneme, že vektor v je* ***lineární kombinací vektorů*** $v, u_1, \ldots, u_k$*, jestliže existují čísla* $c_1, \ldots, c_k \in T$ *tak, že*

$$v = c_1 \cdot u_1 + \cdots + c_k \cdot u_k$$

Poznámka. Symbolem **o** budeme označovat tzv. **nulový vektor**, což je jednotka grupy $(V, +)$. Použitím podmínky 2. dostaneme $\forall u \in V$:

$$0 \cdot u = (c + (-c)) \cdot u = c \cdot u + (-c \cdot u) = o$$

Tedy nulový vektor je lineární kombinací libovolných vektorů z V : je-li $u_1, \ldots, u_k \in V$ pak

$$0 \cdot u_1 + \cdots + 0 \cdot u_k = o$$

Definice 29. *Vektory* $u_1, \dots, u_k$ *z vektorového prostoru* $\mathscr{V}$ *se nazývají* ***lineárně závislé****, jestliže existují čísla* $c_1, \dots, c_k \in T$*, která nejsou všechna rovna nule tak, že nulový vektor* ***o*** *je roven netriviální lineární kombinaci vektorů* $u_1, \dots, u_k$*, tj.*

$$o = c_1 \cdot u_1 + \cdots + c_k \cdot u_k,$$

kde aspoň jedno $c_i \neq 0$*. Jestliže vektory* $u_1, \dots, u_k$ *nejsou lineárně závislé, nazývají se* ***lineárně nezávislé****.*

Poznámka. Zřejmě vektory $u_1, \dots, u_k \in \mathscr{V}$ jsou lineárně nezávislé, právě když

$$o = c_1 \cdot u_1 + \cdots + c_k \cdot u_k \quad \Rightarrow \quad c_1 = c_2 = \cdots = c_k = 0$$

Věta 11. *Jsou-li mezi vektory* $u_1, \dots, u_k \in \mathscr{V}$ *některé lineárně závislé, pak jsou* $u_1, \dots, u_k$ *lineárně závislé.*

Věta 12. *Je-li mezi vektory* $u_1, \dots, u_k$ *vektor nulový* ***o****, pak jsou* $u_1, \dots, u_k$ *lineárně závislé.*

Věta 13. *Nechť* $u_1, \dots, u_k \in \mathscr{V}$*. Pak* $u_1, \dots, u_k$ *jsou lineárně závislé, právě když je aspoň jeden z nich lineární kombinací ostatních vektorů.*

Definice 30. *Nechť* $\mathscr{V} = (V, +, T, \circ)$ *je vektorový prostor nad tělesem* T*, nechť* $\emptyset \neq W \subseteq V$*. Pak* $\mathscr{W} = (W, +, T, \circ)$ *nazveme* ***podprostor vektorového prostoru*** $\mathscr{V}$*, jestliže*

1. $\forall u, c \in W$ *je* $u + v \in W$
2. $\forall u \in W, \forall c \in T$ *je* $c \cdot u \in W$*.*

Definice 31. *nechť* M *je podmnožina vektorového prostoru* $\mathscr{V}$*.* ***Lineárním obalem množiny M ve*** $\mathscr{V}$ *rozumíme množinu všech lineárních kombinací vektorů z* M*.*

Definice 32. *Nechť* $\mathscr{V}$ *je vektorový prostor,* $M \neq \emptyset$ *jeho podmnožina. Je-li* $[M] = \mathscr{V}$*, nazývá se* M *množina generátorů* $\mathscr{V}$*.*

Definice 33. *Řekněme, že vektorový prostor* $\mathscr{V}$ *je konečné dimenze, má-li aspoň jednu konečnou množinu generátorů.*

Definice 34. *Bází vektorového prostoru* $\mathscr{V}$ *konečné dimenze rozumíme libovolnou lineárně nezávislou konečnou množinu* $\{u_1, \dots, u_n\}$ *jeho generátorů.*

Věta 14. *Nechť* $M = \{u_1, \dots, u_n\}$ *je bází* $\mathscr{V}$*. Pak každý vektor* $v \in \mathscr{V}$ *lze jediným způsobem vyjádřit jako lineární kombinaci vektorů* $u_1, \dots, u_n$*.*

Příklad 9. *Příklad báze vektorového prostoru* $e_1 = (1,0,0,0), e_2 = (0,1,0,0), e_3 = (0,0,1,0), e_4 = (0,0,0,1)$

Definice 35. *Je-li* $\mathscr{V} \neq \{o\}$ *vektorový prostor konečné dimenze, pak počet prvků jeho libovolné báze nazýváme dimenze* $\mathscr{V}$ *a značíme* $\dim\mathscr{V}$*, Je-li* $\mathscr{V} = \{o\}$*, položíme* $\dim\mathscr{V} = 0$*.*

5.1 Aritmetické vektorové prostory

Nechť T je číselné těleso, n přirozené číslo. Na n-násobném kartézském součinu $T^n = V$ definujeme operaci $+$ takto: je-li $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in V$ pak

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

Zřejmě $(V, +)$ je abelovská grupa, prvek $o = (0, 0, \ldots, 0)$ je její jednotkou a prvek $(-a_1, \ldots, -a_n)$ je inverzní k prvku $(a_1, \ldots, a_n)$. Definujeme levou vnější operaci: $c \in T, (a_1, \ldots, a_n) \in V$,

$$c \cdot (a_1, \ldots, a_n) = (c \cdot a_1, \ldots, c \cdot a_n).$$

Jednoduše lze ověřit, že $\mathscr{V} = (V, +, T, \cdot)$ je vektorový prostor dimenze n. Tento vektorový prostor nazveme aritmetický a budeme jej značit T^n. Jednou z jeho (nekonečně mnoha) bází je $e_1, \ldots, e_n)$, kde $e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, \ldots, 0),\ \ldots,\ e_n = (0, 0, \ldots, 1)$

Zapisujeme-li aritmetický vektor $\mathbf{a}$ ve tvaru $(a_1, a_2, \ldots, a_n)$, nazýváme tento zápis **řádkový vektor**. zapisujeme-li $\mathbf{a}$ ve tvaru

$$a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

nazýváme jej sloupcový vektor.

5.2 Eukleidovské vektorové prostory

Ve vektorovém prostoru nad tělesem T můžeme vektory sčítat, odčítat a násobit skaláry z tělesa T (levá vnější operace). Nemáme však zaveden pojem délky vektoru, úhlu mezi vektory apod. Zavedeme proto další pojem.

Definice 36. *Nechť $\mathscr{V} = (V, +, \mathbb{R}, \cdot)$ je vektorový prostor nad tělesem reálných čísel $\mathbb{R}$.* ***Skalárním součinem*** *$\circ$ nazveme zobrazení $V \times V$ do tělesa $\mathbb{R}$, které má tyto vlastnosti:*

1. $\forall u, v \in V, u \circ v = v \circ u$
2. $\forall u \in V, u \neq o, u \circ u > 0$
3. $\forall u, v, w \in V, (u + v) \circ w = u \circ w + v \circ w$
4. $\forall u, v \in V, \forall c \in \mathbb{R}, (c \cdot u) \circ v = c \cdot (u \circ v).$

Příklad 10. *Je-li $\mathscr{V} = (\mathbb{R}^n, +, \mathbb{R}, \cdot)$ aritmeticky (n-dimenzionální) vektorový prostor nad $\mathbb{R}, x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n)$, pak $x \circ y = \sum_{i=1}^{n} x_i \cdot y_i$ definuje skalární součin $\circ$.*

Definice 37. *Nechť $\mathscr{V} = (V, +\mathbb{R}, \cdot)$ je vektorový prostor nad tělesem reálných čísel, ve kterém je definován skalární součin. Pak se $\mathscr{V}$ nazývá* ***Eukleidovský vektorový prostor***

Definice 38. *Nechť $\mathscr{V}$ je Eukleidovský vektorový prostor, nechť $u \in V$. Číslo $\|u\| = \sqrt{u \circ u}$ nazveme délka vektoru u.*

Věta 15. *Nechť $\mathscr{V}$ je Eukleidovský vektorový prostor, $u, v \in V$. Pak*

a) $\forall c \in \mathbb{R}$ *je* $\|c \cdot u\| = |c| \cdot \|u\|$

b) $\|o\| = 0$ *a pro* $u \neq o$ *je* $\|u\| > 0$

c) $|u \circ v| \leq \|u\| \cdot \|v\|$ *(Schwarzova nerovnost)*

Definice 39. *Nechť $\mathscr{V}$ je Eukleidovský vektorový prostor, $u, v \in V$, $u \neq o \neq v$. Úhlem φ vektorů u,v nazveme číslo*

$$\varphi = arccos \frac{u \circ v}{\|u\| \cdot \|v\|}$$

Platí tedy $cos\varphi = \frac{u \circ v}{\|u\| \cdot \|v\|}$, kde $0 < \varphi < \pi$

Definice 40. *Vektory u,v nazveme ortogonální (kolmé). ozn. $u \perp v$, je-li $\varphi = \frac{\pi}{2}$ tj. $cos\varphi = 0$, tj. $u \circ v = 0$.*

Definice 41. *Vektory $u_1, \ldots, u_m$ jsou vzájemně ortogonální, platí-li $u_i \perp u_j$ pro každé $i \neq j$.*

Věta 16. *Nenulové vzájemně ortogonální vektory $u_1, \ldots, u_m$ jsou lineárně nezávislé.*

Definice 42. *Jsou-li $u_1, \ldots, u_m$ vzájemně ortogonální vektory, přičemž $\{u_1, \ldots, u_m\}$ generuje celý prostor $\mathscr{V}$, pak je to báze $\mathscr{V}$ (tzv. ortogonální báze).*

6 Matice

Definice 43. *Nechť T je číselné těleso, m,n jsou čísla přirozená a nechť $a_{ij} \in T$ pro $i = 1, \ldots, m, j = 1, \ldots n$. Dvojindexované schéma*

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

se nazývá matice typu $m \times n$ nad T. Číslo a_{ij} se nazývá prvek matice A z i-tého řádku a j-tého sloupce. Číslo i se nazývá řádkový, číslo j sloupcový index prvku a_{ij}.

Poznámka. Někdy budeme matice značit následovně: $A = \|a_{ij}\|$.

Definice 44. *Matice $A = \|a_{ij}\|$ typu $m \times n$, kde $m = n$ se nazývá čtvercová matice stupně n. Čtvercová matice A se nazývá diagonální pokud pro všechny její prvky. která neleží na hlavní diagonále jsou rovny 0. Diagonální matice se nazývá skalární, jestliže všechny její prvky na hlavní diagonále jsou si rovny. Skalární matice se nazývá jednotková stupně n, jsou-li všechny její prvky na hlavní diagonále rovny 1 (budeme ji označovat E_n). Matici N typu $m \times n$ nazveme nulová matice jestliže jsou všechny její prvky rovny 0.*

Označení. Symbolem $\mathscr{M}_{m\times n}(T)$ resp. $\mathscr{M}_n(T)$ označíme množinu všech matic typu $m\times n$ resp. všech čtvercových matic stupně n nad tělesem T.

Definice 45. *Dvě matice A, B z $\mathscr{M}_{m\times n}(T)$ jsou si rovny, jestliže $a_{ij} = b_{ij}$ pro každé $i = 1, \dots, m, j = 1, \dots n$.*

Definice 46. *Mějme matice $A, B \in \mathscr{M}_{m\times n}(T)$. Součtem matice A a B rozumíme matici $A + B = \|c_{ij}\|$, kde $\|c_{ij}\| = a_{ij} + b_{ij}$ pro každé $i = 1, \dots, m, j = 1, \dots n$.*

Věta 17. *Množina $\mathscr{M}_{m\times n}(T)$ spolu se zavedenou operací sčítání matic tvoří abelovskou grupu.*

Definice 47. *Nechť T je číselné těleso, $A \in \mathscr{M}_{m\times n}(T)$. Prvky z T budeme nazývat skaláry. zavedeme levou vnější operaci $\cdot : T \times \mathscr{M}_{m\times n}(T) \to \mathscr{M}_{m\times n}(T)$ takto: $c \in T,\ A = \|a_{ij}\|$ pak $cA = \|c \cdot a_{ij}\|$ je tzv. násobení matice skalárem.*

Definice 48. *Nechť $A = \|a_{ij}\|$ je matice typu $m \times n$. Matici transponovanou k matici A nazýváme matici $A^T = \|a_{ji}\|$ typu $n \times m$ která vznikne z A vzájemnou výměnou řádků a sloupců (tj. otočením A podle hlavní diagonály).*

Definice 49. *Nechť $A = \|a_{ij}\|$ je matice typu $m \times n$ a nechť $B = \|b_{jk}\|$ je matice typu $n\times p$ nad tělesem T. Součinem matic A a B (v tomto pořadí) nazveme matici $AB = \|c_{ik}\|$ typu $m \times p$ pro jejíchž prvky platí:*

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk} = \sum_{j=1}^{n} a_{ij}b_{jk}$$

pro každé $i = 1, \dots, m, k = 1, \dots p$.

Věta 18. *Násobení matic je asociativní, tj. jestliže $A \in \mathscr{M}_{m\times n}(T), B \in \mathscr{M}_{n\times p}(T), C \in \mathscr{M}_{p\times r}(T)$, pak*

$$(AB)C = A(BC).$$

Věta 19. *Nechť T je těleso $n \in \mathbb{N}$. Pak $\mathscr{M}_n(T) = (\mathscr{M}_n(T), +, \cdot)$ je unitární okruh, jehož jednotkou je jednotková matice. Je-li $n > 1$ pak tento okruh není komutativní a obsahuje dělitele nuly. Je-li $n = 1$ pak $\mathscr{M}_1(T)$ je komutativní těleso.*

7 Determinanty

7.1 Permutace

Definice 50. *Nechť $A = \{a_1, a_2, \dots, a_n\}$ konečná (n-prvková) množina. Pořadím π množiny A nazveme libovolnou posloupnost $\pi = (a_{k_1}, a_{k_2}, \dots, a_{k_n})$ prvků z A takovou, že každý prvek z A se v π vyskytuje právě jedenkrát. Permutací na A rozumíme každou bijekci A na A. Permutaci P množiny A lze zapisovat ve tvaru*

$$\mathbf{A} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{\pi(1)} & a_{\pi(2)} & \dots & a_{\pi(n)} \end{pmatrix}$$

kde π je některé pořadí množiny indexů.

Věta 20. *Pro každou n-prvkovou množinu* $(n \geq 1)$ *je počet pořadí roven počtu permutací, tj.* $n!$.

Definice 51. *Nechť* $\pi = \{k_1, k_2, \ldots, k_n\}$ *je pořadím množiny* $A = \{1, 2, \ldots, n\}$. *Prvky* k_i, k_j *tvoří inverzi v* π, *jestliže* $i < j$ *a* $k_i > k_j$. *Označme* $[\pi]$ *počet všech inverzí v* π. *Znaménkem pořadí* π *nazveme číslo* $sgn\pi = (-1)^{[\pi]}$. *Je-li* $sgn\pi = 1$, *pořadí se nazývá sudé, je-li* $sgn\pi = -1$, π *se nazývá liché. Nechť* $P = \binom{\pi_1}{\pi_2}$ *je permutace množiny* A. *Znaménkem permutace* P *rozumíme číslo* $sgnP$, *kde* $sgnP = 1$ *je-li* $sgn\pi_1 = sgn\pi_2$, $sgnP = -1$, *je-li* $sgn\pi_1 = -sgn\pi_2$. *Je-li* $sgnP = 1$, P *je sudá, je-li* $sgnP = -1$, *je* P *lichá.*

Příklad 11. *Nechť* $\pi = (2, 4, 3, 5, 1)$. *Pak všechny jeho inverze jsou: 2,1; 4,3; 4,1; 3,1; 5,1. Tedy* $[\pi] = 5$ *tj.* $sgn\pi = (-1)^5 = -1$, π *je liché. Nechť* $\mathbf{A} = \begin{pmatrix} 2 & 1 & 4 & 5 & 3 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix} = \begin{pmatrix} \pi_1 \\ \pi_2 \end{pmatrix}$. *Ověříme* $[\pi_1] = 3, [\pi_2] = 5$, *tedy* $sgn\pi_1 = -1 = sgn\pi_2$, *odkud* $sgnP = 1$, *tj.* P *je sudá permutace.*

Poznámka. Je-li $P = \begin{pmatrix} \pi_0 \\ \pi_1 \end{pmatrix}$, kde π_0 je základní pořadí, pak zřejmě $sgnP = sgn\pi_1$

Označení. Symbolem P_0 značíme **identickou permutaci**, tj. $P_0 = \begin{pmatrix} \pi_0 \\ \pi_0 \end{pmatrix}$. Je-li $P = \begin{pmatrix} \pi_1 \\ \pi_2 \end{pmatrix}$, symbolem P^{-1} označíme **inverzní permutaci**, tj. $P^{-1} = \begin{pmatrix} \pi_2 \\ \pi_1 \end{pmatrix}$,

Definice 52. ***Transpozicí*** *na* $A = \{1, \ldots, n\}$ *rozumíme permutaci* P *takovou, že existují* $i, j \in A, i \neq j$ *tak, že* $P(i) = j, P(j) = i$ *a* $P(k) = k$ *pro každé* $i \neq k \neq j$.

Příklad 12. $P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$ *je transpozice, zaměňuje 2 a 4.*

Označení. Transpozici P zaměňující i a j budeme zapisovat $P(i, j)$.

Věta 21. *Každou permutaci je možné vyjádřit jako složení konečného počtu transpozic. Permutace* P *je sudá (resp. lichá), je-li tento počet transpozic sudý (resp. lichý).*

7.2 Konečně co je to determinant

Definice 53. *Nechť* $A = \|a_{ij}\|$ *je čtvercová matice stupně* n *nad číselným tělesem* T. *Determinantem* $detA$ *matice* A *rozumíme číslo z* T *takové, že*

$$detA = \sum_P sqnP \cdot a_{1k_1} a_{2k_2} \ldots a_{nk_n},$$

kde sčítáme přes všechny permutace $P = \begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & n \end{pmatrix}$. *Každý ze součinů* $a_{1k_1} a_{2k_2} \ldots a_{nk_n}$ *nazýváme člen determinantu* $detA$.

Tedy determinant matice A je číslo z T, které je rovno součtu všech $n!$ součinů prvků matice A, kde v každém součinu je každý prvek právě z jednoho řádku a právě z jednoho sloupce, přičemž součin je opatřen znaménkem rovným znaménku permutace určené řádkovými a sloupcovými indexy prvků tohoto součinu.

Příklad 13. *Určete determinant matice*

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Jeho členy tedy budou součiny $a_{11}a_{22}, a_{12}a_{21}$ *Určíme jejich znaménka:*

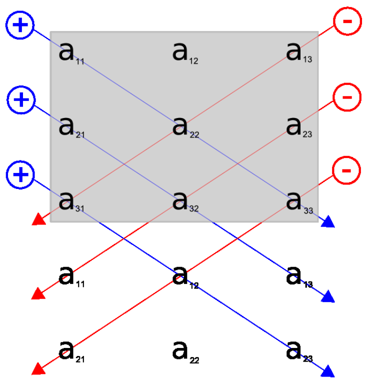
$$\mathbf{sgn} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = 1, \ \mathbf{sgn} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = -1$$

Tedy

$$detA = a_{11}a_{22} - a_{12}a_{21}$$

Věta 22. *Má-li čtvercová matice A v některém řádku (resp. sloupci) samé 0, je* $detA = 0$.

Sarusovo pravidlo pro výpočet determinantu matic maximálně 3-tého stupně. Mějme matici A druhého stupně $A = \begin{pmatrix} 5 & 3 & 2 \\ 1 & 7 & -8 \\ 0 & -2 & 7 \end{pmatrix}$ použijeme následující schéma výpočtu:



Naše „rozšířená matice“ bude vypadat následovně $A = \begin{pmatrix} 5 & 3 & 2 \\ 1 & 7 & -8 \\ 0 & -2 & 7 \\ 5 & 3 & 2 \\ 1 & 7 & -8 \end{pmatrix}$ A determinant

$detA = [5 \cdot 7 \cdot 7 + 1 \cdot (-2) \cdot 2 + 0 \cdot 3 \cdot (-8)] - [2 \cdot 7 \cdot 0 + (-8) \cdot (-2) \cdot 5 + 7 \cdot 3 \cdot 1] = 140$

Věta 23. *Má-li $A \in \mathscr{M}_n(T)$ všechny prvky pod hlavní diagonálou rovny nule, pak* $detA = a_{11}a_{22} \dots a_{nn}$.

Věta 24. *Vznikne-li matice B z matice $A \in \mathscr{M}_n(T)$ záměnou i-tého a j-tého řádku (resp. sloupce), přičemž $i \neq j$, pak* $detB = -detA$.

Věta 25. *Vznikne-li matice B z matice $A \in \mathscr{M}_n(T)$ provedením některé permutace P na řádky (resp. sloupce) matice A, pak $detB = sgnP \cdot detA$.*

Definice 54. *Nechť $A = \|a_{ij}\| \in \mathscr{M}_{m\times n}(T)$. Pak každou matici, která vznikne z A vynecháním některých řádků a některých sloupců nazýváme dílčí matice A. Je-li dílčí matice matice A čtvercová, pak její determinant nazýváme subdeterminant A.*

Definice 55. *Je-li $A = \|a_{ij}\| \in \mathscr{M}_n(T)$, potom subdeterminant dílčí matice A_{ij} stupně $n-1$ vzniklé vynecháním i-tého řádku a j-tého sloupce nazveme **minor matice** A **příslušný k prvku** a_{ij} a značíme jej M_{ij}. **Algebraickým doplňkem prvku** nazýváme číslo $\mathscr{A} = (-1)^{i+j}M_{ij}$.*

Příklad 14. *Určete minory a algebraické doplňky $M_{12}, M_{33}, \mathscr{A}_{12}, \mathscr{A}_{33}$ matice*

$$\mathbf{A} = \begin{pmatrix} 2 & 5 & 1 \\ 0 & -6 & 2 \\ 5 & 1 & -3 \end{pmatrix}.$$

Platí

$$\mathbf{M_{12}} = \begin{vmatrix} 0 & 2 \\ 5 & -3 \end{vmatrix} = -10, \quad \mathbf{M_{33}} = \begin{vmatrix} 0 & 2 \\ 5 & -3 \end{vmatrix} = -12,$$

tedy

$$\mathscr{A}_{12} = (-1)^{1+2}(-10) = 10, \quad \mathscr{A}_{33} = (-1)^{3+3}(-12) = -12.$$

Věta 26 (Laplaceova). *Nechť $A = \|a_{ij}\| \in \mathscr{M}_n(T)$ Pak*

a) $\forall i = 1, \ldots, n$ platí $detA = a_{i1}\mathscr{A}_{i1} + a_{i2}\mathscr{A}_{i2} + \cdots + a_{in}\mathscr{A}_{in}$

b) $\forall i, j = 1, \ldots, n,\ i \neq j$ platí $a_{i1}\mathscr{A}_{j1} + a_{i2}\mathscr{A}_{j2} + \cdots + a_{in}\mathscr{A}_{jn} = 0$

Věta 27. *Vznikne-li matice B z matice $A \in \mathscr{M}_n(T)$ vynásobením i-tého řádku (resp. sloupce) číslem $c \in T$, pak $detB = c \cdot detA$.*

Věta 28. *Je-li i-tý řádek (resp. sloupec) matice $A \in \mathscr{M}_n(T)$ součtem vektorů $\boldsymbol{b}$,$\boldsymbol{c}$ pak*

$$det\begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_i \\ \vdots \\ \boldsymbol{a}_n \end{pmatrix} = det\begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{b} \\ \vdots \\ \boldsymbol{a}_n \end{pmatrix} + det\begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{c} \\ \vdots \\ \boldsymbol{a}_n \end{pmatrix}.$$

Věta 29. *Nechť $A \in \mathscr{M}_n(T)$ a nechť B vznikne z A tak, že některému řádku (sloupci) matice A přičteme libovolnou lineární kombinaci ostatních řádků (sloupců). Pak $detB = detA$.*

Věta 30. *Jsou-li řádkové (sloupcové) vektory matice $A \in \mathscr{M}_n(T)$ lineárně závislé, pak $detA = 0$.*

Příklad 15. *Výpočet determinantu matice n-tého stupně. Mějme matici*

$$A = \begin{pmatrix} -2 & 3 & -1 & 2 \\ 1 & -2 & 0 & 4 \\ 2 & -4 & -2 & 5 \\ -3 & 2 & 1 & -5 \end{pmatrix}$$

Řešení:

$$\begin{vmatrix} -2 & 3 & -1 & 2 \\ 1 & -2 & 0 & 4 \\ 2 & -4 & -2 & 5 \\ -3 & 2 & 1 & -5 \end{vmatrix} = \begin{vmatrix} 0 & -1 & -1 & 10 \\ 1 & -2 & 0 & 4 \\ 0 & 0 & -2 & -3 \\ 0 & -4 & 1 & 7 \end{vmatrix} = (-1)^{1+2} \begin{vmatrix} -1 & -1 & 10 \\ 0 & -2 & -3 \\ -4 & 1 & 7 \end{vmatrix}$$

$$= (-1) \begin{vmatrix} -1 & 0 & 0 \\ 0 & -2 & -3 \\ -4 & 5 & -33 \end{vmatrix} = (-1)(-1)^{1+1}(-1) \begin{vmatrix} -2 & -3 \\ 5 & -33 \end{vmatrix} = 66 + 15 = 81.$$

Věta 31. *Nechť $A, B \in \mathscr{M}_n(T)$. Pak $detAB = detA \cdot detB$.*

8 Řešení soustav lineárních rovnic

Nechť $A \in \mathscr{M}_{m\times n}(T)$. Tedy její řádky jsou řádkové vektory a patří do aritmetického vektorového prostoru T^n.

Definice 56. ***Řádkovým podprostorem matice*** *A rozumíme podprostor prostoru T^n generovaný všemi řádkovými vektory matice A.*

Definice 57. ***Elementárnímí řádkovými transformacemi matice*** *A nazýváme tyto operace:*

1. *výměnu libovolných dvou řádků v A*
2. *vynásobení některého řádku číslem $c \in T$ různým od 0*
3. *přičtením libovolného násobku některého řádku z A k jinému řádku v A.*

Definice 58. *Řekněme, že $A, B \in \mathscr{M}_{m\times n}(T)$ jsou* ***řádkově ekvivalentní****, lze-li B získat z A pomocí konečného počtu elementárních řádkových transformací. Zapisujeme $A \sim B$*

Věta 32. *Jestliže že $A, B \in \mathscr{M}_{m\times n}(T)$ a $A \sim B$ pak A i B určují stejné řádkové podprostory v T^n.*

Definice 59. ***Vedoucím prvkem*** *řádkového vektoru $\boldsymbol{a}_i$ nazveme první nenulový prvek v tomto vektoru (řádku). Matice A se nazývá* ***redukovaná****, je-li vedoucí prvek každého nenulového řádku v A roven 1 a jestliže jsou v každém sloupci A, který obsahuje vedoucí prvek některého řádku všechny zbývající prvky rovny 0. Redukovaná matice se nazývá* ***redukovaná trojúhleníková****, jestliže všechny její nulové řádky (pokud existují) jsou až za nenulovými a jestliže pro každé $i, j, i < j$ platí, že jsou-li a_i, a_j nenulové řádky, vedoucí prvek v a_i je v k_i-tém sloupci, vedoucí prvek v a_j je v k_j-tém sloupci, pak $k_i < k_j$.*

Příklad 16. *Matice A je redukovaná, B redukovaná trojúhelníková:*

$$A = \begin{pmatrix} 0 & 0 & 1 & 2 & -1 \\ 1 & 0 & 0 & 3 & 6 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 8 & 11 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 & 0 & 4 & -1 \\ 0 & 0 & 1 & 0 & 5 & 6 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Věta 33. *Každá matice A je řádkově ekvivalentní s některou redukovanou maticí, kterou leze získat z A pomocí transformací 2) a 3). Každá matice je řádkově ekvivalentní s redukovanou trojúhelníkovou maticí.*

Věta 34. *Nechť* $A \in \mathscr{M}_{m\times n}(T)$ *je redukovaná matice s nenulovými řádky* $\boldsymbol{a}_1, \ldots, textbf{a}_r$. *Pak pro každý vektor* $\boldsymbol{u} = \sum_{i=1}^{r} c_i textbf{a}_i$ *řádkového podprostoru matice A je* c_i *rovno* k_i*-té souřadnici vektoru* $\boldsymbol{u}$.

Důsledek 2. *Nenulové řádky redukované matice jsou lineárně nezávislé.*

Důsledek 3. *Je-li* $A \sim B$, *kde B je redukovaná, pak nenulové řádky matice B tvoří bázi řádkového podprostoru matice A.*

Definice 60. ***Hodností matice*** $A \in \mathscr{M}_{m\times n}(T)$ *rozumíme dimenzi řádkového podprostoru matice A v* T^n. *Hodnost matice A budeme značit h(A).*

Připomenutí. Připomeňme, že **subdeterminantem matice stupně** k **matice** $A \in \mathscr{M}_{m\times n}(T)$ (kde $k \leq min(m.n)$) nazveme determinant libovolné čtvercové dílčí matice stupně k matice A.

Příklad 17. *Je-li* $A = \begin{pmatrix} 5 & 2 & -1 & 0 \\ -2 & 3 & 1 & -1 \\ 6 & -8 & 0 & 9 \end{pmatrix}$, *pak jejími subdeterminanty 2. stupně jsou například determinanty* $\begin{vmatrix} 5 & 2 \\ -2 & 3 \end{vmatrix} = 19$, $\begin{vmatrix} 2 & 0 \\ -8 & 9 \end{vmatrix} = 18$,
subdeterminant 3. stupně je například $\begin{vmatrix} 5 & 2 & 0 \\ -2 & 3 & -1 \\ 6 & -8 & 9 \end{vmatrix} = 119$, *atd.*

Věta 35. *Hodnost matice A je rovna maximálnímu stupni nenulového subdeterminantu matice A.*

Důsledek 4. *Hodnost matice A je rovna maximálnímu počtu lineárně nezávislých sloupců matice A.*

Jinak řečeno pokud matici A zredukujeme tak její hodnost je rovna počtu nenulových řádků.

Definice 61. *Nechť T je číselné těleso,* $a_1, \ldots, a_n, b \in T$. *Úloha určit všechny n-tice* $(x_1, \ldots, x_n) \in T^n$ *pro které platí:*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

se nazývá ***lineární rovnice o*** n ***neznámých nad*** T. *Každá n-tice* $(x_1, \ldots, x_n) \in T^n$ *pro kterou tato rovnost platí se nazývá* ***řešení*** *této rovnice.*

Poznámka Rovnici $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ budeme zkráceně zapisovat

$$\sum_{i=1}^{n} a_ix_i = b$$

Definice 62. *Nechť T je číselné těleso, $a_{ij} \in T$ pro $i = 1, \ldots,\ j = 1, \ldots, m, b_j \in T$ Úloha určit všechny n-tice $(x_1, \ldots, x_n) \in T^n$ pro které platí*

$$\begin{array}{lr} \displaystyle\sum_{i=1}^{n} a_{1i}x_i = b1 & (R_1) \\ \vdots & (S) \\ \displaystyle\sum_{i=1}^{n} a_{mi}x_i = bm & (R_m) \end{array}$$

*se nazývá **soustava** m **lineárních rovnic o** n **neznámých nad** T (S). Každá n-tice $(x_1, \ldots, x_n)$ splňující (S) se nazývá řešení této soustavy. Pokud $b_1 = b_2 = \cdots = b_m = 0$, soustava (S) se nazývá **homogenní**, Není-li (S) homogenní, nazývá se **nehomogenní**.*

Poznámka. Soustavu můžeme zkráceně zapisovat

$$\sum_{i=1}^{n} a_{ji}x_i = b_j, \quad j = 1, \ldots m.$$

Definice 63. *Nechť je dána soustava (S) lineárních rovnic. Pak matici*

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \quad \textit{resp.} \quad \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{pmatrix}$$

*nazýváme **matice soustavy (S)** resp. **rozšířená matice soustavy (S)**.*

Poznámka. Buď (S) soustava lineárních rovnic, A její matice typu $m \times n$. Označíme-li sloupcové vektory $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$, pak $\mathbf{x}$ je matice typu $n \times 1$, $\mathbf{b}$ je matice typu $m \times 1$; lze tedy soustavu (S) psát v tzv. maticovém tvaru

$$A \cdot x = b.$$

Řešením této soustavy je pak každý vektor $u \in T^n$, pro který platí rovnost $A \cdot u = b$. Rozšířenou matici soustavy (S) budeme také zapisovat symbolem (A, b).

Definice 64. *Soustava lineárních rovnic $Ax = b$ se nazývá řešitelná, má-li aspoň jedno řešení. Dvě soustavy $Ax = b$ a $By = c$ se nazývají ekvivalentní, mají-li stejné množiny řešení.*

Definice 65. *Nehomogenní soustava lineárních rovnic $Ax = b$ je řešitelná právě tehdy, je.li vektor b lineární kombinací sloupců matice A.*

Věta 36 **(Frobeniova).** *Nehomogenní soustava lineárních rovnic $Ax = b$ je řešitelná tehdy a jen tehdy, je-li $h(A) = h(A, b))$.*

Věta 37. *Nechť $A\boldsymbol{x} = \boldsymbol{b}, B\boldsymbol{x} = \boldsymbol{c}$ jsou dvě soustavy rovnic o n neznámých nad T. Je-li $(A, \boldsymbol{b}) \sim (B, \boldsymbol{c})$, pak jsou tyto soustavy ekvivalentní.*

Věta 38 **(Frobeniova).** *Nechť $Ax = b$ je soustava m rovnic o n neznámých nad tělesem T. Tato soustava má řešení právě když $h(A) = h(A, b)$, Je-li $h(A) = n$, soustava má jediné řešení. Je-li $h(A) = h < n$, soustava má nekonečně mnoho řešení závislých na $n - h$ parametrech.*

Příklad

Řešte soustavu

$$\begin{aligned} 3x_1 - 5x_2 + 2x_3 + 4x_4 &= 2 \\ 7x_1 - 4x_2 + x_3 + 3x_4 &= 5 \\ 5x_1 + 7x_2 - 4x_3 - 6x_4 &= 3. \end{aligned}$$

Řešení. Rozšířená matice soustavy je

$$\begin{pmatrix} 3 & -5 & 2 & 4 & 2 \\ 7 & -4 & 1 & 3 & 5 \\ 5 & 7 & -4 & -6 & 3 \end{pmatrix} \sim \begin{pmatrix} 7 & -4 & 1 & 3 & 5 \\ -11 & 3 & 0 & -2 & -8 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

Zřejmě tedy $h(A) = 2$, $h((A, \mathbf{b})) = 3$, tedy soustava nemá řešení.

Příklad

Řešte soustavu

$$\begin{aligned} x_1 + 2x_2 + 5x_3 &= -9 \\ x_1 - x_2 + 3x_3 &= 2 \\ 3x_1 - 6x_2 - x_3 &= 25. \end{aligned}$$

Řešení. Pomocí Gaussovy eliminační metody upravíme $(A, \mathbf{b})$:

$$\begin{pmatrix} 1 & 2 & 5 & -9 \\ 1 & -1 & 3 & 2 \\ 3 & -6 & -1 & 25 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 5 & -9 \\ 0 & -3 & -2 & 11 \\ 0 & -12 & -16 & 52 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 2 & 5 & -9 \\ 0 & 3 & 2 & -11 \\ 0 & 3 & 4 & -13 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 5 & -9 \\ 0 & 3 & 2 & -11 \\ 0 & 0 & 2 & -2 \end{pmatrix}.$$

Zřejmě $h(A) = h((A, \mathbf{b})) = 3$, tedy soustava má jediné řešení. Z poslední rovnice: $x_3 = -1$, z předposlední pak: $x_2 = -3$ a následně z první: $x_1 = 2$, tedy soustava má řešení $(2, -3, -1)$.

Věta 39 (Cramerovo pravidlo)**.** *Nechť $Ax = b$ je soustava n lineárních rovnic o n neznámých ($n \geq 1$) nad T taková, že $\det A \neq 0$. Pak pro $j = 1, \ldots, n$ platí $x_j = \frac{\det A_j}{\det A}$, kde A_j je matice která vznikne z A tak, že j-tý sloupec nahradíme vektorem b.*

Definice 66. *Fundamentálním systémem řešení homogenní soustavy lineárních rovnic rozumíme libovolnou bázi řešení této soustavy.*

Příklad

Určete fundamentální systém řešení soustavy:

$$\begin{array}{llllll} x_1 & +2x_2 & -x_3 & +3x_4 & -2x_5 & =0 \\ 2x_1 & +x_2 & & +x_4 & -3x_5 & =0 \\ 5x_1 & +4x_2 & -x_3 & +5x_4 & -8x_5 & =0 \\ & 3x_2 & -2x_3 & +5x_4 & -x_5 & =0. \end{array}$$

Řešení. Matici soustavy upravíme:

$$\begin{pmatrix} 1 & 2 & -1 & 3 & -2 \\ 2 & 1 & 0 & 1 & -3 \\ 5 & 4 & -1 & 5 & -8 \\ 0 & 3 & -2 & 5 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & -1 & 3 & -2 \\ 2 & 1 & 0 & 1 & -3 \\ 4 & 2 & 0 & 2 & -6 \\ -2 & -1 & 0 & -1 & 3 \end{pmatrix} \sim$$

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

Tedy $h(A) = 2$ a řešení bude záviset na 3 parametrech.

Příklad – dokončení

Za parametry zvolme například x_1, x_2, x_5. Pak z prvních dvou rovnic odvodíme snadno obecné řešení:

$$\begin{aligned} x_4 &= -2x_1 - x_2 + 3x_5 \\ x_3 &= -5x_1 - x_2 + 7x_5. \end{aligned}$$

Fundamentální systém řešení získáme (dle důkazu Věty 5.10) například tak, že budeme postupně volit:

x_1	x_2	x_5
1	0	0
0	1	0
0	0	1

Pak fundamentálním systémem řešení je:

$$\mathbf{u}_1 = (1,0,-5,-2,0), \mathbf{u}_2 = (0,1,-1,-1,0), \mathbf{u}_3 = (0,0,7,3,1).$$

9 Okruh čtvercových matic

Definice 67. *Matice $A \in \mathscr{M}_n(T)$ se nazývá regulární, je-li $\det A \neq 0$. Matice A je singulární, je-li $\det A = 0$.*

Definice 68. *Jestliže $A \in \mathscr{M}_n(T)$ a existuje $B \in \mathscr{M}_n(T)$, tak, že $AB = E = BA$, pak se B nazývá inverzní matice k A a značí se $B = A^{-1}$.*

Věta 40. *K matici $A \in \mathscr{M}_n(T)$ existuje matice inverzní právě když je A regulární*

Věta 41. *Množina všech regulárních čtvercových matic stupně n tvoří grupu vzhledem k násobení.*

Příklad

Určete inverzní matici k matici $A = \begin{pmatrix} 2 & -1 & 3 \\ 1 & -1 & -2 \\ -3 & 2 & 1 \end{pmatrix}$.

Řešení. Zřejmě $\det A = -2$. Určíme všechny alg. doplňky:

$\mathscr{A}_{11} = \begin{vmatrix} -1 & -2 \\ 2 & 1 \end{vmatrix} = 3$, $\mathscr{A}_{12} = -\begin{vmatrix} 1 & -2 \\ -3 & 1 \end{vmatrix} = 5$,

$\mathscr{A}_{13} = \begin{vmatrix} 1 & -1 \\ -3 & 2 \end{vmatrix} = -1$, $\mathscr{A}_{21} = -\begin{vmatrix} -1 & 3 \\ -2 & 1 \end{vmatrix} = 7$,

$\mathscr{A}_{22} = \begin{vmatrix} 2 & 3 \\ -3 & 1 \end{vmatrix} = 11$, $\mathscr{A}_{23} = -\begin{vmatrix} 2 & -1 \\ -3 & 2 \end{vmatrix} = -1$,

$\mathscr{A}_{31} = \begin{vmatrix} -1 & 3 \\ -1 & -2 \end{vmatrix} = 5$, $\mathscr{A}_{32} = -\begin{vmatrix} 2 & 3 \\ 1 & -2 \end{vmatrix} = 7$,

$\mathscr{A}_{33} = \begin{vmatrix} 2 & -1 \\ 1 & -1 \end{vmatrix} = -1$. Tedy (dle důkazu Věty 6.1):

$$A^{-1} = -\frac{1}{2} \cdot \begin{pmatrix} 3 & 7 & 5 \\ 5 & 11 & 7 \\ -1 & -1 & -1 \end{pmatrix} = \begin{pmatrix} -\frac{3}{2} & -\frac{7}{2} & -\frac{5}{2} \\ -\frac{5}{2} & -\frac{11}{2} & -\frac{7}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Věta 42. *Je-li $A \in \mathscr{M}_n(T)$ regulární, pak je možné konečnou posloupností $t_1, t_2, ..., t_k$ elementárních řádkových transformací převést A na jednotkovou matici E, přičemž pomocí téže posloupnosti $t_1, t_2, ..., t_k$ lze E převést na A^{-1}.*

10 Svazy

Polosvazem nazýváme komutativní idempotentní pologrupu tj. takový grupoid $(G, \circ)$, kde pro každé tři prvky $a, b, c \in G$ platí tyto identity

a) asociativita: $(a \circ b) \circ c = a \circ (b \circ c)$

b) komutativita: $a \circ b = b \circ a$

c) idempotence: $a \circ a = a$

Definice 69. *Nechť L je neprázdná množina, nechť $\wedge, \vee$ jsou dvě binární operace na L takové, že $(L, \wedge)$ a $(L, \vee)$ jsou polosvazy a platí tzv. zákony absorpce:*

$$(ab) \qquad a \wedge (a \vee b) = a, \qquad a \vee (a \wedge b) = a$$

pro každé $a, b \in L$. Pak se $(L, \vee, \wedge)$ nazývá ***svaz****.*

Poznámka. Operaci $\vee$ ve svazu nazýváme **spojení**, operaci $\wedge$ nazýváme **průsek**.

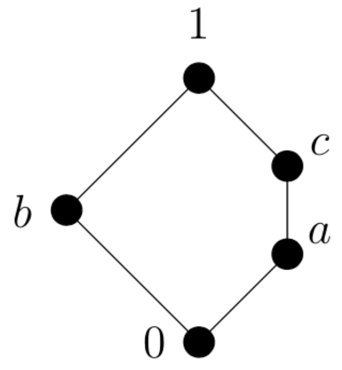
Definice 70. *Nechť $(L, \wedge, \vee)$ je svaz, nechť $\emptyset \neq A \subseteq L$ se nazývá podsvaz svazu $(L, \wedge, \vee)$, jestliže $\forall a, b \in A$ platí $a \vee b \in A,\ a \wedge b \in A$.*

Věta 43. *Nechť L je svaz. Pak pro každé $a, b, c \in L$ platí tzv. distributivní nerovnost tj.*

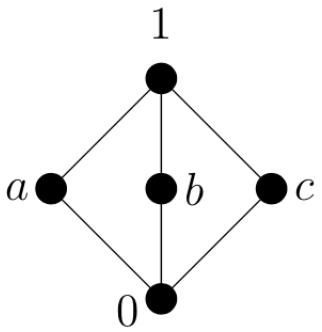
$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c), \qquad (a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c).$$

Pro každé $a, b, c \in L$ splňují tzv. modulární nerovnost tj.

$$a \vee (b \wedge c) \leq (a \vee b) \wedge c$$



Obr.6



Obr.7

Na obrázku 6. je znázorněn svaz N_5 tzv. pentagon. Obrázek 7. ukazuje svaz M_3 jejich význam je popsán níže.

Definice 71. *Svaz L se nazývá distributivní, jestliže pro každé* $a, b, c \in L$ *platí*

$$(D) \qquad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Svaz L se nazývá modulární, jestliže pro každé $a, b, c \in L$ *splňující* $a \leq c$ *platí*

$$(M) \qquad a \vee (b \wedge c) = (a \vee b) \wedge c.$$

Věta 44. *Svaz L je distributivní, právě když pro každé* $a, b, c \in L$ *platí rovnost duální k rovnosti (D), tj.*

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

Věta 45. *Každý distributivní svaz je modulární.*

Definice 72. *Nechť* $(A, \wedge, \vee)$ *a* $(B, \wedge, \vee)$ *jsou svazy. Zobrazení* $h : A \to B$ *se nazývá homomorfismus, jestliže pro každé* $a, b \in A$ *platí:*

$$h(a \vee b) = h(a) \vee h(b), \qquad h(a \wedge b) = h(a) \wedge h(b)$$

Bijektivní homomorfismus se nazývá **izomorfismus**.

Věta 46. *Svaz L je modulární, právě když neobsahuje podsvaz izomorfní s* N_5. *Svaz je distributivní, právě když neobsahuje podsvaz izomorfní s* N_5 *nebo* M_3 *(viz obr. 6.,7.).*

Definice 73. *Nechť L je svaz s 0 a 1. Prvek* $b \in L$ *se nazývá komplement prvku* $a \in L$, *jestliže*

$$a \vee b = 1, \qquad a \wedge b = 0.$$

Svaz L s 0 a 1 se nazývá komplementární, má-li každý prvek aspoň jeden komplement. Nechť L je svaz $a, b \in L, a \leq b$ Nechť $c \in [a, b]$. Prvek $d \in [a, b]$ se nazývá relativní komplement prvku c v intervalu $[a, b]$ jestliže platí

$$c \vee d = b, \qquad c \wedge d = a.$$

Svaz L se nazývá relativně komplementární, má-li každá prvek $c \in [a, b]$ pro libovolné $a, b \in L,\ a \leq b$, aspoň jeden relativní komplement v $[a, b]$.

Věta 47. *Nechť L je distributivní svaz s 0 a 1. Pak každý prvek* $a \in L$. *Pak každý prvek* $a \in L$ *má nejvýše jeden komplement.*

Definice 74. *Svaz s 0 a 1 je* ***jednoznačně komplementární****, má li každý prvek* $a \in L$ *práve jeden komplement.*

Věta 48. *Každý konečný jednoznačně distributivní komplementární svaz je distributivní.*

Afinní prostory a podprostory, vzájemná poloha afinních podprostorů. Afinní báze, matice přechodu. Afinní zobrazení a jejich matice. Eukleidovské afinní prostory. Projektivní prostory a homogenní souřadnice. Aplikace v počítačové grafice.

11 Afinní prostory (AP)

Řekněme, že na neprázdné množině A je dána *struktura afiního prostoru* (stručněji afinní struktura), je-li dán vektorový prostor U a zobrazení $Add_A : A \times U \to A$ takové, že

1. pro všechna $a \in A,\ u, v, \in U$

$$Add_A(Add_A(a, u), v) = Add_A(a, u + v)$$

2. pro všechna $a, b \in A$ existuje právě jedno $u \in U$ tak, že

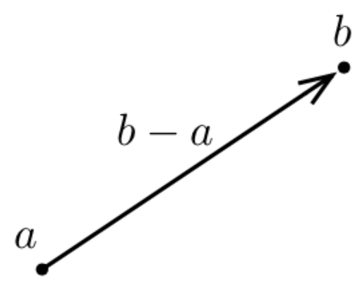
$$Add_A(a, u) = b$$

Množina A se strukturou afinního prostoru se nazývá afinní prostor, její prvky se nazývají body, Vektorový prostor U se nazývá zaměřením afinního prostoru A.

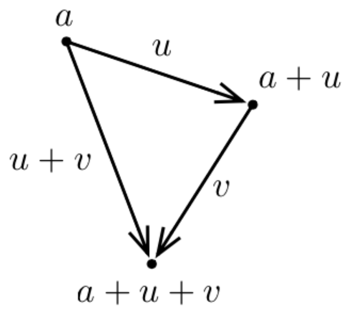
Zobrazení Add_A se nazývá sčítání bodů a vektorů. Pro libovolné $a \in A$ a $u \in U$ se bod $Add_A(a, u)$ označuje $a + u$ a nazývá se součet bodu a a vektoru u.

Jelikož podle bodu 1. definice platí $(a+u)+v = a+(u+v)$, můžeme při sčítání dvou vektorů k bodu vynechat závorky a psát pouze $(a + u + v)$.

Vektor u z 2. bodu definice afinního prostoru se označuje $b-a$. Vzhledem k podmínce bodu 2. tento vektor existuje pro libovolné a a b a to právě jeden. Přiřazením $(a, b) \mapsto b-a$ je tedy jednoznačně určené zobrazení z $A \times A$ do U. Vektoru $b - a$ se říká rozdíl bodů b a a.



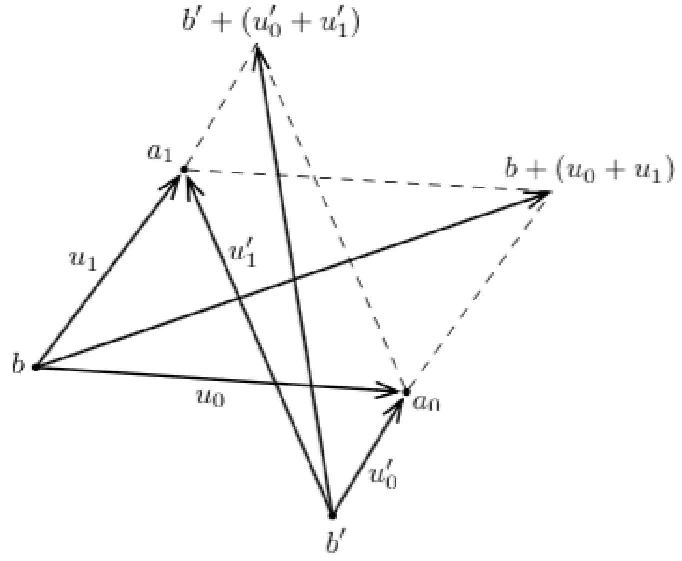
Obrázek 3.1: Body a, b a vektor $b - a$.



Obrázek 3.2: Grafické znázornění podmínky 1. definice afinní struktury.

Je-li vektorový prostor U konečné dimenze $\Rightarrow$ afinní prostor je také konečné dimenze. Dimenzí AP A nazýváme dimenzi vektorového prostoru V. Afinní prostor dimenze 1 se nazývá afinní přímka, afinní prostor dimenze 2 afinní rovina.

11.1 Afinní kombinace a afinní obal



Obrázek 3.3: Pokud součet koeficientů c^0 a c^1 není roven 1, závisí bod $b + (c^0 u_0 + c^1 u_1)$ na volbě bodu b. Obrázek ukazuje případ $c^0 = c^1 = 1$.

Začněme pozorováním. Na obrázku 3.3 vidíme body a_0, a_1, b afinního prostoru A. Dvojice bodů a_0, b a a_1 definují vektory $u_0 = a_0 - b$ a $u_1 = a_1 - b$, které jsou na obrázku rovněž znázorněny. Lineární kombinace $c^0 u_0 + c^1 u_1$ těchto vektorů pak definujeme bod $b + (c^0 u_0 + c^1 u_1)$ (na obrázku je znázorněn případ $c^0 = c^1 = 1$). POkud místo bidu b vybereme nějaký jiný bod b', pak se výsledný bod získaný stejným způsobem, bude od původního lišit:

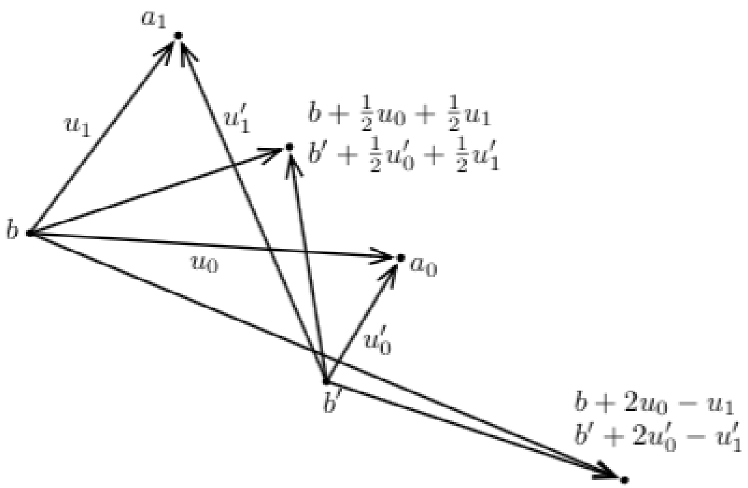
$$b + (c^0 u_0 + c^1 u_1) \neq b' + (c^0 u'_0 + c^1 u'_1),$$

což e patrné i z obrázku

Situace se ovšem mění, pokud $c^0 + c^1 = 1$. To můžeme odhadnout už na obrázku 3.3 když se podíváme na průsečík šipek znázorňující vektory $u_0 + u_1$ a $u_0' + u_1'$. Na obrázku 3.4 jsou zobrazeny případy $c^0 = c^1 = \frac{1}{2}$ a $c^0 = 1$ a $c^1 = -1$. Zřejmě pokud $c^0 + c^1 = 1$, pak $b + (c^0 u_0 + c^1 u_1) = b' + (c^0 u_0' + c^1 u_1')$. Následující věta naši domněnku potvrzuje pro libovolný počet bodů.

Věta 49. *Mějme body $a_0, a_1, \dots, a_m$ afinního prostoru A. Pro libovolné dva body $b, b' \in A$ a čísla $c^0, c^1, \dots, c^m$ taková, že $c^0 + c^1 + \cdots + c^m = 1$ platí*

$$b + c^0(a_0 - b) + c^1(a_1 - b) + \cdots + c^m(a_m - b) = b' + c^0(a_0 - b') + c^1(a_1 - b') + \cdots + c^m(a_m - b')$$



Obrázek 3.4: Pokud součet koeficientů c^0 a c^1 je roven 1, bod $b + c^0 u_0 + c^1 u_1$ nezávisí na volbě bodu b. Obrázek ukazuje dva případy: $c^0 = c^1 = \frac{1}{2}$ a $c^0 = 2, c^1 = -1$

Každou afinní kombinaci více než dvou bodů lze vyjádřit pomocí afinních kombinací dvojic bodů. Ukážeme se to na příkladě afinní kombinace $c^0 a_0 + c^1 a_1 + c^2 a_2$. Pokud je $c^0 + c^1 \neq 0$, platí:

$$c^0 a_0 + c^1 a_1 + c^2 a_2 = (c^0 + c^1)\left(\frac{c^0}{c^0 + c^1} a_0 + \frac{c^1}{c^0 + c^1} a_1\right) + c^2 a_2,$$

přičemž $\frac{c^0}{c^0+c^1} + \frac{c^1}{c^0+c^1} = 1$, takže uvnitř velké závorky je opravdu afinní kombinace dvou bodů, stejně jako je afinní kombinací dvou bodů i celý výraz, protože $(c^0 + c^1) +^2 = 1$.

Afinní obal množiny K je množina značící se $Aff(K)$ definovanou následovně:

$$Aff(K) = \{c^0 a_0 + c^1 a_1 \mid a_0, a_1 \in K, c^0 + c^1 = 1\}$$

Věta 50. *Pro libovolnou neprázdnou množinu $K \subseteq A$ platí $Aff(Aff(K)) = Aff(K)$.*

11.2 Vektorové kombinace

Pokud $c^0 + c^1 + \cdots + c^m = 0$, pak vektor

$$c^0(a_0 - b) + c^1(a_1 - b) + \cdots + c^k(a_k - b)$$

nezávisí na volbě bodu b. Body $a_0, a_1 \ldots, a_k$ spolu s koeficienty $c^0, c^1, \ldots, c^k$ tak jednoznačně definují vektor. který se nazývá vektorová kombinace bodů $a_0, a_1 \ldots, a_k$. tento vektor se značí stejně jako kombinace afinní:

$$c^0 a_0 + c^1 a_1 + \cdots + c^k a_k.$$

Pro neprázdnou množinu $K \subseteq A$ označujeme symbolem $Vec(K)$ množinu všech vektorových kombinací prvků množiny K. Platí

$$Vec(K) = \{c^0 a_0 + \cdots + c^k a_k \mid k \geq 1, a_0, \ldots a_k \in K, c^0 + \cdots + c^k = 0\}$$

Věta 51. *Vec(K) je vektorový podprostor zaměření afinního prostoru.*

Věta 52. *Vec(Aff(K)) = Vec(K)*

11.3 Afinní podprostory

Neprázdná podmnožina B afinního prostoru A se zaměřením U se nazývá afinní podprostor afinního prostoru A, jestliže $Aff(B) = B$

Věta 53. *Neprázdná podmnožina B afinního prostoru A se zaměřením U je jeho afinním podprostorem, právě když existuje vektorový prostor $V \subseteq U$ takový, že jsou splněny následující podmínky:*

1. *Pro každé $a \in B$, $u \in V$ platí $a + u \in B$*
2. *Pro každé $a, b \in B$ platí $b - a \in V$*

Platí V = Vec(B).

11.3.1 Vzájemná poloha afinních podprostorů

Mějme dva afinní podprostory B_1 a B_2 se zaměřeními V_1, V_2 afinního prostoru A se zaměřením U. O afinních podprostorech B_1, B_2 řekneme, že jsou

rovnoběžné , pokud platí $V_1 \subseteq V_2$ nebo $V_2 \subseteq V_1$,

různoběžné , pokud nejsou rovnoběžné a pokud $B_1 \subseteq B_2 \neq \emptyset$.

mimoběžné ve všech ostatních případech.

Věta 54. *Předpokládejme, že afinní podprostory B_1, B_2 jsou rovnoběžné a, že $V_1 \subseteq V_2$. Následující 3 podmínky jsou ekvivalentní:*

1. *Existuje bod $b_0 \in B_1 \cap B_2$.*
2. *Pro každé dva body $b_1 \in B_1$ a $b_2 \in B_2$ platí $b_2 - b_1 \in V_2$.*
3. *Existují body $b_1 \in B_1$ a $b_2 \in B_2$ takové, že $b_2 - b_1 \in V_2$.*

Věta 55. *Předpokládejme, že afinní podprostory B_1, B_2 nejsou rovnoběžné a, že $V_1 \subseteq V_2$. Následující 3 podmínky jsou ekvivalentní:*

1. *B_1 a B_2 jsou různoběžné.*
2. *Pro každé dva body $b_1 \in B_1$ a $b_2 \in B_2$ platí $b_2 - b_1 \in V_1 \vee V_2$.*
3. *Existují body $b_1 \in B_1$ a $b_2 \in B_2$ takové, že $b_2 - b_1 \in V_1 \vee V_2$.*

Poznámka. Symbolem „$\vee$“ označujeme operaci spojení vektorových prostorů.

11.4 Afinní báze

Mějme afinní prostor A dimenze m se zaměřením U. pro bod $a_0 \in A$ a bázi $\alpha = (u_1, \ldots, u_m)$ vektorového prostoru U nazýváme dvojici $\varphi'(\alpha, a_0)$ afinní bázi afinního prostoru A. Bod a_0 nazýváme počátkem báze φ. Afinní bázi φ zapisujeme jako $(m+1)$-tici $(u_1, \ldots, u_m, a_0)$. Pro libovolný bod $a \in A$ nazýváme afinními souřadnicemi (souřadnicovým vyjádřením) bodu a vzhledem k afinní bázi $\varphi = (\alpha, a_0)$ $(m+1)$-tici

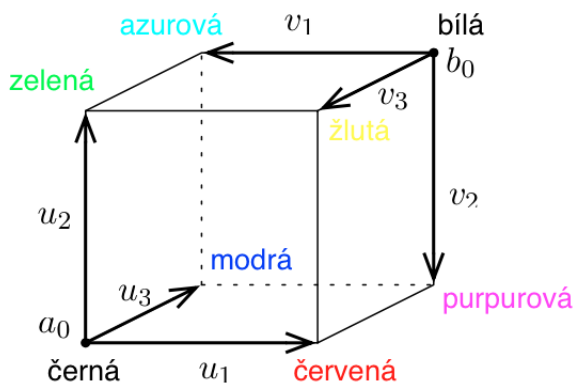
$$\alpha_\varphi = \begin{bmatrix} (a-a_0)^1_\alpha \\ (a-a_0)^2_\alpha \\ \vdots \\ (a-a_0)^m_\alpha \\ 1 \end{bmatrix}$$

11.4.1 Matice přechodu

Mějme dvě afinní báze $\varphi = (\alpha, a_0)$, $\overline{\varphi} = (\overline{\alpha}, \overline{a_0})$ afinního prostoru A dimenze m se zaměřením U. Problém jak najít souřadnicové vyjádření bodu $a \in A$ vzhledem k bázi $\overline{\varphi}$ známe-li souřadnicové vyjádření tohoto bodu vzhledem k bázi φ. K výpočtu potřebujeme znát souřadnice bodu a v afinní bázi φ, matici přechodu od (vektorové) báze α k $\overline{\alpha}$ a souřadnice počátku a_0 vzhledem k afinní bázi $\overline{\varphi}$. Matici $M_{\varphi,\overline{\varphi}}$ přechodu od báze φ k bázi $\overline{\varphi}$ definujeme následovně:

$$M_{\varphi,\bar{\varphi}} = \left(\begin{array}{ccc|c} & M_{\alpha,\bar{\alpha}} & & (a_0)_{\bar{\varphi}} \\ \hline 0 & \cdots & 0 & \end{array}\right)$$

Použití. Pří kreslení v OpenGL se používají dvě základní afinní báze: Báze modelu (Model Coordinate System) a Báze pozorovatele (View Coordinate System). Báze modelu je báze, vzhledem k níž uvádíme souřadnice vykreslovaných objektů. Báze pozorovatele je spojena s kamerou tak, že první vektor její vektorové báze směřuje doprava, druhý nahoru a třetí dozadu.



Obrázek 3.6: Barevná krychle.

Použití. na obrázku 3.6 vidíme základních osm barev (bílou, černou, červenou, zelenou, modrou, žlutou, azurovou a purpurovou) uspořádaných do vrcholů tzv. barevné krychle. Tuto krychli si můžeme představit jako podmnožinu trojrozměrného afinního prostoru; body mimo ni pro nás ovšem nemají význam. Na obrázku jsou zakresleny dvě základní afinní báze, které se používají k vyjádření barev: $\varphi_{RGB} = (u_1, u_2, u_3, a_0)$ a $\varphi_{CMYK} = (v_1, v_2, v_3, b_0)$. Matice přechodu vypadá následovně:

$$M_{\varphi_{RGB},\varphi_{CMY}} = M_{\varphi_{CMY},\varphi_{RGB}} = \begin{pmatrix} -1 & 0 & 0 & 1 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

11.5 Afinní zobrazení

Afinní zobrazení jsou zobrazení, která jsou popsatelná v rámci teorie afinních prostorů. Mezi afinní zobrazení patří mnohá zobrazení, která se používají v počítačové grafice: posunutí, otočení, změna měřítka, atd.

Definice 75. *Zobrazení $f : A \to B$ afinních prostorů A a B se nazývá afinní, jestliže pro libovolné dva body $a_1, a_2 \in A$ a jejich afinní kombinaci $c^1a_1 + c^2a_2$ platí*

$$f(c^1a_1 + c^2a_2) = c^1f(a_1) + c^2f(a_2).$$

Věta 56. *Pro lib. bod $b_0 \in B$ je zobrazení $f : A \to B$, definované předpisem $f(a) = b_0$ (tj. konstantní zobrazení), afinní.*

Věta 57. *Identické zobrazení (identita) na množině X je zobrazení Id_X takové, že $Id_X(x) = x$ pro každé $x \in X$. Identita na afinním prostoru A je afinní zobrazení.*

Věta 58. *Zobecnění předchozí věty: je-li $Y \subseteq X$, pak kanonické vložení podmnožiny Y do X je zobrazení $i_Y : Y \to X$, definované předpisem $i_Y(y) = y$. Je-li $B \subseteq A$ afinní podprostor afinního prostoru A, pak kanonické vložení $i_B : B \to A$ je afinní zobrazení.*

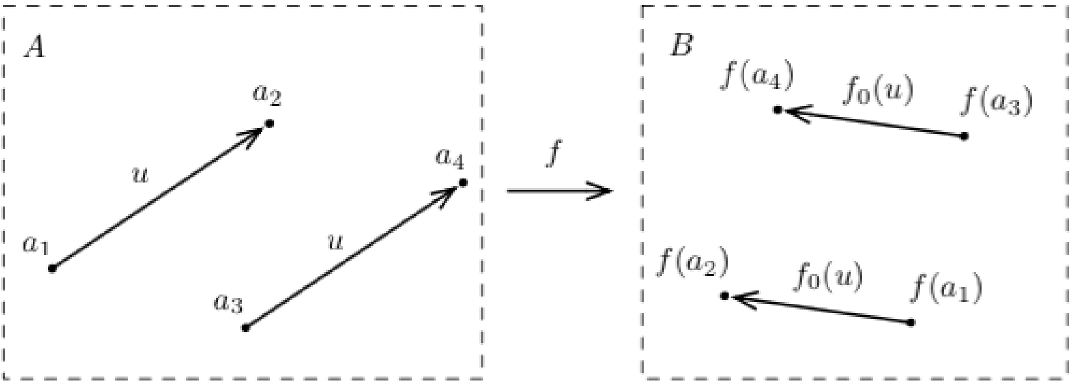
Věta 59. *Zobrazení $f_0 : U \to V$ definované předpisem (věta 45) se nazývá zobrazení podřízene afinnímu zobrazení f.*

Věta 60. *Kompozice dvou afinních zobrazení je afinní zobrazení.*

Věta 61. *Afinní zobrazení $f : A \to A$ se nazývá afinní transformace afinního prostoru A.*

Věta 62. *Příkladem afinní transformace afinního prostoru A je posunutí o vektor $u_0 \in U$, což je zobrazení $tr_{u_0} : A \to A$ (tr jako translace) definované předpisem*

$$r_{u_0}(a) = a + u_0.$$



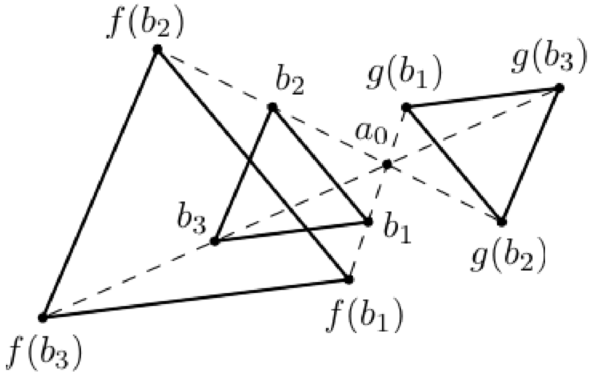
Obrázek 5.1: Afinní zobrazení zachovává rovnoběžnost.

Věta 63. *Středová souměrnost se středem $a_0 \in A$ je zobrazení $f : A \to A$ definované předpisem*

$$f(a) = 2a_0 - a$$

Věta 64. *Zobrazení $f : A \to A$ se nazývá stejnolehlost pokud platí*

$$f(a) = (1 - c)a_0 + ca.$$



Obrázek 5.3: Stejnolehlost f s koeficientem $c = 2$ a g s koeficientem $c = -1$.

11.5.1 Matice affiního zobrazení

Mějme afinní bázi $\varphi = (\alpha, a_0)$, $\alpha = (u_1, \ldots, u_m)$ afinního prostoru A se zaměřením U a afinní bázi $\psi = (\beta, b_0)$, $\beta = (v_1, \ldots, v_n)$ afinního prostoru B se zaměřením V. Dále mějme afinní zobrazení $f : A \to B$ s podřízeným lineárním zobrazením $f_0 : U \to V$. Naším cílem je najít způsob, jak ze souřadnicového vyjádření a_φ bodu $a \in A$ vzhledem k bázi φ vypočítat souřadnicové vyjádření $f(a)_\psi$ jeho obrazu $f(a)$ při zobrazení f vzhledem k bázi ψ.

Máme
$$f(a) = f_0(a - a_0) + f(a_0),$$
čili podle příkladu 3.34 a s použitím matice $M^{f_0}_{\alpha,\beta}$ lineárního zobrazení f_0 vzhledem k bazím α, β,
$$\begin{aligned} f(a)_\psi &= \begin{pmatrix} f_0(a-a_0)_\beta \\ 0 \end{pmatrix} + f(a_0)_\psi = \begin{pmatrix} M^{f_0}_{\alpha,\beta} \cdot (a-a_0)_\alpha \\ 0 \end{pmatrix} + f(a_0)_\psi \\ &= \left(\begin{array}{c} M^{f_0}_{\alpha,\beta} \\ \hline 0 \quad \cdots \quad 0 \end{array}\right) \cdot (a-a_0)_\alpha + f(a_0)_\psi. \end{aligned}$$
Pokud nyní sestavíme blokovou matici
$$M^f_{\varphi,\psi} = \left(\begin{array}{c|c} M^{f_0}_{\alpha,\beta} & f(a_0)_\psi \\ \hline 0 \quad \cdots \quad 0 & \end{array}\right), \tag{5.7}$$
dostaneme
$$f(a)_\psi = M^f_{\varphi,\psi} \cdot a_\varphi.$$
Matice $M^f_{\varphi,\psi}$ se nazývá *matice afinního zobrazení f vzhledem k bazím φ, ψ.*

K sestavení této matice potřebujeme následující údaje: matici lineárního zobrazení f_0 vzhledem k vektorovým bazím α, β a souřadnice bodu $f(a_0)$ vzhledem k afinní bázi ψ.

12 Eukleidovské prostory

Většina vlastností eukleidovských prostorů úzce souvisí s vlastnostmi skalárního součinu na vektorových prostorech. Zde uvedeme jejich stručný souhrn.

Skalární součin na vektorovém prostoru U je zobrazení $\langle\cdot,\cdot\rangle : U \times U \to R$, které je pozitivně definitní symetrickou bilineární formou, což znamená, že pro každé tři vektory $u, v, w \in U$ a dva skaláry $c, d \in R$ platí

$$\langle u,u\rangle > 0 \quad \text{pro } u \neq 0, \tag{6.1}$$

$$\langle u,v\rangle = \langle v,u\rangle, \tag{6.2}$$

$$\langle cu+dv,w\rangle = c\langle u,w\rangle + d\langle v,w\rangle. \tag{6.3}$$

Vektorové prostory se skalárním součinem se také nazývají *unitární prostory*.

Na vektorovém prostoru R^n je definován tzv. standardní (kanonický) skalární součin známým předpisem

$$\langle u,v\rangle = u^1v^1 + u^2v^2 + \cdots + u^nv^n, \tag{6.4}$$

kde u^i resp. v^i jsou složky vektorů u resp. v.

Délka vektoru u (také *norma*) se značí $\|u\|$ a je definována předpisem

$$\|u\| = \sqrt{\langle u,u\rangle}.$$

Pokud $\|u\| = 1$, je vektor u *jednotkový*. Každý vektor má nenulovou délku, právě když je nenulový. Z libovolného nenulového vektoru můžeme vytvořit jednotkový vektor tzv. *normováním*, které spočívá ve vynásobení vektoru převrácenou hodnotou jeho délky:

$$u_0 = \frac{1}{\|u\|}u.$$

53

Pro libovolné dva vektory $u, v \in U$ platí *Cauchyho-Schwartzova nerovnost*:

$$\langle u, v\rangle^2 \leq \langle u, u\rangle \cdot \langle v, v\rangle.$$

Pomocí délek vektorů lze nerovnost přepsat takto:

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

Rovnost nastává právě když jsou vektory u a v lineárně závislé.

Podle Cauchyho-Schwartzovy nerovnosti je

$$\frac{|\langle u, v\rangle|}{\|u\| \|v\|} \leq 1,$$

takže v následující definici $\arccos(\langle u, v\rangle / (\|u\| \|v\|))$ vždy existuje. *Odchylka ϑ vektorů u, v* je definována předpisem

$$\vartheta = \arccos \frac{\langle u, v\rangle}{\|u\| \|v\|}$$

Tyto vektory jsou *kolmé* (*ortogonální*), jestliže $\langle u, v\rangle = 0$ (což je právě když je jejich odchylka rovna $\frac{\pi}{2}$). *Odchylka jednorozměrných vektorových podprostorů, generovaných vektory u a v* je menší z odchylek vektorů u, v a u, $-v$.

Ortogonální doplněk vektorového podprostoru $V \subseteq U$ je vektorový podprostor U, složený z vektorů, kolmých ke každému vektoru z V. Dva vektorové podprostory jsou *kolmé* (*ortogonální*), je-li jeden z nich podmnožinou ortogonálního doplňku druhého (tato definice je poněkud omezující; nezahrnuje např. dvě kolmé roviny v trojrozměrném prostoru, ale pro naše potřeby bude dostatečná).

Pro libovolné dva vektory u, v platí *Pythagorova věta*:

$$\|u - v\|^2 = \|u\|^2 + \|v\|^2 \quad \text{právě když} \quad \langle u, v\rangle = 0.$$

Pythagorovu větu lze snadno odvodit z vlastností skalárního součinu:

$$\begin{aligned} \|u - v\|^2 &= \langle u - v, u - v\rangle = \langle u, u\rangle - \langle v, u\rangle - \langle u, v\rangle + \langle v, v\rangle \\ &= \|u\|^2 - 2\langle u, v\rangle + \|v\|^2, \end{aligned}$$

takže

$$2\langle u, v\rangle = \|u\|^2 + \|v\|^2 - \|u - v\|^2, \tag{6.5}$$

což znamená přesně tvrzení Pythagorovy věty.

13 Projektivní prostory

Tato kapitola obsahuje úvod do teorie projektivních prostorů, který by měl čtenáři umožnit pochopit základy geometrických transformací používaných v trojrozměrné počítačové grafice.

Ve většině textu této kapitoly jsou prvky afinních prostorů současně vektory v nějakých prostorech vektorových. Proto není vždy možné striktně rozlišovat mezi body a vektory, což se projevuje i na značení například tím, že se volba mezi hranatými a kulatými závorkami nemůže řídit přísnými kritérii.

7.1 Projektivní prostory a jejich vztah k afinním prostorům

Začneme několika na sebe navazujícími motivačními příklady.

Příklad 7.1. Uvažme nadrovinu A ve vektorovém prostoru prostoru R^3 danou předpisem

$$A = \{(a^1, a^2, a^3) \in R^3 \mid a^3 = 1\}. \tag{7.1}$$

Zaměřením této nadroviny je vektorový podprostor

$$U = \{(a^1, a^2, a^3) \in R^3 \mid a^3 = 0\}. \tag{7.2}$$

Prvky nadroviny A hrají dvojí roli. Jsou to body v afinním prostoru A a současně vektory ve vektorovém prostoru R^3. Prvky vektorového podprostoru U, který je zaměřením afinního prostoru A, jsou tedy vektory téhož vektorového prostoru jako prvky afinního prostoru A. Podívejme se podrobněji, co lze z těchto souvislostí vytěžit.

Nejprve si uvědomme, jak lze v této situaci interpretovat sčítání bodu a vektoru. Víme, že prostor R^3 je afinní prostor, v němž je sčítání bodu a vektoru totožné se sčítáním vektorů ve vektorovém prostoru. Protože afinní prostor A je afinním podprostorem afinního prostoru R^3 a jeho zaměřením je vektorový podprostor $U \subset R^3$, přenese se tato vlastnost i na tento podprostor: pro libovolný bod $a \in A$ a vektor $u \in U$ je součet bodu a vektoru $a + u$ roven součtu $a + u$ vektorů v R^3.

Ze vztahů (7.1) a (7.2) vyplývá, jak vypadají složky vektorů a a u. Zatímco třetí složka vektoru a je rovna jedné, vektor u má třetí složku nulovou:

$$a = \begin{pmatrix} a^1 \\ a^2 \\ 1 \end{pmatrix}, u = \begin{pmatrix} u^1 \\ u^2 \\ 0 \end{pmatrix}. \tag{7.3}$$

Odtud je také vidět, že součet $a + u$ bude prvkem podprostoru A, protože bude mít stejně jako bod a třetí složku rovnu jedné:

$$a + u = \begin{pmatrix} a^1 \\ a^2 \\ 1 \end{pmatrix} + \begin{pmatrix} u^1 \\ u^2 \\ 0 \end{pmatrix} = \begin{pmatrix} a^1 + u^1 \\ a^2 + u^2 \\ 1 \end{pmatrix}. \tag{7.4}$$

13.1 Projektivní zobrazení

7.2 Projektivní zobrazení

Příklad 7.11. V počítačové grafice je potřeba kromě afinních zobrazení používat ještě zobrazení jiného typu. Platí to především o *perspektivním promítání*.

Uveďme jednoduchý příklad z dvourozměrného prostoru. Představme si pozorovatele umístěného v prostoru R^2 do bodu $[0,0]$ a hledícího ve směru osy y. Veškeré předměty, které pozorovatel vidí, se mu promítají na přímku (v přirozenějším trojrozměrném příkladě by to byla rovina). Nazvěme tuto přímku *projekční plátno* a stanovme, že bude mít rovnici $y = 1$. Každý viditelný bod z prostoru R^2 se na projekčním plátně zobrazí do bodu, který vznikne jako jeho průsečík se spojnicí bodu a umístění pozorovatele.

Popsaným způsobem vzniká zobrazení f podmnožiny R^2 na projekční plátno, které je příkladem perspektivního promítání. Není těžké odvodit rovnici tohoto zobrazení:

$$f[x,y] = \left[\frac{x}{y}, 1\right]. \tag{7.16}$$

Zobrazení f ovšem není afinní; jistě neexistuje matice

$$M = \begin{pmatrix} p_1^1 & p_2^1 & p_3^1 \\ p_1^2 & p_2^2 & p_3^2 \\ 0 & 0 & 1 \end{pmatrix} \tag{7.17}$$

taková, že

$$\begin{pmatrix} p_1^1 & p_2^1 & p_3^1 \\ p_1^2 & p_2^2 & p_3^2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{x}{y} \\ 1 \\ 1 \end{bmatrix}. \tag{7.18}$$

Zajímavé ovšem je, že pokud zvolíme matici M takto:

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \tag{7.19}$$

dostaneme

$$M \cdot \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} x \\ y \\ y \end{bmatrix}, \tag{7.20}$$

Posloupnosti a jejich limity. Funkce jedné reálné proměnné a jejich vlastnosti. Limita a spojitost funkce. Derivace funkce, geometrický význam. Základní věty diferenciálního počtu a jejich aplikace. Vyšetřování průběhu funkce. Neurčitý integrál, určitý Riemannův integrál. Číselné řady, konvergence a součty, kriteria konvergence

14 Funkcia jednej reálnej premennej a jej vlastnosti

Funkciou reálnej premennej rozumieme lubovolné zobrazenie $f : X \to \mathbb{R}$, kde $X \subseteq \mathbb{R}$. $(f : X \subseteq \mathbb{R} \to \mathbb{R})$

14.1 Vlastnosti

Definice 76. *Funckia $f : X \subseteq \mathbb{R} \to \mathbb{R}$ sa nazýva **ohraničená** (zhora, zdola alebo len ohraničená) na množine $X' \subseteq X$, ak je taká množina $f(X') \subseteq \mathbb{R}$.*

Definice 77. ***Maximom** funkcie $f : X \subseteq \mathbb{R} \to \mathbb{R}$ na množine $X' \subseteq X$ nazývame číslo $\boldsymbol{max} f(X')$ (značenie: $max_{x \in X'} f(X)$). Povieme že funkcia f tejto hodnoty nabýva v bode $x \in X'$, ak $f(x) = max f(X')$.*

Definice 78. ***Minimom** funkcie $f : X \subseteq \mathbb{R} \to \mathbb{R}$ na množine $X' \subseteq X$ nazývame číslo $\boldsymbol{min} f(X')$ (značenie: $min_{x \in X'} f(X)$). Povieme že funkcia f tejto hodnoty nabýva v bode $x \in X'$, ak $f(x) = min f(X')$.*

O maxime (poprípade minime) funkcie f na množine $X' \subseteq X$ je **ostré**, ak existuje práve jeden bod tejto množiny, v ktorej funkcia f maxima (poprípade minima) nabýva. Ak je takých bodov viac, hovoríme že maximum (poprípade minimum) je **neostré**. Maximum a minimum sa súhrne nezývajú **extrémy**. Bod, v ktorom funkcia nabýva maxima (poprípade minima) na danej množine vždy existuje. To ale nemusí platiť o supréme a infime (definície nasledujú). Majme množiny $B \subseteq A$ (na množine A je zavedené usporiadanie) pričom platí $A, B \subseteq \mathbb{R}$, potom **hornou závorou** množiny B rozumieme taký prvok $a \in A$, že $\forall b \subseteq B$ platí, $b \leq a$. Analogicky **dolnou závorou** množiny B rozumieme taký prvok $a \in A$, že $\forall b \subseteq B$ platí, $a \leq b$.

Definice 79. ***Supremom funkcie** $f : X \subseteq \mathbb{R} \to \mathbb{R}$ na množine $X' \subseteq X$ nazývame číslo $\boldsymbol{sup} f(X')$ (značenie: $sup_{x \in X'} f(X)$). (Sedlácky povedané, supremum je najmenší prvok z množiny všetkých horných závor oboru hodnot funkcie na danom intervale.)*

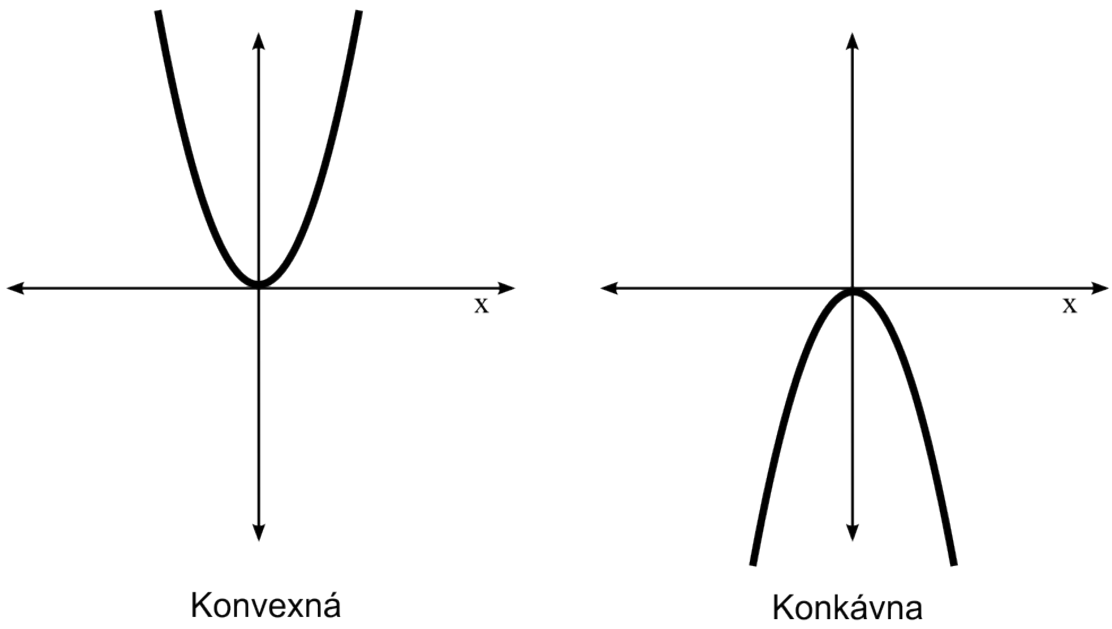
Definice 80. ***Infimom funkcie** $f : X \subseteq \mathbb{R} \to \mathbb{R}$ na množine $X' \subseteq X$ nazývame číslo $\boldsymbol{inf} f(X')$ (značenie: $inf_{x \in X'} f(X)$). (Sedlácky povedané, infimum je najvačší prvok z množiny všetkých dolných závor oboru hodnot funkcie na danom intervale.)*

Definice 81. *Povieme že funkcia $f : X \subseteq \mathbb{R} \to \mathbb{R}$ je na množine $X' \subseteq X$ **rastúca (nerastúca, klesajúca, neklesajúca)**, ak pre každé 2 body $x, y \in X', x < y$, platí*

*$f(x) < f(y)(f(x) \geq f(y), f(x) > f(y), f(x) \leq f(y))$. Ak je funkcia f rastúca (nerastúca, klesajúca, neklesajúca) na celej množine X, nazýva sa proste rastúca (nerastúca, klesajúca, neklesajúca). Súhrne sa taká funkcia nazýva **monotónnou**.*

Definice 82. *Povieme že funkcia $f : X \subseteq \mathbb{R} \to \mathbb{R}$ je **konvexná** na intervale $I \subseteq X$, ak pre každé tri body $x, y, z \in I, x < y < z$, platí $f(x)(z-y)+f(y)(x-z)+f(z)(y-x) \geq 0$.*

Definice 83. *Povieme že funkcia $f : X \subseteq \mathbb{R} \to \mathbb{R}$ je **konkávna** na intervale $I \subseteq X$, ak pre každé tri body $x, y, z \in I, x < y < z$, platí $f(x)(z-y)+f(y)(x-z)+f(z)(y-x) \leq 0$.*



Obrázek 1: **Hint:** Do konkávnej kávu nenaleješ!

Definice 84. *Funkcia $f : X \subseteq \mathbb{R} \to \mathbb{R}$ sa nazýva **sudá (lichá)**, ak pre každý bod $x \in X$ platí $-x \in X$ a $f(-x) = f(x)(f(-x) = -f(x))$ (Príklad lichej: $f(x) = x^3$).*

Definice 85. *Funkcia $f : X \subseteq \mathbb{R} \to \mathbb{R}$ sa nazýva **periodická**, ak existuje číslo $p > 0$ také, že $x \in X$, práve vtedy keď $x + p \in X$ a ak $x \in X$, potom $f(x + p) = f(x)$. Číslo p na nazýva **perióda funkcie** f. (Príklad: $f(x) = sin(x)$ s periódou $p = 2\pi$)*

Definice 86. *Funkcia $f : X \subseteq \mathbb{R} \to \mathbb{R}$ taká, že jej obor hodnot je jednoprvková množina, sa nazýva **konštantná funkcia***

Definice 87. *Funkcia $f : \mathbb{R} \to \mathbb{R}$ sa nazýva **afinná**, ak existujú čísla $p, q \in \mathbb{R}$ také, že pre každé $x \in \mathbb{R}$ platí $f(x) = px + q$. Množina $Y \subseteq \mathbb{R}^2$ sa nazýva **priamka**, ak existujú čísla $a, b \in \mathbb{R}$ ktoré niesú súčastne rovné 0, také, že $Y = \{(x, y) \in \mathbb{R}^2 | ax+by = 0\}$. (Veta: Funkcia $f : \mathbb{R} \to \mathbb{R}$ je afinná, práve vtedy keď je jej grafom priamka. Dokaz si podľa doc. Krupku urobíme s radosťou sami.)*

14.2 Operácie s funkciami

Majme funkcie $f, g : X \subseteq \mathbb{R} \to \mathbb{R}$. Funkciu $(f+g) : X \to \mathbb{R}$, definovanú pre každé $x \in X$ prepisom $(f+g)(x) = f(x) + g(x)$ nazveme **súčtom fumkcií** f a g. **Súčinom týchto funkcií** nazývame funkciu $(f \cdot g) : X \to \mathbb{R}$, definovanú pre každé $x \in X$ predpisom $(f \cdot g)(x) = f(x) \cdot g(x)$

14.3 Príklady špeciálnych funkcií

Absolútnou hodnotou reálneho čísla x nazývame číslo $|x|$, ktoré je rovné x, ak je $x \geq 0$ a rovné $-x$, ak je $x < 0$. Tým dostávame funkciu $[\cdot] : \mathbb{R} \to \mathbb{R}$

Celou časťou reálneho čísla x nazývame najvačšie celé číslo, ktoré je menšie alebo rovné x. Dostávame funkciu $[x] : \mathbb{R} \to \mathbb{R}$

Pre reálne číslo x kladieme $\chi(x) = 0$, ak $x \in \mathbb{I}$, a $\chi(x) = 1$, ak $x \in \mathbb{Q}$. Dostávame **Dirichletovu funkciu** $\chi : \mathbb{R} \to \mathbb{R}$

Obrázek 2: Dirichletova funkcia

15 Limita a spojitosť funkcie

15.1 Opakovanie základov topológie

Z topológie sú tu len pojmy potrebné na definíciu spojitosti funkcie.

Definice 88. ***Topologický priestor:*** *Na množine X je zadaná topólogia, ak je určrný systém τ(Tau) podmnožín X splňujúci podmienky(axiómy topológie):*

1. $\emptyset, X \in \tau$
2. *ak sú $Y, Z \in \tau$, potom $Y \cap Z \in \tau$*
3. *ak je $S \subseteq \tau$ potom $\cup S \in \tau$*

Prvkom τ hovoríme ***otvorené množiny****, množine X hovoríme* ***topologický priestor****. Otvorenej množine obsahujúcej bod $x \in X$ budeme hovoriť* ***okolie bodu*** *x. Množina $Y \subseteq X$ sa nazýva* ***uzavretá****, ak $X \backslash Y$ je otvorená. Topologický priestor X nazveme* ***Hausdorfov****, ak pre každé dva body $x, y \in X, x \neq y$ existuje okolie U bodu x a okolie V bodu y také, že $U \cap V = \emptyset$.* ***Hromadným bodom*** *množiny X nazveme taký bod množiny, v ktorého okolí je nekonečne veľa bodov množiny X.*

15.2 Spojitosť funkcie cez topológiu

Majme X, Y topologické priestory. Povedzme, že zobrazenie $f : X \to Y$ je **spojité v bode** $x \in X$ ak pre každé okolie U bodu $f(x)$ existuje okolie V bodu x také, že $f(V) \subseteq U$. Zobrazenie f je spojité, ak je spojité v každom bode $x \in X$. Zobrazenie f je **nespojité v bode** $x \in X$ ak v ňom nieje spojité (definícia ako ju máme radi). Zobrazenie f je nespojité, ak nieje spojité v každom bode $x \in X$. Bijektívne zobrazenie $f : X \to Y$ nazveme **homeomorfizmus**, ak f a f^{-1} sú spojité zobrazenia.

15.3 Prirodzená topológia na $\mathbb{R}$

Iba nutné pojmy na definíciu spojitosti funkcie v $\mathbb{R}$.

Definice 89. ***Prirodzená topológia na*** $\mathbb{R}$*: Množina $U \subseteq \mathbb{R}$ sa nazýva* ***otvorená****, ak ku každému bodu $x \in U$ existuje otvorený interval I taký, že $x \in I \subseteq U$. Nech $X \subseteq \mathbb{R}$ je množina taká, že pre každé $x, y \in X, x < y$, platí $[x, y] \subseteq X$. Potom je X* ***interval****.*

15.4 Spojité funkcie na $\mathbb{R}$

Důsledek 5. *(Bolzano) Ak je $I \subseteq \mathbb{R}$ interval a $f : I \to \mathbb{R}$ spojitá funkcia, potom je $f(I)$ interval.*

Důsledek 6. *(Darbouxova vlastnosť) Nech $f : [a, b] \to \mathbb{R}$ je spojitá funkcia, c také, že $f(a) < c < f(b)$(poprípade $f(a) > c > f(b)$), potom existuje $x \in (a, b)$ také, že $f(x) = c$.*

Definice 90. ***Vlastnosti spojitých funkcií v*** $\mathbb{R}$*: Funkcia $f : X \subseteq \mathbb{R} \to \mathbb{R}$ sa nazýva* ***spojitá zľava(poprípade zprava)*** *v bode $x_0 \in X$, ak je v tomto bode spojité jej zúženie na množinu $X \cap (-\infty, x_0]$(poprípade $[x_0, \infty)$). Nasleduje pár tvrdení.*

Věta 65. *Funkcia $f : X \subseteq \mathbb{R} \to \mathbb{R}$ je spojitá v bode $x_0 \in X$, práve keď je v tomto bode spojitá zľava aj zprava.*

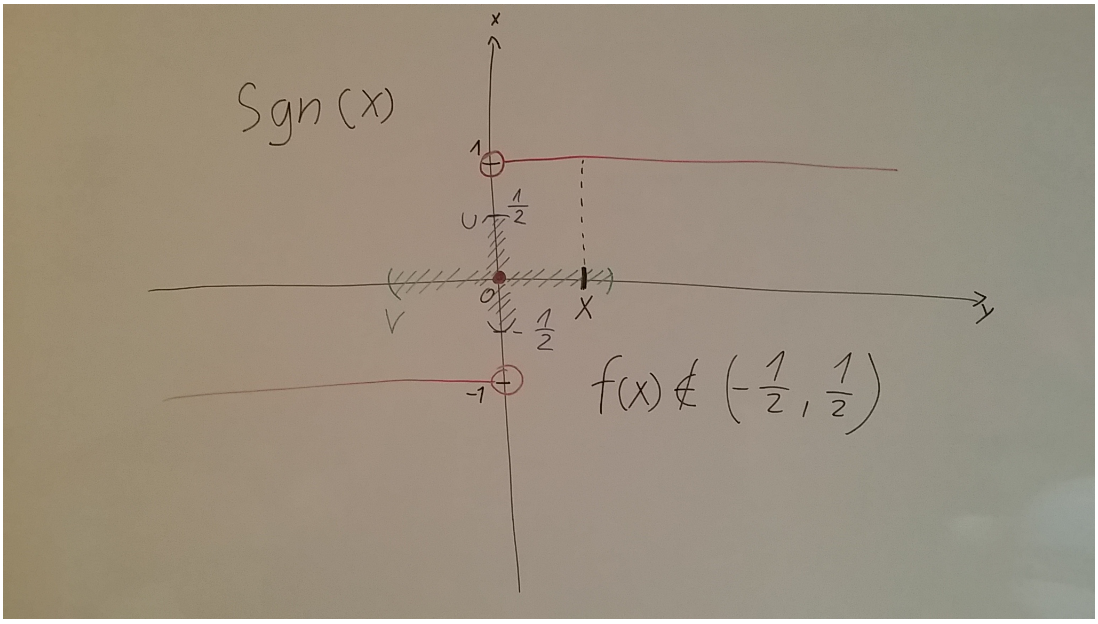
Věta 66. *Funkcia $f : X \subseteq \mathbb{R} \to \mathbb{R}$ je spojitá v bode $x_0 \in X$, práve keď ku každému otvorenému intervalu J so stredom v bode $f(x_0)$ existuje otvorený interval I so stredom v bode x_0 tak, že $f(I \cap X) \subseteq J$.*

Důsledek 7. *($\epsilon - \delta$* ***kritérium spojitosti****) Funkcia $f : X \subseteq \mathbb{R} \to \mathbb{R}$ je spojitá v bode x_0, práve keď ku každému číslu $\epsilon > 0$ existuje číslo $\delta > 0$, že pre každé $x \in X$, ktoré splňuje $|x - x_0| < \delta$, platí $|f(x) - f(x_0)| < \epsilon$*

Příklad 18. *Definujme si funkciu signum(sgn) a dokážeme na nej nespojitosť v bode 0 nasledovne:* $sgn(x) : \mathbb{R} \to \mathbb{R}$ *s predpisom:*

$$sgn(x) = \begin{cases} -1, ak & x < 0 \\ 0, ak & x = 0 \\ 1, ak & x > 0 \end{cases}$$

Musíme nájsť okolie U *bodu* $sgn(0) = 0$ *tak že pre každé okolie* V *bodu 0 neplatí* $f(V) \subseteq U$. *Položíme* $U = (-\frac{1}{2}, \frac{1}{2})$ *a zvolíme ľubovolné okolie* V *bodu 0 a ukážme, že* V *obsahuje bod* x *taký, že* $f(x) \notin (-\frac{1}{2}, \frac{1}{2})$. *Pretože* V *je otvorená množina, obsahuje interval* I *so stredom v 0. Zvolme* $x \in I, x > 0$. *Platí* $sgn(x) = 1 \notin (-\frac{1}{2}, \frac{1}{2})$.



Obrázek 3: Príklad nespojitosti sgn v bode 0

15.5 Limita funkcie

Majme topologický priestor X, Hausdorfov topologický priestor Y, zobrazenie $f : A \subseteq X \to Y$ a bod x_0 ktorý je hromadným bodom množiny A. **Limitou zobrazenia** f v bode x_0 nazývame prvok $y_0 \in Y$ taký, že zobrazenie:

$$f'(x) = \begin{cases} f(x), ak & x \neq x_0 \\ y_0, ak & x = x_0 \end{cases}$$

je spojité v bode x_0. Ak je y_0 limitou zobrazenia f v bode x_0, píšeme $y_0 = \lim_{x \to x_0} f(x)$. Dalo by sa povedať že limita je taký prvok priestoru Y, ktorý je treba funkcii f v bode x_0 dodefinovať(predefinovať), aby bola v x_0 spojitá.

Důsledek 8. *($\epsilon - \delta$ **kritérium limity po prvé**) Funkcia $f : X \subseteq \mathbb{R} \to \mathbb{R}$ má v hromadnom bode x_0 množiny X limitu y_0, práve vtedy keď ku každému číslu $\epsilon > 0$ existuje číslo $\delta > 0$ také, že pre každé $x \in X, x \neq x_0$, ktoré splňuje $|x - x_0| < \delta$, platí $|f(x) - y_0| < \epsilon$.*

Věta 67. *Každé zobrazenie má v dannom bode najviac jednu limitu. (Dokaz sporom, predpokladáme že funkcia má v nejakom bode 2 limity a na základe definície prídeme ku sporu).*

Teraz si zavedieme **rozšírenú množinu reálnych čísel**. Nazývame ňou množinu $\mathbb{R}' = R \cup \{-\infty, \infty\}$, kde $-\infty$ a ∞ sú ľubovolné dva rozličné prvky, takzvané **nevlastné body**, ktoré niesú reálne čísla.

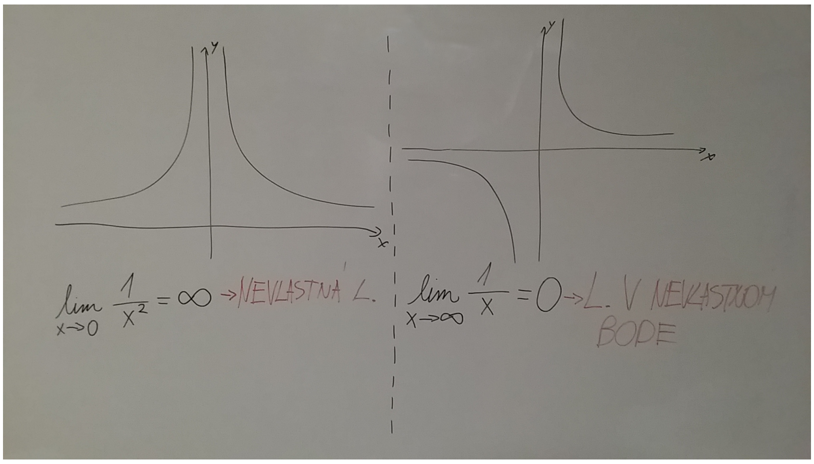
Limity funkcií reálnej premennej vždy uvažujeme na množine $\mathbb{R}'$. V limite $\lim_{x \to x_0} f(x)$ teda može byť $x_0 = -\infty$ alebo $x_0 = \infty$(ak sú $-\infty$ alebo ∞ hromadným bodom definičného oboru funkcie f) a može nám tiež vyjsť že $\lim_{x \to x_0} f(x) = -\infty$ alebo $\lim_{x \to x_0} f(x) = \infty$. V prvom prípade hovoríme o **limite v nevlastnom bode**, v druhom o **nevlastnej limite**.

Důsledek 9. *($\epsilon - \delta$ **kritérium limity po druhé**) Nech je $X \subseteq \mathbb{R}$ taká, že ∞ je jej hromadný bod, $f : X \subseteq \mathbb{R} \to \mathbb{R}$ funkcia. Prvok $y_0 \in \mathbb{R}'$ je limitou f v bode ∞, práve vtedy keď ku každému číslu $\epsilon > 0$ existuje číslo $\delta > 0$ také, že pre každé $x \in X$, ktoré splňuje $x > \delta$, platí $|f(x) - y_0| < \epsilon$, ak je $y_0 \in \mathbb{R}$; poprípade $f(x) > \epsilon$, ak je $y_0 = \infty$; poprípade $f(x) < -\epsilon$, ak je $y_0 = -\infty$. Podbne pre limitu v bode $-\infty$.*

Majme limity:

1. $\lim_{x \to x_0} f(x)$ pre $x < x_0$
2. $\lim_{x \to x_0} f(x)$ pre $x > x_0$

Limitu 1 nazývame **limitou zľava** (značíme: $\lim_{x \to x_0^-} f(x)$) a limitu 2 nazývame **limitou zprava** (značíme: $\lim_{x \to x_0^+} f(x)$).



Obrázek 4: Príklady limít

16 Diferenciálny počet v $\mathbb{R}$

Táto sekcia obsahuje vysvetlenie pojmu **derivácia funkcie**, jej **geometrický význam** a základné **vety diferenciálneho počtu** v $\mathbb{R}$. Ďalej obsahuje využitie derviácií pri hľadaní extrémov funkcie, odahade hodnoty funkcie ... (**Vyšetrovanie priebehu funkcie**).

16.1 Derivácia a jej geometrický význam

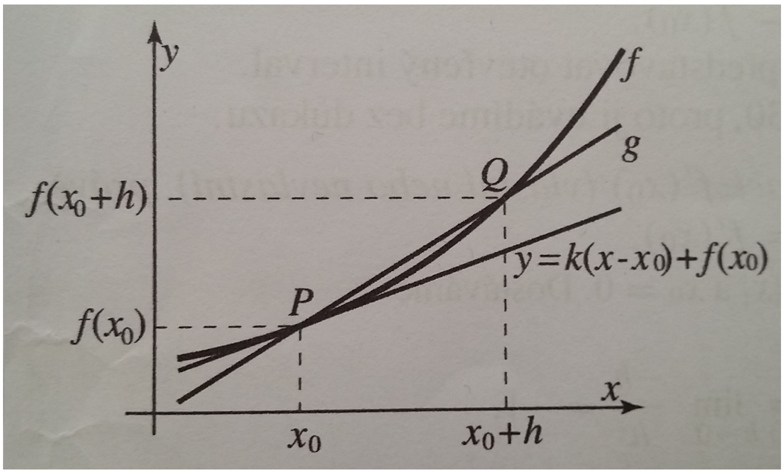
Postupnými úvahami sa pokúsime definovať pojem **tečny ku grafu funkcie**. Uvažujme funkciu $f : I \subseteq \mathbb{R} \to \mathbb{R}$ definovanú na otvorenom intervale I. Zvolme si ľubovolný bod $x_0 \in I$ a kladné celé číslo $h \in \mathbb{R}$ tak, aby $x_0 + h \in I$. Označme si $P = (x_0, f(x_0))$ a $Q = (x_0 + h, f(x_0 + h))$ ako 2 body na grafe funkcie f. Na základe vety ktorá je uvedená v definícii **??** vieme, že grafom afinnej funkcie je **priamka**, pozri obrázok **??**. Predstavme si priamku, ktorá prechádza nami definovanými bodmi P a Q. Táto priamka je grafom afinnej funkcie $g : \mathbb{R} \to \mathbb{R}$ s predpisom:

$$g(x) = \tfrac{f(x_0+h)-f(x_0)}{h}(x - x_0) + f(x_0)$$

Smernica tejto priamky je $g(x) = \frac{f(x_0+h)-f(x_0)}{h}$. Limitu smerníc takýchto priamok (ak existuje), nazývame **derivácia funkcie** f v bode x_0 a značíme ju $f'(x_0)$. Formálne:

$$f'(x_0) = \lim_{h\to 0} \frac{f(x_0 + h) - f(x_0)}{h} \quad alebo \quad f'(x_0) = \lim_{x\to x_0} \frac{f(x) - f(x_0)}{x - x_0}$$

Ak nahradíme limitu limitou zľava(zprava) dostaneme **deriváciu zľava(zprava)** funkcie f v bode x_0. Značíme ju $f'_-(x_0)$ $(f'_+(x_0))$. Ak je limita nevlastná, hovoríme že f má v bode x_0 **nevlastnú deriváciu** (obdobne pre vlastnú deriváciu).



Obrázek 5: Grafické znázornenie úvah o derivácii

Označenie derivácie $f'(x_0)$, pripomína hodnotu nejakej funkcie (zámerne). Majme funkciu $f : J \subseteq \mathbb{R} \to \mathbb{R}$. Ak je $X \subseteq J$ je množina obsahujúca všetky body, v ktorých má f vlastnú deriváciu. Potom funkciu $f' : X \to \mathbb{R}$, ktorá bodu X priradí deriváciu funkcie f v tomto bode, nazveme **derivácia funkcie**.

Příklad 19. *Ak je f konštantná funkcia, potom jej derivácia $f' = 0$. Konkrétne $f(x) = c$ je konštantná funkcia. Stačí dosadiť...*

$$f'(x_0) = \lim_{h\to 0} \frac{f(x_0+h) - f(x_0)}{h} = \lim_{h\to 0} \frac{c-c}{h} = \lim_{h\to 0} \frac{0}{h} = 0$$

... a preto je derivácia konštanty rovná 0.

Definice 91. *Teraz už máme dostatočný aparát na zadefinovanie pojmu tečna. Priamka prechádzajúca bodom $(x_0, f(x_0))$ majúca smernicu $f'(x_0)$ je **tečna ku grafu funkcie** f v bode $(x_0, f(x_0))$.*

Věta 68. *Funkcia $f : J \to \mathbb{R}$ má v bode $x_0 \in J$ deriváciu $f'(x_0)$ práve vtedy, keď existujú $f'_-(x_0)$, $f'_+(x_0)$ a platí $f'_-(x_0) = f'_+(x_0) = f'(x_0)$. (Antidebilne povedané, funkcia má v bode deriváciu, ak má v danom bode deriváciu zľava aj zprava, ktoré sa rovnajú derivácii funkcie v danom bode) Príklad nasleduje ...*

Příklad 20. *Za funkciu si zvolme absolútnu hodnotu a ideme hľadať deriváciu v bode 0 takže: $f(x) = |x|$ a $x_0 = 0$. (Fúfam že každý vie ako vyzerá funkcia absolútnej hodnoty ... kto nie, tak gooooogle!) Dostávame:*

$$f'_-(0) = \lim_{h\to 0_-} \frac{f(x_0+h) - f(x_0)}{h} = \lim_{h\to 0_-} \frac{|h|}{h} = \lim_{h\to 0_-} \frac{-h}{h} = -1$$

$$f'_+(0) = \lim_{h\to 0_+} \frac{f(x_0+h) - f(x_0)}{h} = \lim_{h\to 0_+} \frac{|h|}{h} = \lim_{h\to 0_+} \frac{h}{h} = 1$$

*Ako vidíme tak absolútna hodnota ma deriváciu zľava v bode 0 rovnú -1 a zprava rovnú 1. Preto na základe predchádzajúcej vety **nemá** deriváciu v bode 0.*

Věta 69. *Majme funkcie $f, g : J \subseteq \mathbb{R} \to \mathbb{R}$ majúce deriváciu v $x_0 \in J$ a $c \in \mathbb{R}$. Potom:*

1. $(f+g)'(x_0) = f'(x_0) + g'(x_0)$
2. $(fg)'(x_0) = f'(x_0)g(x_0) + f(x_0)g'(x_0)$
3. $(cf)'(x_0) = cf'(x_0)$

Věta 70. ***(Derivácia zloženej funkcie)*** *Nech $f : J \to \mathbb{R}, g : I \to J, x_0 \in I$ a nech existujú vlastné derivácie $g'(x_0)$ a $f'(g(x_0))$. Potom existuje vlastná derivácia $(f \circ g)'(x_0)$ a platí $(f \circ g)'(x_0) = f'(g(x_0)) \cdot g'(x_0)$.*

Důsledek 10. *Majme $f, g : J \subseteq \mathbb{R} \to \mathbb{R}$ funkcie majúce driváciu v $x_0 \in J$ a $g(x_0) \neq 0$. Potom:*

$$\left(\frac{f}{g}\right)'(x_0) = \frac{f'(x_0)g(x_0) - f(x_0)g'(x_0)}{g^2(x_0)}$$

.

Věta 71. ***(Derivácia inverznej funkcie)*** *Nech $f : J \to I \subseteq \mathbb{R}$ je spojitá rastúca alebo klesajúca, $x_0 \in J, f^{-1} : I \to J$ je inverzia f. Ak existuje vlastná $f'(x_0) \neq 0$, potom existuje vlastná $(f^{-1})'(f(x_0))$ a platí:*

$$(f^{-1})'(f(x_0)) = \frac{1}{f'(x_0)}$$

.

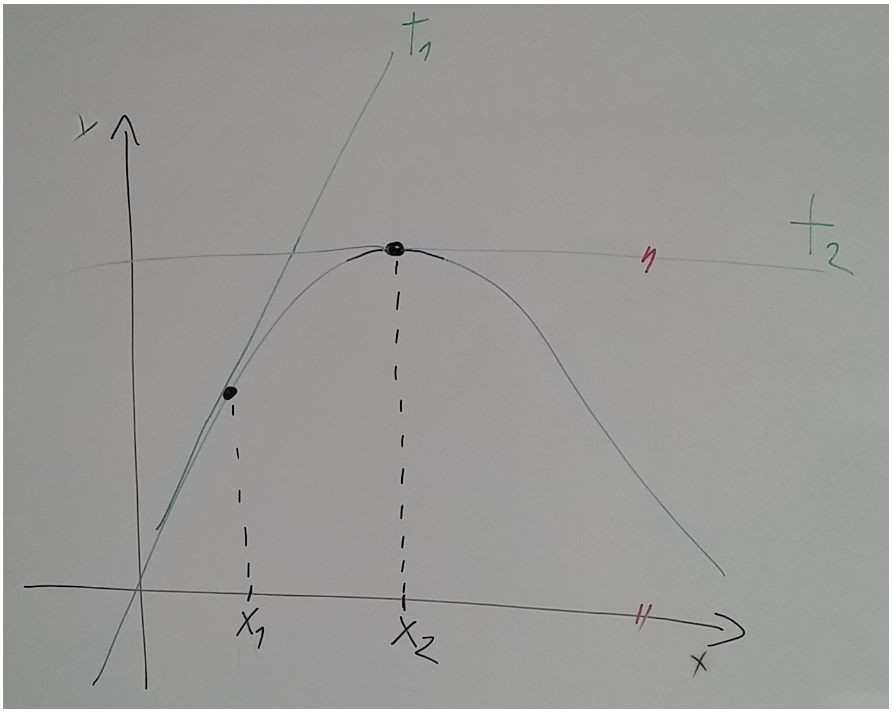
Definice 92. *Uvažujme funkciu $f : J \to \mathbb{R}$ a $x_0 \in J$. Lineárne homogénne zobrazenie $A : \mathbb{R} \to \mathbb{R}$ nazývame **diferenciál funkcie** f v bode x_0, ak*

$$\lim_{h \to 0} \frac{f(x_0 + h) - f(x_0) - A(h)}{h} = 0$$

Diferencál funkcie f v bode x_0 označujeme $df(x_0)$.

16.2 Vyšetrovanie priebehu funkcie

Pomocou derivácií možeme vyšetriť priebeh funkcie. Definovali sme tečnu ku grafu funkcie. Strmosť tečny nám určuje, ako moc sa hodnoty menia. Derivácia v bode extrému je rovná 0, v tom istom bode je tečna rovnobežná s osou x (toto je jeden z ukazovatelov že sa nachádzame v extréme). Pozri obrázok **??**.



Obrázek 6: Tečna ku grafu funkcie v bode x_1 a x_2, v bode x_1 vidíme že tečna je strmá(hodnoty sa menia výrazne), v bode x_2 vidíme že tečna je rovnobežná s osou x, takže sa nachádzame v extréme (derivácia by v x_2 bola rovná 0)

16.2.1 Extrémy

Nech $f : X \subseteq \mathbb{R} \to \mathbb{R}$. Povedzme že funkcia f je **rastúca (respektívne klesajúca, nerastúca, neklesajúca)** v bode $x_0 \in X$, ak existuje okolie $(x_0 - \delta, x_0 + \delta)$ bodu x_0 také, že $f((x_0 - \delta, x_0) \cap X) < f(x_0) < f((x_0, x_0 + \delta) \cap X)$ (respektívne $f((x_0 - \delta, x_0) \cap X) > f(x_0) > f((x_0, x_0 + \delta) \cap X)$, $f((x_0 - \delta, x_0) \cap X) \geq f(x_0) \geq f((x_0, x_0 + \delta) \cap X)$, $f((x_0 - \delta, x_0) \cap X) \leq f(x_0) \leq f((x_0, x_0 + \delta) \cap X)$).

Povedzme, že funkcia f nabýva v x_0 **lokálne maxima (minima)** ak existuje okolie U bodu x_0 také, že $f|_{U \cap X}$ (tento zápis znamená zúženie funkcie f na okolie U) nabýva v x_0 maxima (minima).

Věta 72. *Majme $f : J \to \mathbb{R}$, potom:*

1. *Ak je $f'(x_0) > 0$ (poprípade ak je $f'(x_0) = \infty$), potom je f v bode x_0 **rastúca**.*
2. *Ak je $f'(x_0) < 0$ (poprípade ak je $f'(x_0) = -\infty$), potom je f v bode x_0 **klesajúca**.*

Důsledek 11. *Ak je $x_0 \in J$ bodom extrému funkcie $f : J \to \mathbb{R}$ a existuje $f'(x_0)$, potom $f'(x_0) = 0$ (ako sme tvrdili v úvode).*

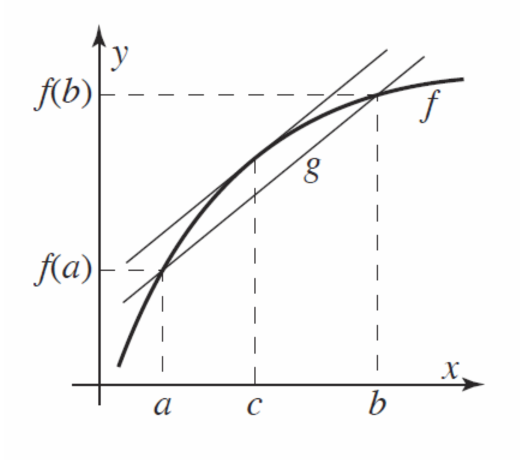
16.3 Základné vety diferenciálneho počtu

Věta 73. ***(Rolleova)*** *Majme $f : [a, b] \to \mathbb{R}$ spojitá funkcia majúca deriváciu (vlastnú alebo nevlastnú) v každom vnútornom bode $[a, b]$. Ak $f(a) = f(b)$, potom existuje $c \in (a, b)$ také, že$f'(c) = 0$.*

D: Ak je f konštantná, potom c je ľubovolný bod intervalu (a, b). Uvažujme 2 rozne prípady. **Prvý:** Ak existuje bod v (a, b), v ktorom funkcia f nabýva hodnoty vačšej než $f(a)$, potom vezmeme za c bod v ktorom funkcia f nabýva na $[a, b]$ svojho maxima. Taký bod existovať bude (na základe vety 4.9 ... neviem kde ju doc. Krupka dal ale ja som ju nenašiel) a bude rozny od a, b, pretože funkcia f nabýva hodnoty vaščej než $f(a)$ v nejakom bode (a, b). Ostáva ukázať že $f'(c) = 0$. To ale plynie z dosledku číslo **??**.

Věta 74. ***(Lagrangeova veta o strednej hodnote)*** *Majme $f : [a, b] \to \mathbb{R}$ spojitá funkcia majúca deriváciu (vlastnú alebo nevlastnú) v každom vnútornom bode $[a, b]$. Potom existuje $c \in (a, b)$ také, že $f'(c) = \frac{f(b)-f(a)}{b-a}$. (Používa sa k odhadu, ako rýchlo funkcia rastie)*

D: Vetu dokážeme pomocou Rolleovej vety tak, že ju aplikujeme na rozdiel funkcie f a afinnej funkcie g prechádzajúcej bodmi $(a, f(a))a(b, f(b))$. Uvažujme teda funkciu $F : [a, b] \to \mathbb{R}$ s predpisom $F(x) = f(x) - \frac{f(b)-f(a)}{b-a}(x - a) - f(a)$. Táto funkcia spĺňa všetky predpoklady Rolleovej vety. Preto existuje $c \in (a, b)$ také, že $F'(c) = 0$. Pretože $F(x) = f(x) - \frac{f(b)-f(a)}{b-a}$ pre $x = c$ dostávame $F(c) = f(c) - \frac{f(b)-f(a)}{b-a} = 0$.



Obrázek 7: Lagrangeova veta

Důsledek 12. *Majme $f, g : [a, b] \to \mathbb{R}$ spojité funkcie. Ak platí že $f' = g'$, potom existuje $c \in \mathbb{R}$ také, že $f = g + c$. (Inak povedané, funkcie s rovnakou deriváciou sa na intervale líšia iba o konštantu.)*

Věta 75. ***(Couchova veta o strednej hodnote)*** *Majme $f, g : [a, b] \to \mathbb{R}$ spojité funkcie a nech existuje v každom bode $x \in (a, b)$ derivácia $f'(x)$ (vlastná alebo nevlastná) a vlastná derivácia $g'(x) \neq 0$. Potom exituje $x \in (a, b)$ také, že $\frac{f'(c)}{g'(c)} = \frac{f(b)-f(a)}{g(b)-g(a)}$.*

D: Vetu dokážeme obdobným sposobom ako tú predchádzajúcu. Najprv, pretože $g'(x) \neq 0$ na (a, b), podľa Lagrangeovej vety máme, že $g(a) \neq g(b)$. Definujeme funkciu $F : [a, b] \to \mathbb{R}$ s predpisom $F(x) = (f(x) - f(a))(g(b) - g(a)) - (g(x) - g(a))(f(b) - f(a))$. Táto funkcia spĺňa podmienky Rolleovej vety a preto existuje $c \in (a, b)$ také, že $F'(c) = 0$, teda $F'(c) = f'(x)(g(b) - g(a)) - g'(c)(f(b) - f(a)) = 0$.

Příklad 21. *Uvažujme funkciu $f = ln$ na intervale $[a, b] = [5, 10]$. Podľa vety o strednej hodnote existuje $c \in (5, 10)$ také, že $(10 - 5)ln'(c) = 5/c = ln10 - ln5 = ln2$. Pretože $5 < c < 10$, znamená to, že $\frac{5}{10} < 5/c = ln2 < \frac{5}{5}$. Dostávame prvý odhad funkcie ln v bode 2: $\frac{1}{2} < ln2 < 1$. Pokračujme ďalej, z nerovnice $1 < 2ln2$ a z monotonie funkcie exp dostaneme $e = exp(1) < exp(2ln2) = 4$. Číslo e je teda menšie ako 4.*

17 Postupnosti a ich limity

17.1 Postupnosti

Ako **postupnosť** sa označuje usporiadný súbor matematických objektovy očíslovaných spravidla prirodzenými číslam. Postupnosť je možné definovať ako zobrazenie z množiny prirodzených do ľubovolnej množiny. Členmi postupnosť možu byť čísla (číselné postupnosti), funkcie (funkčné postupnosti), množiny ... číslená postupnosť priraďuje každému $n \in \mathbb{N}$ číslo a_n (v prípade funkčnej postupnosti to je $f_n(x)$). Postupnosť obvykle značíme

$(a_n)_{n=1}^{\infty}$. Postupnosť može byť vyjedrená aj výrazom na výpočet n-tého člena postupnosti a_n (napr. $a_n = \frac{n}{n+1}$ odpovedá postupnosti : $a_1 = \frac{1}{2}$, $a_2 = \frac{2}{3}$, $a_3 = \frac{3}{4} \ldots$). Postupnosť možeme zadať aj rekurentne (ďaľší člen postupnosti sa vypočíta pomocou predchádzajúcich členov). Rekurentne je zadaná napr. **Fibonacciho postupnosť** a to nasledovne: $a_1 = 1$, $a_2 = 1$, $a_{n+2} = a_n + a_{n+1}$.

17.2 Vlastnosti postupností

Kedže postupnosť je možné zadefinovať ako zobrazenie, tak bude mať rovnaké vlastnosti ako zobrazenie. Postupnosť je:

1. **rastúca**, ak pre všetky i platí, $a_i > a_{i-1}$
2. **nerastúca**, ak pre všetky i platí, $a_i \leq a_{i-1}$
3. **klesajúca**, ak pre všetky i platí, $a_i < a_{i-1}$
4. **neklesajúca**, ak pre všetky i platí, $a_i \geq a_{i-1}$
5. **zhora ohraničená** na množine A, ak existuje taká $L \subseteq A$, že pre všetky i platí $a_i \leq L$ (tým sú myslené prvky z L)
6. **zdola ohraničená** na množine A, ak existuje taká $L \subseteq A$, že pre všetky i platí $a_i \geq L$

Ak je postupnosť nerastúca alebo neklesajúca, hovoríme, že je **monotónna**. Ak je rastúca alebo klesajúca hovorýme že je **rýdzo monotónna**. Ak je postupnosť zároveň zhora aj zdola ohraničená, hovoríme že je **ohraničená**. Ak sa v ľubovolne malom ϵ - okolí bodu b na intervale $(b - \epsilon, b + \epsilon)$ nachádza nekonečne veľa bodov postupnosti (a_n), potom bod b nazývame **hromadným bodom postupnosti** (a_n).

17.3 Príklady postupností

17.3.1 Aritmetická postupnosť

Je druh postupnosti kde je stály rozdiel medzi susednými členmi postupnosti. Tento rozdiel sa volá diferencia a značí sa **d**. Ďalej su to 3-prdele vzorcov na počítanie s aritmetickou postupnosťou (tie ale uvádzať nebudeme).

Příklad 22. *Majme aritmetickú postupnosť zadanú prvým členom a diferenciou:* $a_1 = 5$, $d = 5$. *Vypočítajte* a_2, a_3. *(Je to hard … berte kalkulačky súdruhovia).*

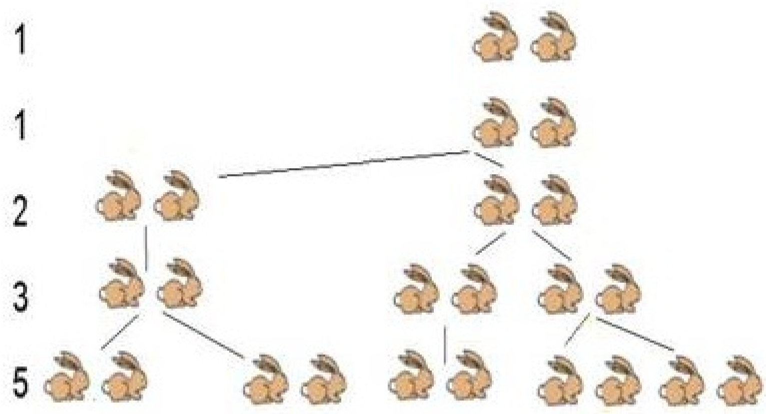
17.3.2 Geometrická postupnosť

Druh postupnosti kde je každý člen (okrem prvého) stálym násobkom predchádzjúceho člena. Tento násobok sa volá kvocient a značí sa **q**. Je možné ju chápať ako zúženie exponenciálnej funkcie na obor prirodzených čísel. Obsahuje podobné množstvo vzorcov ako aritmetická ...

Příklad 23. *Majme geometrickú postupnosť zadanú prvým členom a kvocientom:* $a_1 = 2$, $d = 2$. *Vypočítajte* a_2, a_3, a_4. *(*$a_2 = 4$, $a_3 = 8$, $a_4 = 16$*).*

17.3.3 Fibonacciho postupnosť

Všetkým známa.



Obrázek 8: Fibonacciho postupnosť ilustratívne

17.4 Limita postupnosti

Definice 93. *Postupnosť* $(a_n)_{n=1}^{\infty}$ *má* ***limitu*** L, *ak sa jej hodnotami može k* L *priblížiť. Teda pre každé kladné číslo* ϵ *platí, že existuje nejaký člen postupnosti od ktorej sú už jej hodnoty od* L *vzdialené menej než* ϵ. *Formálne zapísané, ak pre pre každéb* $\epsilon > 0$ *existuje* n_0 *také, že pre každé* $n > n_0$ *platí, že* $|a_n - L| < \epsilon$.

Ak k ľubovolnému $\epsilon > 0$ existuje n_0 také, že pre každé $n > n_0$ platí, že $|a_n - L| < \epsilon$ hovoríme, že postupnosť (a_n) má **vlastnú a konečnú limitu L**. Inak povedané postupnosť **konverguje** k L. To že postupnosť konverguje k L zapisujeme:

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

. Ak má postupnosť vlastnú limitu, tak postupnosť označujeme ako **konvergentnú**. V opačnom prípade hovoríme o **divergentnej** postupnosti. O postupnosti hovríme že je:

1. **konvergentná**, ak má vlastnú limitu
2. **divergentná**, ak má nevlastnú limitu $+\infty$ alebo $-\infty$, je oscilujúca alebo nemá limitu
3. **oscilujúca**, ak nemá vlastnú limitu ani nevlastnú limitu

18 Číselné rady, konvergencia a súčty, kritéria konvergencie

Majme postupnosť (x_n) reálnych čísel. **Nekonečným radom** určeným postupnosťou (x_n) rozumieme symbol $\sum x_n$. Postupnosť (s_n), ktorej členy su danné predpisom $s_n = x_1 + \cdots + x_n$ (kde $n = 1, 2, 3\ldots$), nazývame **postupnosťou čiastočných súčtov radu** $\sum x_n$. Ak postupnosť čiastočných súčtov radu $\sum x_n$ konverguje, hovoríme o **konvergentnom rade** a číslo s_n nazývame jeho **súčtom**. V opačnom prípade hovoríme o **divergentnom rade**. Súčet nekonečného radu $\sum x_n$ označujeme rovnako $\sum x_n$. Tvrdenie $\sum x_n = s$ znamená: Rad $\sum x_n$ konverguje a jeho súčtom je s. Okrem tohoto zápisu sa používa aj zápis $\sum_{n=1}^{\infty} x_n$. Zápis $\sum_{n=k}^{\infty} x_n$ znamená $\sum_{n=1}^{\infty} x_n + k - 1$. V takom prípade budeme používať nasledujúce značenie pre postupnosť čiastočných súčtov radu: $s_n = x_k + x_{k+1} + \cdots + x_{k+n-1}$.

18.1 Príklady radov

Nech $q \in \mathbb{R}$. Rad $\sum q^{n-1}$ sa nazýva **geometrický rad** s kvocientom q. Ak je $q \neq 1$, potom pre n-tý člen s_n jeho postupnosti čiastočných súčtov platí:

$$s_n = 1 + q + q^2 + q^3 + \cdots + q^{n-1} = \frac{1-q}{1-q}(1 + q + q^2 + q^3 + \cdots + q^{n-1}) = \frac{1-q^n}{1-q}$$

Ak je $q = 1$, platí $s_n = n$

Vidíme teda, že $lim\ s_n$ existuje, práve vtedy keď $|q| < 1$, a je rovná $1/(1-q)$. Uvedený rad teda konverguje práve vtedy, keď $|q| < 1$, a v tom prípade platí $\sum q^{n-1} = 1/(1-q)$.

Geometrický rad s $q = -1$ sa nazýva **Grandiho rad**. Rad $\sum 1/n$ sa nazýva **harmonický rad**. Pre postupnosť (s_n) jeho čiastočných súčtov platí:

$$s_1 = 1$$

$$s_2 = 1 + \frac{1}{2}$$

$$s_3 = 1 + \frac{1}{2} + \frac{1}{3}$$

$$s_4 = s_2 + \frac{1}{3} + \frac{1}{4} > s_2 + \frac{1}{4} + \frac{1}{4} = s_{2+\frac{1}{2}}$$

$$\cdots$$

$$s_{2^{n+1}} = s_{2^n} + \frac{1}{2}$$

Z toho je možné vysledovať, že harmonický rad diveruje, hoci spĺňa nutnú podmienku konvergencie (uvedená nižšie).

Věta 76. ***(Cauchyho-Bolzanovo kritérium konvergencie)*** *Rad $\sum x_n$ konverguje, práve vtedy keď ku každému $\epsilon > 0$ existuje číslo $n_0 \in \mathbb{N}$ také, že pre každé $n_1, n_2 > n_0$; $n_2 \geq n_1$, platí: $|x_{n_1} + \cdots + x_{n_2}| < \epsilon$.*

Důsledek 13. ***(Nutná podmienka konvergencie radu)*** *Ak rad $\sum x_n$ konverguje, potom platí že: lim $x_n = 0$ (Poznámka: zamyslite sa nad geometrickým radom)*

Věta 77. *Majme 2 postupnosti reálnych čísel (x_n), (y_n) a číslo c. Ak rady $\sum x_n$ a $\sum y_n$ konvergujú, potom konvergujú aj rady $\sum(x_n + y_n)$ a $\sum cx_n$ a platí*

$$\sum(x_n + y_n) = \sum x_n + \sum y_n$$

$$\sum cx_n = c \sum x_n$$

Věta 78. *Ešte sa tu nachádzajú asi 2 (podľa mňa) menej podstatné vety o konvergencii radov. Ide v nich asi o to že ak sa 2 rady rovnajú a prvý z nich konverguje, tak konverguje aj ten druhý atď . . .*

18.2 Rady s nezápornými členmi

Nech $(x_n) \geq 0$. Postupnosť čiastočných súčtov radu $\sum x_n$ je neklesajúca. Konverguje práve vtedy, keď je ohraničená a práve vtedy, keď nejaká jej podpostupnosť. Inak diverguje k $+\infty$.

Věta 79. ***(Zrovnávacie kritérium)*** *Nech $\sum x_n$ a $\sum y_n$ sú rady s nezápornými členmi a nech existuje číslo n_0 také, že pre každé $n \geq n_0$ platí $x_n \leq y_n$. Potom s konvergencie radu $\sum y_n$ plynie konvergencia radu $\sum x_n$.*

Věta 80. *Zase sú tu aj iné vety ... ale myslím že nám chýbať nebudú.*

18.3 Alternujúce a absolutne konvergentné rady

Povieme, že rada $\sum x_n$ je **alternujúca**, ak pre každý člen x_n má člen x_{n+1} opačné znamienko. Rad x_n, pre ktorý rad $\sum |x_n|$ konverguje, sa nazýva **absolutne konvergentný**. Z vety ktorá nasleduje plynie, že absolútne konvergentná rada je konvergentná. Konvergentná rada ktorá nieje absolútne konvergentná, sa nazýva **neabsolútne konvergentná** (relatívne konvergentná).

Věta 81. *Ak konverguje rad $\sum |x_n|$, konverguje aj rad $\sum x_n$ a platí $|\sum x_n| \leq \sum |x_n|$*
D: *(Iba naznačenie) Pre ľubovolné čísla $n_1 \leq n_2$ platí*

$$|x_{n_1} + \cdots + x_{n_2}| \leq |x_{n_1}| + \cdots + |x_{n_2}|$$

.

19 Neurčitý a určitý Riemannov integrál

V deriváciách sme hľadali zo zadanej funkcie jej deriváciu. Pomocou integrálov sa rieši opačný problém, takže zo zadanej derivácie určiť povodnú funkciu.

19.1 Neurčitý integrál

Predpokladajme, že máme danú funkciu f, o ktorej vieme, že vznikla derivovaním nejakej funkcie F na intervale (a,b), teda, že $f(x) = F'(x)$ pre každé $x \in (a,b)$. Otázka je: Aká bola povodná funkcia F? Funkcia F, ktorú hľadáme, sa preto niekedy nazýva **primitívna funkcia**.

Příklad 24. *Majme funckiu $f(x) = 8x^3$ pre $x \in (-\infty, \infty)$ Úlohou je nájsť funkciu F. ($F = 2x^4$ pretože pre každé $x \in (-\infty, \infty)$ platí, že $F'(x) = 2 \cdot 4x^3$).*

Definice 94. *Nech (a,b) je ľubovolný otvorený interval. Funkcia F sa nazýva primitívnou funkciou k funkcii f na intervale (a,b) ak pre každé $x \in (a,b)$ platí*

$$f(x) = F'(x)$$

Věta 82. *Nech funkcia F je primitívnou funkciou k funkcii f na intervale (a,b). Funkcia G je primitívnou funkciou k funkcii f na intervale (a,b) práve vtedy, ak existuje reálne číslo c také, že pre každé $x \in (a,b)$ platí*

$$G(x) = F(x) + c$$

To znamená, že primitívne funkcie k rovnakej funkcii f sa môžu líšiť len konštantou. Ak hľadáme ktorúkoľvek z primitívnych funkcií, tak hovoríme, že hľadáme **neurčitý integrál z funkcie f** a značíme

$$\int f(x)dx$$

Na základe predchádzajúcej vety možeme neurčitý integrál písať aj v tvare

$$\int f(x)dx = F(x) + c$$

kde F je jedna z možných primitívnych funkcií.

19.1.1 Substitučná metóda (iba informatívne)

Prvá veta o substitučnej metóde umožňuje hľadať neurčité integrály funkcií, ktoré sú súčinom nejakej zloženej funkcie a derivácie jej vnútornej zložky, napr. integrály typu

$$\int (\varphi(x)) \cdot \varphi'(x)dx$$

Příklad 25. *Vypočítajte integrál:*

$$\int \frac{cos(ln\ x)}{x}dx$$

Funkcia $cos(ln\ x)$ je zložená funkcia, pričom $ln\ x$ je vnútorná zložka. Použijeme substitúciu

$$t = ln\ x \ \Rightarrow\ dt = \frac{1}{x}dx$$

Pos substitúcii dostaneme

$$\int \frac{cos(ln\ x)}{x} dx = \int cos\ t\ dt = sin\ t + c = sin\ (ln\ x) + c$$

19.1.2 Metóda Per-Partes (iba informatívne)

Aj keď vo všeobecnosti nejaké pravidlo pre integrovanie súčinu dvoch funkcií nemáme, v niektorých prípadoch nám môže pomôcť nasledujúca veta, známa ako veta o metóde "per-partes"(krátko MPP).

Věta 83. *Nech funkcie u a v majú na intervale (a, b) spojité derivácie u' resp. v'. Potom na intervale (a, b) platí*

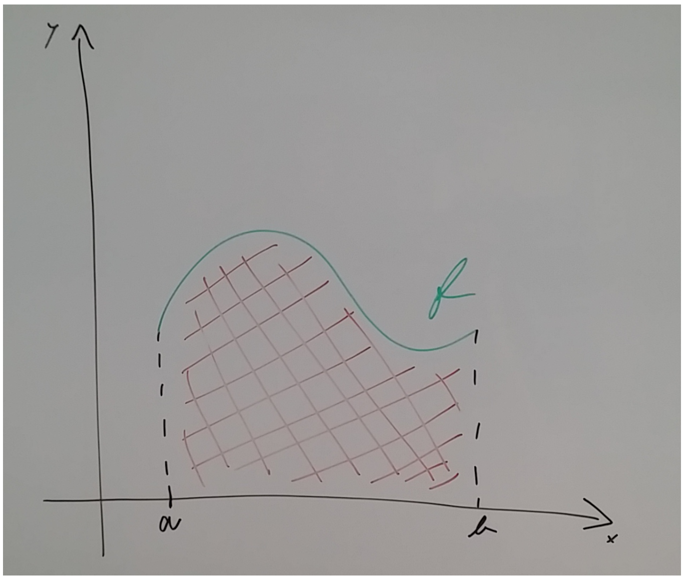
$$\int u(x) \cdot v'(x)dx = u(x) \cdot v(x) - \int u'(x) \cdot v(x)dx$$

Na pravej strane sme dotsali jednoduhší integrál. Niekedy vieme výsledok z neho určiť priamo, inokedy treba použiť vhodný postup na jeho určenie.

19.2 Určitý Riemannov integrál

Sú 2 sposoby ako zadefinovať určitý Riemannov integrál. Jeden z nich je použitím (Cauchyových) integrálnych súčtov (Ten sme si v MATA nedefinovali) a druhý je použitím **horných a dolných integrálov**. Nižšie je popísaný druhý sposob.

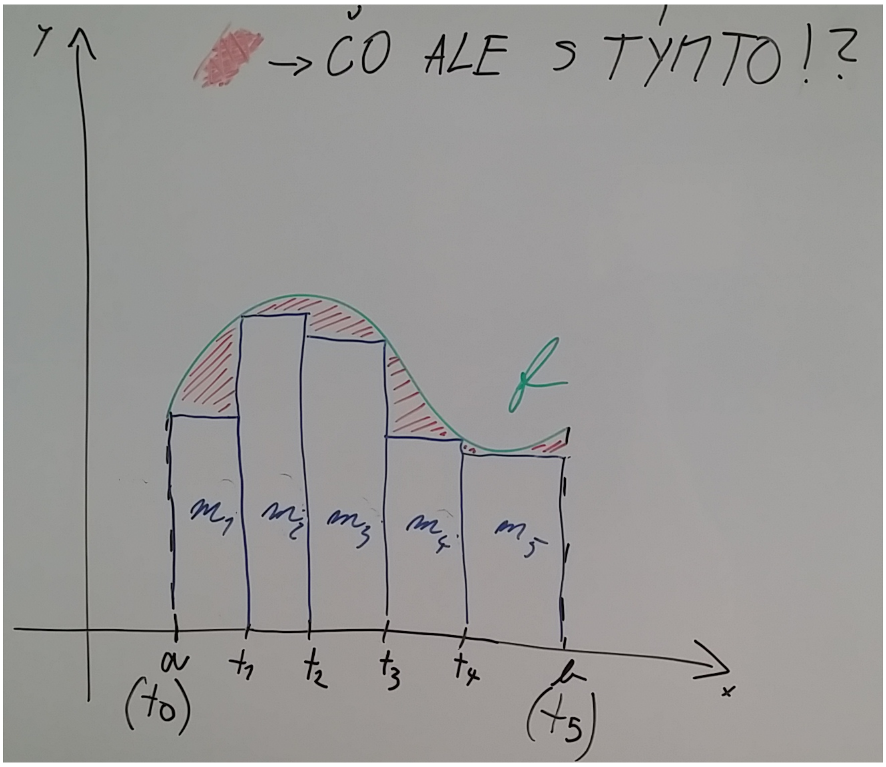
Na začiatok si je treba uvedomiť pri určitom Riemannovom itegrále ide o vyýpočet obsahu polchy pod krivkou nejakej funkcie (Riemannov integrál definujeme v $\mathbb{R}$). Predstavme si teda funkciu f obmedzenú na interval $[a, b]$ (Pozri obrázok **??**).



Obrázek 9: Funkcia f obmedzená na interval $[a, b]$

Úlohou je teda vypočítať obsah plochy pod krivkou funckie f obmedzenú na interval $[a, b]$. Interval $[a, b]$ možeme rodeliť na mnešie časti $t_0 \ldots t_5$; $m_1 \ldots m_5$ sú výšky obdľžnikov (Pozri obrázok **??**). Ich obsah potom možeme vypočítať ako

$$m_1 \cdot (t_1 - t_0) + m_2 \cdot (t_2 - t_1) + \cdots + m_5 \cdot (t_5 - t_4)$$



Obrázek 10: Naznačenie obdĺžnikov pre dolný integrálny súčet

Otázne je ako vypočítať výšky obdĺžnikov. Ako výšku obdĺžnika budeme brať infimum funkcie f obmedzenej na daný podinterval $[t_{i-1}, t_i]$. Takže platí

$$m_i = inf\{f(x)|x \in [t_{i-1}, t_i]\}$$

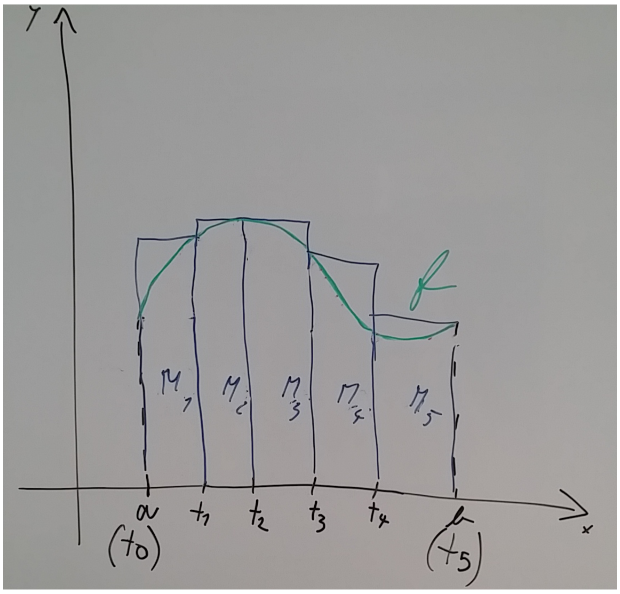
Pre potreby zápisu zadefinujeme **delenie** P pričom bude platiť

$$P : a = t_0 < t_1 < \cdots < t_n < t_{n+1} = b$$

Definice 95. *Definujeme **dolný integrálny súčet** ako* $L(f, P) = \sum_{i=1}^{n+1} m_{i(t_i, t_{i-1})}$

Podobnými úvahami možeme prísť k hornému integrálnemu súčtu. (Pozri obrázok **??**). Výška obdĺžnikov pri hornom integrálnom súčte je zadefinovaná ako

$$M_i = sup\{f(x)|x \in [t_{i-1}, t_i]\}$$



Obrázek 11: Naznačenie obdĺžnikov pre horný integrálny súčet

Definice 96. *Potom zadefinujeme* ***holný integrálny súčet*** *ako* $U(f,P) = \sum_{i=1}^{n+1} M_{i(t_i,t_{i-1})}$

Jednoznačne platí že $L(f,P) \leq U(f,P)$. Teraz máme k dispozícii všetko potrebné aby sme zadefinovali horný a dolný integrál.

Definice 97. $L\int_a^b f$ *nazveme* ***dolný integrál*** *pričom platí že:*

$$L\int_a^b f = sup\{L(f,P)|P \dots je\ delenie\ [a,b]\}$$

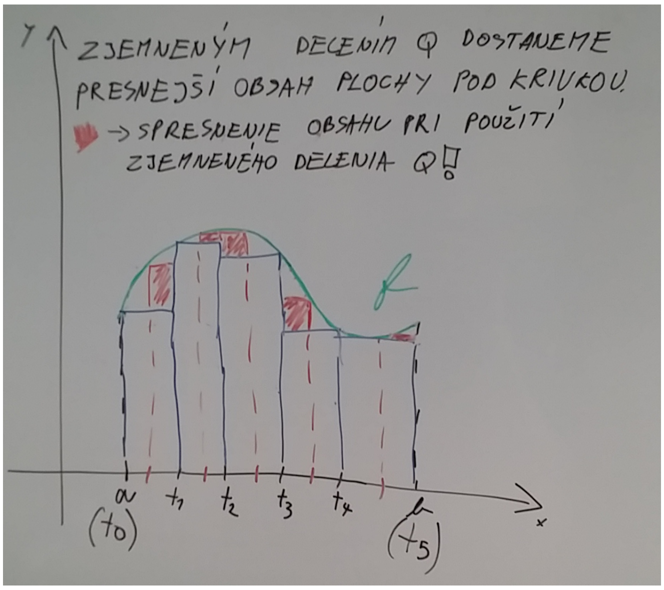
Definice 98. $U\int_a^b f$ *nazveme* ***horný integrál*** *pričom platí že:*

$$U\int_a^b f = inf\{U(f,P)|P \dots je\ delenie\ [a,b]\}$$

NASLEDUJE DEFINÍCIA INTEGRÁLU KONEČNE !!!!

Definice 99. *Funkcia f je integrovatelná na $[a,b]$ ak $L\int_a^b f = U\int_a^b f$, potom číslo $\int_a^b f = L\int_a^b f = U\int_a^b f$ sa nazýva **integrál funkcie** f na intervale $[a,b]$.*

Otázne je ako zvoliť delenie P ... pretože musí byť dostatočne jemné na to aby platil vzťah z definície. Pre zavádzame **zjemnené delenie** Q pre ktoé platí, že $P \subset Q$ (Pozri obrázok **??**)



Obrázek 12: Zjemnené delenie Q

Věta 84. *Funkcia f je integrovatelná na intervale $[a,b]$ práve vtedy, keď pre každé číslo $\epsilon > 0$ exituje delenie P (Ide iba o značenie ... úlaha je nájsť dostatočne jemné delenie) tak, že $U(f,P) - L(f,P) < \epsilon$.*

Kombinatorika: pravidlo součtu a součinu, permutace, variace, kombinace, binomická věta, princip inkluze a exkluze. Popisná statistika: číselné charakteristiky výběrů a grafické metody.

20 Kombinatorika

20.1 Pravidlo součtu a součinu

20.1.1 Pravidlo součtu

Definice 100. *Lze-li úkol A provést m-způsoby a lze-li úkol B provést n-způsoby, přičemž žádný z m-způsobů provedení úkolu A není totožný s žádným z n-způsobů provedení úkolu B, pak provést úkol A nebo úkol B lze provést m + n způsoby.*

20.1.2 Pravidlo součinu

Definice 101. *Lze-li úkol C rozložit na po sobě následující úkoly A a B (tj. provést C znamená provést nejdřív A a potom B) a lze-li úkol A provést m způsoby a úkol B lze provést n způsoby, pak lze úkol C provést $m \cdot n$ způsoby.*

20.2 Variace

20.2.1 bez opakování

Definice 102. *Je dáno n (navzájem různých) objektů a číslo $r \leq n$. Variace r (objektů) z n (objektů) je libovolný výběr r objektů z daných n objektů, ve kterém záleží na pořadí vybíraných objektů. Počet takových variací značíme V(n, r).*

Věta 85. $V(n,r) = n \cdot (n-1) \cdot \dots \cdot (n-r+1)$

Poznámka. $V(n,r) = \frac{n!}{(n-r)!} = \frac{n\cdot(n-1)\cdot\dots\cdot(n-r+1)\cdot(n-r)\cdot\dots\cdot 1}{(n-r)\cdot\dots\cdot 1} = n \cdot (n-1) \cdot \dots \cdot (n-r+1)$

20.2.2 s opakováním

Definice 103. *Jsou dány objekty n různých typů. Objektů každého typu je neomezeně mnoho a jsou navzájem nerozlišitelné. Variace r (objektů) z n (objektů) s opakováním je libovolný výběr r objektů z daných objektů n typů, ve kterém záleží na pořadí vybíraných objektů. Počet takových variací značíme $\overline{V}(n,r)$.*

Věta 86. $\overline{V}(n,r) = n^r$.

20.3 Permutace

20.4 bez opakování

Definice 104. *Permutace n (navzájem různých) objektů je libovolné seřazení těchto objektů, tj. seřazení od prvního k n-tému. Počet permutací n objektů budeme značit P(n).*

Věta 87. $P(n) = V(n,n) = n!$

20.5 s opakováním

Definice 105. *Je dáno n objektů rozdělených do r skupin, které mají po řadě* $n_1, \ldots, n_r$ *objektů, tj.* $n_1 + \cdots + n_r = n$*. Objekty v každé ze skupin jsou navzájem nerozlišitelné. Každé seřazení těchto n objektů se nazývá permutace s opakováním (daným parametry* $(n_1, \ldots, n_r)$*). Počet takových permutací značíme* $P(n_1, \ldots, n_r)$*.*

Věta 88. *Pro* $n_1 + \cdots + n_r = n$ *je* $P(n_1, \ldots, n_r) = \frac{n!}{n_1! \cdot \cdots \cdot n_r!}$.

20.6 Kombinace

20.6.1 bez opakování

Definice 106. *Je dáno n (navzájem různých) objektů a číslo* $r \leq n$*. Kombinace r (objektů) z n (objektů) je libovolný výběr r objektů z daných n objektů, ve kterém nezáleží na pořadí vybíraných objektů. Počet takových kombinací značíme* $\binom{n}{r}$ *(nebo C(n, r)).*

Věta 89. $\binom{n}{r} = \frac{n!}{(n-r)! \cdot r!}$

$$\binom{n}{r} = \binom{n}{n-r}$$

$$\binom{n}{n} = 1 \text{ a } \binom{n}{0} = 1$$

Poznámka. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

20.6.2 s opakováním

Definice 107. *Jsou dány objekty n různých typů. Objektů každého typu je neomezeně mnoho a jsou navzájem nerozlišitelné. Kombinace r (objektů) z n (objektů) s opakováním je libovolný výběr r objektů z daných objektů n typů, ve kterém nezáleží na pořadí vybíraných objektů. Počet takových kombinací značíme* $\overline{C}(n,r)$*.*

Věta 90. $\overline{C}(n,r) = \binom{n+r-1}{n-1}$.

20.7 Binomická věta

Věta 91. *Pro reálné číslo x a nezáporné celé n je*

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

20.8 Princip inkluze a exkluze

Věta 92. *Pro množiny $A_1, \dots, A_n$ platí*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\emptyset \neq I \subseteq \{1,2,\dots,n\}} (-1)^{|I|+1} |\bigcap_{i \in I} A_i|$$

Příklad 26. *V nabídce volitelných předmětů je němčina a angličtina. Němčinu si zvolilo 15, angličtinu 30 a oba jazyky 5 studentů. Kolik studentů si jako volitelný předmět vybralo cizí jazyk (tj. NJ + AJ)? Označme N a A po řadě množiny studentů, kteří si zapsali NJ a AJ. Sečteme-li $|N|$ (počet co si zapsali němčinu) a $|A|$ (počet co si zapsali angličtinu), počítáme dvakrát ty, kteří si zapsali NJ a AJ (těch je $|N \cap A|$. Ty tedy musíme od $|N| + |A|$ odečíst. Počet $|N \cup A|$ těch, kteří si zapsali NJ nebo AJ tedy*

$$|N \cup A| = |N| + |A| - |N \cap A| = 15 + 30 - 5 = 40$$

Poznámka. $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$

21 Popisná statistika

21.1 Číselné charakteristiky výběrů

21.1.1 Výběrový (aritmetický) průměr

Míry centrální tendence: výběrový průměr

Definice (Výběrový (aritmetický) průměr)

Výběrový (aritmetický) průměr $\overline{x}$ výběru $x_1, \ldots, x_n$ je číslo definované

$$\overline{x} = \frac{1}{n} \sum_{i=1}^{n} x_i \,.$$

Poznámky:

- interpretace: $\overline{x} =$ „střední hodnota z výběru“
- $\overline{x}$ nemusí být jednou z hodnot $x_1, \ldots, x_n$
- triviální případy:
  - $n = 1$ (jednoprvkový výběr): $\overline{x} = x_1$;
  - $x_1 = x_2 = \cdots = x_n$ (uniformní výběr): $\overline{x} = x_1 = x_2 = \cdots = x_n$.
- další typy průměru: geometrický, harmonický (požívané zřídka)

Vlastnosti výběrového průměru

Věta (o výběrovém průměru)

Pro každý výběr $x_1, \ldots, x_n$ a jeho průměr $\overline{x}$ platí:

1. $\overline{x} = \sum_{i=1}^{n} \frac{x_i}{n}$,
2. $\sum_{i=1}^{n} (x_i - \overline{x}) = 0$,
3. *funkce $f\colon \mathbb{R} \to \mathbb{R}$ definovaná $f(x) = \sum_{i=1}^{n} (x_i - x)^2$ nabývá v bodě $\overline{x}$ svého globálního minima.*

Důsledek: $\overline{x}$ minimalizuje hodnotu $\sum_{i=1}^{n} (x_i - x)^2$.

21.1.2 Výběrový rozptyl a Směrodatná odchylka

Míry rozptýlenosti: výběrový rozptyl a směrodatná odchylka

Definice (výběrový rozptyl / výběrová variance / výběrová disperze)

Výběrový rozptyl s^2 výběru $x_1, \ldots, x_n$ je číslo definované

$$s^2 = \frac{1}{n-1} \sum_{i=1}^{n} (x_i - \overline{x})^2 .$$

Definice (výběrová směrodatná odchylka)

Výběrová směrodatná odchylka s výběru $x_1, \ldots, x_n$ je číslo definované

$$s = \sqrt{s^2} = \sqrt{\frac{1}{n-1} \sum_{i=1}^{n} (x_i - \overline{x})^2} .$$

angl.: *sample variance, sample standard deviation*

Vlastnosti výběrového rozptylu a směrodatné odchylky

Výběrový rozptyl s^2

- míra rozptýlenosti hodnot ve výběru od jeho průměru,
- $s^2 \geq 0$,
- pokud je hodnota s^2 malá, pak je většina hodnot ve výběru blízko $\overline{x}$,
- triviální případy:
  - pro $n = 1$ (jednoprvkový výběr) není s^2 definovaná,
  - $s^2 = 0$ právě když $x_1 = x_2 = \cdots = x_n = \overline{x}$ (uniformní výběr).

Výběrová směrodatná odchylka s

- podobné vlastnosti a význam jako výběrový rozptyl,
- používá stejné jednotky jako data ve výběru.

Například: data ve výběru v m (metrech) $\Longrightarrow$ s^2 v m^2 $\Longrightarrow$ s v m.

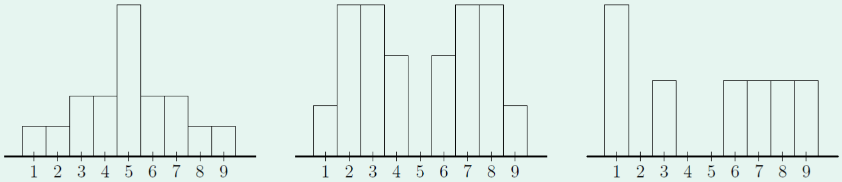
21.2 Grafické metody

Grafická reprezentace dat z tabulek četností

Histogram absolutní četnosti / **histogram relativní četnosti**:

- diagram zakreslený do kartézské roviny,
- pro každý $x \in \Omega$: obdélník s výškou rovnou absolutní/relativní četnosti x,
- šířka všech obdélníků je konstantní.

Příklad



- možné znázorňovat i v jiném tvaru (koláče a podobně)
- tvar histogramu – vztah k hustotě pravděpodobnosti (PŘEDNÁŠKA 7)

Skupinové (intervalové) rozdělení četností

Pokud je Ω spojitá (např. reálný interval) nebo obsahuje-li Ω mnoho hodnot, rozdělíme Ω na disjunktní podmnožiny (skupiny) a uvažujeme četnosti celých skupin.

Postup:

1. Určíme největší (max) a nejmenší (min) hodnotu ve výběru.
   Rozdíl $r = max - min$ se nazývá **variační rozpětí**, angl.: *range*.
2. Zvolíme $\boldsymbol{k}$ **intervalů**, angl.: *class intervals*, které tvoří rozklad na (min, max):
   $$(c_0, c_1), (c_1, c_2), \ldots, (c_{k-1}, c_k)$$
   Číslo k volíme obvykle $5 \leq k \leq 20$ (Sturgessovo pravidlo: $k \approx 1 + 3.3 \log n$).
3. Čísla c_{i-1} a c_i se nazývají **hranice intervalu** $(\boldsymbol{c_{i-1}}, \boldsymbol{c_i})$, angl.: *class boundaries*.
4. Číslo $\dfrac{c_{i-1} + c_i}{2}$ se nazývá **střed intervalu** $(\boldsymbol{c_{i-1}}, \boldsymbol{c_i})$, angl.: *class mark*.

Tabulky intervalového rozdělení četností

Meze intervalu (c_{i-1}, c_i), angl.: *class limits*, jsou hodnoty d_{i-1} a d_i z výběru $x_1, \ldots, x_n$, zapisované (d_{i-1}, d_i), pro které platí

1. $d_{i-1} \leq d_i$ a dále
2. $\{x_1, \ldots, x_n\} \cap (c_{i-1}, d_{i-1}) = \emptyset$ a $\{x_1, \ldots, x_n\} \cap (d_i, c_i) = \emptyset$.

Četnost intervalu (c_{i-1}, c_i), angl.: *class frequency*, je číslo f_i označující počet hodnot z výběru patřících do (c_{i-1}, c_i), to jest $f_i = |(c_{i-1}, c_i) \cap \{x_1, \ldots, x_n\}|$.

Tabulka absolutních četností:

- řádky: korespondují s *intervaly* (c_{i-1}, c_i)
- sloupce: *interval*, *meze intervalu*, *střed intervalu*, *četnost intervalu*

Tabulka relativních četností: jako tabulka absolutních četností + sloupec h_i:

$$h_i = \frac{f_i}{n \cdot (c_i - c_{i-1})}, \qquad \text{hodnota } \frac{f_i}{n} \text{ je } \textbf{relativní četnost intervalu } (c_{i-1}, c_i).$$

Histogramy intervalového rozdělení četností

Histogram int. rozdělení absolutních četností: pro každý interval (c_{i-1}, c_i) zakreslíme obdélník daný body $[c_{i-1}, 0]$, $[c_i, 0]$, $[c_i, f_i]$ a $[c_{i-1}, f_i]$.

Histogram int. rozdělení relativních četností: pro každý interval (c_{i-1}, c_i) zakreslíme obdélník daný body $[c_{i-1}, 0]$, $[c_i, 0]$, $[c_i, h_i]$ a $[c_{i-1}, h_i]$.

Věta

Obsah všech obdélníků v histogramu int. rozdělení relativních četností je rovna 1.

Důkaz.

$$\sum_{i=1}^{k} ((c_i - c_{i-1}) \cdot h_i) = \sum_{i=1}^{k} \frac{(c_i - c_{i-1}) \cdot f_i}{n \cdot (c_i - c_{i-1})} = \sum_{i=1}^{k} \frac{f_i}{n} = \frac{1}{n} \sum_{i=1}^{k} f_i = \frac{1}{n} \cdot n = 1. \qquad \square$$

Poznámka. Další metody jsou např.: sloupcový graf, koláčový graf nebo bodový graf (myslím, že k tomu není třeba nic psát)

Náhodné jevy, pravděpodobnostní míra. Podmíněná pravděpodobnost, nezávislost jevů. Náhodná veličina, distribuční funkce. Příklady rozdělení diskrétních a spojitých náhodných veličin. Náhodné vektory: sdružené a marginální rozdělení. Bodové odhady. Základy testování hypotéz.

22 Pravděpodobnost

22.1 Náhodné jevy

Náhodný jev a jeho výskyt

Definice (Náhodný jev, výskyt náhodného jevu)

Uvažujme náhodný pokus s prostorem elementárních jevů Ω. Každou podmnožinu $A \subseteq \Omega$ nazveme **náhodný jev** (angl.: *event*). Speciálně,

- $\emptyset$ nazveme **jev nemožný** (angl.: *empty event, impossible event*),
- Ω nazveme **jev jistý** (angl.: *universal event, certain event*).

Předpokládejme, že je proveden náhodný pokus a jeho výsledkem je $x \in \Omega$. Pokud $x \in A$, pak mluvíme o **výskytu náhodného jevu** A (angl.: *event* A *occurred*).

Množinový pohled na náhodné jevy:

náhodný jev $=$ *libovolná podmnožina* Ω

Poznámka:

Elementární jev $x \in \Omega$ (Přednáška 1) lze chápat jako náhodný jev $\{x\} \subseteq \Omega$.

Vztahy náhodných jevů

Definice (Vzájemně neslučitelné jevy, úplný systém jevů)

Uvažujme prostor Ω a spočetně mnoho náhodných jevů $A_1, A_2, \ldots$ v tomto prostoru. Náhodné jevy $A_1, A_2, \ldots$ nazveme

- **vzájemně neslučitelné** (angl.: *mutually exclusive events*) pokud pro každé i, j, kde $i \neq j$, platí $A_i \cap A_j = \emptyset$;
- **úplným systémem jevů** (angl.: *exhaustive events*) pokud $\Omega = A_1 \cup A_2 \cup \cdots$;
- **úplným systémem neslučitelných jevů** (angl.: *mutually exclusive and exhaustive events*) pokud jsou vzájemně neslučitelné a tvoří úplný systém jevů.

Poznámky:

- vzájemně neslučitelné jevy: nemohou nastat současně;
- úplným systémem jevů: alespoň jeden z jevů vždy nastane;
- úplný systém neslučitelných jevů = nastává právě jeden z jevů

Operace s náhodnými jevy

Množinové operace:

- $A \cap B = \{x \in \Omega \,|\, x \in A \text{ a } x \in B\}$ (**průnik**)
- $A \cup B = \{x \in \Omega \,|\, x \in A \text{ nebo } x \in B\}$ (**sjednocení**)
- $A - B = \{x \in \Omega \,|\, x \in A \text{ a } x \notin B\}$ (**rozdíl**)
- $A' = \{x \in \Omega \,|\, x \notin A\} = \Omega - A$ (**doplněk**, neboli **komplement**)
- $A \div B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$ (**symetrický rozdíl**)

Význam:

- $A \cap B$ nastane p.k. A nastane a současně nastane $B, \ldots$

Vybrané zákony:

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
- $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$, $(A \cup B)' = A' \cap B'$, $(A \cap B)' = A' \cup B', \ldots$

22.2 Pravděpodobnostní míra

Míra, pravděpodobnostní míra, pravděpodobnostní prostor

Definice (Míra a pravděpodobnostní míra)

Mějme σ-algebru $\mathcal{F} \subseteq 2^{\Omega}$. Každé zobrazení $m\colon \mathcal{F} \to \mathbb{R} \cup \{\infty\}$ splňující

- $m(A) \geq 0$ pro každou $A \in \mathcal{F}$,
- $m(\emptyset) = 0$,
- $m\left(\bigcup_{i \in I} A_i\right) = \sum_{i \in I} m(A_i)$ pro libovolnou spočetnou $\{A_i \in \mathcal{F} \mid i \in I\}$, kde $A_i \cap A_j = \emptyset$ pro každé $i, j \in I$ takové, že $i \neq j$ (**σ-aditivita**).

nazýváme **míra na $\mathcal{F}$** (angl.: *measure*). Míra m na $\mathcal{F}$ splňující $m(\Omega) = 1$ se nazývá **pravděpodobnostní míra na $\mathcal{F}$** (angl.: *probability measure*). Pravděpodobnostní míru na $\mathcal{F}$ obvykle označujeme $P\colon \mathcal{F} \to \mathbb{R}$.

Definice (Pravděpodobnostní prostor)

Je-li $P\colon \mathcal{F} \to \mathbb{R}$ pravděpodobnostní míra na σ-algebře $\mathcal{F} \subseteq 2^{\Omega}$, pak trojici $\langle \Omega, \mathcal{F}, P \rangle$ nazýváme **pravděpodobnostní prostor**, (angl.: *probability space*).

V. Vychodil (KMI/PRAS, Přednáška 3) Pravděpodobnost Pravděpodobnost a statistika 24 / 58

22.3 Podmíněná pravděpodobnost

Podmíněná pravděpodobnost

Definice (Podmíněná pravděpodobnost, angl.: *conditional probability*)

Mějme pravděpodobnostní prostor $\langle \Omega, \mathcal{F}, P \rangle$ a náhodný jev $B \in \mathcal{F}$ takový, že $P(B) > 0$. Pak **podmíněná pravděpodobnost $P(A|B)$** výskytu náhodného jevu $A \in \mathcal{F}$ za podmínky, že nastal náhodný jev B, je definovaná vztahem

$$P(A|B) = \frac{P(A \cap B)}{P(B)},$$

Funkce $P(\cdot|B)\colon \mathcal{F} \to \mathbb{R}$ se nazývá **podmíněná pravděpodobnostní míra**.

Poznámky:

- $P(A|B)$ čteme „pravděpodobnost A za předpokladu (výskytu) B“;
- $P(\cdot|B)$ je funkce, která každému A přiřazuje $P(A|B) \in \mathbb{R}$;
- dále prokážeme, že $P(\cdot|B)$ je vskutku pravděpodobnostní míra.

V. Vychodil (KMI/PRAS, Přednáška 4) Podmíněná pravděpodobnost a nezávislost jevů Pravděpodobnost a statistika 6 / 55

Věta (Základní vlastnosti podmíněné pravděpodobnosti)

Mějme pravděpodobnostní prostor $\langle \Omega, \mathcal{F}, P \rangle$ *a* $B \in \mathcal{F}$ *takový, že* $P(B) > 0$. *Potom*

1. $P(A|B) \geq 0$ *pro každou* $A \in \mathcal{F}$;
2. $P(C|B) = 1$ *pro každou* $C \in \mathcal{F}$ *takovou, že* $B \subseteq C$;
3. *pokud* $A \cap B = \emptyset$, *pak* $P(A|B) = 0$; *speciálně:*
4. *pokud* $\{x\} \in \mathcal{F}$ *a* $x \notin B$, *pak* $P(\{x\}|B) = 0$.

Důkaz.

První tvrzení je zřejmé: $P(A|B) = \dfrac{P(A \cap B)}{P(B)} \geq 0$.

Mějme $B \subseteq C$, to jest $B \cap C = B$. Odtud $P(C|B) = \dfrac{P(C \cap B)}{P(B)} = \dfrac{P(B)}{P(B)} = 1$.

Pokud $A \cap B = \emptyset$, pak $P(A \cap B) = 0$, to jest $P(A|B) = \dfrac{P(A \cap B)}{P(B)} = 0$. $\square$

22.4 Nezávislost jevů

Nezávislé náhodné jevy

Nezávislost *dvou náhodných jevů* formazilujeme následovně:

Definice (Nezávislé náhodné jevy)

Mějme pravděpodobnostní prostor $\langle \Omega, \mathcal{F}, P \rangle$. Náhodné jevy $A, B \in \mathcal{F}$ nazveme **nezávislé** (angl.: *independent*), pokud

$$P(A \cap B) = P(A) \cdot P(B)$$

V opačném případě nazýváme A a B **závislé** (angl.: *dependent*).

Terminologie: Existuje několik různých pojmů pro totéž, například

- statisticky nezávislé jevy, angl.: *statistically independent events*,
- stochasticky nezávislé jevy, angl.: *stochastically independent events*,
- jevy nezávislé ve smyslu pravděpodobností výskytu, ...

Vlastnosti nezávislých jevů

Nezávislost jevů se přenáší i na jejich doplňky:

Věta (Vlastnosti nezávislých jevů)

Mějme pravděpodobnostní prostor $\langle \Omega, \mathcal{F}, P \rangle$ a libovolné náhodné jevy $A, B \in \mathcal{F}$. Pokud jsou A a B nezávislé, pak jsou i následující dvojice náhodných jevů nezávislé:

1. A *a* B',
2. A' *a* B,
3. A' *a* B'.

Poznámka: Druhé a třetí tvrzení plyne z prvního, protože:

- druhé tvrzení dostáváme z prvního záměnou A a B;
- pokud jsou A a B nezávislé, pak i A a B' jsou nezávislé (z prvního tvrzení) a tedy i A' a B' jsou nezávislé (z druhého tvrzení).

Věta (Triviálně nezávislé náhodné jevy)

Mějme pravděpodobnostní prostor $\langle \Omega, \mathcal{F}, P \rangle$ a libovolný náhodný jev $A \in \mathcal{F}$. Pak následující dvojice náhodných jevů jsou nezávislé:

1. A *a* $\emptyset$,
2. A *a* Ω.

Důkaz.

Platí $A \cap \emptyset = \emptyset$, to jest

$$P(A \cap \emptyset) = P(\emptyset) = 0 = P(A) \cdot 0 = P(A) \cdot P(\emptyset).$$

Dále platí $A \cap \Omega = A$, to jest

$$P(A \cap \Omega) = P(A) = P(A) \cdot 1 = P(A) \cdot P(\Omega).$$

$\square$

22.5 Náhodná veličina

Náhodná veličina

Definice (Náhodná veličina / náhodná proměnná)

Mějme pravděpodobnostní prostor $\langle \Omega, \mathcal{F}, P \rangle$. Zobrazení $X : \Omega \to \mathbb{R}$ nazýváme **náhodnou veličinou** v $\langle \Omega, \mathcal{F}, P \rangle$ (angl.: *random variable*) pokud

$$\{\omega \in \Omega \,|\, X(\omega) \leq a\} \in \mathcal{F}$$

platí pro každé $a \in \mathbb{R}$. Množinu reálných čísel $\{X(\omega) \,|\, \omega \in \Omega\}$ nazveme **prostor** nebo **obor hodnot** náhodné veličiny X, angl.: *space*.

Význam:

- náhodné veličiny označujeme $X, Y, Z, \ldots$
- $X(\omega) \in \mathbb{R}$ je výsledek měření na elementárním jevu ω,
- obor hodnot X je množina všech možných výsledků měření,
- termín „náhodná veličina“ *není příliš šťastný* (každá $X(\omega)$ je jednoznačná).

22.6 Distribuční funkce

Distribuční funkce

Snaha o jednoduchý popis P_X:

- rozdělení P_X je zobrazení z $\mathcal{B}$ do $[0, 1]$ (množinová funkce);
- nevýhoda: těžko si lze „představit“ nebo „zakreslit“;
- obtížná přímá analýza vlastností funkce P_X;
- snaha o vyjádření P_X pomocí reálné funkce jedné proměnné;
- vede na pojem *distribučí funkce*:

Definice (Distribuční funkce)

Mějme náhodnou veličinu X s rozdělením P_X. Potom funkce $F_X : \mathbb{R} \to \mathbb{R}$, kde

$$F_X(x) = P_X\big((-\infty, x]\big), \qquad \text{pro každé } x \in \mathbb{R}$$

se nazývá **distribuční funkce** náhodné veličiny X, angl.: *distribution function*.

22.7 Rozdělení diskrétních náhodných veličin

22.7.1 Alternativní rozdělení

Alternativní (Bernoulliho) rozdělení

Definice (Náhodná veličina s alternativním rozdělením)

Náhodná veličina X má **alternativní rozdělení** (angl.: *Bernoulli distribution*) pokud existuje $p \in (0, 1)$ tak, že její pravděpodobnostní funkce f_X je ve tvaru

$$f_X(x) = p^x \cdot (1 - p)^{1-x} \qquad \text{pro } x = 0, 1,$$

a $f_X(x) = 0$ jinak.

Interpretace:

- náhodný pokus (Bernoulliho pokus) končící úspěchem 1 nebo neúspěchem 0;
- po provedení pokusu X nabude právě jedné z hodnot 0, 1;
- p je *parametr* interpretovaný jako **pravděpodobnost úspěchu**; platí totiž:

$$f_X(0) = p^0 \cdot (1 - p)^1 = 1 - p, \qquad f_X(1) = p^1 \cdot (1 - p)^0 = p.$$

V. Vychodil (KMI/PRAS, Přednáška 6) Diskrétní rozdělení Pravděpodobnost a statistika 12 / 53

22.7.2 Binomické rozdělení

Binomické pokusy a binomické rozdělení

Definice (Náhodná veličina s binomickým rozdělením)

Náhodná veličina X má **binomické rozdělení** (angl.: *binomial distribution*) pokud existují $n \in \mathbb{N}$ a $p \in (0,1)$ tak, že její pravděpodobnostní funkce f_X je

$$f_X(x) = \binom{n}{x} \cdot p^x \cdot (1-p)^{n-x} \qquad \text{pro } x = 0, 1, 2, \ldots, n,$$

a $f_X(x) = 0$ jinak; X se pak nazývá **binomická veličina** s rozdělením $b(n,p)$.

Binomický experiment (angl.: *binomial experiment*) je posloupnost pokusů:

- Bernoulliho pokus je proveden n krát (*parametr*);
- jednotlivé pokusy jsou nezávislé ve smyslu výskytu úspěchu či neúspěchu;
- pravděpodobost výskytu úspěchu každého z pokusů je rovna p (*parametr*);
- náhodná veličina X = „počet úspěchů z celkových n pokusů“.

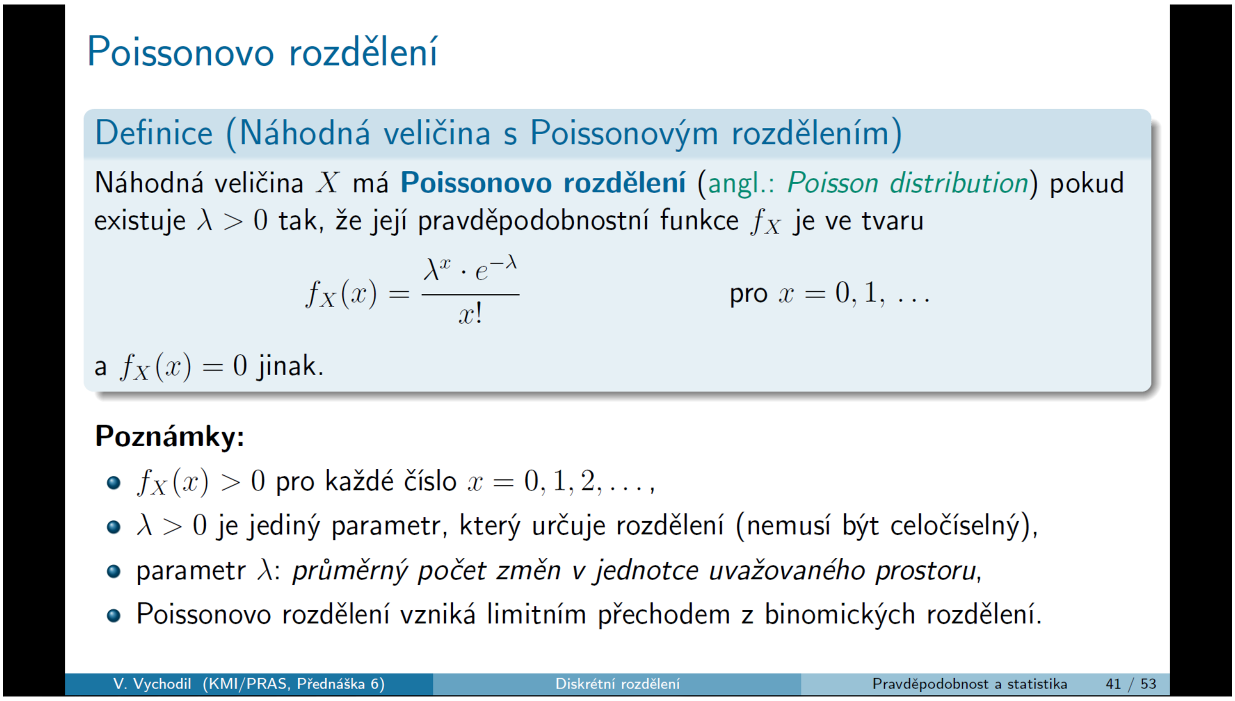
V. Vychodil (KMI/PRAS, Přednáška 6) Diskrétní rozdělení Pravděpodobnost a statistika 16 / 53

Budeme uvažovat náhodný pokus, ve kterém určitý náhodný jev nastane s pravděpodobností p. Tento pokus opakujeme nezávisle n-krát a sledujeme výskyt sledovaného náhodného jevu v těchto n nezávislých opakováních téhož náhodného pokusu, přičemž pravděpodobnost, že v každém jednotlivém opakování náhodného pokusu je sledovaný náhodný jev, je rovna p.

Náhodná veličina X představující počet opakování daného náhodného pokusu z celkového počtu n nezávislých opakování, ve kterých sledovaný náhodný jev nastane, má binomické rozdělení $b(n,p)$.

Poznámka. Typickým příkladem je výběr prvku s vracením, vícenásobný hod kostkou.

22.7.3 Poissonovo rozdělení



Poznámka. Tímto rozdělením se řídí počet nějakých událostí během určitého časového intervalu. (Počet zákazníků za 1 hodinu, počet poruch za 100 hodin...)

22.7.4 Geometrické rozdělení

Geometrické rozdělení

Definice (Náhodná veličina s geometrickým rozdělením)

Náhodná veličina X má **geometrické rozdělení** (angl.: *geometric distribution*) pokud existuje $p \in (0, 1)$ tak, že její pravděpodobnostní funkce f_X je

$$f_X(x) = (1-p)^{x-1} \cdot p \qquad \text{pro } x = 0, 1, 2, 3, \ldots,$$

a $f_X(x) = 0$ jinak.

Pravděpodobnostní funkce f_X geometrické veličiny je dobře definovaná:

$$\sum\nolimits_{x=1}^{\infty} f_X(x) = \sum\nolimits_{x=1}^{\infty} (1-p)^{x-1} \cdot p = \frac{p}{1-(1-p)} = 1,$$

což je speciální případ součtu prvků geometrické řady, protože pro $|r| < 1$ máme:

$$\sum\nolimits_{k=1}^{\infty} a \cdot r^{k-1} = \sum\nolimits_{k=0}^{\infty} a \cdot r^{k} = \frac{a}{1-r}.$$

V. Vychodil (KMI/PRAS, Přednáška 6) Diskrétní rozdělení Pravděpodobnost a statistika 27 / 53

Geometrickým rozdělením se řídí počet neúspěšných opakování náhodného pokusu předcházejících prvnímu úspěšnému opakování při nezávislých opakováních téhož náhodného pokusu, kde úspěšnost každého pokusu je p

Počet pokusů nutných k dosažení 1. úspěchu je $x + 1$. $f_x(x)$ udává pravděpodobnost, že prvních x pokusů bude neúspěšných a $x + 1$ skončí úspěchem.

22.8 Rozdělení spojitých náhodných veličin

22.8.1 Rovnoměrné (uniformní) rozdělení

Uniformní rozdělení

Definice (Náhodná veličina s uniformním rozdělením)

Spojitá náhodná veličina X s hustotou f_X má **uniformní rozdělení** (angl.: *uniform distribution*) pokud existují $a, b \in \mathbb{R}$ tak, že $a < b$ a f_X je ve tvaru

$$f_X(x) = \frac{1}{b-a}, \qquad \text{pokud } a < x \leq b,$$

a $f_X(x) = 0$ jinak; zkráceně značíme, že X má rozdělení $U(a, b)$.

Poznámky:

- rozdělení má dva parametry: meze intervalu $(a, b]$;
- důsledek spojitosti F_X: interval lze chápat také jako $[a, b]$, $(a, b), \ldots$
  - obecně lze z $[a, b]$ „vyjmout spočetně mnoho bodů",
  - distribuční funkce F_X bude na intervalu $[a, b]$ stále ve tvaru $F_X(x) = \dfrac{x-a}{b-a}$,
- neplést s diskrétním uniformním rozdělením (Přednáška 6).

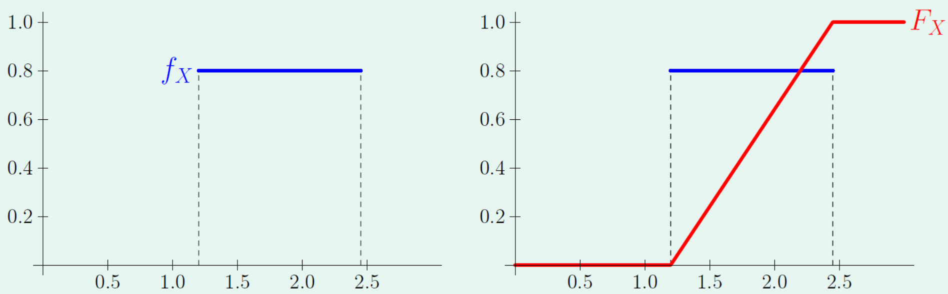
V. Vychodil (KMI/PRAS, Přednáška 7) Spojité náhodné veličiny Pravděpodobnost a statistika 37 / 60

Příklad (Distribuční funkce a funkce hustoty pro $U(a, b)$)

Mějme náhodnou veličinu X s rozdělením $U(1.2, 2.45)$. Potom je f_X ve tvaru:

$$f_X(x) = \frac{1}{b-a} = \frac{1}{1.25} = 0.8, \qquad \text{pokud } 1.2 < x \leq 2.45$$

a $f_X(x) = 0$ pro $x \leq 1.2$ nebo $x > 2.45$.



Poznámka: Pokud položíme například $f_X(1.2) = 10$, nezměníme tím F_X ani P_X.

V. Vychodil (KMI/PRAS, Přednáška 7) Spojité náhodné veličiny Pravděpodobnost a statistika 38 / 60

Náhodné veličiny řídící se rovnoměrným rozdělením:

- chyba při zaokrouhlení čísla
- doba čekání na uskutečnění jevu, který se vyskytuje v pravidelných intervalech

22.8.2 Normální rozdělení

Normální rozdělení pravděpodobnosti

Definice (Normální rozdělení, angl.: *normal distribution*)

Spojitá náhodná veličina X má **normální rozdělení** pravděpodobnosti pokud existují konstanty $\mu \in \mathbb{R}$ a $\sigma^2 > 0$ tak, že její funkce hustoty f_X je ve tvaru

$$f_X(x) = \frac{1}{\sigma \cdot \sqrt{2 \cdot \pi}} \cdot \exp\left(-\frac{(x-\mu)^2}{2 \cdot \sigma^2}\right), \qquad \text{pro každé } x \in \mathbb{R}.$$

Zkráceně zapisujeme, že X má rozdělení $N(\mu, \sigma^2)$. Pokud má X rozdělení $N(0,1)$ pak říkáme, že X má **standardní normální rozdělení** pravděpodobnosti.

Poznámky:

- Korektnost definice plyne z přechodí věty (f_X je vskutku funkce hustoty);
- označení parametrů μ a σ^2 není náhodné (uvidíme dále);
- standardní normální rozdělení má velký teoretický i praktický význam.

V. Vychodil (KMI/PRAS, Přednáška 9) | Normální rozdělení a centrální limitní věta | Pravděpodobnost a statistika 21 / 57

Normální rozdělení má zásadní význam v teorii pravděpodobnosti a v matematické statistice. Má význam tam kde je kolísání náhodné veličiny způsobeno součtem velkého počtu nepatrných vzájemně nezávislých vlivů.

22.8.3 Exponenciální rozdělení

Exponenciální rozdělení

Definice (Náhodná veličina s exponenciálním rozdělením)

Spojitá náhodná veličina X s hustotou f_X má **exponenciální rozdělení** (angl.: *exponential distribution*) pokud existuje $\theta > 0$ tak, že f_X je ve tvaru

$$f_X(x) = \frac{1}{\theta} \cdot e^{\frac{-x}{\theta}}, \qquad \text{pokud } x \geq 0,$$

a $f_X(x) = 0$ jinak.

Poznámky:

- parametr θ je převrácená hodnota (výchozího) parametru λ,
- intuice: θ je „průměrná doba čekání na změnu“ (později dokážeme),
- interpretace: $P(\{a \leq X \leq b\})$ pravděpodobnost, že první změna (od počátku pozorování) nastane v časovém rozmezí $[a, b]$.

V. Vychodil (KMI/PRAS, Přednáška 7) Spojité náhodné veličiny Pravděpodobnost a statistika 44 / 60

Využívá se k popisu reálných dějů - životnost součástí strojů, dobu bezporuchové činnosti ...

22.9 Náhodné vektory

22.9.1 Sdružené rozdělení

Sdružené rozdělení pravděpodobnosti

Definice (Sdružené rozdělení pravděpodobnosti)

Mějme náhodné veličiny $X_1, \dots, X_n$ v pravděpodobnostním prostoru $\langle \Omega, \mathcal{F}, P \rangle$. Pak se zobrazení $P_{X_1,\dots,X_n} \colon \mathcal{B}^n \to \mathbb{R}$, pro které platí

$$P_{X_1,\dots,X_n}(A_1, \dots, A_n) = P(\{X_1 \in A_1\} \cap \dots \cap \{X_n \in A_n\})$$

pro každé $A_1, \dots, A_n \in \mathcal{B}$, nazývá **sdružené rozdělení pravděpodobnosti** náhodných veličin $X_1, \dots, X_n$ (angl.: *joint probability distribution*).

Poznámky:

- $\{X_1 \in A_1, \dots, X_n \in A_n\}$ je zkrácená notace pro $\{X_1 \in A_1\} \cap \dots \cap \{X_n \in A_n\}$.
- Pokud známe $\langle \Omega, \mathcal{F}, P \rangle$ a $X_i \colon \Omega \to \mathbb{R}$ (pro každé $i = 1, \dots, n$), pak

  $$P_{X_1,\dots,X_n}(A_1, \dots, A_n) = P_{\boldsymbol{X}}(A_1, \dots, A_n) = P(\{\boldsymbol{X} \in A_1 \times \dots \times A_n\}),$$

  kde $\boldsymbol{X}(\omega)(i) = X_i(\omega)$ pro každé $i = 1, \dots, n$ a $\omega \in \Omega$.

22.9.2 Marginální rozdělení

Marginální náhodné veličiny a rozdělení pravděpodobnosti

S využitím projekcí můžeme zavést:

Definice (Marginální náhodná veličina a rozdělení pravděpodobnosti)

Mějme náhodný vektor $\boldsymbol{X} \colon \Omega \to \mathbb{R}^n$ s rozdělením $P_{\boldsymbol{X}}$, pak každá $\pi_i(\boldsymbol{X}) \colon \Omega \to \mathbb{R}$ se nazývá **marginální náhodná veličina** (angl.: *marginal random variable*) a $P_{\pi_i(\boldsymbol{X})}$ se nazývá **marginální rozdělení pravděpodobnosti** (angl.: *marginal distribution*).

Poznámka: Podle definice lze každé rozdělení $P_{\pi_i(\boldsymbol{X})} \colon \mathcal{B} \to \mathbb{R}$ vyjádřit

$$P_{\pi_i(\boldsymbol{X})}(B) = P(\{\pi_i(\boldsymbol{X}) \in B\}) = P(\{\boldsymbol{X} \in \{\pi_i \in B\}\}) = P_{\boldsymbol{X}}(\{\pi_i \in B\})$$

$$= \boxed{P_{\boldsymbol{X}}(\underbrace{\mathbb{R} \times \dots \times \mathbb{R}}_{i-1} \times B \times \underbrace{\mathbb{R} \times \dots \times \mathbb{R}}_{n-i})},$$

pro každou Borelovskou množinu $B \in \mathcal{B}$ *pouze na základě znalosti* $P_{\boldsymbol{X}}$. (!!)

V praxi obvykle známe $\langle \mathbb{R}^n, \mathcal{B}^n, P_{\boldsymbol{X}} \rangle$, kdežto $\langle \Omega, \mathcal{F}, P \rangle$ a $\boldsymbol{X} \colon \Omega \to \mathbb{R}^n$ jsou neznámé.

23 Bodové odhady

Statistická inference

Populace:

- naivní pojem *základní populace* (PŘEDNÁŠKA 1);
- při statistickém usuzování: **populace** = náhodná veličina s jejím rozložením.

Základní úkol statistické inference:

- zajímáme se o **parametr** = číselnou hodnotu, jež platí pro celou populaci (například: střední hodnota μ_X, rozptyl σ_X^2, hodnota p pro $b(n, p), \ldots$);
- používáme **výběr** (z populace) pro odhad $\mu_X, \sigma_X^2, p, \ldots$;
- **odhad parametru** = získání číselné hodnoty nebo intervalu hodnot z výběru cíl: odhad by měl být „dost blízko" skutečné hodnotě parametru.

Obvykle rozlišujeme dva druhy odhadů:

- **bodové odhady** (angl.: *point estimates*) = odhadem je *jedna hodnota*,
- **intervalové odhady** (angl.: *interval estimates*) = odhadem je *interval hodnot*.

Náhodný výběr

Definice (Náhodný výběr, angl.: *random sample*)

Mějme pravděpodobnostní prostor $\langle \Omega, \mathcal{F}, P \rangle$ a n nezávislých náhodných veličin $X_1, X_2, \ldots, X_n$ v prostoru $\langle \Omega, \mathcal{F}, P \rangle$, které mají stejné rozdělení pravděpodobnosti, to jest $P(\{X_i \in A\}) = P(\{X_j \in A\})$ pro každé i, j a $A \in \mathcal{B}$. Označme toto rozdělení P_X. Pak náhodný vektor $\boldsymbol{X} : \Omega \to \mathbb{R}^n$ definovaný $\big(\boldsymbol{X}(\omega)\big)(i) = X_i(\omega)$ se nazývá **náhodný výběr** z rozdělení P_X.

Poznámky:

- Náhodný výběr $\boldsymbol{X} : \Omega \to \mathbb{R}^n$ značíme $\boldsymbol{X} = \langle X_1, \ldots, X_n \rangle$, nebo jen $X_1, \ldots, X_n$;
- posloupnost nezávislých náhodných veličin se stejným rozdělením;
- abstrakce pojmu *výběr* (PŘEDNÁŠKA 1):
  - místo konkrétních hodnot ve výběru máme náhodné veličiny;
  - má smysl uvažovat rozdělení $P_{\boldsymbol{X}}(A) = P(\{\boldsymbol{X} \in A\})$.
- dále se budeme zabývat *statistikami*: funkcemi náhodných výběrů.

Statistiky a výběrová rozdělení

Definice (Statistika a výběrové rozdělení)

Mějme pravděpodobnostní prostor $\langle \Omega, \mathcal{F}, P \rangle$, náhodný výběr $\boldsymbol{X}\colon \Omega \to \mathbb{R}^n$ a Borelovskou funkci $g\colon \mathbb{R}^n \to \mathbb{R}$. Pak náhodnou veličinu $\vartheta\colon \Omega \to \mathbb{R}$ definovanou $\vartheta = g(\boldsymbol{X})$ nazveme **(výběrová) statistika** nebo **výběrová charakteristika** (angl.: *sample statistics*) náhodného výběru $\boldsymbol{X}$. Rozdělení pravděpodobnosti $P_\vartheta\colon \mathcal{B} \to [0,1]$ veličiny ϑ nazýváme **výběrové rozdělení**, angl.: *sampling distribution*.

Poznámky:

- Z definice složené funkce pro statistiku ϑ máme $\vartheta(\omega) = g(\boldsymbol{X}(\omega)) \in \mathbb{R}$;
- z definice rozdělení pravděpodobnosti: $P_\vartheta(A) = P(\{g(\boldsymbol{X}) \in A\})$;
- Pro konkrétní výběr $x_1, \ldots, x_n$ je $g(x_1, \ldots, x_n)$ konkrétní hodnota;
- Například: $\overline{X} = \frac{1}{n} \cdot \sum_{i=1}^{n} X_i$; $S^2 = \frac{1}{n-1} \cdot \sum_{i=1}^{n} (X_i - \overline{X})^2$.

Bodové odhady parametrických funkcí

Definice (Bodový odhad)

Mějme pravděpodobnostní prostor $\langle \Omega, \mathcal{F}, P \rangle$ a náhodný výběr $\boldsymbol{X} = \langle X_1, \ldots, X_n \rangle$ z rozdělení, které závisí na neznámých parametrech $\Theta_1, \ldots, \Theta_k$. Pak **bodový odhad** (angl.: *point estimate*) parametrické funkce $\tau(\Theta_1, \ldots, \Theta_k)$ na základě $\boldsymbol{X}$ je libovolná statistika $\vartheta = g(\boldsymbol{X})$, kde g nezávisí na $\Theta_1, \ldots, \Theta_k$.

Poznámky:

- výše definovaný pojem sám o sobě nic neříká o „kvalitě odhadu“, to jest o tom, jak jsou hodnoty dané odhadem blízko $\tau(\Theta_1, \ldots, \Theta_k)$;
- nejčastěji se zajímáme o jediný parametr Θ a parametrická funkce τ je identita:
  - to jest pokud $\tau(\Theta) = \Theta$,
  - potom bodový odhad značíme $\widehat{\Theta}$,
  - například: pro parametry μ a σ^2 jsou jejich bodové odhady značeny $\widehat{\mu}$ a $\widehat{\sigma^2}$.

Nestranné bodové odhady

Bodové odhady, jejichž střední hodnoty jsou rovny hodnotám parametrických funkcí:

Definice (Nestranný / nezkreslený / nevychýlený bodový odhad)

Mějme pravděpodobnostní prostor $\langle \Omega, \mathcal{F}, P \rangle$ a náhodný výběr $\boldsymbol{X} = \langle X_1, \ldots, X_n \rangle$ z rozdělení, které závisí na neznámých parametrech $\Theta_1, \ldots, \Theta_k$. Bodový odhad $\vartheta = g(\boldsymbol{X})$ parametrické funkce $\tau(\Theta_1, \ldots, \Theta_k)$ se nazývá **nestranný bodový odhad** (angl.: *unbiased estimate*), pokud platí $E(\vartheta) = \tau(\Theta_1, \ldots, \Theta_k)$. Rozdíl hodnot $E(\vartheta) - \tau(\Theta_1, \ldots, \Theta_k)$ se nazývá **zkreslení** nebo **vychýlení** (angl.: *bias*).

Poznámky:

- Parametrická funkce $\tau(\Theta_1, \ldots, \Theta_k)$ má obecně nekonečně mnoho odhadů;
- nestranný odhad = odhad, pro který klademe omezení na střední hodnotu;

Příklad (Nestranný odhad parametru p pro binomické rozdělení)

Problém: Výrobce automobilů testuje odolnost nárazníků vyhodnocením výsledků série n kontrolovaných srážek nárazníku s umělou překážkou. Výsledkem každého pokusu je *úspěch* (nárazník odolal) nebo *neúspěch* (neodolal).

Úkol: *Uvažujme náhodnou veličinu X označující počet jednotlivých pokusů končících úspěchem. Stanovte nestranný bodový odhad pravděpodobnosti úspěchu jednotlivého testu.*

Řešení: Každý jednotlivý pokus X_i má alternativní rozdělení s parametrem p. Počet (nezávislých) pokusů končících úspěchem je potom $X = \sum_{i=1}^{n} X_i$, přitom X má binomické rozdělení $b(n, p)$. Dále platí:

$$E\left(\frac{X}{n}\right) = \frac{1}{n} \cdot E(X) = \frac{1}{n} \cdot n \cdot p = p.$$

Závěr: Pokud má X rozdělení $b(n, p)$, potom je $\boxed{\widehat{p} = \frac{X}{n}}$ nestranný odhad p.

Nestranné bodové odhady pro střední hodnotu a rozptyl

Plyne z toho, co víme o střední hodnotě $\overline{X}$:

Věta (Nestranný bodový odhad pro střední hodnotu)

Mějme náhodný výběr $X_1, \ldots, X_n$, kde všechny X_i jsou náhodné veličiny se střední hodnotou μ. Potom je $\overline{X}$ nestranný bodový odhad pro μ.

Dále máme:

Věta (Nestranný bodový odhad pro rozptyl)

Mějme náhodný výběr $X_1, \ldots, X_n$, kde všechny X_i jsou náhodné veličiny se střední hodnotou μ a rozptylem σ^2. Potom je

$$\widehat{\sigma^2} = S^2 = \frac{1}{n-1} \cdot \sum_{i=1}^{n} (X_i - \overline{X})^2$$

nestranný bodový odhad pro σ^2.

24 Základy testování hypotéz

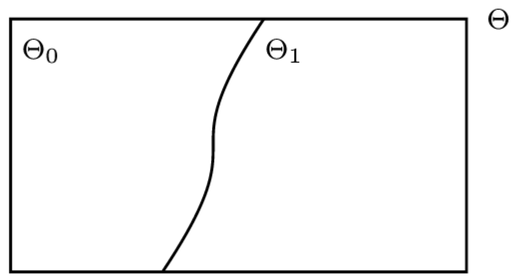
Hypotézou rozumíme tvrzení o rozdělení pozorované náhodné veličiny (např. o rozdělení náhodného výběru).

Jsou-li rozdělení, která přicházejí v úvahu, parametrizována pomocí parametru $\theta \in \Theta$, považujeme za hypotézu také tvrzení o hodnotě tohoto parametru.

Jednoduchou hypotézu představuje hypotéza $H : \theta = \theta_0$, že parametr θ je roven danému číslu $\theta_0 \in \Theta$. Hypotéza $H' : \theta \in \Theta_0$, že parametr θ pochází z dané (víceprvkové) množiny $\Theta_0 \subset \Theta$, je **hypotézou složenou**.

Test hypotézy je pravidlo, které pozorované hodnotě náhodné veličiny (obvykle realizaci náhodného výběru) přiřadí rozhodnutí hypotézu zamítnout nebo nezamítnout.

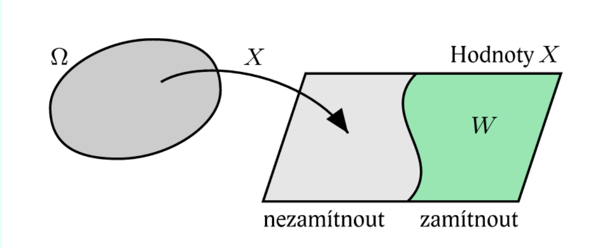
Obvykle proti **nulové hypotéze** $H_0 : \theta \in \Theta_0$, že hodnota parametru θ pochází z dané množiny $\Theta_0 \subset \Theta$, kde Θ je množina možných hodnot parametru, stavíme **alternativní hypotézu** $H_1 : \theta \in \Theta_1$, kde $\Theta_1 = \Theta \setminus \Theta_0$, že tomu tak není.



Nulová a alternativní hypotéza

Zamítnutí H_0 pak fakticky znamená rozhodnout se pro H_1.

Je-li test založen na náhodné veličině (pozorování) X s hodnotami v $\mathbf{R}^n$, pak jeho **kritický obor** je množina $W \subset \mathbf{R}^n$ těch hodnot X, pro něž test hypotézu zamítá.

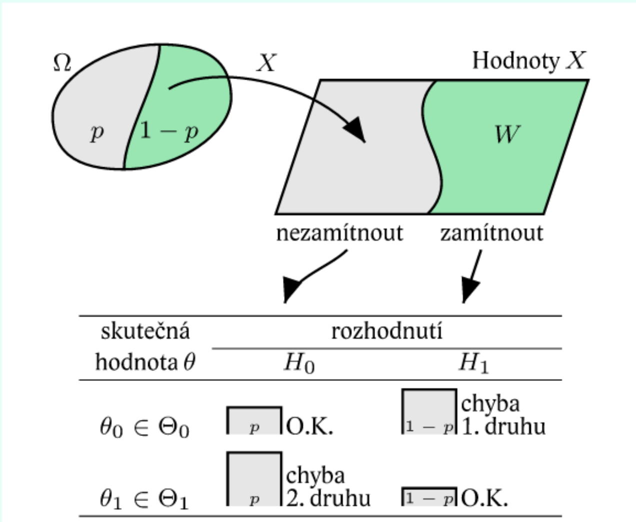


Kritický obor

Kritický obor lze často popsat prostřednictvím kritického oboru pro vhodnou (jednorozměrnou) statistiku pozorovaných hodnot.

Rozhodnutí testu o hypotéze nemusí být vždy správné. **Chyba 1. druhu** nastává, když je hypotéza zamítnuta, přestože platí, **chyba 2. druhu**, když hypotéza zamítnuta není, přestože neplatí.

Kvalita testu je dána pravděpodobnostmi, s jakými tyto chyby nastávají. Je-li test hypotézy $H_0 : \theta \in \Theta_0$ proti alternativě $H_1 : \theta \in \Theta_1$ o parametru θ založený na hodnotách náhodné veličiny X s kritickým oborem W, pak pravděpodobnost chyby 1. druhu je



Chyby 1. a 2. druhu a jejich pravděpodobnosti

$$\mathrm{P}_\theta[X \in W], \quad \theta \in \Theta_0$$

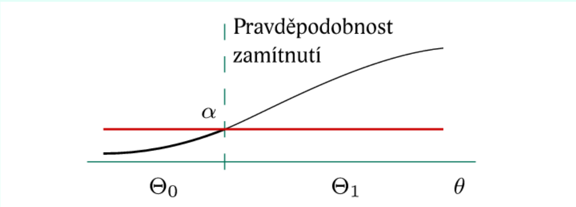
a chyby 2. druhu

$$\mathrm{P}_\theta[X \notin W], \quad \theta \in \Theta_1,$$

kde P_θ označuje pravděpodobnostní míru, při níž má X rozdělení s parametrem θ.

Při daném rozsahu výběru obvykle nelze současně minimalizovat pravděpodobnosti obou druhů chyb.

Testem na **hladině významnosti** α (α-testem), $\alpha \in (0,1)$, rozumíme test, u nějž pravděpodobnost chyby 1. druhu nepřekračuje hodnotu α.



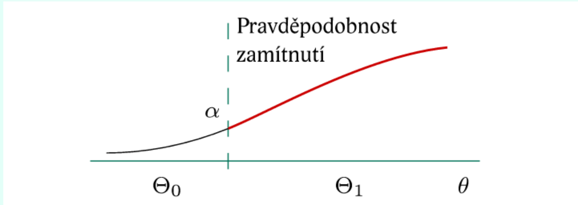
Hladina významnosti

Je žádoucí, aby test měl nízkou hladinou významnosti, rozhodnutí o zamítnutí hypotézy pak interpretujeme ve smyslu, že hypotéza neplatí. Obvykle volené hodnoty pro hladinu α bývají 0,05, 0,01 nebo 0,001.

Má-li test (s kritickým oborem W) pravděpodobnost chyby 2. druhu $\mathrm{P}_\theta[X \notin W]$, pak hodnota

$$\mathrm{P}_\theta[X \in W] = 1 - \mathrm{P}_\theta[X \notin W]$$

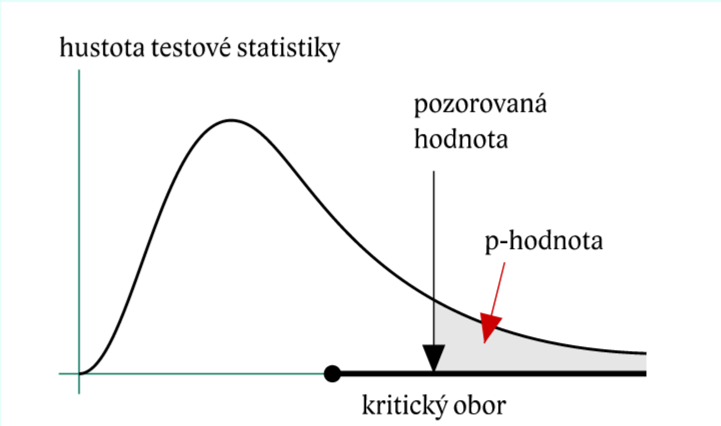
se nazývá **síla testu** proti alternativě $\theta \in \Theta_1$.



Síla testu

Při hledání optimálního testu stanovíme hladinu významnosti α (omezíme pravděpodobnost chyby 1. druhu) a mezi α-testy hledáme ten s největší sílou (nejmenší chybou 2. druhu).

P-hodnota testu je u testů, kde má tato definice smysl, pravděpodobnost, s jakou testovací statistika nabývá hodnot „horších" (více svědčících proti testované hypotéze), než je pozorovaná hodnota statistiky.



P-hodnota

P-hodnota je obvyklým výstupem počítačových programů na testování hypotéz, udává mezní hladinu významnosti, při které bychom hypotézu ještě zamítali.

Hypotézu H_0 zamítáme na hladině α, právě když p-hodnota je menší než α.