

IB112 Základy matematiky

Základy naivní teorie množin, relace, zobrazení, číselné obory

Jan Strejček

- *Množiny*
 - základní operace
 - Russellův paradox
- *Relace*
 - skládání relací
 - ekvivalence a rozklad množiny
 - uspořádání, Hasseův diagram
- *Zobrazení*
 - injekce, surjekce, bijekce
- *Číselné obory* \mathbb{N} , \mathbb{Z} , \mathbb{Q} a \mathbb{R}
- *Mohutnost*
 - spočetnost a nespočetnost
 - Cantorova věta
 - princip inkluze a exkluze

Množiny

- **Množina** je základní pojem matematiky.
- Teorii množin vybudoval *Georg Cantor* (1845–1918) v roce 1872.
- Naivní pohled: *Množina je soubor prvků.*

Zápis

- $a \in A$ značí *a je prvkem množiny A.*
- $a \notin A$ značí *a není prvkem množiny A.*
- \emptyset značí *prázdnou množinu.*
- $\{a, b, c\}$ zapisuje množinu obsahující právě prvky *a, b, c.*

- Množina může být prvkem množiny.
- Ve skutečnosti v teorii množin neexistuje nic jiného než množiny, tedy každý prvek a množiny A je opět množina.

Příklady množin

- $\{a, b\}$
- $\{a\}, \{\{a\}\}, \{\{\{a\}\}\}, \{a, \{a\}, \{\{a\}\}\}$
- $\{x \mid x \text{ je přirozené číslo dělitelné } 3\}$
- $\mathbb{N} = \{1, 2, 3, \dots\}$ - množina všech *přirozených čísel*
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ - množina všech *celých čísel*
- \mathbb{Q} - množina všech *racionálních čísel*
- \mathbb{R} - množina všech *reálných čísel*

Russellův paradox

- Proč je uvedená definice množiny označena jako naivní?
- Protože existují soubory prvků, které nelze považovat za množinu. Jeden takový soubor popsal *Bertrandem Russellem* (1872–1970) v roce 1901.

Russellův paradox

Množina X se nazývá *normální*, jestliže $X \notin X$.

Nechť N je množina všech normálních množin.

Je-li N normální, pak $N \in N$ a tedy N není normální.

Není-li N normální, pak $N \notin N$ a tedy N je normální.

V seriózní teorii množin se za množiny považují pouze soubory prvků, které vznikly z prázdné množiny pomocí sady axiomů.

Vztahy mezi množinami

Definice (Podmnožina)

Množina A je **podmnožina** množiny B , psáno $A \subseteq B$, jestliže každý prvek z A je i prvkem z B .

- Pokud $A \subseteq B$, pak také říkáme, že B je **nadmnožinou** A .
- Pro každou množinu A platí $\emptyset \subseteq A$ a $A \subseteq A$.
- Vztah \subseteq nazýváme také **inkluzí**.

Definice (Rovnost)

Množina A je **rovná** množině B , psáno $A = B$, pokud platí $A \subseteq B$ a $B \subseteq A$.

- Množiny jsou shodné, pokud mají stejné prvky.
- A je vlastní podmnožinou B , psáno $A \subset B$, pokud $A \subseteq B$ a $A \neq B$.

- *sjednocení*: $A \cup B = \{x \mid x \in A \text{ nebo } x \in B\}$
- *průnik*: $A \cap B = \{x \mid x \in A \text{ a } x \in B\}$
- *rozdíl*: $A \setminus B = \{x \mid x \in A \text{ a } x \notin B\}$
- *symetrický rozdíl*: $A \div B = (A \setminus B) \cup (B \setminus A)$
- Nechť $A \subseteq M$. *Doplňek* A (vzhledem k nosné množině M) je množina $\bar{A} = M \setminus A$.

- Doplňek se nazývá také *komplement*.
- Množiny A a B jsou *disjunktní*, pokud $A \cap B = \emptyset$. V opačném případě se množiny nazývají *incidentní*.

Průnik a sjednocení jsou

- *komutativní* $A \cap B = B \cap A$
 $A \cup B = B \cup A$
- *asociativní* $A \cap (B \cap C) = (A \cap B) \cap C$
 $A \cup (B \cup C) = (A \cup B) \cup C$
- *idempotentní* $A \cap A = A$
 $A \cup A = A$

Dále platí *distributivní zákony*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Vlastnosti množinových operací

U doplňku velmi záleží na nosné množině M :

- $A = \{a\}, M = \{a\}: \bar{A} = \emptyset$
- $A = \{a\}, M = \{a, b\}: \bar{A} = \{b\}$
- $A = \{a\}, M = \{a, b, c\}: \bar{A} = \{b, c\}$

Pro doplněk dále platí

- $\overline{\bar{A}} = A$

- *De Morganovy zákony* $\overline{A \cap B} = \bar{A} \cup \bar{B}$
 $\overline{A \cup B} = \bar{A} \cap \bar{B}$

De Morganovy zákony lze dále zobecnit

$$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$$
$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$$

Definice (Zobecněný průnik a sjednocení)

Necht' A_i je množina pro každé $i \in I \neq \emptyset$. Definujeme

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ pro každé } i \in I\}$$

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ pro nějaké } i \in I\}.$$

- Příklad: $\bigcup_{i \in \mathbb{N}} \{2i\} = \{2, 4, 6, \dots\}$
- Dále se definuje $\bigcup_{i \in \emptyset} A_i = \emptyset$.
- Je-li dána nosná množina M , lze definovat i $\bigcap_{i \in \emptyset} A_i = M$.

Definice (Uspořádaná dvojice)

Uspořádanou dvojici (a, b) definujeme jako množinu $\{\{a\}, \{a, b\}\}$.

- Platí $(a, b) = (c, d)$ právě když $a = c$ a $b = d$.
- Jaká množina je dvojice (a, a) ?

Definice (Kartézský součin)

Kartézský součin množin A, B je množina

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

- Příklad: $\{a, b\} \times \{c, d\} = \{(a, c), (a, d), (b, c), (b, d)\}$
- Pro každou množinu A platí $\emptyset \times A = A \times \emptyset = \emptyset$.
- Obecně **neplatí** $A \times B = B \times A$ (komutativita).
- Obecně **neplatí** $A \times (B \times C) = (A \times B) \times C$ (asociativita).

Definice (Uspořádaná k-tice)

Pro každé $k \in \mathbb{N}$ definujeme *uspořádanou k-tici* (a_1, a_2, \dots, a_k) induktivně:

- $(a_1) = a_1$
- $(a_1, \dots, a_i, a_{i+1}) = ((a_1, \dots, a_i), a_{i+1})$

- Platí $(a_1, \dots, a_k) = (b_1, \dots, b_k)$ právě když $a_i = b_i$ pro všechna $1 \leq i \leq k$.

Definice (Kartézský součin více množin)

Nechť $k \in \mathbb{N}$. **Kartézská součin** množin A_1, \dots, A_k je množina

$$A_1 \times \dots \times A_k = \{(a_1, \dots, a_k) \mid a_i \in A_i \text{ pro každé } 1 \leq i \leq k\}.$$

- Pro $k = 2$ se uvedená definice shoduje s původní definicí kartézského součinu.
- Lze definovat i mocniny: $A^3 = A \times A \times A$.
- Definujeme $A^0 = \{\emptyset\}$.

Definice (Potenční množina)

Potenční množinu množiny A definujeme jako množinu všech podmnožin množiny A , t.j.

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}.$$

- Někdy se používá značení 2^A místo $\mathcal{P}(A)$
- Příklad: $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- $\mathcal{P}(\emptyset) = \{\emptyset\}$

Relace

Definice (Relace)

Nechť $n \in \mathbb{N}$. *n -ární relace* (nebo *relace arity n* nebo jen *relace*) R je podmnožina kartézského součinu

$$R \subseteq A_1 \times \dots \times A_n.$$

- Je-li $A_1 = \dots = A_n = A$, mluvíme o *n -ární relaci na množině A* .
- *Unární* relace je relace arity 1 $R \subseteq A$, tj. podmnožina.
- Dále se budeme zabývat jen binárními relacemi.

- *Binární* relace (mezi množinami A, B) je relace $R \subseteq A \times B$.
- *Definiční obor* relace $R \subseteq A \times B$ je množina

$$\{a \in A \mid \text{existuje } b \in B \text{ tak, že } (a, b) \in R\}.$$

- *Obor hodnot* relace $R \subseteq A \times B$ je množina

$$\{b \in B \mid \text{existuje } a \in A \text{ tak, že } (a, b) \in R\}.$$

- Alternativní notace $(a, b) \in R$: aRb nebo $R(a, b)$

Definice

Identita na množině A je binární relace

$$id_A = \{(a, a) \mid a \in A\} \subseteq A \times A.$$

Definice (Inverzní relace)

Inverzní relací k relaci $R \subseteq A \times B$ rozumíme relaci

$$R^{-1} = \{(b, a) \mid (a, b) \in R\} \subseteq B \times A.$$

- Platí $(R^{-1})^{-1} = R$.

Definice (Skládání relací)

Nechť $R \subseteq A \times B$ a $S \subseteq B \times C$ jsou relace. Jejich složením rozumíme relaci

$$S \circ R = \{(a, c) \mid \text{existuje } b \in B \text{ splňující } (a, b) \in R \text{ a } (b, c) \in S\}.$$

- $S \circ R$ se čte jako “ S po R ”.
- Platí $S \circ R \subseteq A \times C$.
- Skládání relací je asociativní: $T \circ (S \circ R) = (T \circ S) \circ R$

Definice (Vlastnosti relací)

Relace $R \subseteq A \times A$ na množině A se nazývá

- **reflexivní**, pokud platí $(a, a) \in R$ pro každé $a \in A$,
- **symetrická**, pokud $(a, b) \in R$ implikuje $(b, a) \in R$,
- **tranzitivní**, pokud $(a, b), (b, c) \in R$ implikuje $(a, c) \in R$,
- **antisymetrická**, pokud $(a, b), (b, a) \in R$ implikuje $a = b$,
- **úplná**, pokud pro každé $a, b \in A$ platí $(a, b) \in R$ nebo $(b, a) \in R$,
- **univerzální**, pokud pro každé $a, b \in A$ platí $(a, b), (b, a) \in R$.

Příklad

- Uvažte binární relaci R na množině $A = \{1, 2\}$:
$$R = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$$
- Jaké vlastnosti má tato relace?
- Změní se odpověď, uvážíme-li tutéž relaci na množině $A' = \{1, 2, 3\}$?

Příklad

- Uvažte binární relaci inkluze (\subseteq) na množině $\mathcal{P}(\{a, b\})$.
- Vypište všechny prvky této binární relace.
- Jaké vlastnosti má tato relace?

Definice (Ekvivalence)

Relace $R \subseteq A \times A$ se nazývá **ekvivalence**, jestliže R je reflexivní, symetrická a tranzitivní.

Definice

Bud' R ekvivalence na A . Pro $a \in A$ položíme $R_a = \{b \in A \mid (a, b) \in R\}$. Množinu R_a nazýváme **třída** relace ekvivalence R určená prvkem a .

Příklad

- Uvažte relaci R na \mathbb{N} : $(x, y) \in R \iff x \bmod 4 = y \bmod 4$.
- Kolik existuje různých tříd ekvivalence?

Věta

Bud' R ekvivalence na A a $a \in A$. Pak platí:

- 1 $a \in R_a$
- 2 $R_a = R_b \iff (a, b) \in R$
- 3 $R_a \cap R_b \neq \emptyset \iff R_a = R_b$

Důkaz

- 1 Plyne z reflexivity.



Věta

Bud' R ekvivalence na A a $a \in A$. Pak platí:

- 1 $a \in R_a$
- 2 $R_a = R_b \iff (a, b) \in R$
- 3 $R_a \cap R_b \neq \emptyset \iff R_a = R_b$

Důkaz

- 2 Nechť $R_a = R_b$. Jelikož $a \in R_a = R_b$, platí $(b, a) \in R$. Ze symetrie pak plyne i $(a, b) \in R$.

Nechť $(a, b) \in R$. Pak pro každé $c \in R_b$ platí $(b, c) \in R$. Z tranzitivity plyne $(a, c) \in R$ a tudíž $c \in R_a$. Tedy $R_b \subseteq R_a$. Ze symetrie R pak plyne i $R_a \subseteq R_b$. □

Věta

Bud' R ekvivalence na A a $a \in A$. Pak platí:

- 1 $a \in R_a$
- 2 $R_a = R_b \iff (a, b) \in R$
- 3 $R_a \cap R_b \neq \emptyset \iff R_a = R_b$

Důkaz

- 3 Nechť $R_a \cap R_b \neq \emptyset$. Pak existuje $c \in R_a \cap R_b$ a proto $(a, c), (b, c) \in R$. Ze symetrie a tranzitivity plyne $(a, b) \in R$ a tedy $R_a = R_b$.

Implikace " \Leftarrow " je zřejmá.



Definice (Rozklad)

Rozklad \mathcal{R} množiny A je množina $\mathcal{R} \subseteq \mathcal{P}(A)$ splňující

- pro každé $X \in \mathcal{R}$ platí $X \neq \emptyset$,
- $\bigcup_{X \in \mathcal{R}} X = A$,
- pro každé $X_1, X_2 \in \mathcal{R}$ platí $X_1 \cap X_2 \neq \emptyset \implies X_1 = X_2$.

$X \in \mathcal{R}$ se nazývá třída rozkladu \mathcal{R} .

- $\{A\}$ je nejhrubší rozklad množiny A (má pouze 1 třídu).
- $\{\{x\} \mid x \in A\}$ je nejjemnější rozklad.
- Ukážeme, že rozklady přesně odpovídají relacím ekvivalence.

Věta

Nechť \mathcal{R} je rozklad množiny A . Pak relace

$$R_{\mathcal{R}} = \{(a, b) \mid \text{existuje } X \in \mathcal{R} \text{ splňující } a, b \in X\}$$

je ekvivalence na A .

- $R_{\mathcal{R}}$ se nazývá *ekvivalence příslušná rozkladu \mathcal{R}* .
- Ekvivalence příslušná nejjemnějšímu rozkladu je identita.
- Ekvivalence příslušná nejhrubšímu rozkladu je univerzální relace.

Věta

Nechť R je ekvivalence na množině $A \neq \emptyset$. Pak množina

$$A/R = \{R_a \mid a \in A\}$$

je rozkladem množiny A .

- A/R se nazývá *faktorová množina* relace ekvivalence R na A .
- A/R se také nazývá *rozklad příslušný ekvivalenci R* .

Věta

Nechť A je neprázdná množina.

- *Je-li R ekvivalence na A , pak $R = R_{A/R}$.*
- *Je-li \mathcal{R} rozklad množiny A , pak $\mathcal{R} = A/R_{\mathcal{R}}$.*

Definice (Uspořádání)

Relace $R \subseteq A \times A$ se nazývá **(částečné) uspořádání** na A , jestliže R je reflexivní, antisymetrická a tranzitivní.

Je-li relace R navíc úplná, nazývá se **lineární uspořádání** nebo **totální uspořádání** na A .

- Uspořádání obvykle značíme \leq .
- $a < b$ je zkrácený zápis pro $a \leq b$ a $a \neq b$.
- Je-li $a \leq b$ nebo $b \leq a$, pak řekneme, že a, b jsou **srovnatelné**.
- V opačném případě jsou a, b **nesrovnatelné**.
- Příklad uspořádání na \mathbb{N} : $a \preceq b$ pokud a je dělitel b .

Definice

Dvojice (A, \leq) se nazývá **uspořádaná množina**, pokud \leq je uspořádání na A .

Dvojice (A, \leq) se nazývá **lineárně uspořádaná množina**, pokud \leq je lineární uspořádání na A .

Příklady

- Lineárně uspořádané množiny: (\mathbb{N}, \leq) , (\mathbb{Z}, \leq) , (\mathbb{Q}, \leq) , (\mathbb{R}, \leq) , ...
(\leq značí přirozené uspořádání na příslušném číselném oboru)
- Uspořádaná množina $(\mathcal{P}(\{a, b, c\}), \subseteq)$
- Uspořádaná množina $(\mathbb{N}, \{(1, i), (i, i) \mid i \in \mathbb{N}\})$

Příklad

- Uvažme množinu $\mathcal{P}(\{1, 2, \dots, 10\})$ s relací \preceq definovanou pro $X, Y \in \mathcal{P}(\{1, 2, \dots, 10\})$ jako
$$X \preceq Y \text{ pokud } X \text{ má nejvýše tolik prvků jako } Y.$$
- Je $(\mathcal{P}(\{1, 2, \dots, 10\}), \preceq)$ uspořádaná množina?

- Grafická reprezentace konečných uspořádaných množin.
- Použil *Henry Gustav Vogt* v roce 1895, zpopularizoval *Helmut Hasse* (1898–1979)

Hasseův diagram reprezentující uspořádanou množinu (A, \leq) je graf, kde

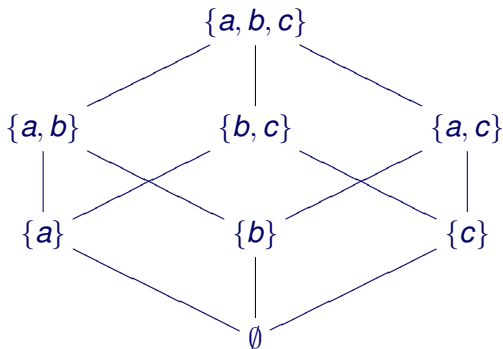
- vrcholy jsou prvky A
- z a vede hrana nahoru do b , pokud $a < b$, $a \neq b$ a neexistuje c splňující $a < c < b$.

Hasseův diagram: příklady

Potenční množina množiny $\{a, b, c\}$ s relací inkluze (podmnožina),
t.j. $(\mathcal{P}(\{a, b, c\}), \subseteq)$.

Hasseův diagram: příklady

Potenční množina množiny $\{a, b, c\}$ s relací inkluze (podmnožina), t.j. $(\mathcal{P}(\{a, b, c\}), \subseteq)$.

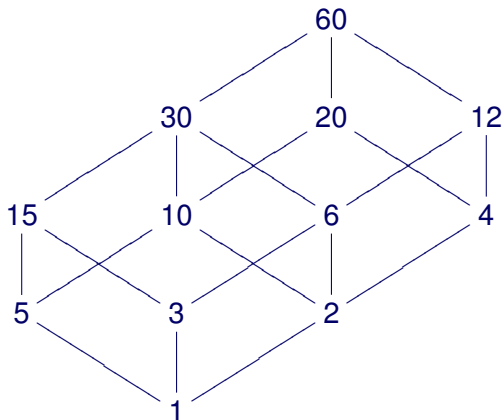


Hasseův diagram: příklady

Množina všech dělitelů čísla 60 uspořádaných relací dělitelnost.

Hasseův diagram: příklady

Množina všech dělitelů čísla 60 uspořádaných relací dělitelnost.



Největší, nejmenší, maximální a minimální prvek

Definice

Nechť (A, \leq) je uspořádané množina. Prvek $a \in A$ je

- **největší**, jestliže pro všechna $b \in A$ platí $b \leq a$,
- **nejmenší**, jestliže pro všechna $b \in A$ platí $a \leq b$,
- **maximální**, jestliže pro všechna $b \in A$ platí $a \leq b \implies a = b$,
- **minimální**, jestliže pro všechna $b \in A$ platí $b \leq a \implies a = b$.

- Existuje-li v množině největší prvek, pak je jediný. Navíc je i maximální a neexistuje jiný maximální prvek.
- Existuje-li v lineárně uspořádané množině maximální prvek, pak je to i prvek největší.
- Analogie platí i pro nejmenší a minimální prvky.
- Existují usp. množiny bez největšího a bez maximálního prvků?
A co množiny bez největšího prvku, ale s maximálními prvky?

Zobrazení

Definice (Zobrazení)

Zobrazení množiny A do množiny B , psáno $f : A \rightarrow B$ je relace $f \subseteq A \times B$ taková, že pro každé $a \in A$ existuje **právě jedno** $b \in B$ splňující $(a, b) \in f$.

Množinu všech zobrazení z A do B značíme B^A .

- Místo $(a, b) \in f$ obvykle píšeme $f(a) = b$, a je **vzor**, b **obraz**.
- Někdy se místo “právě jedno” požaduje “nejvýše jedno”. Tím se definuje **částečné zobrazení** neboli zobrazení z A do B . Pokud pro $a \in A$ neexistuje $b \in B$ splňující $(a, b) \in f$, říkáme, že zobrazení f není pro a definováno a píšeme $f(a) = \perp$.
- Chceme-li zdůraznit, že zobrazení není částečné, nazveme ho **totální**.
- Zobrazení se také nazývá **funkce**.

Definice (Injekce a surjekce)

Zobrazení $f : A \rightarrow B$ se nazývá

- *prosté (injektivní, injekce)*, jestliže $f(a_1) = f(a_2) \implies a_1 = a_2$,
- *zobrazení A na množinu B (surjektivní, surjekce)*, jestliže pro každé $b \in B$ existuje $a \in A$ splňující $f(a) = b$,

Příklady

- $f : \mathbb{N} \rightarrow \mathbb{N}$, kde $f(x) = 2x$ je prosté, ale není surjektivní.
- $f : \mathbb{N} \rightarrow \{1\}$, kde $f(x) = 1$ je surjektivní, ale není prosté.

Definice (Injekce a surjekce)

Zobrazení $f : A \rightarrow B$ se nazývá **bijektivní** nebo **bijekce**, jestliže je současně prosté i surjektivní.

Množiny A, B nazveme **izomorfní**, jestliže existuje bijekce $f : A \rightarrow B$, píšeme $A \cong B$.

Příklady

- $f : \{1, 2, 3\} \rightarrow \{3, 4, 5\}$, kde $f(x) = x + 2$ je bijekce.
- Množiny \mathbb{N} a \mathbb{Z} jsou izomorfní.

- Pojmy *definiční obor*, *obor hodnot* zůstávají stejné jako u relací.
- Inverzní relace k zobrazení nemusí být zobrazení.
- Inverzní relace k bijekci je bijekce.
- Skládání zobrazení se definuje stejně jako skládání relací.
- Identita na A je bijekce.

Věta

Nechť $f : A \rightarrow B$ a $g : B \rightarrow C$ jsou bijekce. Platí

- $f^{-1} \circ f = id_A$ a $f \circ f^{-1} = id_B$,
- $(f^{-1})^{-1} = f$,
- $g \circ f$ je bijekce a $(g \circ f)^{-1} = g^{-1} \circ f^{-1}$,
- $f \circ id_A = f = id_B \circ f$.

Číselné obory \mathbb{N} , \mathbb{Z} , \mathbb{Q} a \mathbb{R}

Definice (Přirozená čísla)

Necht' 0 značí prázdnou množinu \emptyset . Přirozená čísla lze definovat induktivně jako množiny:

$$n = \{0, 1, 2, \dots, n-1\}$$

Značíme $\mathbb{N} = \{1, 2, 3, 4, \dots\}$ a $\omega = \{0, 1, 2, 3, \dots\}$.

$$0 = \emptyset$$

$$1 = \{\emptyset\}$$

$$2 = \{\emptyset, \{\emptyset\}\}$$

$$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$$

$$4 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$$

\vdots

Množina odpovídající n má právě n prvků. Toho využijeme při definici uspořádání a operací.

- *uspořádání*

$$n \leq m \iff \text{existuje injekce } f : n \rightarrow m$$

- *sčítání*

$$n + m = k \text{ pro } k \cong (\{0\} \times n) \cup (\{1\} \times m)$$

- *násobení*

$$n \cdot m = k \text{ pro } k \cong (n \times m)$$

Definice (Celá čísla)

Necht' \sim je relace na množině $\omega \times \omega$ definovaná následovně:

$$(a, b) \sim (c, d) \iff a + d = c + b$$

Relace \sim je ekvivalence. \mathbb{Z} je rozklad $(\omega \times \omega) / \sim$, tedy celé číslo je třída rozkladu $(\omega \times \omega) / \sim$.

- Třidu ekvivalence obsahující (a, b) označíme $\overline{(a, b)}$.
- Třída $\overline{(a, b)}$ reprezentuje celé číslo $a - b$.
- Nezávisí na výběru reprezentanta:
 $(a, b) \sim (c, d) \implies a - b = c - d$

Uspořádání a operace na celých číslech

Pomocí reprezentantů definujeme uspořádání a operace nad \mathbb{Z} :

■ *uspořádání*

$$\overline{(a, b)} \leq \overline{(c, d)} \iff a + d \leq b + c$$

■ *sčítání*

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(a + c, b + d)}$$

■ *násobení*

$$\overline{(a, b)} \cdot \overline{(c, d)} = \overline{(ac + bd, ad + bc)}$$

Měli bychom dokázat, že v uvedené definice nezávisí na výběru reprezentantů, např. pro sčítání platí:

$$\left. \begin{array}{l} (a, b) \sim (a', b') \\ (c, d) \sim (c', d') \end{array} \right\} \implies (a + c, b + d) \sim (a' + c', b' + d')$$

Definice (Racionální čísla)

Nechť \sim je relace na množině $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ definovaná následovně:

$$(a, b) \sim (c, d) \iff ad = cb$$

Relace \sim je ekvivalence. \mathbb{Q} je rozklad $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \sim$, tedy racionální číslo je třída rozkladu $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \sim$.

- Třidu ekvivalence obsahující (a, b) označíme $\overline{(a, b)}$.
- Třída $\overline{(a, b)}$ reprezentuje racionální číslo $\frac{a}{b}$.
- Nezávisí na výběru reprezentanta: $(a, b) \sim (c, d) \implies \frac{a}{b} = \frac{c}{d}$

Uspořádání a operace na racionálních číslech

Pomocí reprezentantů definujeme i uspořádání a operace nad \mathbb{Q} :

- *uspořádání*

$$\overline{(a, b)} \leq \overline{(c, d)} \iff ad \leq bc$$

- *sčítání*

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)}$$

- *násobení*

$$\overline{(a, b)} \cdot \overline{(c, d)} = \overline{(ac, bd)}$$

Měli bychom dokázat, že v uvedené definice nezávisí na výběru reprezentantů, např. pro sčítání platí:

$$\left. \begin{array}{l} (a, b) \sim (a', b') \\ (c, d) \sim (c', d') \end{array} \right\} \implies (ad + bc, bd) \sim (a'd' + b'c', b'd')$$

Definice

Řez v množině \mathbb{Q} je dvojice (X, Y) , kde $X, Y \subseteq \mathbb{Q}$ splňují:

- 1 $X \cap Y = \emptyset$
- 2 $X \cup Y = \mathbb{Q}$
- 3 pro všechna $x \in X$ a $y \in Y$ platí $x < y$.

Řezy v \mathbb{Q} jsou jednoho z následujících tří typů:

- **mezera**: X nemá největší prvek a Y nemá nejmenší prvek
- **dedekindovský řez 1.druhu**: X má největší prvek a Y nemá nejmenší prvek
- **dedekindovský řez 2.druhu**: X nemá největší prvek a Y má nejmenší prvek

\mathbb{R} je množina všech řezů, které jsou mezerami nebo dedekindovskými řezy 1. druhu.

- Mezery odpovídají *iracionálním číslům*, dedekindovské řezy 1. druhu racionálním číslům.
- Neexistují řezy (X, Y) , kde X má největší prvek a Y nejmenší prvek. (Protože \mathbb{Q} je hustá množina.)
- Řez (X, Y) reprezentuje nejmenší číslo $r \in \mathbb{R}$ splňující $x \leq r$ pro všechna $x \in X$.
- Kupříkladu π odpovídá mezeře

$$(\{x \in \mathbb{Q} \mid x \leq \pi\}, \{x \in \mathbb{Q} \mid x > \pi\}).$$

■ *uspořádání*

$$(X, Y) \leq (X', Y') \iff X \subseteq X'$$

■ *sčítání*

$$(X, Y) + (X', Y') = (X + X', Y + Y')$$

■ *násobení*

$$(X, Y) \cdot (X', Y') = (X \cdot X', Y \cdot Y')$$

kde

$$\begin{aligned} X + Y &= \{x + y \mid x \in X, y \in Y\} \\ X \cdot Y &= \{x \cdot y \mid x \in X, y \in Y\} \end{aligned}$$

Mohutnost

Definice

Jestliže existuje bijekce mezi množinami A, B (tj. $A \cong B$), pak také říkáme, že A a B mají **stejnou mohutnost**.

Definice (Konečnost)

Množina A je **konečná**, jestliže má stejnou mohutnost jako některá z množin $n = \{0, 1, 2, \dots, n-1\}$, kde $n \in \omega$. V opačném případě je množina **nekonečná**.

- Mohutností množiny A rozumíme “počet prvků v množině A ” a značíme $|A|$.
- Pro konečné množiny platí $|A \times B| = |A| \cdot |B|$.
- Množiny \mathbb{Z} a $2\mathbb{Z} = \{2x \mid x \in \mathbb{Z}\}$ mají stejnou mohutnost neboť zobrazení $f : \mathbb{Z} \rightarrow 2\mathbb{Z}$ dané předpisem $f(x) = 2x$ je bijekce.

Definice (Spočetnost)

*Množina, která má stejnou mohutnost jako ω se nazývá **spočetná**. Množina, která je konečná nebo spočetná se nazývá **nejvýše spočetná**. Ostatní množiny jsou **nespočetné**.*

Někdy se jako spočetná množina označuje každá množina, která má stejnou mohutnost jako libovolná podmnožina ω , tedy i každá konečná množina je spočetná.

Hrátky s nekonečnem: spočetný hotel.

Věta

Množiny \mathbb{N} a \mathbb{Z} jsou spočetné.

Důkaz

Existují bijekce $f : \omega \rightarrow \mathbb{N}$ a $g : \omega \rightarrow \mathbb{Z}$ dané předpisem:

$$f(x) = x + 1 \quad g(n) = \begin{cases} \frac{n}{2} & \text{je-li } n \text{ sudé} \\ -\frac{n+1}{2} & \text{je-li } n \text{ liché} \end{cases} \quad \square$$

Věta

Množina \mathbb{Q} je spočetná.

Důkaz

Stačí dokázat pro kladná rac. čísla \mathbb{Q}^+ (dále dle důkazu pro \mathbb{Z}).
Reprezentujme \mathbb{Q}^+ nekonečnou tabulkou: v i -tém řádku jsou seřazeny všechny vykrácené zlomky s čitatelem i .

1	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$...
2	$\frac{2}{3}$	$\frac{2}{5}$	$\frac{2}{7}$...
3	$\frac{3}{2}$	$\frac{3}{4}$	$\frac{3}{5}$...
⋮	⋮	⋮	⋮	⋮

Čísla seřadíme do posloupnosti po diagonálách: $1, \frac{1}{2}, 2, \frac{1}{3}, \frac{2}{3}, 3, \dots$
Nyní stačí číslu ω přiřadit číslo z \mathbb{Q}^+ na příslušné pozici. Tím je popsána bijekce a \mathbb{Q}^+ je spočetná. □

Věta (Cantorova věta)

Množiny A a $\mathcal{P}(A)$ nikdy nemají stejnou mohutnost.

Důkaz

Nechť A a $\mathcal{P}(A)$ mají stejnou mohutnost, tj. necht' $f : A \rightarrow \mathcal{P}(A)$ je bijekce. Položme

$$B = \{a \in A \mid a \notin f(a)\}.$$

Jelikož $B \subseteq A$ a f je bijekce, musí existovat $b \in A$ takové, že $f(b) = B$. Pak platí

$$b \in B \iff b \notin B$$

a to je spor. □

Tedy existují množiny, které jsou nespočetné: např. $\mathcal{P}(\mathbb{N})$.
(Tato množina zjevně není konečná.)

Věta

Množina \mathbb{R} je nespočetná.

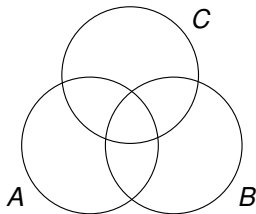
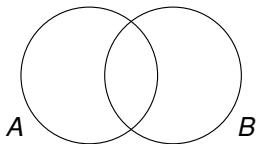
Důkaz

Ukážeme, že i interval reálných čísel $[0,1]$ je nespočetný. Předpokládáme, že existuje bijekce $f : \omega \rightarrow [0,1]$. Následující (nekonečná) tabulka tedy obsahuje všechna čísla z $[0,1]$.

$$\begin{array}{rcccccc} f(0) & = & 0, & 5 & 1 & 0 & \dots \\ f(1) & = & 0, & 4 & 1 & 3 & \dots \\ f(2) & = & 0, & 8 & 2 & 4 & \dots \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \ddots \\ \hline r & = & 0, & 6 & 2 & 5 & \dots \end{array}$$

Zkonstruujeme číslo r , které se bude lišit od každého čísla v tabulce (alespoň v číslici na diagonále). Jelikož r je číslo z $[0,1]$ a není v tabulce, dostáváme spor. □

Princip inkluze a exkluze



Věta (Princip inkluze a exkluze)

Pro libovolné konečné množiny A, B, C platí:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$$

- Slouží pro praktické výpočty počtu prvků v množině či v průniku.
- Lze zobecnit pro libovolný počet konečných množin A_1, A_2, \dots, A_n :

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{\emptyset \neq I \subseteq \{1, 2, \dots, n\}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right|$$