(LOTEM 2017/18, handout k §3.1)

3. Základní množinové pojmy

3.1 Vybrané prerekvizity

Značení. Uspořádanou dvojici prvků a, b značíme $\langle a, b\rangle$, uzavřený interval od a do b značíme $[a, b]$, otevřený (a, b).

Číselné obory. Předpokládáme znalost běžných pojmů středoškolské matematiky, zejména následujících číselných oborů a jejich aritmetiky:

- *Přirozená čísla* $0, 1, 2, 3, \ldots$

  Číslo 0 budeme vždy zahrnovat mezi přirozená čísla. Pro tvrzení o přirozených číslech předpokládáme znalost metody důkazu matematickou indukcí.

- *Celá čísla,* tj. čísla přirozená spolu s celými zápornými čísly $-1, -2, \ldots$

- *Racionální čísla* definujeme jako zkrácené celočíselné zlomky s nenulovým jmenovatelem.

- *Reálná čísla* nám postačí chápat jako nekonečné desetinné rozvoje, s touto výhradou:

  Protože některá reálná čísla mají dva desetinné rozvoje (např. 1,0000… = 0,9999…), pro zachování jednoznačnosti *vyloučíme* rozvoje s koncovou periodou 9. Podobně pro číselné soustavy o jiném základu – např. číslo 2/3 ztotožňujeme s trojkovým rozvojem 0,2000… a vylučujeme rozvoj 0,1222…

  Reálná čísla jsou souřadnicemi bodů v eukleidovských prostorech, tj. jsou v jednoznačné korespondenci s body přímky, jejich uspořádané dvojice s body roviny atd.

- *Komplexní čísla* můžeme ztotožnit s uspořádanými dvojicemi čísel reálných.

- *Algebraická čísla* jsou (komplexní) kořeny celočíselných polynomů.

(LOTEM 2017/18, handout k §3.2)

3.2 Pojem množiny

Počátky teorie množin. Studium množin bylo motivováno potřebou matematické analýzy zkoumat stále složitější části reálné přímky (obory spojitosti trigonometrických rozvojů apod.). Pojem množiny zavedl Bernard Bolzano (kniha Paradoxy nekonečna, vyd. 1851), systematicky jej začal zkoumat Georg Cantor od roku 1873.

Bernard Bolzano

Georg Cantor

Cantorova definice množiny. Zpočátku budeme vycházet z Cantorovy neformální definice množiny (1895):

> „Množinou“ rozumíme souhrn M konkrétních rozlišených objektů našeho vnímání nebo myšlení (jež budeme nazývat „prvky“ M) v jeden celek.

Příklady množin:

- Množina $\mathbb{N}$ všech přirozených čísel; $\mathbb{Z}$ všech celých čísel; $\mathbb{Q}$ všech racionálních čísel; $\mathbb{R}$ všech reálných čísel; $\mathbb{C}$ všech komplexních čísel.
- Interval $[a, b]$ definujeme jako množinu všech reálných čísel x takových, že $a \leq x \leq b$. Geometrické útvary chápeme jako množiny bodů.

Náležení prvku do množiny.

- Zápis $x \in A$ vyjadřuje, že x je prvkem množiny A. Příklady: $3 \in \mathbb{N}$, $\pi \in \mathbb{R}$.
- Zápis $x \notin A$ vyjadřuje, že x není prvkem množiny A. Příklady: $-1 \notin \mathbb{N}$, $\sqrt{2} \notin \mathbb{Q}$.

Z hlediska logiky je $\in$ binární predikát, zvaný *predikát náležení.* Zápis $x \notin A$ lze chápat jako zkratku za $\neg(x \in A)$.

Principy teorie množin. Cantorova definice je jen výchozím vymezením pojmu množiny, které bude třeba v několika ohledech upřesnit. Tato upřesnění budeme nazývat množinovými *principy.*

Princip dvojhodnotovosti. V klasické teorii množin uvažujeme pouze takové množiny A, že pro všechny prvky x platí buď $x \in A$, nebo $x \notin A$. (Též nazýváno *princip bivalence.*)

Za množiny tedy nepovažujeme např. vágně vymezené souhrny s nejasnou hranicí (souhrn všech *vysokých* lidí, všech *malých* čísel apod.), souhrny paradoxní (jako je souhrn A všech objektů, které nejsou prvkem A) atp. Těmi se zabývají různé *neklasické* teorie množin (např. teorie fuzzy množin); v tomto kurzu se však omezíme na klasickou („Cantorovu“) teorii množin.

Princip extenzionality. Množiny považujeme za určené svými prvky. Tzn. má-li množina A tytéž prvky jako množina B (bez ohledu na pořadí, způsob zadání apod.), jde o tutéž množinu $A = B$ (tentýž souhrn prvků).

Formálně: $(\forall x)(x \in A \leftrightarrow x \in B) \rightarrow A = B$.

Příklad: $\{x \in \mathbb{R} \mid x^2 - 1 < 0\} = \{x \in \mathbb{R} \mid \sum_{n=1}^{\infty} |x|^n < +\infty\}$

Uvědomte si: opačná implikace k principu extenzionality plyne z logických axiomů rovnosti.

Důsledek:

- K důkazu $A = B$ stačí ukázat, že pro kterýkoli prvek x je $x \in A \leftrightarrow x \in B$ (ekvivalence, ne implikace!). Příklad: $\mathbb{R} = (-\infty, +\infty)$, neboť $x \in \mathbb{R} \leftrightarrow -\infty < x < +\infty$.
- K důkazu nerovnosti dvou množin stačí najít prvek jedné z nich, který není prvkem té druhé. Příklad: $\mathbb{R} \neq \mathbb{Q}$, neboť $\sqrt{2} \in \mathbb{R}$, ale $\sqrt{2} \notin \mathbb{Q}$.

Komprehenzní termy.

- Množinu, do které náležejí právě prvky $a_1, \ldots, a_n$, značíme $\{a_1, \ldots, a_n\}$.

  Jsou-li prvky množiny členy pravidelné posloupnosti, můžeme to vyznačit trojtečkou, např. $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.
- Množinu právě těch prvků x, které mají vlastnost Φ, značíme $\{x \mid \Phi\}$; např.:

  $$\begin{aligned} \{2, 4, 6, 8, \ldots\} &= \{2n \mid n \in \mathbb{N} \;\&\; n > 0\}; \\ \{a_1, \ldots, a_n\} &= \{x \mid x = a_1 \vee \ldots \vee x = a_n\}. \end{aligned}$$

  Pozorujte: $z \in \{x \mid \Phi(x)\} \leftrightarrow \Phi(z)$.

  Místo $\{x \mid x \in A \;\&\; \Psi\}$ lze psát stručněji $\{x \in A \mid \Psi\}$, např.: $\mathbb{N} = \{z \in \mathbb{Z} \mid z \geq 0\}$.

Cvičení:

1. Může jeden komprehenzní term označovat dvě různé množiny? Mohou dva různé komprehenzní termy označovat tutéž množinu?
2. Dokažte (zdůvodněte vždy *oba* směry ekvivalence):
   (a) $\{a, b\} = \{a, b, c\} \leftrightarrow (a = c \vee b = c)$;
   (b) $\{1, x\} \neq \{z, 2\} \leftrightarrow (x \neq 2 \vee z \neq 1)$.
3. Dokažte, že množina všech kořenů polynomů s celočíselnými koeficienty je rovna množině všech kořenů polynomů s racionálními koeficienty.
4. Dokažte, nebo vyvraťte: $\{2n \mid n \in \mathbb{N} \;\&\; n > 1\} = \{p + q \mid p, q \text{ prvočísla}\}$. (Řešte až po vyřešení všech ostatních úloh.)

(LOTEM 2017/18, handout k §3.3)

3.3 Elementární teorie množin

Inkluze. Říkáme, že množina A je *podmnožinou* (též: *částí*) množiny B a píšeme $A \subseteq B$, jestliže každý prvek množiny A je zároveň prvkem množiny B. Formálně:

$$A \subseteq B \equiv_{\mathrm{df}} (\forall x)(x \in A \to x \in B).$$

Vztah $\subseteq$ nazýváme *inkluze.* Zápis $\neg(A \subseteq B)$ zkracujeme $A \nsubseteq B$. Vztah $A \subseteq B \mathbin{\&} A \neq B$ bývá zapisován $A \subset B$ či $A \subsetneq B$ a hovoříme o *ostré inkluzi* a *vlastní podmnožině.*

Inkluze a náležení. Inkluzi a náležení je třeba pečlivě rozlišovat: náležení je vztah prvku a množiny (do které patří), inkluze je vztah dvou množin (daný náležením prvků). Příklady:

- Číslo π je prvkem, ale nikoli částí množiny $\mathbb{R}$ (je to reálné číslo, nikoli množina reálných čísel). Symbolicky: $\pi \in \mathbb{R}$, ale $\pi \nsubseteq \mathbb{R}$.
- Množina $\mathbb{N}$ je částí, ale nikoli prvkem množiny $\mathbb{Z}$ (každé přirozené číslo je celé, ale množina všech přirozených čísel není celé číslo). Symbolicky: $\mathbb{N} \subseteq \mathbb{Z}$, ale $\mathbb{N} \notin \mathbb{Z}$.

Vlastnosti inkluze.

1. $A \subseteq A$
2. $A \subseteq B \mathbin{\&} B \subseteq C \to A \subseteq C$
3. $A \subseteq B \mathbin{\&} B \subseteq A \to A = B$

Důkaz:

1. Každý prvek množiny A je prvkem množiny A, tedy $A \subseteq A$.
2. Nechť $A \subseteq B$ a $B \subseteq C$. Pak každé $x \in A$ musí být i prvkem B (neboť $A \subseteq B$), a tedy i prvkem C (neboť $B \subseteq C$). Dle definice tedy $A \subseteq C$.
3. Podle předpokladu $A \subseteq B \mathbin{\&} B \subseteq A$ je každý prvek množiny A i prvkem množiny B a každý prvek množiny B i prvkem množiny A. Obě množiny tudíž mají stejné prvky, podle principu extenzionality jsou tedy totožné. ☐

Inkluze a rovnost. Podle 3. vlastnosti inkluze stačí k důkazu rovnosti dvou množin dokázat oba směry inkluze. K tomu přitom podle principu extenzionality stačí ukázat, že libovolně zvolený prvek jedné množiny je i prvkem druhé a naopak; to je častá metoda důkazu rovnosti či jednoznačnosti množin v celé matematice (nejen v teorii množin).

Prázdná množina. Množinu, která nemá žádné prvky, nazýváme *prázdnou množinou* a označujeme $\emptyset$. Příklad: $\{x \in \mathbb{R} \mid x^2 = -1\} = \emptyset$.

Protože $x = x$ je logický axiom, lze $\emptyset$ definovat např. jako množinu $\{x \mid x \neq x\}$. Z principu extenzionality plyne, že existuje *jediná* prázdná množina (zdůvodněte!). Prázdná množina není totéž, co „nic“: spíše ji lze přirovnat k „prázdné přihrádce“, „prázdnému měšci“ atp.

Tvrzení: Prázdná množina je částí každé množiny: $\emptyset \subseteq A$. (Dokažte.)

Jednoprvkové množiny. V teorii množin je třeba pečlivě rozlišovat *prvek* x od *jednoprvkové množiny* $\{x\}$. Jednoprvkovým množinám se též říká *singletony* (angl., česky slangově).

Příklad: π je *reálné číslo,* kdežto singleton $\{\pi\}$ je *množina* (reálných čísel, shodou okolností s jediným prvkem); $\pi \in \mathbb{R}$, ale $\{\pi\} \notin \mathbb{R}$. (Je však $\{\pi\} \subseteq \mathbb{R}$.) Platí $\pi \in \{\pi\}$, ale $\pi \nsubseteq \{\pi\}$.

Tvrzení: $\{a\} = \{b\}$, právě když $a = b$. (Zdůvodněte.)

Elementární množinové operace. Definujeme *sjednocení, průnik* a *rozdíl* množin A, B:

$$\begin{aligned}
A \cup B &=_{\mathrm{df}} \{x \mid x \in A \vee x \in B\}, &&\text{tj.}\quad x \in A \cup B \leftrightarrow x \in A \vee x \in B;\\
A \cap B &=_{\mathrm{df}} \{x \mid x \in A \mathbin{\&} x \in B\}, &&\text{tj.}\quad x \in A \cap B \leftrightarrow x \in A \mathbin{\&} x \in B;\\
A \smallsetminus B &=_{\mathrm{df}} \{x \mid x \in A \mathbin{\&} x \notin B\}, &&\text{tj.}\quad x \in A \smallsetminus B \leftrightarrow x \in A \mathbin{\&} x \notin B.
\end{aligned}$$

Je-li $B \subseteq A$, říká se rozdílu $A \smallsetminus B$ také *doplněk* B do A.

Příklad: Množinu všech iracionálních čísel definujeme jako $\mathbb{R} \smallsetminus \mathbb{Q}$.

Mají-li množiny A a B prázdný průnik, říkáme, že jsou *disjunktní.* Příklady: $[0, 1]$ a $[2, 3]$ jsou disjunktní intervaly; $\mathbb{Z}$ je disjunktní s $\mathbb{R} \smallsetminus \mathbb{Q}$.

Vlastnosti elementárních množinových operací. Elementární množinové operace dědí vlastnosti výrokových spojek, jimiž jsou definovány. Z platných výrokových ekvivalencí plynou odpovídající množinové identity (a z implikací odpovídající inkluze).

Příklad: $(A \cap B) \cup (A \smallsetminus B) = A$, neboť výrokově platí (ověřte!): $\models (p \mathbin{\&} q) \vee (p \mathbin{\&} \neg q) \leftrightarrow p$.

Důkaz. $x \in (A \cap B) \cup (A \smallsetminus B) \longleftrightarrow (\underbrace{x \in A}_{p} \mathbin{\&} \underbrace{x \in B}_{q}) \vee (\underbrace{x \in A}_{p} \mathbin{\&} \underbrace{x \notin B}_{\neg q}) \longleftrightarrow \underbrace{x \in A}_{p}.$ □

Podobně např. $\models p \mathbin{\&} \neg q \to p$, pročež $A \smallsetminus B \subseteq A$ (dokažte podrobně).

Tato pozorování lze zobecnit a dokázat indukcí dle stavby výrokových formulí. Inkluze a identity elementárních množinových operací se tak redukují na výrokový počet, a tím trivializují: lze je ověřovat např. *tabulkovou metodou* nebo *Vennovými diagramy.* Netriviální partie teorie množin se týkají hlavně situací, kdy uvažujeme nejen množiny prvků, ale i množiny množin.

Cvičení:

1. Určete, která tvrzení platí: $5 \in \{5\}$, $5 \subseteq \{5\}$, $\{5\} \in \mathbb{N}$, $\{5\} \subseteq \mathbb{N}$.

2. Dokažte:

    (a) $X \subseteq A \cap B \leftrightarrow X \subseteq A \wedge X \subseteq B$;
    (b) $X \subseteq A \vee X \subseteq B \to X \subseteq A \cup B$.

    Najděte protipříklad k obrácené implikaci v (b).

3. Dokažte distributivní a De Morganovy zákony:

$$\begin{aligned}
A \cap (B \cup C) &= (A \cap B) \cup (A \cap C), \qquad & X \smallsetminus (A \cup B) &= (X \smallsetminus A) \cap (X \smallsetminus B),\\
A \cup (B \cap C) &= (A \cup B) \cap (A \cup C), \qquad & X \smallsetminus (A \cap B) &= (X \smallsetminus A) \cup (X \smallsetminus B).
\end{aligned}$$

(LOTEM 2017/18, handout k §3.4)

3.4 Množiny množin

Množiny jako prvky množin. Dle Cantorovy definice je množina souhrnem prvků v *jeden celek,* tedy konkrétním rozlišeným objektem našeho myšlení. Podle téže definice proto může být prvkem dalších množin.

Příklady: množina všech podmnožin $\mathbb{R}$, množina všech reálných intervalů, množina všech dvouprvkových množin přirozených čísel atp.

Náležení do prvku množiny. Vedle náležení a inkluze je také třeba pečlivě rozlišovat náležení do *množiny* od náležení do *prvku množiny.*

- Prvek prvku množiny A nemusí být prvkem A. Příklad: Nechť $A = \{\{1,2,3\},\{3,4,5\}\}$. Pak $1 \notin A$; pouze $1 \in \{1,2,3\} \in A$. Pozorujte: $\{1,2,3\}$ není částí, nýbrž prvkem A.
- Prvek množiny může být zároveň její částí. Příklad: $\emptyset \in \{\emptyset\}$ a také $\emptyset \subseteq \{\emptyset\}$. (Rozlišujte: $\emptyset \neq \{\emptyset\} \neq \{\{\emptyset\}\}$ – zdůvodněte!) Pozorujte: $\emptyset$ i $\{\emptyset\}$ jsou zároveň prvkem i částí $\{\emptyset,\{\emptyset\}\}$.

Potenční množina. Množina všech podmnožin množiny A se nazývá *potencí* množiny A a značí se $\mathscr{P}(A)$. Formálně: $\mathscr{P}(A) =_{\mathrm{df}} \{X \mid X \subseteq A\}$.

Příklady:

- $\mathscr{P}(\{a,b\}) = \{\emptyset,\{a\},\{b\},\{a,b\}\}$.
- Jsou-li $a_1,\dots,a_n$ vzájemně různé, pak $\mathscr{P}(\{a_1,\dots,a_n\})$ má 2^n prvků (zdůvodněte!).
- $\mathscr{P}(\{a\}) = \{\emptyset,\{a\}\}$, $\mathscr{P}(\emptyset) = \{\emptyset\}$, $\mathscr{P}(\mathscr{P}(\emptyset)) = \mathscr{P}(\{\emptyset\}) = \{\emptyset,\{\emptyset\}\}$.
- $\mathscr{P}(\mathbb{Z}) = \{X \mid X \subseteq \mathbb{Z}\}$ je množina všech množin celých čísel, obdobně $\mathscr{P}(\mathbb{R})$, $\mathscr{P}(\mathscr{P}(\mathbb{N}))$ atp.

Vlastnosti potence.

1. $\mathscr{P}(A) \subseteq \mathscr{P}(B)$, právě když $A \subseteq B$.
2. $\mathscr{P}(A \cap B) = \mathscr{P}(A) \cap \mathscr{P}(B), \quad \mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$

Důkaz:

1. Nechť $\mathscr{P}(A) \subseteq \mathscr{P}(B)$, tj. $(\forall X)(X \subseteq A \to X \subseteq B)$. Speciálně tedy:
$$(\forall x)\big(\underbrace{\{x\} \subseteq A}_{\leftrightarrow\, x\in A} \to \underbrace{\{x\} \subseteq B}_{\leftrightarrow\, x\in B}\big), \text{ tj. } A \subseteq B.$$
Naopak, nechť $A \subseteq B$. Pak pro libovolnou množinu X dostáváme: $X \in \mathscr{P}(A) \longleftrightarrow X \subseteq A \subseteq B \longrightarrow X \subseteq B \longleftrightarrow X \in \mathscr{P}(B)$; tedy $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.
2. $X \in \mathscr{P}(A \cap B) \longleftrightarrow X \subseteq A \cap B \overset{\S 3.3}{\longleftrightarrow} X \subseteq A \wedge X \subseteq B \longleftrightarrow$
$\longleftrightarrow X \in \mathscr{P}(A) \wedge X \in \mathscr{P}(B) \longleftrightarrow X \in \mathscr{P}(A) \cap \mathscr{P}(B)$.
Druhé tvrzení dokažte obdobně (k obrácené inkluzi najděte protipříklad). $\square$

Sjednocení a průnik množiny množin.

Sjednocení množiny množin $\mathscr{A}$ je množina všech prvků, které náleží *alespoň jednomu* prvku množiny $\mathscr{A}$. Značení: $\bigcup\mathscr{A}$.

Průnik množiny množin $\mathscr{A}$ je množina všech prvků, které náleží *všem* prvkům množiny $\mathscr{A}$. Značení: $\bigcap\mathscr{A}$. Formálně:

$$x \in \bigcup\mathscr{A} \leftrightarrow (\exists A)(A \in \mathscr{A} \wedge x \in A), \quad \text{tj. } \bigcup\mathscr{A} =_{\mathrm{df}} \{x \mid (\exists A \in \mathscr{A})(x \in A)\}$$
$$x \in \bigcap\mathscr{A} \leftrightarrow (\forall A)(A \in \mathscr{A} \rightarrow x \in A), \quad \text{tj. } \bigcap\mathscr{A} =_{\mathrm{df}} \{x \mid (\forall A \in \mathscr{A})(x \in A)\}$$

Časté značení: $\bigcup\limits_{i\in I} A_i =_{\mathrm{df}} \bigcup\{A_i \mid i \in I\}$, $\bigcup\limits_{i=0}^{\infty} A_i =_{\mathrm{df}} \bigcup\{A_i \mid i \in \mathbb{N}\}$, obdobně pro $\bigcap$.

Vlastnosti sjednocení a průniku.

1. $\bigcup\{A,B\} = A\cup B, \quad \bigcap\{A,B\} = A\cap B, \quad \bigcup\{A\} = \bigcap\{A\} = A, \quad \bigcup\emptyset = \bigcup\{\emptyset\} = \bigcap\{\emptyset\} = \emptyset$
2. Jestliže $A \in \mathscr{A}$, pak $\bigcap\mathscr{A} \subseteq A \subseteq \bigcup\mathscr{A}$.
   Jestliže $\emptyset \neq \mathscr{A} \subseteq \mathscr{B}$, pak $\bigcup\mathscr{A} \subseteq \bigcup\mathscr{B}$ a $\bigcap\mathscr{B} \subseteq \bigcap\mathscr{A}$.
3. $\bigcup\mathscr{P}(A) = A, \quad \bigcap\mathscr{P}(A) = \emptyset, \quad \mathscr{A} \subseteq \mathscr{P}\big(\bigcup\mathscr{A}\big)$
4. $A \cap \bigcup\mathscr{B} = \bigcup\{A \cap B \mid B \in \mathscr{B}\}, \quad A \smallsetminus \bigcup\mathscr{B} = \bigcap\{A \smallsetminus B \mid B \in \mathscr{B}\},$
   $A \cup \bigcap\mathscr{B} = \bigcap\{A \cup B \mid B \in \mathscr{B}\}, \quad A \smallsetminus \bigcap\mathscr{B} = \bigcup\{A \smallsetminus B \mid B \in \mathscr{B}\}$

Důkaz. Dokážeme jen první část tvrzení 4, ostatní dokažte sami z definic.

$$\begin{aligned} x \in \bigcup\{A \cap B \mid B \in \mathscr{B}\} &\longleftrightarrow x \in A \cap B \text{ pro nějakou } B \in \mathscr{B} \\ &\longleftrightarrow x \in A \wedge x \in B \text{ pro nějakou } B \in \mathscr{B} \\ &\longleftrightarrow x \in A \wedge x \in \bigcup\mathscr{B} \longleftrightarrow x \in A \cap \bigcup\mathscr{B}. \end{aligned}$$

□

Nefundované množiny. Může být množina svým vlastním prvkem, např. $X = \{X\}$ či $Y = \{a, Y\}$? Aparát teorie množin pro takové množiny funguje dobře, lze ale proti nim mít konceptuální námitky: shrnujeme v jeden celek prvky, které jsou teprve tímto shrnutím vytvářeny. Tutéž výhradu lze mít i vůči cyklům náležení jako $X = \{\{\{X\}\}\}$ a nekonečným sestupům náležení, např. $\{\{\{\{\ldots\ \ldots\}\}\}\}$. Jako další vyjasnění Cantorovy definice se proto často přijímá *princip fundovanosti,* který je vylučuje.

Princip fundovanosti. Množiny musejí být *fundované,* tj. vztahem náležení $\in$ z nich nezískáme žádnou nekonečnou sestupnou posloupnost $A \ni X_1 \ni X_2 \ni X_3 \ni \ldots$ (vč. cyklů).

Tj. sestupem podle $\in$ musíme v každé cestě dříve či později narazit na prvek, který již nemá prvky (čili na $\emptyset$ nebo na *urelement* = prvek, který není množinou). Alternativní název: princip *regularity.*

Cvičení:

1. Označme $\mathcal{A}_2 = \{\emptyset, \{\emptyset\}\}$. Určete výčtem prvků: $\mathscr{P}(\mathcal{A}_2)$, $\bigcup\mathcal{A}_2$, $\bigcap\mathcal{A}_2$.
2. Jestliže $X \in \mathscr{A}$, pak $\bigcap\mathscr{A} \in \mathscr{P}(X)$. Dokažte.
3. Dokažte: $A \cup \bigcup\mathscr{B} = \bigcup\{A \cup B \mid B \in \mathscr{B}\}$, a obdobně pro průnik.
4. V teorii množin bez principu fundovanosti mějme $X = \{\{a\}, X\}$. Určete: $\mathscr{P}(X)$, $\bigcup X$, $\bigcap X$.

(LOTEM 2017/18, handout #1 k §3.5)

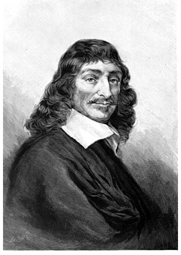
3.5 Relace

Kartézský součin. *Kartézský součin* dvou množin A, B je množina všech uspořádaných dvojic $\langle a, b\rangle$ takových, že $a \in A$ a $b \in B$. Značení: $A \times B$.

Kartézský součin n množin $A_1, \dots, A_n$ je množina všech uspořádaných n-tic $\langle a_1, \dots, a_n\rangle$ takových, že $a_1 \in A_1$, …, $a_n \in A_n$. Značení: $A_1 \times \dots \times A_n$. Formálně:

$$A \times B =_{\mathrm{df}} \{\langle a, b\rangle \mid a \in A \wedge b \in B\}$$
$$A_1 \times \dots \times A_n =_{\mathrm{df}} \{\langle a_1, \dots, a_n\rangle \mid a_1 \in A_1 \wedge \ldots \wedge a_n \in A_n\}$$

Je-li $A_1 = A_2 = \dots = A_n$, hovoříme o *kartézské mocnině* $A^n =_{\mathrm{df}} A \times \dots \times A$. Příklad: $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ (srv. kartézskou soustavu souřadnic v rovině).



René Descartes (Cartesius)

Vlastnosti kartézského součinu. (Tvrzení 3.–5. platí i pro opačné pořadí činitelů.)

1. $A \times \emptyset = \emptyset \times A = \emptyset$, $\quad A \times B = \emptyset \leftrightarrow A = \emptyset \vee B = \emptyset$
2. $A \times B = C \times D \neq \emptyset$, jen když $A = C$ a $B = D$.
3. $A \subseteq B \rightarrow A \times C \subseteq B \times C$
4. $A \times (B \cup C) = (A \times B) \cup (A \times C)$, $\quad A \times (B \setminus C) = (A \times B) \setminus (A \times C)$,
   $A \times (B \cap C) = (A \times B) \cap (A \times C)$
5. $A \times \bigcup \mathscr{B} = \bigcup\{A \times B \mid B \in \mathscr{B}\}$, $\quad A \times \bigcap \mathscr{B} = \bigcap\{A \times B \mid B \in \mathscr{B}\}$

Důkaz. Dokážeme pouze některá tvrzení, ostatní dokažte podobně sami.

2. Nechť $\langle x_0, y_0\rangle \in A \times B = C \times D$; tedy $x_0 \in A$, $y_0 \in B$ a také $x_0 \in C$, $y_0 \in D$. Pak: $x \in A \longleftrightarrow x \in A \wedge y_0 \in B \longleftrightarrow \langle x, y_0\rangle \in A \times B \longleftrightarrow \langle x, y_0\rangle \in C \times D \longleftrightarrow x \in C \wedge y_0 \in D \longleftrightarrow x \in C$; tedy $A = C$. Obdobně $B = D$. (Zdůvodněte všechny kroky důkazu!)
4. $\langle a, x\rangle \in A \times (B \cup C) \longleftrightarrow a \in A \wedge x \in B \cup C \longleftrightarrow a \in A \wedge (x \in B \vee x \in C) \longleftrightarrow (a \in A \wedge x \in B) \vee (a \in A \wedge x \in C) \longleftrightarrow \langle a, x\rangle \in A \times B \vee \langle a, x\rangle \in A \times C \longleftrightarrow \langle a, x\rangle \in (A \times B) \cup (A \times C)$. $\square$

Relace. Binární relace je vztah mezi dvěma objekty (n-ární relace je vztah mezi n objekty). Příklady:

- Vztah $\leq$ mezi reálnými čísly: $5 \leq 6$, $\pi \not\leq \sqrt{2}$.
- Dělitelnost (mezi celými čísly): $5 \mid 125$, $6 \nmid 10$.
- Rovnost (čísel, objektů, množin): $1 = 1$, $[0, +\infty) \neq \left(-\frac{\pi}{2}, +\frac{\pi}{2}\right)$.
- Inkluze (vztah dvou množin): $\emptyset \subseteq \{\emptyset\}$, $\mathbb{R} \not\subseteq \mathbb{Z}$.
- Relace náležení (vztah prvku a množiny): $5 \in \mathbb{R}$, $\{-1\} \notin \mathscr{P}(\mathbb{N})$.
- Příklad ternární relace: „C leží mezi A a B“.

Množinově lze relace modelovat jako množiny uspořádaných dvojic (resp. n-tic) objektů, kam zařadíme právě ty dvojice (n-tice), které jsou v daném vztahu (relaci).

Příklad: Relaci $\leq$ mezi reálnými čísly ztotožníme s množinou $R_{\leq} = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$. Pozorujte: $R_{\leq} \subseteq \mathbb{R} \times \mathbb{R}$.

Definice: *Binární relací* z množiny A do množiny B rozumíme jakoukoli podmnožinu kartézského součinu $A \times B$. (Je-li $A = B$, mluvíme o relaci *na* množině A.)

Formálně: $R \subseteq A \times B$ (n-ární: $R \subseteq A_1 \times \cdots \times A_n$). Relace na množině: $R \subseteq A^2$ (či $R \subseteq A^n$).

Značení: $\langle a, b\rangle \in R$ píšeme též Rxy či xRy.

Význačné obecné příklady:

- *Identita* na množině A je relace $\mathrm{Id}_A = \{\langle a, b\rangle \in A^2 \mid a = b\}$.
- Relace *inverzní* k relaci $R \subseteq A \times B$ je relace $R^{-1} = \{\langle b, a\rangle \mid Rab\} \subseteq B \times A$; např. $\leq^{-1} = \geq$.
- *Prázdná* relace $\emptyset \subseteq A \times B$; např. $\{\langle x, y\rangle \in \mathbb{R}^2 \mid |x - y| = +\infty\} = \emptyset \subseteq \mathbb{R}^2$.

  Plná relace $A \times B \subseteq A \times B$; např. $\{\langle x, y\rangle \in \mathbb{R}^2 \mid |x - y| < +\infty\} = \mathbb{R}^2 \subseteq \mathbb{R}^2$.

Všimněte si: relaci z A do B ztotožňujeme s množinou uspořádaných dvojic z $A \times B$, tj. jejím *grafem.* To je množinové (extenzionální) pojetí relací – ztotožňujeme relace, které mají stejný graf, bez ohledu na způsob jejich zadání (předpis), např. $\{\langle x, y\rangle \in \mathbb{R}^2 \mid x^4 = y^4\} = \{\langle x, y\rangle \in \mathbb{R}^2 \mid |x| = |y|\}$.

Kvůli principu bivalence (§3.2) uvažujeme v klasické teorii množin pouze dvouhodnotové (ano–ne) relace, kdy vztah buď platí, nebo neplatí. Vztahy, jež mohou platit ve větší či menší míře (např. „čísla x, y jsou si *blízká*“), je třeba zpřesnit na dvojhodnotové (např. $|x - y| < 0{,}1$); případně je lze modelovat funkcemi: např. definovat stupeň blízkosti jako $B(x, y) = 1/(1 + |x - y|)$.

Cvičení:

1. Dokažte $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$. (Platí totéž pro $\cup$ či $\setminus$? Které inkluze?)
2. Množiny $\{0\} \times A$ a $\{1\} \times B$ jsou vždy disjunktní. Zdůvodněte.
3. Je-li R binární relace na A, pak $R = R^{-1}$, právě když $R \subseteq \mathrm{Id}_A$. Dokažte.

(LOTEM 2017/18, **handout #2 k §3.5**)

Elementární vlastnosti binárních relací na množině. Nechť $R \subseteq A^2$. Řekneme, že:

- R je *reflexivní,* když $(\forall x \in A)Rxx$.

  Ekvivalentně: když $\mathrm{Id}_A \subseteq R$. Příklady: $=$, $\leq$, $\geq$, $\subseteq$, $\mid$ (dělitelnost) aj.

- R je *symetrická,* když $(\forall x, y \in A)(Rxy \to Ryx)$.

  Ekvivalentně: když $R^{-1} \subseteq R$ (nebo také, když $R^{-1} = R$ – zdůvodněte!).

  Příklady: $=$, $\equiv_n$ (kongruence modulo n), $\cong$ (shodnost geometrických útvarů) aj.

- R je *tranzitivní,* když $(\forall x, y, z \in A)(Rxy \wedge Ryz \to Rxz)$.

  Příklady: $=$, $\leq$, $\geq$, $<$, $>$, $\subseteq$, $\mid$, $\equiv_n$, $\cong$, $\sim$ (podobnost geometrických útvarů) aj.

- R je *antisymetrická,* když $(\forall x, y \in A)(Rxy \wedge Ryx \to x = y)$.

  Ekvivalentně: když $R \cap R^{-1} \subseteq \mathrm{Id}_A$. Příklady: $=$, $\leq$, $\geq$, $<$, $>$, $\subseteq$, $\mid$ na $\mathbb{N}$ (na $\mathbb{Z}$ ne) aj.

Relace ekvivalence. Binární relaci na A, která je reflexivní, symetrická a tranzitivní, nazýváme *relací ekvivalence* (krátce: *ekvivalencí*) na A.

Příklady: $=$, $\equiv_n$, $\cong$, $\sim$ aj.

Třídy ekvivalence. Pro ekvivalenci R na A a $x \in A$ nazveme množinu $[x]_R =_{\mathrm{df}} \{y \mid Rxy\}$ *třídou ekvivalence* prvku x.

Příklady: $[x]_= = \{x\}$, $[5]_{\equiv_3} = \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\}$.

Tvrzení: Různé třídy ekvivalence R jsou vzájemně disjunktní (tj. mají prázdný průnik).

Důkaz: Nechť y je v jiné třídě ekvivalence než x a nechť $z \in [x]_R \cap [y]_R$. Pak $Rxz \wedge Ryz$, ze symetrie R tedy také Rzy; z tranzitivity R tudíž Rxy, tj. $y \in [x]_R$ – spor. $\square$

Důsledek: Třídy ekvivalence tvoří *rozklad* množiny A (značený $A/R =_{\mathrm{df}} \{[x]_R \mid x \in A\}$).

Příklady: $A/\mathrm{Id}_A = \{\{x\} \mid x \in A\}$, $\mathbb{N}/{\equiv_2} = \{\{0, 2, 4, 6, \ldots\}, \{1, 3, 5, 7, \ldots\}\}$.

Fakt: Ekvivalence a rozklady na A si vzájemně odpovídají: ekvivalence určuje třídy rozkladu dle definice výše, rozklad určuje ekvivalenci „náležet stejné parketě rozkladu“ (rozmyslete).

Relace uspořádání. Binární relaci R na A, která je reflexivní, tranzitivní a antisymetrická, nazýváme *(částečným) uspořádáním* množiny A.

Platí-li navíc $(\forall x, y \in A)(Rxy \vee Ryx)$, mluvíme o *lineárním* uspořádání.

Příklady:

- $\leq$ je uspořádání na $\mathbb{R}$ a $\subseteq$ je uspořádání na $\mathscr{P}(A)$.
- $\leq$ je lineární na $\mathbb{R}$. Má-li A aspoň dva různé prvky, pak $\subseteq$ není lineární na $\mathscr{P}(A)$.
- $=$ je uspořádání (v němž jsou všechny prvky neporovnatelné).
- Relace $<$, $>$ (např. na $\mathbb{R}$) *nejsou* uspořádáními podle uvedené definice, která je šita na míru *neostrým* uspořádáním jako $\leq, \subseteq$. Od neostrých uspořádání se ale ostré relace $<, >$ liší jen o identitu: $< \; = \; \leq \setminus \mathrm{Id}_{\mathbb{R}}$ a naopak, $\leq \; = \; < \cup \, \mathrm{Id}_{\mathbb{R}}$.

Nejmenší a největší prvek množiny v uspořádání. Nechť $\leq$ je libovolné částečné uspořádání množiny X a nechť $A \subseteq X$. Řekneme, že:

- $a \in A$ je *nejmenší prvek* množiny A v uspořádání $\leq$, když $(\forall x \in A)(a \leq x)$.
- $a \in A$ je *největší prvek* množiny A v uspořádání $\leq$, když $(\forall x \in A)(x \leq a)$.

Příklady:

- V uspořádání reálných čísel podle velikosti:
  - Interval $[5, 10]$ má nejmenší prvek 5 a největší 10.
  - Polouzavřený interval $(5, 10]$ má největší prvek 10, ale nemá nejmenší prvek (proč?).
  - $\mathbb{N}$ má nejmenší prvek 0, ale nemá největší prvek. Množina $\mathbb{R}$ nemá nejmenší ani největší prvek.
- $\mathscr{P}(A)$ má v uspořádání inkluzí nejmenší prvek $\emptyset$ a největší prvek A (zdůvodněte).
- Je-li R uspořádání, pak R^{-1} je také uspořádání. Je-li a nejmenší prvek množiny A v uspořádání R, pak a je největší prvek A v uspořádání R^{-1}. (Rozmyslete podle definic.)

Tvrzení: Nejmenší prvek, pokud existuje, je určen jednoznačně. (Totéž pro největší prvek.)

Důkaz: Nechť a, a' jsou nejmenšími prvky A. Pak dle definice $a \leq a'$, $a' \leq a$, tedy (antisymetrie) $a = a'$. $\square$

Cvičení:

1. Nechť S je pevně zvolený bod roviny. Uvažujme binární relaci $\odot$ mezi body roviny definovanou tak, že $A \odot B$, právě když $|SA| = |SB|$, tj. právě když A, B mají stejnou vzdálenost od bodu S. Ověřte, že $\odot$ je relací ekvivalence v rovině, a určete rozklad roviny na třídy ekvivalence podle $\odot$.
2. Najděte nejmenší a největší prvky (pokud existují):
   - (a) množiny $\{\frac{1}{n+1} \mid n \in \mathbb{N}\}$ v uspořádání reálných čísel podle velikosti;
   - (b) množiny $\mathbb{N}$ v uspořádání dělitelností;
   - (c) množiny všech relací ekvivalence na dané množině A v uspořádání inkluzí.
3. Která přirozená čísla mají množinu všech svých dělitelů *lineárně* uspořádanou relací dělitelnosti?

(LOTEM 2017/18, handout k §3.6)

3.6 Funkce

Zobrazení. Relace $F \subseteq A \times B$ je:

- *zobrazení,* když $(\forall x \in A)(\forall y, y' \in B)(Fxy \wedge Fxy' \to y = y')$, tj. když každý vzor má nejvýše jeden obraz;
- *totální,* když $(\forall x \in A)(\exists y \in B)Fxy$, tj. když každý vzor má aspoň jeden obraz;
- *surjektivní,* když $(\forall y \in B)(\exists x \in A)Fxy$, tj. když každý obraz má aspoň jeden vzor (čili když F^{-1} je totální);
- *injektivní,* když $(\forall x, x' \in A)(\forall y \in B)(Fxy \wedge Fx'y \to x = x')$, tj. když každý obraz má nejvýše jeden vzor (neboli když F^{-1} je zobrazení);
- *bijekce,* je-li totálním injektivním a surjektivním zobrazením, tj. když každý vzor má právě jeden obraz a každý obraz má právě jeden vzor.

Terminologie:

- Zobrazením se také říká *částečné* (či *parciální*) *funkce* a mluví se o zobrazení *z* A *do* B.
- Totální zobrazení se též nazývají *totální funkce* či prostě *funkce* a mluví se o zobrazení (celé) množiny A do B.
- Surjektivní zobrazení se též označují jako *surjekce* a mluví se o zobrazení *na* B.
- Injektivním zobrazením se též říká *prostá* zobrazení či stručně *injekce.*
- Bijekce se též označují jako *vzájemně jednoznačná* zobrazení mezi množinami A a B.

Značení:

- Je-li F zobrazení, pak Fxy lze psát i jako $y = F(x)$ nebo $F\colon x \mapsto y$.
- Fakt, že F je totální zobrazení A do B, se zapisuje jako $F\colon A \to B$.
- Fakt, že F je bijekce mezi A a B, zapisujeme $F\colon A \leftrightarrow B$.
- V praxi se funkce obvykle vyjadřují funkčními předpisy, např. $F(x) = x^2$ či $F\colon x \mapsto x^2$ (musí být ovšem znám obor hodnot x). Funkčními předpisy funkce často i označujeme, např. funkcí $\sin 2x$ míníme zobrazení $\{\langle x, \sin 2x\rangle \mid x \in \mathbb{R}\}$.

Příklady:

- Mezi zobrazeními z $\mathbb{R}$ do $\mathbb{R}$ je $1/x$ částečná funkce, x^2 totální funkce, tg částečná surjekce, arctg totální injekce a x^3 bijekce.
- Prázdná relace $\emptyset$ je prostým zobrazením z libovolné A do libovolné B. Je také totální funkcí z $\emptyset$ do libovolné množiny A, tj. $\emptyset\colon \emptyset \to A$, a bijekcí $\emptyset\colon \emptyset \leftrightarrow \emptyset$.
- Identita je bijekcí každé množiny na sebe samu, $\mathrm{Id}_A\colon A \leftrightarrow A$.
- Funkce $F\colon \mathbb{N} \to A$ lze ztotožnit s posloupnostmi prvků množiny A. Např. každá funkce $F\colon \mathbb{N} \to \mathbb{R}$ vzájemně jednoznačně odpovídá posloupnosti reálných čísel $F(0), F(1), \ldots$

Obraz množiny v zobrazení. Buď $F\colon A \to B$ a $X \subseteq A$. Množinu $\{y \in B \mid (\exists x \in X)Fxy\}$ nazýváme *obraz množiny* X v zobrazení F a značíme $F[X]$.

Pozorujte: Injekce $F\colon A \to B$ je bijekcí $F\colon A \leftrightarrow F[A]$.

Skládání funkcí. *Složením* funkcí $F\colon A \to B$ a $G\colon B \to C$ je funkce $F \circ G\colon A \to C$ taková, že $(F \circ G)(x) = G(F(x))$ pro každé $x \in A$.

Formálně: $F \circ G =_{\mathrm{df}} \{\langle x, z\rangle \in A \times C \mid z = G(F(x))\}$.

Značení: také GF, tj. $GF(x) = G(F(x))$. (Pozor: někteří autoři píší též $F \circ G$ jako $G \circ F$.)

Příklad: $\sin 2x = 2x \circ \sin$ (tj. pro $F\colon x \mapsto 2x$ a $G\colon y \mapsto \sin y$ je $F \circ G\colon x \mapsto \sin 2x$).

Tvrzení: Nechť $F\colon A \to B$ a $G\colon B \to C$.

1. Jsou-li F, G prostá zobrazení, pak také GF je prosté.
2. Jsou-li F, G surjektivní, pak také GF je surjektivní.
3. Jsou-li F, G bijekce, pak je i GF bijekce.

Důkaz.

1. $GF(x) = GF(x') \longleftrightarrow G(F(x)) = G(F(x')) \longrightarrow F(x) = F(x') \longrightarrow x = x'$. (Zdůvodněte jednotlivé kroky z definic a předpokladů.)
2. Vezměme $z \in C$. Funkce G je surjektivní, tedy $z = G(y)$ pro nějaké $y \in B$. Funkce F je také surjektivní, tedy $y = F(x)$ pro nějaké $x \in A$. Tudíž $z = G(F(x))$ pro nějaké $x \in A$.
3. Je důsledkem tvrzení 1 a 2. $\square$

Kartézská mocnina. *Kartézská mocnina* A^B je množina všech funkcí $F\colon B \to A$.

Formálně: $A^B =_{\mathrm{df}} \{F \mid F\colon B \to A\}$. Příklady:

- $\mathbb{R}^{\mathbb{R}} = \{F \mid F\colon \mathbb{R} \to \mathbb{R}\}$ je množina všech totálních reálných funkcí reálné proměnné.
- $\mathbb{R}^{\mathbb{N}} = \{F \mid F\colon \mathbb{N} \to \mathbb{R}\}$ je množina všech posloupností reálných čísel $F(0), F(1), F(2) \ldots$
- $A^{\emptyset} = \{\emptyset\}$, neboť jediná funkce $F\colon \emptyset \to A$ je prázdná funkce $F = \emptyset$. Speciálně $\emptyset^{\emptyset} = \{\emptyset\}$.
- $\emptyset^A = \emptyset$ pro $A \neq \emptyset$, neboť neexistuje žádná totální funkce $F\colon A \to \emptyset$ (zdůvodněte).

Cvičení:

1. Pro funkce cos, e^x, log, $\sqrt[3]{x}$ určete, zda jsou na $\mathbb{R}$ totální, injektivní, surjektivní.
2. Porovnejte injektivitu a surjektivitu funkce x^2 na množinách $\mathbb{N}$, $\mathbb{Q}$ a $[0, +\infty)$.
3. Nechť $F(x) = x + 1$, $G(x) = x^2$ pro všechna $x \in \mathbb{R}$. Určete funkce FG, GF, FF, GG, FF^{-1} a $(FF)^{-1}$, kde F^{-1} je funkce inverzní k F.
4. Určete všechny prvky kartézských mocnin: $\{a\}^{\{b\}}$, $A^{\{a\}}$, $\{a\}^B$, $\{a, b\}^{\{c,d\}}$.

(LOTEM 2017/18, handout k §4.1)

4. Mohutnosti množin

4.1 Konečné množiny

Počet prvků. Velikosti množin můžeme srovnávat např. inkluzí, mnoho dvojic množin je ale inkluzí neporovnatelných. U konečných množin je použitelnější mírou velikosti *počet prvků.* Počítání prvků množiny A je vlastně postupné vytváření prostého zobrazení množiny $\{1,\dots,n\}$ do A; spočítáním *všech* prvků dostaneme *bijekci* mezi $\{1,\dots,n\}$ a A.

Definice: Množina A je *n-prvková* (kde $n \in \mathbb{N}$), pokud existuje bijekce $F\colon \{1,\dots,n\} \leftrightarrow A$. Množina je *konečná,* jestliže je n-prvková pro nějaké $n \in \mathbb{N}$; jinak je *nekonečná.*

Značení: $|A| = n$ (též: $\operatorname{card} A = n$ aj.). Je-li $n = 0$, zápisem $\{1,\dots,n\}$ rozumíme $\emptyset$.

Terminologie: Říkáme také, že A má *mohutnost* (či *kardinalitu*) n (či *konečnou, nekonečnou*).

Příklady: $|\emptyset| = 0$, $\big|\{-5\}\big| = 1$, $\big|\{\pi, \sqrt{2}, 15\}\big| = 3$.

Jednoznačnost: ukážeme podle následujících dvou lemmat.

Lemma 1: Každá neprázdná množina přirozených čísel má nejmenší prvek.

Důkaz: Nepřímo – nechť $A \subseteq \mathbb{N}$ nemá nejmenší prvek; ukážeme $A = \emptyset$. Vezměme množinu $B = \{n \in \mathbb{N} \mid (\forall m \leq n)(m \notin A)\}$; tj. $n \in B$, právě když žádné $m \leq n$ nepatří do A. Matematickou indukcí ověřme $B = \mathbb{N}$:

1. Platí $0 \in B$, jinak by 0 byla nejmenším prvkem A (rozmyslete).
2. Jestliže $n \in B$, pak také $n + 1 \in B$, jinak by $n + 1$ byl nejmenší prvek A (proč?).

Tudíž vskutku $B = \mathbb{N}$, a tedy $A = \emptyset$ (zdůvodněte: kdyby $n \in A$, tak $n \notin B$). ☐

Lemma 2: Mezi $\{1,\dots,m\}$ a $\{1,\dots,n\}$ existuje bijekce, právě když $m = n$.

Důkaz: Směr $\leftarrow$ je triviální, bijekcí je např. identita na $\{1,\dots,m\}$. Opačný směr dokážeme sporem; nechť $F\colon \{1,\dots,m\} \leftrightarrow \{1,\dots,n\}$ pro nějaká $m \neq n$. Vezměme *nejmenší* takové m (dle Lemmatu 1). Nutně $m > 0$, neboť pro $n > 0$ neexistuje $F\colon \emptyset \leftrightarrow \{1,\dots,n\} \neq \emptyset$. Uvažujme $F'\colon \{1,\dots,m-1\} \leftrightarrow \{1,\dots,n\} \smallsetminus \{F(m)\}$ a $G\colon \{1,\dots,n\} \smallsetminus \{F(m)\} \leftrightarrow \{1,\dots,n-1\}$, kde:

$$F'(k) = F(k) \quad \text{pro } k < m, \qquad G(\ell) = \begin{cases} \ell & \text{pro } \ell < F(m) \\ \ell - 1 & \text{pro } \ell > F(m). \end{cases}$$

Pak zjevně $F' \circ G\colon \{1,\dots,m-1\} \leftrightarrow \{1,\dots,n-1\}$, tedy m nebylo nejmenší takové, spor. ☐

Důsledek: Každá konečná množina má jednoznačně určený počet prvků.

Důkaz: Buď $F\colon \{1,\dots,m\} \leftrightarrow A$; $G\colon \{1,\dots,n\} \leftrightarrow A$. Pak $F \circ G^{-1}\colon \{1,\dots,m\} \leftrightarrow \{1,\dots,n\}$, tedy $m = n$ (Lemma 2). ☐

Tvrzení: Podmnožina konečné množiny je konečná (tedy nadmnožina nekonečné nekonečná).

Důkaz: Sporem – nechť $m \in \mathbb{N}$ je nejmenší (Lemma 1) takové, že m-prvková A má nekonečnou podmnožinu B. Kdyby $A = B$, byla by B konečná; tedy existuje $a \in A \smallsetminus B$, čili $B \subseteq A \smallsetminus \{a\}$; přitom $A \smallsetminus \{a\}$ má $m-1$ prvků (dokažte jako Lemma 2 nebo použijte tvrzení 2 níže), tudíž m nebylo nejmenší takové, spor. (Důsledek v závorce odvoďte sami.) ☐

Mohutnosti výsledků operací s konečnými množinami. Nechť $|A| = m$, $|B| = n$.

1. Pokud $A \cap B = \emptyset$, pak $|A \cup B| = m + n$.
2. Pokud $B \subseteq A$, pak $|A \smallsetminus B| = m - n$.
3. $|A \cup B| = |A| + |B| - |A \cap B|$
4. $|A \times B| = m \cdot n$
5. $\left|A^B\right| = m^n$ (přičemž definujeme $0^0 = 1$)
6. $|\mathscr{P}(A)| = 2^m$

Důkaz:

1. Dle předpokladu existují $F\colon \{1, \dots, m\} \leftrightarrow A$; $G\colon \{1, \dots, n\} \leftrightarrow B$. Buď $H\colon \{1, \dots, m+n\} \to A \cup B$, kde $H(k) = F(k)$ pro $k \le m$ a $H(k) = G(k-m)$ pro $k > m$. Ujasněte si, že H je bijekce.
2. Platí $(A \smallsetminus B) \cap B = \emptyset$, $(A \smallsetminus B) \cup B = A$ (dokažte, srv. §3.3). Podle tvrzení 1 tedy dostaneme: $|A| = |A \smallsetminus B| + |B|$, tj. $|A \smallsetminus B| = |A| - |B| = m - n$.
3. Označme $|A \cap B| = k$. Podle tvrzení 1 (zdůvodněte splnění jeho podmínek) dostaneme: $|A \cup B| = \big|A \smallsetminus (A \cap B)\big| + |A \cap B| + \big|B \smallsetminus (A \cap B)\big| = (m - k) + k + (n - k) = m + n - k$.
4. Dle předpokladu existují $F\colon \{1, \dots, m\} \leftrightarrow A$; $G\colon \{1, \dots, n\} \leftrightarrow B$. Pro každé $i \in \{1, \dots, m\}$, $j \in \{1, \dots, n\}$ buď $H\big(\big\langle F(i), G(j)\big\rangle\big) = n(i-1) + j$. Ujasněte si, že $H\colon A \times B \leftrightarrow \{1, \dots, mn\}$.
5. Tvrzení 5 a 6 dokážeme pomocí lemmat platných pro všechny (nejen konečné) množiny.

   Lemma 3: Pro libovolné disjunktní množiny B, C a libovolnou množinu A existuje bijekce $H\colon A^{B \cup C} \leftrightarrow A^B \times A^C$.

   Důkaz: Pro každé $F\colon B \to A$ a $G\colon C \to A$ je $F \cup G\colon B \cup C \to A$ (nahlédněte). Přiřazení $H\colon \langle F, G\rangle \mapsto F \cup G$ je bijekce mezi $A^B \times A^C$ a $A^{B \cup C}$ (rozmyslete). ☐

   Důkaz tvrzení 5 provedeme matematickou indukcí podle n:

   - Pro $n = 0$ je $|A^B| = |A^\emptyset| = \big|\{\emptyset\}\big| = 1 = m^0$.
   - Pro $n > 0$ existuje $b \in B$, takže

     $$|A^B| = \big|A^{(B \smallsetminus \{b\}) \cup \{b\}}\big| = \big|A^{B \smallsetminus \{b\}} \times A^{\{b\}}\big| = \big|A^{B \smallsetminus \{b\}}\big| \cdot \big|A^{\{b\}}\big| = m^{n-1} \cdot m^1 = m^n,$$

     kde druhá rovnost plyne z Lemmatu 3, třetí z tvrzení 4 a čtvrtá z indukčního předpokladu.

6. **Lemma 4:** Pro libovolnou množinu A existuje bijekce $H\colon \mathscr{P}(A) \leftrightarrow \{0,1\}^A$.

   Důkaz: Každé podmnožině $Y \subseteq A$ přiřaďme její tzv. *charakteristickou funkci* $\chi_Y\colon A \to \{0,1\}$ definovanou tak, že $\chi_Y(x) = 1$, pokud $x \in Y$; a $\chi_Y(x) = 0$, pokud $x \notin Y$. Rozmyslete, že $H\colon Y \mapsto \chi_Y$ je bijekce mezi $\mathscr{P}(A)$ a $\{0,1\}^A$. ☐

   Tvrzení 6 nyní plyne přímo z tvrzení 5: $|\mathscr{P}(A)| = \big|\{0,1\}^A\big| = \big|\{0,1\}\big|^{|A|} = 2^m$. ☐

Důsledky: Jsou-li A, B konečné, pak i $A \cap B$, $A \cup B$, $A \smallsetminus B$, $A \times B$, A^B, $\mathscr{P}(A)$ jsou konečné. Sjednocení, průnik a kartézský součin konečně mnoha konečných množin je konečný.

Cvičení: Určete mohutnosti těchto konečných množin:

1. $\{2n \mid n \in \mathbb{N} \cap [0, 1000]\}$ (zdůvodněte podle definice – najděte bijekci);
2. množina všech možných nejvýše 10-znakových hesel složených z písmen A–Z a číslic 0–9;
3. množina všech *parciálních* funkcí (§3.6) z 5-prvkové množiny do 6-prvkové.

(LOTEM 2017/18, handout k §4.2)

4.2 Nekonečné množiny

Lemma: Pro žádné $n \in \mathbb{N}$ neexistuje bijekce $F\colon \{1,\dots,n\} \leftrightarrow \mathbb{N}$.

Důkaz: Sporem, nechť n je nejmenší takové, že existuje $F\colon \{1,\dots,n\} \leftrightarrow \mathbb{N}$. Vezměme $F' = F \smallsetminus \{\langle n, F(n)\rangle\}$ a $G\colon \mathbb{N} \leftrightarrow \mathbb{N} \smallsetminus \{F(n)\}$ tak, že $G(k) = k$ pro $k < F(n)$ a $G(k) = k-1$ pro $k > F(n)$. Ujasněte si (jako v §4.1 Lem. 2), že $F' \circ G\colon \{1,\dots,n-1\} \leftrightarrow \mathbb{N}$, tedy n nebylo nejmenší takové, spor. ☐

Důsledek: Množina $\mathbb{N}$ je nekonečná. (Její nadmnožiny $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ tudíž také.)

Tvrzení: Množina A je nekonečná, právě když existuje prosté zobrazení $F\colon \mathbb{N} \to A$.

Důkaz: Zleva doprava: Buď A nekonečná, pak:

- $A_0 = A \neq \emptyset$ (jinak by A byla 0-prvková), tedy existuje $a_0 \in A_0$; přiřaď $F(0) = a_0$;
- $A_1 = A \smallsetminus \{a_0\} \neq \emptyset$ (jinak by A byla 1-prvková), tedy existuje $a_1 \in A_1$; přiřaď $F(1) = a_1$;
- $A_2 = A \smallsetminus \{a_0, a_1\} \neq \emptyset$ (jinak by A byla 2-prvková), tedy existuje $a_2 \in A_2$; přiřaď $F(2) = a_2$;
- atd. indukcí, v n-tém kroku:
  $A_n = A \smallsetminus \{a_0,\dots,a_{n-1}\} \neq \emptyset$ (jinak by $|A| = n$), tedy existuje $a_n \in A_n$; přiřaď $F(n) = a_n$.

Takto vybereme prvek $F(n) \in A$ pro každé $n \in \mathbb{N}$, tedy $F\colon \mathbb{N} \to A$. Zobrazení F je prosté, protože jsme v každém kroku vzali prvek různý od všech předchozích.

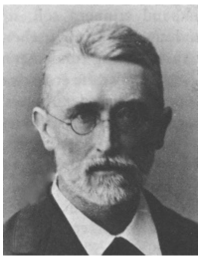
Zprava doleva: Nechť $F\colon \mathbb{N} \to A$ je injekce. Pak $F\colon \mathbb{N} \leftrightarrow F[\mathbb{N}] = \{x \in A \mid (\exists n \in \mathbb{N})Fxy\}$, tedy $F[\mathbb{N}]$ je nekonečná, tedy $A \supseteq F[\mathbb{N}]$ je nekonečná. ☐

Příklad důsledku: Každý alespoň dvoubodový interval v $\mathbb{R}$ či $\mathbb{Q}$ je nekonečná množina. (Dokažte jako cvičení – najděte vhodnou injekci $\mathbb{N}$.)

Tvrzení (*Dedekindova definice konečnosti*): Množina A je nekonečná, právě když existuje bijekce A na její vlastní část.

Důkaz: Zleva doprava: Buď A nekonečná, tedy existuje injekce $F\colon \mathbb{N} \to A$. Vezměme opět $F[\mathbb{N}] = \{x \in A \mid (\exists n \in \mathbb{N})Fxy\} \subseteq A$ a definujme $G(x) = x$, pokud $x \in A \smallsetminus F[\mathbb{N}]$, a $G(x) = F(n+1)$, pokud $x = F(n) \in F[\mathbb{N}]$. Ujasněte si, že $G\colon A \leftrightarrow A \smallsetminus \{F(0)\}$.

Zprava doleva (nepřímo): Buď A konečná, tedy $|A| = m$ pro nějaké $m \in \mathbb{N}$. Pokud $B \subsetneq A$, pak $|A \smallsetminus B| > 0$, tedy $|B| = |A| - |A \smallsetminus B| < m$ a dle §4.1 Lem. 2 neexistuje bijekce mezi množinami různých konečných mohutností. ☐



Richard Dedekind

V předchozích tvrzeních jsme použili dva dosud explicitně neuvedené množinové principy (v minulosti kontroverzní – aktuální nekonečno, nekonstruktivní vymezení výběrové množiny):

Princip nekonečna: Obor všech přirozených čísel tvoří množinu.

Odmítnutí principu nekonečna vede k budování *teorie konečných množin* (pozorujte, že množinové operace jsou na konečných množinách uzavřené).

Princip výběru: Pro každou množinu neprázdných disjunktních množin existuje množina obsahující právě po jednom prvku z každé z nich („výběrová množina“).

Existenci výběrové množiny lze ve mnoha případech dokázat i bez použití principu výběru (např. pro konečné systémy množin nebo lze-li z každé množiny systému vybrat nějaký prvek explicitně). Princip výběru tvrdí existenci výběrové množiny obecně, i pro množiny množin, kde prvky explicitně vybrat neumíme. Princip výběru i jeho negace mají některé neintuitivní důsledky (např. Banachův-Tarského paradox vs. prázdnost kartézského součinu systému neprázných množin). Princip výběru přitom nelze dokázat ani vyvrátit z ostatních principů teorie množin (nevyvratitelnost prokázal Gödel 1940, nedokazatelnost Cohen 1963).

Cvičení.

1. Určete, které z množin jsou nekonečné:
   (a) $\mathbb{N} \cup \emptyset$, $\mathbb{N} \cup \{\emptyset\}$, $\{\mathbb{N}\} \cup \{\emptyset\}$, $\mathbb{N} \times \{\emptyset\}$, $\{\mathbb{N}\} \times \{\emptyset\}$
   (b) $\emptyset^{\mathbb{N}}$, $\mathbb{N}^{\emptyset}$, $\{\emptyset\}^{\mathbb{N}}$, $\{\emptyset\}^{\{\mathbb{N}\}}$, $\mathbb{N}^{\{\emptyset\}}$
2. Rozhodněte, která z následujících tvrzení jsou pravdivá:
   (a) Každá nekonečná množina má nekonečně mnoho nekonečných podmnožin.
   (b) Je-li A nekonečná a B konečná, pak $A \smallsetminus B$ je nekonečná.
   (c) Je-li A nekonečná a B konečná, pak žádná surjekce $F\colon A \to B$ není prostá.
   (d) Každou nekonečnou množinu lze rozdělit na dvě disjunktní nekonečné části.
   (e) Množina všech prvočísel p takových, že $p + 2$ je také prvočíslo, je nekonečná. (Řešte až po vyřešení všech ostatních úloh.)

(LOTEM 2017/18, handout k §4.3)

4.3 Ekvivalence a subvalence množin

Počty prvků dobře porovnávají velikosti konečných množin, o nekonečných ale neříkají nic. Porovnávání velikostí pomocí prostých zobrazení lze ale snadno zobecnit na všechny množiny.

Definice. Množiny A, B jsou *ekvivalentní* pokud existuje bijekce $F\colon A \leftrightarrow B$. Značení: $A \approx B$ či $F\colon A \approx B$. (Terminologie též: *ekvipolentní, ekvipotentní,* či *stejné mohutnosti*).

Množina A je *subvalentní* množině B, pokud existuje injekce $F\colon A \to B$. Značení: $A \preceq B$ či $F\colon A \preceq B$. Zápis $A \prec B$ (striktní subvalence) je zkratkou za $A \preceq B \wedge A \not\approx B$.

Vlastnosti ekvivalence a subvalence.

1. $A \approx A$ (Důkaz: $\mathrm{Id}_A\colon A \leftrightarrow A$.)
2. $A \approx B \to B \approx A$ (Důkaz: pokud $F\colon A \leftrightarrow B$, pak $F^{-1}\colon B \leftrightarrow A$.)
3. $A \approx B \wedge B \approx C \to A \approx C$ (Důkaz: složení bijekcí je bijekce.)
4. $A \preceq A$ (Důkaz: $\mathrm{Id}_A\colon A \to A$ je injekce.)
5. $A \preceq B \wedge B \preceq C \to A \preceq C$ (Důkaz: složení injekcí je injekce.)
6. $A \subseteq B \to A \preceq B$ (Důkaz: $\mathrm{Id}_A\colon A \to B$ je injekce.)
7. $A \approx B \to A \preceq B$ (Důkaz: každá bijekce je injekce.)

Ekvivalence množin je tedy relací ekvivalence (§3.5). Subvalence je reflexivní a tranzitivní, ale není antisymetrická (najděte protipříklad). Platí však alespoň následující věta („antisymetrie“ vůči $\approx$ místo rovnosti), díky níž k prokázání $A \approx B$ stačí najít injekce A do B a B do A.

Věta (Cantorova-Bernsteinova). Pokud $A \preceq B$ a $B \preceq A$, pak $A \approx B$.

Důkaz: Nechť $A \preceq B \preceq A$, tedy existují $F\colon A \leftrightarrow F[A] \subseteq B$, $G\colon B \leftrightarrow G[B] \subseteq A$. Označme:

$$\begin{aligned} A_0 &= A \\ B_0 &= B \\ A_{i+1} &= G[B_i] \subseteq A_i \\ B_{i+1} &= F[A_i] \subseteq B_i, \end{aligned}$$

pro každé $i \in \mathbb{N}$. Protože $B \approx G[B] = A_1$, stačí ukázat $A \approx A_1$. Označme dále:

$$\begin{aligned} C &= \bigcap_{i\in\mathbb{N}} A_i \\ S &= \bigcup_{i\in\mathbb{N}} (A_{2i} \setminus A_{2i+1}) \\ L &= \bigcup_{i\in\mathbb{N}} (A_{2i+1} \setminus A_{2i+2}) \\ S_1 &= \bigcup_{i\in\mathbb{N}} (A_{2i+2} \setminus A_{2i+3}). \end{aligned}$$

Pozorujte: $A = S \cup L \cup C$, $A_1 = S_1 \cup L \cup C$. Přitom $(F \circ G)[A_{2i} \setminus A_{2i+1}] = A_{2i+2} \setminus A_{2i+3}$, tedy $(F \circ G)[S] = S_1$, a protože $F \circ G$ je prostá, $S \approx S_1$. □

Cvičení.

1. Najděte všechny ekvivalence a subvalence mezi množinami: $\emptyset$, $\{\pi, -1\}$, $\mathbb{N}$, $\mathbb{N} \setminus \{0\}$.
2. Rozhodněte, zda platí:
   - (a) $A \cap B \preceq A$
   - (b) $A \times \{0\} \approx A$
   - (c) $A \preceq A^2$
   - (d) Pokud $A_1 \preceq A_2 \preceq A_3 \preceq A_1$, pak $A_1 \approx A_2 \approx A_3$.
   - (e) $A \preceq A \times B$ (Jak lze toto tvrzení opravit na platné?)
   - (f) Pokud $A \preceq B$, pak existuje surjekce $F\colon B \to A$. (Jak lze opravit na platné?)

(LOTEM 2017/18, handout k §4.4)

4.4 Spočetné a nespočetné množiny

Dle §4.2 je množina A nekonečná, právě když $\mathbb{N} \preceq A$. Množiny ekvivalentní $\mathbb{N}$ tedy mají nejmenší nekonečnou mohutnost. To motivuje následující pojem.

Definice: Množina A je *spočetná,* pokud $A \preceq \mathbb{N}$; jinak je *nespočetná.*

Někteří autoři definují spočetnost podmínkou $A \approx \mathbb{N}$ (naše nekonečná spočetnost) a množiny $A \preceq \mathbb{N}$ nazývají nejvýše spočetnými. Nespočetnost vždy znamená $A \not\preceq \mathbb{N}$.

Tvrzení: Množiny $\mathbb{Z}$, $\mathbb{N}^2$, $\mathbb{Q}$ jsou spočetné.

Důkaz: Funkce $F(z) = 2z$ pro $z \geq 0$ a $F(z) = -2z - 1$ pro $z < 0$ je bijekce $F\colon \mathbb{Z} \leftrightarrow \mathbb{N}$. Cantorova párovací funkce $\pi(m,n) = \frac{1}{2}(m+n)(m+n+1)+n$ je bijekcí $\pi\colon \mathbb{N}^2 \leftrightarrow \mathbb{N}$. Racionální čísla jsou zkrácené celočíselné zlomky, tj. některé dvojice celých čísel; proto $\mathbb{Q} \preceq \mathbb{Z}^2 \approx \mathbb{N}^2 \approx \mathbb{N}$. □

Věta: Množina $\mathbb{R}$ je nespočetná.

Důkaz (Cantorova diagonalizace): Sporem. Nechť $F\colon \mathbb{N} \leftrightarrow \mathbb{R}$ a nechť pro každé $n \in \mathbb{N}$ je $F(n) = \sum_{i=0}^{\infty} d_{n,i} \cdot 10^{-i}$ jednoznačně určený (viz §1.1) desetinný rozvoj čísla $F(n)$. Buď $r = \sum_{i=0}^{\infty} d_i \cdot 10^{-i}$, kde $d_i = 1$, pokud $d_{n,n} = 0$, a $d_i = 0$, pokud $d_{n,n} \neq 0$. Zjevně $r \in \mathbb{R}$ (nemá periodu 9) a $F(n) \neq r$ (neboť $d_{n,n} \neq d_n$) pro žádné $n \in \mathbb{N}$. Tedy F není surjektivní, spor. □

Definice: Množina A má *mohutnost kontinua,* pokud $A \approx \mathbb{R}$.

Příklady: Reálný interval $(0,1)$ má mohutnost kontinua, neboť $\mathrm{tg}(\pi x - \frac{\pi}{2})\colon (0,1) \leftrightarrow \mathbb{R}$. Reálný interval $[0,1)$ má rovněž mohutnost kontinua, neboť $\mathbb{R} \approx (0,1) \subseteq [0,1) \subseteq \mathbb{R}$.

Věta: $\mathbb{R}^2 \approx \mathbb{R}$.

Důkaz: Dokážeme $[0,1)^2 \approx [0,1)$. Zřejmě $[0,1) \preceq [0,1)^2$; podle Cantorovy-Bernsteinovy věty stačí najít injekci $F\colon [0,1)^2 \to [0,1)$. Dvojici čísel $r_1, r_2 \in [0,1)$ s desetinnými rozvoji $r_1 = \sum_{i=1}^{\infty} d_{1,i} \cdot 10^{-i}$, $r_2 = \sum_{i=1}^{\infty} d_{2,i} \cdot 10^{-i}$ přiřadíme $F(r_1, r_2) = \sum_{i=1}^{\infty} d_{1,i} \cdot 10^{-2i} + \sum_{i=1}^{\infty} d_{2,i} \cdot 10^{-2i-1}$. Zjevně $F(r_1, r_2) \in \mathbb{R}$ (mohlo by mít periodu 9, jen kdyby r_1, r_2 měla periodu 9) a F je prostá (zdůvodněte). □

Tvrzení: $\mathscr{P}(\mathbb{N}) \approx \mathbb{R}$.

Důkaz: Najdeme injekce $F\colon [0,1) \to \mathscr{P}(\mathbb{N})$, $G\colon \mathscr{P}(\mathbb{N}) \to [0,1)$. Číslu $r \in [0,1)$ s dvojkovým rozvojem $r = \sum_{i=1}^{\infty} b_i \cdot 2^{-i}$ (bez periody 1) přiřadíme množinu $F(r) = \{i \in \mathbb{N} \mid b_i = 1\} \in \mathscr{P}(\mathbb{N})$. Naopak množině $A \subseteq \mathbb{N}$ přiřadíme číslo $G(A) = \sum_{i=1}^{\infty} d_i \cdot 10^{-i}$, kde $d_i = 1$, pokud $i \in A$, a $d_i = 0$, pokud $i \notin A$. Obě funkce jsou zjevně prosté (zdůvodněte). □

Tvrzení:

1. Jsou-li A, B spočetné, pak $A \cup B$, $A \times B$ jsou spočetné.
2. Mají-li A, B mohutnost kontinua, pak $A \cup B$, $A \times B$ mají mohutnost kontinua.
3. Sjednocení spočetně mnoha spočetných množin je spočetné.

4. Sjednocení spočetně mnoha množin mohutnosti kontinua má mohutnost kontinua.
5. Každá nekonečná množina má nekonečnou spočetnou část.

Důkaz: (Tvrzení 3–5 používají princip výběru. Rozmyslete, že silnější předpoklady důkazů tvrzení 3–4 nejsou na újmu obecnosti.)

1. Pokud $A, B \preceq \mathbb{N}$, pak $A \cup B \preceq \mathbb{Z} \approx \mathbb{N}$, $A \times B \preceq \mathbb{N} \times \mathbb{N} \approx \mathbb{N}$.
2. Pokud $A, B \approx \mathbb{R}$, pak $\mathbb{R} \preceq A \cup B \preceq [0,1) \cup [1,2) = [0,2) \approx \mathbb{R}$, $A \times B \approx \mathbb{R} \times \mathbb{R} \approx \mathbb{R}$.
3. Nechť pro každé $i \in \mathbb{N}$ je $F_i \colon \mathbb{N} \leftrightarrow A_i$, kde A_i jsou vzájemně disjunktní. Pak $G(i,j) = F_i(j)$ je bijekce mezi spočetnou $\mathbb{N}^2$ a $\bigcup_{i\in\mathbb{N}} A_i$.
4. Mějme vzájemně disjunktní $A_i \approx \mathbb{R} \approx [i, i+1)$ pro každé $i \in \mathbb{N}$; pak $\bigcup_{i\in\mathbb{N}} A_i \approx \bigcup_{i\in\mathbb{N}} [i, i+1) \approx [0, +\infty) \approx \mathbb{R}$.
5. Je-li A nekonečná, pak (§4.2) existuje prostá $F \colon \mathbb{N} \to A$ a $\mathbb{N} \approx F[\mathbb{N}] \subseteq A$.

Důsledky:

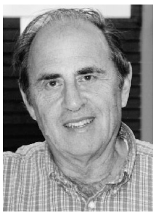
- Množina $\mathbb{A}$ všech algebraických čísel je spočetná. (Rozmyslete: celočíselných polynomů stupně n je spočetně mnoho a každý má nejvýše n kořenů.)
- Množiny $\mathbb{R} \setminus \mathbb{Q}$ všech iracionálních a $\mathbb{R} \setminus \mathbb{A}$ všech transcendentních čísel jsou nespočetné.

Hypotéza kontinua. Všechny dosud uvažované podmnožiny $\mathbb{R}$ byly buď spočetné, nebo měly mohutnost kontinua. To vedlo Cantora (1878) k formulaci hypotézy, kterou se léta marně snažil dokázat:

> Každá množina reálných čísel je buď spočetná, nebo má mohutnost kontinua.

Hilbert (1900) zařadil Cantorovu hypotézu (CH) jako první položku na seznam otevřených problémů pro 20. století. Gödel (1940) dokázal, že pomocí ostatních principů teorie množin nelze CH vyvrátit; Cohen (1963) ukázal, že ji pomocí nich nelze ani dokázat.


Kurt Gödel


Paul Cohen

Cvičení.

1. Určete, které z těchto množin jsou spočetné a které mají mohutnost kontinua: $\mathbb{Q} \times \mathbb{N}$, $\mathbb{R} \times \mathbb{Z}$, $\mathbb{R} \setminus \mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathscr{P}(\mathbb{Z})$, $\mathbb{C}$.
2. Najděte bijekci mezi: a) reálnými intervaly $[0,1]$ a $(0,1)$; b) otevřeným jednotkovým kruhem a celou rovinou; c) uzavřeným jednotkovým kruhem a celou rovinou.
3. Dokažte, že: a) Množina všech konečných řetězců písmen latinské abecedy je spočetná. b) Množina všech programů ve vašem oblíbeném programovacím jazyce je spočetná. c) Existují reálná čísla, která nejsou algoritmicky vyčíslitelná (tj. jejichž desetinný rozvoj nelze generovat žádným programem).

(LOTEM 2017/18, handout k §4.5)

4.5 Cantorova věta

Věta (Cantorova): $A \prec \mathscr{P}(A)$.

Důkaz: Platí $A \preceq \mathscr{P}(A)$, neboť přiřazení $a \mapsto \{a\}$ je prosté; stačí tedy dokázat $A \not\approx \mathscr{P}(A)$. Ukážeme, že žádné $F\colon A \to \mathscr{P}(A)$ není surjektivní.

Buď $F\colon A \to \mathscr{P}(A)$. Dokážeme, že $B = \{x \in A \mid x \notin F(x)\}$ není obrazem žádného $z \in A$. Sporem: nechť $F(z) = B$; pak dle definice B je $z \in B$, právě když $z \notin F(z) = B$, spor. ☐

Důsledky:

- $\mathbb{R} \prec \mathscr{P}(\mathbb{R})$. Říkáme, že množiny ekvivalentní $\mathscr{P}(\mathbb{R})$ mají *mohutnost potence kontinua.*

  Příklad: Množina $\mathbb{R}^{\mathbb{R}}$ všech reálných funkcí reálné proměnné (§3.6) má mohutnost potence kontinua.

  Důkaz: $\mathbb{R}^{\mathbb{R}} \supseteq \{0,1\}^{\mathbb{R}} \approx \mathscr{P}(\mathbb{R})$ dle §4.1 (Lem. 4), tedy $\mathbb{R}^{\mathbb{R}} \succeq \mathscr{P}(\mathbb{R})$; a také $\mathbb{R}^{\mathbb{R}} \preceq \mathscr{P}(\mathbb{R})$, neboť každá funkce $F \in \mathbb{R}^{\mathbb{R}}$ je relací $F \subseteq \mathbb{R}^2$, takže $\mathbb{R}^{\mathbb{R}} \subseteq \mathscr{P}(\mathbb{R}^2) \approx \mathscr{P}(\mathbb{R})$. ☐

- $\mathscr{P}(\mathbb{R}) \prec \mathscr{P}(\mathscr{P}(\mathbb{R})) \prec \mathscr{P}(\mathscr{P}(\mathscr{P}(\mathbb{R}))) \prec \cdots$

  Existuje tedy nekonečně mnoho různých nekonečných mohutností.

- Uvažujme množinu všech množin, $\mathrm{V} = \{A \mid A = A\}$. Dle Cantorovy věty je $\mathrm{V} \prec \mathscr{P}(\mathrm{V})$; ale $\mathscr{P}(\mathrm{V})$ je množina množin, tedy $\mathscr{P}(\mathrm{V}) \subseteq \mathrm{V}$, a tedy $\mathscr{P}(\mathrm{V}) \preceq \mathrm{V}$ – spor s Cantorovou větou (tzv. *Cantorův paradox*).

  Řešení Cantorova paradoxu: Podle Cantorovy definice množiny (§3.2) je množina „souhrn … objektů … v jeden celek“. Cantorův paradox lze chápat tak, že všechny množiny není možné shrnout v jeden celek (předpokládáme-li, že lze, odvodíme spor); tedy že *neexistuje* množina všech množin.

  Obor všech množin tak nelze chápat jako „hotový“, definitivně vytvořený objekt. Takovýmto „neaktualizovatelným“ souborům prvků se říká *vlastní třídy.* Cantorův paradox lze tedy formulovat jako sporem dokázanou větu: V je vlastní třída. (Později uvidíme další vlastní třídy.)

Cvičení.

1. Určete mohutnost množiny: a) množin iracionálních čísel; b) všech množin bodů v rovině; c) všech trojúhelníků v rovině; d) všech množin reálných funkcí reálné proměnné.
2. Porovnejte mohutnosti množin:
   (a) $\mathscr{P}(\mathbb{R}) \times \emptyset$, $\mathscr{P}(\mathbb{R} \times \emptyset)$, $\mathbb{R} \times \mathscr{P}(\emptyset)$, $\mathscr{P}(\mathbb{R}) \times \mathscr{P}(\emptyset)$
   (b) $\mathbb{N}$, $\{0\}^{\mathbb{N}}$, $\{0,1\}^{\mathbb{N}}$, $\mathbb{N}^{\mathbb{N}}$
   (c) všech množin přirozených čísel a všech konečných množin přirozených čísel
   (d) všech množin dvojic přirozených čísel a všech dvojic množin přirozených čísel

3. Rozhodněte, která z následujících tvrzení jsou pravdivá:

   (a) Žádné zobrazení $F\colon \mathscr{P}(\mathbb{R}) \to \mathbb{R}$ není prosté.

   (b) Každá množina mohutnosti potence kontinua má alespoň jednu podmnožinu mohutnosti kontinua.

   (c) Jestliže $A \preceq B$, pak $\mathscr{P}(A) \preceq \mathscr{P}(B)$
   (Návod: pomocí injekce $F\colon A \to B$ sestrojte funkci $G\colon \mathscr{P}(A) \to \mathscr{P}(B)$, přiřazující každé podmnožině $X \subseteq A$ množinu $F[X]$ obrazů jejích prvků v F, a dokažte, že je prostá.)

(LOTEM 2017/18, handout k §4.6)

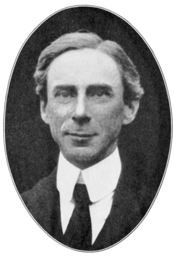
4.6 Axiomatická teorie množin

Naivní princip komprehenze: Každá dobře definovaná vlastnost $\varphi(x)$ vyděluje množinu $\{x \mid \varphi(x)\}$ těch prvků, které ji splňují.

Pozorování: Naivní princip komprehenze vede ke sporu.

Důkaz: Viděli jsme, že vlastnost být množinou (§4.5) vyděluje vlastní třídy – předpoklad, že vyděluje množinu, vedl ke sporu s Cantorovou větou.

Jednodušší důkaz (tzv. *Russellův paradox*): Třída $R = \{X \mid X \notin X\}$ je vlastní – dle její definice je $R \in R \leftrightarrow R \notin R$ = spor. □



Bertrand Russell

Problém: Jak poznat množinu od vlastní třídy? (Čekat, zda se objeví spor, je nepraktické.)

Matematici si brzy všimli, že některé množinové konstrukce (např. sjednocení, potence, záměna prvků či princip nekonečna) je nikdy ke sporu nedovedly.

Opatrné komprehenzní principy:

1. $\mathbb{N}$ je množina.
2. Je-li A množina, pak potence $\mathscr{P}(A)$ je množina.
3. Je-li $\mathcal{A}$ množina množin, pak sjednocení $\bigcup \mathcal{A}$ je množina.
4. Je-li A množina a $\varphi(x, y)$ formule určující funkci, pak $\{y \mid (\exists x \in A)\varphi(x, y)\}$ je množina.

Důsledky opatrných komprehenzních principů: (Důkazy = obtížnější cvičení.)

1. Je-li A množina a $\varphi(x)$ formule, pak $\{x \in A \mid \varphi(x)\}$ je množina.
2. Konečně mnoho libovolných prvků $x_1, \ldots, x_n$ tvoří množinu $\{x_1, \ldots, x_n\}$.
3. Jsou-li A, B množiny, pak $A \cup B$, $A \cap B$, $A \setminus B$, $A \times B$, A^B jsou množiny.
4. Je-li $\mathcal{A} \neq \emptyset$, pak $\bigcap \mathcal{A}$ je množina.
5. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{R}^n, \mathscr{P}(\mathbb{R})$ atp. jsou množiny.

Řešení: Opatrné komprehenzní principy se zdají dostačovat pro většinu množinových konstrukcí. Spolu s množinovými principy (extenzionality, fundovanosti, nekonečna, výběru) tak mohou tvořit axiomatický základ teorie množin.

Definice: *Zermelova-Fraenkelova teorie množin s axiomem výběru* (ZFC) je axiomatická teorie v klasické prvořádové logice s rovností, s jediným binárním predikátem $\in$ a axiomy:

1. *Axiom extenzionality:* $(\forall q)(q \in x \leftrightarrow q \in y) \to x = y$.

   Značení: $x \subseteq y \equiv_{\mathrm{df}} (\forall q)(q \in x \to q \in y)$.

2. *Axiom prázdné množiny:* $(\exists z)(\forall q)\neg(q \in z)$.

   Značení: $z = \emptyset$.

3. *Axiom dvojice:* $(\forall x)(\forall y)(\exists z)(\forall q)(q \in z \leftrightarrow q = x \vee q = y)$.

   Značení: $z = \{x, y\}$, $\{x\} =_{\mathrm{df}} \{x, x\}$.

4. *Axiom sjednocení:* $(\forall x)(\exists z)\big(q \in z \leftrightarrow (\exists u)(q \in u \wedge u \in x)\big)$.

   Značení: $z = \bigcup x$, $u \cup v =_{\mathrm{df}} \bigcup \{u, v\}$.

5. *Axiom potence:* $(\forall x)(\exists z)(\forall q)(q \in z \leftrightarrow q \subseteq x)$.

   Značení: $z = \mathscr{P}(x)$.

6. *Axiom nekonečna:* $(\exists z)\big(\emptyset \in z \wedge (\forall q)(q \in z \to q \cup \{q\} \in z)\big)$.

7. *Schéma axiomů vydělení:* $(\forall x)(\exists z)(\forall q)\big(q \in z \leftrightarrow q \in x \wedge \varphi(q)\big)$

   Značení: $z = \{q \in x \mid \varphi(q)\}$, $x \cap y = \{q \in x \mid q \in y\}$.

8. *Schéma axiomů nahrazení:*

$$(\forall u)(\forall v)(\forall w)\big(\psi(u, v) \wedge \psi(u, w) \to v = w\big) \to \\ (\forall x)(\exists z)(\forall v)\big(v \in z \leftrightarrow (\exists u)(u \in x \wedge \psi(u, v))\big).$$

9. *Axiom fundovanosti:* $(\forall x)\big(x \neq \emptyset \to (\exists u)(u \in x \wedge u \cap x = \emptyset)\big)$.

10. *Axiom výběru:*

$$(\forall x)\big(\emptyset \notin x \wedge (\forall u)(\forall v)(u \in x \wedge v \in x \wedge u \neq v \to u \cap v = \emptyset) \to \\ (\exists z)(\forall u)(u \in x \to (\exists q)(u \cap z = \{q\}))\big).$$

Poznámky:

- Axiomy ZFC zachycují jednotlivé množinové principy, které byly probírány na přednášce: 1 = princip extenzionality (§3.1); 9 = princip fundovanosti (ekvivalentní formulace, §3.3); 10 = princip výběru (§4.2); 6 = princip nekonečna (§4.2), 2–8 = principy opatrné komprehenze a jejich důsledky (axiom 6 je ekvivalentní tvrzení, že $\mathbb{N}$ je množina).

- 7 a 8 jsou *schémata axiomů:* pro každou formuli φ resp. ψ jazyka teorie množin z nich dostaneme jeden axiom. (ZFC má tedy *nekonečně mnoho* axiomů.)

- Axiomy nejsou nezávislé: 2 plyne z 6; 3 plyne z 2+5+8; a 7 plyne z 8. K axiomatizaci ZFC tedy stačí axiomy 1, 4, 5, 6, 8, 9 a 10.

- Studují se i různé variace ZFC (např. ZFC + Cantorova hypotéza nebo ZF = ZFC bez axiomu výběru) a jiné množinové axiomatiky. ZFC je však v současnosti nejobvyklejší axiomatizací teorie množin (a celé matematiky).

(LOTEM 2017/18, handout #1 k §4.7)

4.7 Kardinální čísla

Kardinální čísla. *Kardinální čísla* (krátce: *kardinály*) jsou abstraktní matematické objekty přiřazené množinám tak, že dvě množiny mají přiřazeno totéž kardinální číslo, právě když jsou ekvivalentní.

Kardinální číslo přiřazené množině A značíme $|A|$ a nazýváme *mohutností* (*kardinalitou*) množiny A. Pro kardinální čísla používáme proměnné $\kappa, \lambda, \mu, \ldots$

Kardinality konečných množin (neboli konečné kardinály) ztotožňujeme s přirozenými čísly: pro m-prvkovou množinu A píšeme $|A| = m$ (srv. §4.1). Pro význačné nekonečné kardinality zavedeme zvláštní symboly:

- Mohutnost nekonečných spočetných množin značíme $\aleph_0$ (alef nula): $|\mathbb{N}| = \aleph_0$.
- Mohutnost kontinua značíme $\mathfrak{c}$ (gotické c): $|\mathbb{R}| = \mathfrak{c}$.
- Vzájemně různé (viz §4.5) mohutnosti množin $\mathbb{N}, \mathscr{P}(\mathbb{N}), \mathscr{P}(\mathscr{P}(\mathbb{N})), \mathscr{P}(\mathscr{P}(\mathscr{P}(\mathbb{N}))), \ldots$ značíme $\beth_0, \beth_1, \beth_2, \beth_3, \ldots$ (bét n).

  Tedy: $\beth_0 = \aleph_0$, $\beth_1 = \mathfrak{c}$, $\beth_2$ je mohutnost potence kontinua, $\beth_3 = |\mathscr{P}(\mathscr{P}(\mathbb{R}))|$, atd.

Kardinální aritmetika. Nechť $\kappa = |A|$, $\lambda = |B|$ a $A \cap B = \emptyset$. Pak definujeme:

- $\kappa \leq \lambda$, právě když $A \preceq B$ (a tedy $\kappa < \lambda$, právě když $A \prec B$)
- $\kappa + \lambda = |A \cup B|$, $\kappa \cdot \lambda = |A \times B|$, $\kappa^\lambda = \left|A^B\right|$

Pozorování:

- Definice aritmetiky kardinálů je korektní, tj. nezáleží na výběru množin mohutností κ, λ. (Důkaz: složením s příslušnými bijekcemi, např. pokud $A' \approx A \preceq B \approx B'$, pak $A' \preceq B'$.)
- $\leq$ je uspořádání (§3.5) kardinálních čísel (srv. §4.3: $\preceq$ je reflexivní a tranzitivní; antisymetrii $\leq$ tvrdí Cantorova–Bernsteinova věta).
- $0 < 1 < 2 < 3 < \cdots < \aleph_0 < \mathfrak{c} < \beth_2 < \beth_3 < \beth_4 < \cdots$ (ostré nerovnosti dle §4.1–2, §4.5).

  Cantorova hypotéza kontinua (§4.4) říká, že $\neg(\exists\kappa)(\aleph_0 < \kappa < \mathfrak{c})$.
- Aritmetika konečných kardinalit souhlasí s aritmetikou přirozených čísel (§4.1).
- $\aleph_0 + \aleph_0 = \aleph_0$, $\mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$, $2^{\aleph_0} = \mathfrak{c}$ atd. (podrobněji viz dále).

  Důkazy: $\mathbb{N} \cup \mathbb{Z}^- = \mathbb{Z} \approx \mathbb{N}$, $\mathbb{R} \times \mathbb{R} \approx \mathbb{R}$, $\{0,1\}^\mathbb{N} \approx \mathscr{P}(\mathbb{N}) \approx \mathbb{R}$ (vše dle §4.4).
- Pokud $|A| = \kappa$, pak $|\mathscr{P}(A)| = 2^\kappa$. (Důkaz: $\mathscr{P}(A) \approx \{0,1\}^A$, viz §4.1 Lem. 4.)

  Speciálně tedy $\beth_{n+1} = 2^{\beth_n}$ pro každé $n \in \mathbb{N}$.

Zákony kardinální aritmetiky.

1. *Komutativita a asociativita sčítání a násobení:*

$$\begin{aligned} \kappa+\lambda &= \lambda+\kappa & \qquad \kappa\cdot\lambda &= \lambda\cdot\kappa \\ (\kappa+\lambda)+\mu &= \kappa+(\lambda+\mu) & \qquad (\kappa\cdot\lambda)\cdot\mu &= \kappa\cdot(\lambda\cdot\mu) \end{aligned}$$

2. *Chování* 0 *a* 1*:*

$$\begin{array}{llll} \kappa+0=\kappa & \kappa\cdot 0=0 & \kappa^0=1 & 0^\kappa=0 \quad \text{pro } \kappa>0 \\ & \kappa\cdot 1=\kappa & \kappa^1=\kappa & 1^\kappa=1 \end{array}$$

3. *Distributivita:* $\kappa\cdot(\lambda+\mu)=\kappa\cdot\lambda+\kappa\cdot\mu$

4. *Zákony mocnění:* $(\kappa\cdot\lambda)^\mu=\kappa^\mu\cdot\lambda^\mu$, $\kappa^{\lambda+\mu}=\kappa^\lambda\cdot\kappa^\mu$, $\left(\kappa^\lambda\right)^\mu=\kappa^{\lambda\cdot\mu}$

5. *Monotonie:* Pokud $\kappa_1\le\kappa_2$, pak:

$$\kappa_1+\lambda\le\kappa_2+\lambda, \qquad \kappa_1\cdot\lambda\le\kappa_2\cdot\lambda, \qquad \kappa_1^\lambda\le\kappa_2^\lambda, \qquad \lambda^{\kappa_1}\le\lambda^{\kappa_2} \text{ (kromě } 0^0>0^{\kappa+1}\text{)}.$$

6. *Sčítání a násobení nekonečných kardinálů* (s principem výběru): Je-li aspoň jeden z kardinálů κ,λ nekonečný, pak:

$$\kappa+\lambda=\max(\kappa,\lambda), \qquad\qquad \kappa\cdot\lambda=\max(\kappa,\lambda) \quad \text{pro } \kappa,\lambda\ne 0$$

Důkaz: Většina uvedených vlastností vyplývá přímo z vlastností množinových operací (např. distributivita z $A\times(B\cup C)=(A\times B)\cup(A\times C)$, viz §3.5), u jiných snadno najdete příslušnou bijekci (např. $A\times B\approx B\times A$) či injekci (např. $A\cup B\preceq A'\cup B$ pro $A\preceq A'$). Pro tvrzení 1–5 proveďte sami jako cvičení (pro mocniny mírně obtížnější; použijte mj. §4.1 Lem. 3). Důkaz tvrzení 6 přesahuje rámec kurzu. □

Tvrzení: Kardinální čísla tvoří vlastní třídu (značenou Card).

Důkaz: Stačí ukázat, že ke každé množině kardinálů A existuje kardinál λ větší než všechna $\kappa\in A$. Ke každému $\kappa\in A$ vezměme množinu A_κ mohutnosti κ. Pak dle Cantorovy věty je $\mathscr{P}\big(\bigcup_{\kappa\in A}A_\kappa\big)\succ\bigcup_{\kappa\in A}A_\kappa\supseteq A_\kappa$, tedy $\lambda=\big|\mathscr{P}\big(\bigcup_{\kappa\in A}A_\kappa\big)\big|>\kappa$, pro každé $\kappa\in A$. □

Speciálně nechť $A_0=\mathbb{N}$ a $A_{n+1}=\mathscr{P}(A_n)$ pro každé $n\in\mathbb{N}$. Pak $\beth_\omega=\big|\mathscr{P}\big(\bigcup_{n\in\mathbb{N}}A_n\big)\big|>\beth_n$ pro všechna $n\in\mathbb{N}$, a dále $\beth_\omega<2^{\beth_\omega}=\beth_{\omega+1}<2^{\beth_{\omega+1}}=\beth_{\omega+2}<2^{\beth_{\omega+2}}=\beth_{\omega+3}$ atd. nade všechny meze.

(LOTEM 2017/18, handout #2 k §4.7)

Kardinální „násobilka“. Dosud uvedené poznatky umožňují určit výsledky aritmetických operací pro některá význačná kardinálními čísla (zejm. konečná či tvaru $\beth_n$ pro $n \in \mathbb{N}$):

$+$	n	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\cdots$
m	$m{+}n$	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\cdots$
$\aleph_0$	$\aleph_0$	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\cdots$
$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\beth_2$	$\cdots$
$\beth_2$	$\beth_2$	$\beth_2$	$\beth_2$	$\beth_2$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

$\cdot$	0	n	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\cdots$
0	0	0	0	0	0	$\cdots$
m	0	$m{\cdot}n$	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\cdots$
$\aleph_0$	0	$\aleph_0$	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\cdots$
$\mathfrak{c}$	0	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\beth_2$	$\cdots$
$\beth_2$	0	$\beth_2$	$\beth_2$	$\beth_2$	$\beth_2$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

κ^λ	0	n	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\cdots$
0	1	0	0	0	0	$\cdots$
1	1	1	1	1	1	$\cdots$
m	1	m^n	$\mathfrak{c}$	$\beth_2$	$\beth_3$	$\cdots$
$\aleph_0$	1	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\beth_3$	$\cdots$
$\mathfrak{c}$	1	$\mathfrak{c}$	$\mathfrak{c}$	$\beth_2$	$\beth_3$	$\cdots$
$\beth_2$	1	$\beth_2$	$\beth_2$	$\beth_2$	$\beth_3$	$\cdots$
$\beth_3$	1	$\beth_3$	$\beth_3$	$\beth_3$	$\beth_3$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Důkaz: Jen pro některá obtížnější políčka, ostatní zdůvodněte na základě probraného sami.

- $\aleph_0^{\aleph_0} = \mathfrak{c}$: Každá funkce $F\colon \mathbb{N} \to \mathbb{N}$ je relací $F \subseteq \mathbb{N} \times \mathbb{N}$, tudíž $\mathbb{N}^{\mathbb{N}} \subseteq \mathscr{P}(\mathbb{N} \times \mathbb{N}) \approx \mathscr{P}(\mathbb{N})$. Odtud $\aleph_0^{\aleph_0} \leq 2^{\aleph_0}$ a $2^{\aleph_0} \leq \aleph_0^{\aleph_0}$ dostaneme z monotonie kardinální mocniny (handout #1 k §4.7). Obdobně pro každé $\aleph_0^{\beth_n}$.
- $\beth_2^{\beth_3} = \left(2^{\beth_1}\right)^{\beth_3} = 2^{\beth_1 \cdot \beth_3} = 2^{\beth_3} = \beth_4$. Obdobně pro libovolné $\beth_{n+1}^{\beth_m}$. $\square$

Cvičení.

1. Vypočítejte: $\aleph_0 \cdot (\mathfrak{c} + \aleph_0)$, $\mathfrak{c} + \aleph_0 \cdot \beth_2$, $(65535 + \mathfrak{c})^{32767+8191}$, $m\mathfrak{c}^2$ (kde $m \in \mathbb{N}$).
2. Seřaďte kardinály podle velikosti: $(2 + \aleph_0)^2$, $2^{\aleph_0} + \aleph_0^2$, $\mathfrak{c}^2 + 2^{\mathfrak{c}}$, $\beth_4$, $2^{\beth_2}$.
3. Dejte příklad množin mohutností: $\aleph_0^2 + 1$, $(\aleph_0 + 1)^2$, $2^{\aleph_0+1}$.
4. Určete n takové, že $\beth_n$ je rovno: $\aleph_0^{\aleph_0^{\aleph_0}}$, $\mathfrak{c}^{\mathfrak{c}^{\mathfrak{c}}}$, $\beth_2^{\beth_2^{\beth_2}}$.

(LOTEM 2017/18, handout k §4.8)

4.8 Ordinální čísla

Iterováním operací potence a sjednocení jsme v §4.7 vytvořili shora neomezenou „transfinitní“ posloupnost nekonečných kardinálů:

$$\beth_0 < \beth_1 < \beth_2 < \cdots \ < \beth_\omega < \beth_{\omega+1} < \beth_{\omega+2} < \cdots \ < \beth_{\omega+\omega} < \beth_{\omega+\omega+1} < \cdots \ \cdots$$

Pro indexování této transfinitní posloupnosti potřebujeme nová nekonečná čísla ($\omega, \omega+1, \dots$). Na rozdíl od čísel kardinálních, vyjadřujících *počet* („kolik?“), zde jde o *pořadí* („kolikátý index?“); nepůjde tedy o nekonečné číslovky základní (kardinální), ale *řadové* (ordinální).

Pozorujte: Transfinitní posloupnost kardinálů $\beth_\alpha$ se vyznačuje tím, že ke každé množině kardinálů lze sestrojit (sjednocením nebo potencí – viz §4.7) nejblíže větší prvek této posloupnosti. Chceme-li takto vytvářené kardinály indexovat ordinálními čísly, musí jejich posloupnost mít tuto vlastnosti také.

Definice: *Ordinální čísla* (krátce: *ordinály*) jsou abstraktní matematické objekty vytvořené tímto *vytvořujícím principem:*

> Ke každé množině ordinálních čísel existuje ordinální číslo nejblíže vyšší (tj. nejmenší ordinální číslo větší než všechny prvky oné množiny).

Transfinitní posloupnost ordinálů. Dle vytvořujícího principu existuje k prázdné množině ordinálů nejblíže vyšší ordinál; označme jej 0. K jednoprvkové množině ordinálů $\{0\}$ existuje nejblíže vyšší ordinál, označme jej 1. K množině již vytvořených ordinálů $\{0, 1\}$ existuje nejblíže vyšší ordinál, označme jej 2; atd. Každé přirozené číslo tedy označuje nějaký ordinál; k množině ordinálů $\mathbb{N}$ existuje dle vytvořujícího principu nejblíže vyšší ordinál, označme jej ω; atd. Postupně tak vytváříme neomezenou transfinitní posloupnost ordinálních čísel:

$$\begin{aligned}
&0 < 1 < 2 < \cdots \ < \omega < \omega + 1 < \omega + 2 < \cdots \ < \omega + \omega = \\
&= \omega \cdot 2 < \omega \cdot 2 + 1 < \cdots \ < \omega \cdot 3 < \omega \cdot 3 + 1 < \cdots \ < \omega \cdot 4 < \cdots \ \cdots \ < \omega \cdot \omega = \\
&= \omega^2 < \omega^2 + 1 < \cdots \ < \omega^2 + \omega < \omega^2 + \omega + 1 < \cdots \ < \omega^2 + \omega \cdot 2 < \cdots \ < \omega^2 + \omega \cdot \omega = \\
&= \omega^2 \cdot 2 < \omega^2 \cdot 2 + 1 < \cdots \ < \omega^2 \cdot 3 < \cdots \ < \omega^2 \cdot \omega = \omega^3 < \cdots \ < \omega^\omega < \cdots \ < \omega^\omega \cdot \omega = \\
&= \omega^{\omega+1} < \cdots \ < \omega^{\omega \cdot 2} < \cdots \ < \omega^{\omega \cdot \omega} = \omega^{\omega^2} < \cdots \ < \omega^{\omega^\omega} < \cdots \ < \omega^{\omega^{\omega^\omega}} < \cdots \ < \omega^{\omega^{\omega^{\omega^{\cdots}}}} = \\
&= \varepsilon_0 < \varepsilon_0 + 1 < \cdots \ < \varepsilon_0^{\varepsilon_0} < \cdots \ < \varepsilon_0^{\varepsilon_0^{\varepsilon_0^{\cdots}}} = \varepsilon_1 < \cdots \ < \varepsilon_{\varepsilon_{\varepsilon_0}} < \cdots \ \cdots \ < \\
&< \omega_1 < \omega_1 + 1 < \cdots \ \cdots \ \cdots \quad \text{atd. nade všechny meze.}
\end{aligned}$$

Definice: Ordinál je *izolovaný,* pokud má bezprostředního předchůdce či je roven 0; jinak je *limitní.* Ordinál je konečný (spočetný), pokud má konečnou (spočetnou) množinu předchůdců.

Konečné ordinály ztotožňujeme s přirozenými čísly. První nekonečný ordinál značíme ω, první nespočetný ω_1. Izolované ordinály jsou např. 0, 1, 2, $\omega + 1$, $\omega + 2$, $\omega^2 + 4$ aj.; limitní např. ω, $\omega \cdot 2$, ω^2, ω^ω aj. Pro ordinály používáme proměnné $\alpha, \beta, \gamma, \dots$

Tvrzení: Ordinální čísla tvoří vlastní třídu (značenou Ord).

Důkaz: Kdyby šlo o množinu, dle vytvořujícího principu by za ní existoval další ordinál. $\square$

Pro ordinální čísla lze zavést nekonečnou aritmetiku (sčítání, násobení, mocnění atp.), odlišnou od kardinální. (Protože v ní jde o *pořadí* prvků, sčítání a násobení ordinálů není komutativní: např. $1 + \omega = \omega < \omega + 1$.) Ordinální aritmetika již přesahuje letošní rozsah kurzu.

Tvrzení: Každá neprázdná množina ordinálů má nejmenší prvek.

Důkaz: Buď A neprázdná množina ordinálů. Ukážeme, že následník γ množiny $B = \{\beta \in \mathrm{Ord} \mid (\forall\alpha \in A)(\beta < \alpha)\}$ je nejmenším prvkem A. Dle vytvořujícího principu je γ nejmenší ze striktních majorant B; a dle definice B jsou prvky A striktními majorantami B; tedy γ je minorantou A. Přitom $\gamma \in A$, jinak by nebylo rovno žádnému prvku A, a splňovalo by tak podmínku náležení do B, tedy by nebylo striktní majorantou B (spor). $\square$

Dobrá uspořádání. Uspořádáním, v nichž každá neprázdná množina má nejmenší prvek, se říká *dobrá.* — Pozorujte:

1. Každé dobré uspořádání je lineární. (Důkaz: uvažte nejmenší prvek $\{a, b\}$.)
2. V dobrém uspořádání neexistuje nekonečná klesající posloupnost $a_0 > a_1 > a_2 > \cdots$ (množina $\{a_0, a_1, a_2, \ldots\}$ by neměla nejmenší prvek).

   Důsledek: Každá klesající posloupnost ordinálů je konečná.
3. V dobrých uspořádáních lze tvrzení dokazovat *transfinitní indukcí,* tj. dokázat, že platí-li φ pro všechny předchůdce α, pak platí i pro α. (Pak totiž kdyby φ pro nějaké α neplatilo, vzali bychom nejmenší takové a dostali spor.)

Věta (Zermelo, 1904): Každou množinu lze dobře uspořádat.

Nástin důkazu: Prvky dané množiny A očíslujeme ordinály: transfinitní indukcí postupně přiřazujeme ordinálům vždy nějaký další dosud nepřiřazený prvek, dokud všechny nevyčerpáme. (Důkaz používá princip výběru, srv. §4.2.) $\square$

Ernst Zermelo

Důsledky Zermelovy věty:

1. Princip výběru. (Důkaz: v dobrém uspořádání lze vždy vybírat nejmenší prvky.)
2. Uspořádání kardinálních čísel podle velikosti je dobré. (Důkaz: každému kardinálu κ přiřadíme nejmenší ordinál, jehož předchůdci lze očíslovat množinu mohutnosti κ.)
3. Vždy $A \preceq B$ nebo $B \preceq A$. (Plyne z předchozího.)
4. S principem výběru lze tedy všechny nekonečné kardinály očíslovat po řadě ordinálními čísly:

   $$\aleph_0 < \aleph_1 < \aleph_2 < \cdots < \aleph_\omega < \aleph_{\omega+1} < \cdots < \aleph_{\omega\cdot 2} < \cdots$$

   Cantorovu hypotézu pak lze formulovat i jako tvrzení $\beth_1 = \aleph_1$, neboli $\aleph_1 = 2^{\aleph_0}$.

   Zobecněná Cantorova hypotéza (GCH): $\beth_\alpha = \aleph_\alpha$ pro všechny ordinály α.

   Stejně jako CH je i GCH nezávislá na ostatních principech teorie množin (nevyvratitelnost Gödel 1940, nedokazatelnost Cohen 1963).

Cvičení. 1. Určete, které z těchto podmnožin $\mathbb{R}$ jsou dobře uspořádané: $\emptyset$, $\{0\}$, $\{1, 2, \mathrm{e}, \pi\}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\left\{\frac{1}{n+1} \,\middle|\, n \in \mathbb{N}\right\}$, $\{1 - 2^{-n} \mid n \in \mathbb{N}\} \cup \{1\}$. 2. U těch z nich, které jsou, najděte ordinál, jehož předchůdci lze tuto množinu po řadě vzestupně očíslovat (tzv. *typ* dobrého uspořádání).

(LOTEM 2016/17, handout k §5.3)

Zákony ordinální aritmetiky:

1. *Asociativita:*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \qquad\qquad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

   Pozor, komutativita neplatí: $1 + \omega = \omega \neq \omega + 1$, $2 \cdot \omega = \omega \neq \omega + \omega = \omega \cdot 2$.

2. *Chování* 0 *a* 1:

$$\begin{array}{lll} \alpha + 0 = 0 + \alpha = \alpha & \alpha \cdot 0 = 0 \cdot \alpha = 0 & 0^\alpha = 0 \quad \text{pro } \alpha > 0 \\ & \alpha \cdot 1 = 1 \cdot \alpha = \alpha & 1^\alpha = 1 \\ & & \alpha^1 = \alpha \end{array}$$

3. *Distributivita zprava:* $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$
   Pozor, distributivita zleva neplatí: $(1 + 1) \cdot \omega = 2 \cdot \omega = \omega \neq \omega + \omega = \omega \cdot (1 + 1)$.

4. *Zákony mocnění:*

$$\begin{aligned} \alpha^{\beta+\gamma} &= \alpha^\beta \cdot \alpha^\gamma \\ \left(\alpha^\beta\right)^\gamma &= \alpha^{\beta \cdot \gamma} \end{aligned}$$

   Pozor, obecně neplatí $(\alpha \cdot \beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$, např. $(\omega \cdot 2)^2 = (\omega \cdot 2) \cdot (\omega \cdot 2) = \omega \cdot (2 \cdot \omega) \cdot 2 = \omega^2 \cdot 2 \neq \omega^2 \cdot 2^2$.

5. *Monotonie:* Pokud $\alpha_1 < \alpha_2$, pak:

$$\begin{array}{cc} \alpha_1 + \beta \leq \alpha_2 + \beta & \beta + \alpha_1 < \beta + \alpha_2 \\ \alpha_1 \cdot \beta \leq \alpha_2 \cdot \beta & \beta \cdot \alpha_1 < \beta \cdot \alpha_2 \\ {\alpha_1}^\beta \leq {\alpha_2}^\beta & \beta^{\alpha_1} < \beta^{\alpha_2} \end{array}$$

   Pozor, monotonie zleva nelze zesílit na striktní (protipříklady = cvičení).

Důkazy: konstrukcí izomorfismu nebo transfinitní indukcí.

(LOTEM 2016/17, handout k §5.4)

Tvrzení závislá na principu výběru:

- Tvrzení z §4.1: A je nekonečná, právě když existuje injekce $\mathbb{N} \to A$
- Důsledky předchozího tvrzení:
  - Každá nekonečná množina má spočetnou část
  - $\mathbb{N} \preceq A$ pro každou nekonečnou A (§4.3)
  - $\aleph_0$ je nejmenší nekonečná mohutnost (§4.5)
  - Každou nekonečnou množinu lze rozdělit na dvě disjunktní nekonečné podmnožiny (cvičení k §4.1)
  - Množina je nekonečná, právě když ji lze bijektivně zobrazit na její vlastní část (tj. ekvivalence naší a Dedekindovy definice konečnosti, §4.1)
- Tvrzení z §4.3:
  - Sjednocení spočetně mnoha spočetných množin je spočetné
  - Sjednocení spočetně mnoha množin mohutnosti kontinua má mohutnost kontinua
- Zákony kardinální aritmetiky z §5.1 pro $\max(\kappa, \lambda)$ nekonečné:
  - $\kappa + \lambda = \max(\kappa, \lambda)$
  - $\kappa \cdot \lambda = \max(\kappa, \lambda)$ pro $\kappa, \lambda > 0$
- Tvrzení ze Cvičení k §5.3: Pokud uspořádání není dobré, pak v něm existuje nekonečná klesající posloupnost. (Opačná implikace princip výběru nepotřebuje.)
- Zermelova věta a její důsledky v §5.4

(LOTEM 2016/17, handout 2 k §5.4)

Tvrzení: Zermelova věta je ekvivalentní principu výběru.

Důkaz: PV → ZV byl důkaz Zermelovy věty. ZV → PV: Buď $\mathcal{A}$ množina neprázdných množin, $\bigcup \mathcal{A}$ lze dle předpokladu dobře uspořádat; z každé množiny v $\mathcal{A}$ pak vybereme (již jednoznačně specifikovaný) nejmenší prvek. Výběrová množina je tedy $\{a \in \bigcup \mathcal{A} \mid (\exists A \in \mathcal{A})(a = \min A)\}$.

Důsledek principu výběru: Uspořádání kardinálů podle velikosti je *dobré.*

Důkaz: Každému kardinálu κ přiřaďme nejmenší ordinál α takový, že množinu A kardinality κ lze dobře uspořádat podle typu α (viz §5.2), tj. že $\exists F\colon A \leftrightarrow [0, \alpha)$; nazýváme jej *iniciální ordinál* ι_κ kardinality κ. (Ten existuje, neboť dle Zermelovy věty lze A dobře uspořádat; tedy množina ordinálů, jež jsou typy dobrých uspořádání A, je neprázdná; tedy existuje nejmenší takový, jelikož ordinály jsou dobře uspořádané. Rozmyslete, že ι_κ nezávisí na volbě množiny A mohutnosti κ – uvažte bijekce mezi množinami téže mohutnosti.)

Tím máme bijekci Card na iniciální ordinály, která je zjevně izomorfizmem vůči uspořádání (rozmyslete: větší kardinál má větší iniciální ordinál, jinak bychom měli bijekci mezi různými kardinalitami). Dobré uspořádání iniciálních ordinálů se tak přenáší na uspořádání kardinálů.

Důsledky:

- Uspořádání kardinálních čísel podle velikosti je lineární.
- Ekvivalentně předchozímu důsledku, pro každé množiny A, B:
  - $A \preceq B$ nebo $B \preceq A$.
  - Existuje injekce $A \to B$ nebo injekce $B \to A$.
  - Existuje injekce nebo surjekce $A \to B$
    (Viz cvičení k §4.2 – rozmyslete, jak z injekce $B \to A$ získat surjekci $A \to B$.)
- Kardinály lze očíslovat ordinálními čísly.
  (Viz §5.3 – každé dobré uspořádání je izomorfní počátečnímu úseku ordinálů.)
  Takové očíslování *nekonečných* kardinálů se nazývá *funkce* $\aleph$:

$$\begin{aligned}
\aleph_0 &= \text{nejmenší nekonečný kardinál}\\
\aleph_1 &= \text{první další (nejmenší nespočetný kardinál)}\\
\aleph_2 &= \text{druhý nespočetný kardinál}\\
&\vdots\\
\aleph_\omega &= \text{kardinál s } \omega \text{ nekonečnými předchůdci}\\
\aleph_{\omega+1} &= \text{kardinál s } \omega+1 \text{ nekonečnými předchůdci, atd.}
\end{aligned}$$

Card: $0, 1, 2, \ldots, \aleph_0, \aleph_1, \aleph_2, \ldots, \aleph_\omega, \aleph_{\omega+1}, \ldots, \aleph_{\omega\cdot 2}, \ldots \;\ldots\;\ldots$
Iniciální ordinál kardinality $\aleph_\alpha$ se označuje ω_α; tj.:

$$\begin{aligned}
\omega_0 &= \omega\\
\omega_1 &= \text{první ordinál s nespočetně předchůdci}\\
\omega_2 &= \text{první ordinál s } \aleph_2 \text{ předchůdci}\\
&\vdots\\
\omega_\omega &= \text{iniciální ordinál kardinality } \aleph_\omega\text{, atd.}
\end{aligned}$$

(Ordinály ω_α rovněž číslují kardinály – např. $\aleph_{\omega_1}$ je první kardinál s nespočetně předcházejícími kardinalitami; jeho iniciální ordinál je ω_{ω_1}.)

Vybrané vlastnosti iniciálních ordinálů – viz cvičení.

Přiřazení $\kappa \mapsto \iota_\kappa$ je bijekce mezi kardinály a iniciálními ordinály. Kardinály lze proto ztotožnit s iniciálními ordinály, což se obvykle činí (viz §6.3); pak $\mathrm{Card} \subseteq \mathrm{Ord}$ (je však stále třeba rozlišovat kardinální aritmetiku od ordinální!).

Další ekvivalentní formulace Cantorovy hypotézy kontinua (s principem výběru):

$$\mathfrak{c} = \aleph_1, \quad 2^{\aleph_0} = \aleph_1, \quad \beth_1 = \aleph_1.$$

(CH říká, že mezi $\aleph_0$ a $\mathfrak{c} = 2^{\aleph_0} = \beth_1$ není žádný další kardinál, tedy že $\mathfrak{c} = \beth_1 = \aleph_1$.)

Zobecněná Cantorova hypotéza kontinua (GCH): Přímé následnictví platí nejen pro $\beth_0$ a $\beth_1$, ale i pro všechny další mohutnosti $\beth_\alpha$ – nejsou mezi nimi žádné další kardinály:

$$\text{GCH:}\qquad \beth_\alpha = \aleph_\alpha \quad (\text{ekvivalentně:}\ \ 2^{\aleph_\alpha} = \aleph_{\alpha+1}) \quad \text{pro všechna } \alpha \in \mathrm{Ord}.$$

GCH určuje hodnoty kardinálních mocnin a implikuje princip výběru, je ale stejně jako CH a princip výběru nedokazatelná (Cohen 1963–4) a nevyvratitelná (Gödel 1940) z ostatních principů teorie množin. (Tyto výsledky výrazně převyšují rámec kurzu, jejich důkazy jsou nicméně uvedeny v Balcarově a Štěpánkově knize; tam se lze poučit i o dalších nezávislých tvrzeních teorie množin, např. tzv. nedosažitelných kardinálech.)

Card s GCH: $0, 1, 2, \ldots,\ \aleph_0 = \beth_0,\ \mathfrak{c} = \aleph_1 = \beth_1,\ \aleph_2 = \beth_2,\ \ldots,\ \aleph_\omega = \beth_\omega,\ \ldots\ \ldots\ \ldots$

(LOTEM 2016/17, handout k §6.1)

§6. Univerzum množin

§6.1 Zermelovo kumulativní univerzum množin

Problém: Jak poznat množinu od vlastní třídy? (Čekat, zda se objeví spor, je nepraktické.)

Ideálně bychom chtěli, aby každá vlastnost vydělovala množinu (to však víme, že nejde: některé vlastnosti vydělují vlastní třídy).

Naivní princip komprehenze: Každá dobře definovaná vlastnost $\varphi(x)$ vyděluje množinu $\{x \mid \varphi(x)\}$ těch prvků, které ji splňují.

Pozorování: Naivní princip komprehenze vede ke sporu.

Důkaz: Viděli jsme, že vlastnosti být množinou (§4.4), být kardinálem (§4.5) či ordinálem (§5.1) vydělují vlastní třídy – předpoklad, že vydělují množiny, vedl ke sporu.

Jednodušší důkaz (Russellův paradox): třída $R = \{X \mid X \notin X\}$ je vlastní – dle její definice je $R \in R \leftrightarrow R \notin R =$ spor.

Řešení: Matematici si všimli, že některé množinové konstrukce (např. sjednocení, potence, záměna prvků či předpoklad, že $\mathbb{N}$ je množina) je nikdy ke sporu nedovedly.

Opatrné komprehenzní principy:

1. $\mathbb{N}$ je množina.
2. Je-li A množina, pak potence $\mathscr{P}(A)$ je množina.
3. Je-li $\mathcal{A}$ množina množin, pak sjednocení $\bigcup \mathcal{A}$ je množina.
4. Je-li A množina a $\varphi(x, y)$ formule určující funkci, pak $\{y \mid (\exists x \in A)\varphi(x, y)\}$ je množina.

Důsledky opatrných komprehenzních principů: (Důkazy = obtížnější cvičení.)

1. Je-li A množina a $\varphi(x)$ formule, pak $\{x \in A \mid \varphi(x)\}$ je množina.
2. Konečně mnoho libovolných prvků $x_1, \dots, x_n$ tvoří množinu $\{x_1, \dots, x_n\}$.
3. Jsou-li A, B množiny, pak $A \cup B$, $A \cap B$, $A \setminus B$, $A \times B$, A^B jsou množiny.
4. Je-li $\mathcal{A} \neq \emptyset$, pak $\bigcap \mathcal{A}$ je množina.
5. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{R}^n, \mathscr{P}(\mathbb{R})$ atp. jsou množiny.
6. Každá shora omezená třída ordinálů či kardinálů je množina.

Opatrné komprehenzní principy se tak zdají dostačovat pro většinu potřebných konstrukcí. Velikost množin přitom zvětšují pouze komprehenzcní principy sjednocení a potence. Uvažujme tedy pouze množiny, které dostaneme z $\emptyset$ transfinitní iterací operací $\mathscr{P}$ a $\bigcup$.

Kumulativní univerzum množin: Buď U libovolná množina urelementů (prvků, jež nejsou množinami). *Kumulativní univerzum množin* nad U je definováno transfinitní rekurzí:

$$\begin{aligned} V_0(U) &= U \\ V_{\alpha+1}(U) &= \mathscr{P}\big(V_\alpha(U)\big) \\ V_\lambda(U) &= \bigcup_{\beta<\lambda} V_\beta(U) \\ V(U) &= \bigcup_{\alpha\in\mathrm{Ord}} V_\alpha(U) \end{aligned}$$

Prvky $V_0(U)$ jsou urelementy, prvky $V_1(U)$ jsou množiny urelementů, prvky $V_2(U)$ jsou množiny množin urelementů atd. *Rank* množiny $A \in V(U)$ je nejmenší α takové, že $A \subseteq V_\alpha(U)$ (tj. že $A \in V_{\alpha+1}(U)$). Prvky $V_\alpha(U)$ jsou vždy prvky či množiny (množin) z nižších úrovní hierarchie (nižšího ranku). Lze ukázat, že $V(U)$ splňuje všechny opatrné komprehenzní principy, princip extenzionality, princip výběru (pokud jej pro množiny předpokládáme) i princip fundovanosti.

Kumulativní univerzum ryzích množin: Speciální případ $V(\emptyset)$ = von Neumannovo kumulativní univerzum *ryzích množin* (obsahuje pouze množiny množin).

Pozorujte:

- $|V_0(\emptyset)| = 0, \quad |V_{n+1}(\emptyset)| = 2^{|V_n(\emptyset)|} < \aleph_0$ pro $n < \omega, \quad |V_\alpha(\emptyset)| = \beth_\alpha$ pro $\alpha \geq \omega$.
- $V(\emptyset) \subseteq V(U)$
- $V_\beta(U') \subseteq V_{\alpha+\beta}(\emptyset)$ pro $U \approx U' \subseteq V_\alpha(\emptyset)$ a $|U| \leq \beth_\alpha$; tj. $V(U)$ lze reprezentovat ve $V(\emptyset)$

(snadné důkazy transfinitní indukcí). Stačí se tedy omezit na *ryzí množiny.*

Teorie ZFC, jež bude uvedena v §6.2, (neúplně) axiomatizuje právě kumulativní univerzum *ryzích* množin: objekty teorie ZFC jsou pouze množiny, jakékoli nemnožinové prvky (např. čísla) jsou v ní reprezentovány vhodnými množinami (viz §6.3).

§6.2 Axiomatická teorie množin

Definice: *Zermelova-Fraenkelova teorie množin s axiomem výběru* (ZFC) je axiomatická teorie v klasické prvořádové logice s rovností, s jediným binárním predikátem $\in$ a axiomy:

1. *Axiom extenzionality:* $(\forall q)(q \in x \leftrightarrow q \in y) \to x = y$.
   Značení: $x \subseteq y \equiv_{\mathrm{df}} (\forall q)(q \in x \to q \in y)$.
2. *Axiom prázdné množiny:* $(\exists z)(\forall q)\neg(q \in z)$.
   Značení: $z = \emptyset$.
3. *Axiom dvojice:* $(\forall x)(\forall y)(\exists z)(\forall q)(q \in z \leftrightarrow q = x \vee q = y)$.
   Značení: $z = \{x, y\}$, $\{x\} =_{\mathrm{df}} \{x, x\}$.
4. *Axiom sjednocení:* $(\forall x)(\exists z)\big(q \in z \leftrightarrow (\exists u)(q \in u \wedge u \in x)\big)$.
   Značení: $z = \bigcup x$, $u \cup v =_{\mathrm{df}} \bigcup \{u, v\}$.
5. *Axiom potence:* $(\forall x)(\exists z)(\forall q)(q \in z \leftrightarrow q \subseteq x)$.
   Značení: $z = \mathscr{P}(x)$.
6. *Axiom nekonečna:* $(\exists z)\big(\emptyset \in z \wedge (\forall q)(q \in z \to q \cup \{q\} \in z)\big)$.
7. *Schéma axiomů vydělení:* $(\forall x)(\exists z)(\forall q)\big(q \in z \leftrightarrow q \in x \wedge \varphi(q)\big)$
   Značení: $z = \{q \in x \mid \varphi(q)\}$, $x \cap y = \{q \in x \mid q \in y\}$.
8. *Schéma axiomů nahrazení:*
   $$(\forall u)(\forall v)(\forall w)\big(\psi(u, v) \wedge \psi(u, w) \to v = w\big) \to \\ (\forall x)(\exists z)(\forall v)\big(v \in z \leftrightarrow (\exists u)(u \in x \wedge \psi(u, v))\big).$$
9. *Axiom fundovanosti:* $(\forall x)\big(x \neq \emptyset \to (\exists u)(u \in x \wedge u \cap x = \emptyset)\big)$.
10. *Axiom výběru:*
   $$(\forall x)\big(\emptyset \notin x \wedge (\forall u)(\forall v)(u \in x \wedge v \in x \wedge u \neq v \to u \cap v = \emptyset) \to \\ (\exists z)(\forall u)(u \in x \to (\exists q)(u \cap z = \{q\}))\big).$$

Poznámky:

- Axiomy ZFC zachycují jednotlivé množinové principy, které byly probírány na přednášce: 1 = princip extenzionality (§3.1); 9 = princip fundovanosti (ekvivalentní formulace, §3.3); 10 = princip výběru (§5.4); 2–8 = principy opatrné komprehenze a jejich důsledky (§6.1; axiom 6 je ekvivalentní tvrzení, že $\mathbb{N}$ je množina).
- 7 a 8 jsou *schémata axiomů:* pro každou formuli φ resp. ψ jazyka teorie množin z nich dostaneme jeden axiom. (ZFC má tedy *nekonečně mnoho* axiomů.)
- Axiomy nejsou nezávislé: 2 plyne z 6; 3 plyne z 2+5+8; a 7 plyne z 8. K axiomatizaci ZFC tedy stačí axiomy 1, 4, 5, 6, 8, 9 a 10.
- Studují se i různé variace ZFC (např. ZFC + GCH nebo ZF = ZFC bez axiomu výběru) a jiné axiomatiky; ZFC je však v současnosti nejobvyklejší axiomatizací teorie množin.

(LOTEM 2016/17, handout k §6.3)

§6.3 Reprezentace matematických objektů v ZFC

Problém: Jsou-li jedinými objekty teorie ZFC množiny, je třeba ostatní matematické objekty (uspořádané dvojice, čísla) v ZFC reprezentovat vhodnými množinami.

- *Uspořádané dvojice* (Kuratowského definice):

  $$\langle x, y\rangle =_{\mathrm{df}} \{\{x\}, \{x, y\}\}.$$

  Platí: $\langle x_1, y_1\rangle = \langle x_2, y_2\rangle \leftrightarrow x_1 = x_2 \wedge y_1 = y_2$ (viz cvičení k §6.3).

- *Přirozená čísla* (von Neumannova definice): Každé přirozené číslo je ztotožněno s množinou svých předchůdců, tj.:

  $$\begin{aligned} 0 &= \emptyset \\ 1 &= \{0\} = \{\emptyset\} \\ 2 &= \{0, 1\} = \{\emptyset, \{\emptyset\}\} \\ 3 &= \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \end{aligned}$$

  atd., vždy $n + 1 = n \cup \{n\}$.

  Množina $\mathbb{N}$ všech přirozených čísel je definována jako nejmenší *induktivní množina,* tj. množinou obsahující $\emptyset$ a s každým n obsahující $n \cup \{n\}$. (Axiom nekonečna říká, že existuje nějaká induktivní množina z, průnik všech induktivních částí z pak definuje $\mathbb{N}$.)

- *Celá* čísla lze definovat jako dvojice $\langle s, n\rangle$ pro $s \in \{-1, 1\}$ a $n \in \mathbb{N}$, *racionální* jako nesoudělné dvojice celých čísel, *reálná* jako desetinné rozvoje čili posloupnosti celých čísel, *komplexní* čísla jako dvojice čísel reálných.

  Množiny $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ lze tedy získat pomocí axiomů vydělení vhodnými podmínkami z množin $\mathbb{N}^2$, $\mathbb{N}^{\mathbb{N}}$ a $\mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}}$.

- *Ordinální čísla* $\alpha \in \mathrm{Ord}$ jsou ztotožněna s množinami $[0, \alpha)$ svých předchůdců, tedy konečná s přirozenými čísly, $\omega = \mathbb{N}$, $\omega + 1 = \omega \cup \{\omega\}$ atd., vždy $\alpha + 1 = \alpha \cup \{\alpha\}$ a limitní $\lambda = \bigcup_{\alpha<\lambda} \alpha$. (Množina $\mathbb{N}$ se proto často v matematice označuje i ω.)

  Společná (umělá) podmínka vydělující třídu všech ordinálů je např. tato: ordinální číslo je tranzitivní množina α (tj. taková, že $(\forall x)(x \in \alpha \to x \subseteq \alpha)$) dobře uspořádaná relací $\in$.

- *Kardinální čísla* jsou ztotožněna se svými iniciálními ordinály, tedy konečná s konečnými ordinály, $\aleph_0 = \omega$, $\aleph_1 = \omega_1$ atd., vždy $\aleph_\alpha = \omega_\alpha$.

Ukazuje se, že prakticky všechny matematické pojmy lze takto reprezentovat množinami a jejich vlastnosti dokázat v teorii ZFC. Teorie množin ZFC tak může sloužit jako *základová teorie* pro (téměř) celou současnou matematiku.