(LOTEM 2018/19, handout k §1.1)

1. Pojem množiny

1.1 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.

Logické symboly. Některé slovní obraty mají v matematickém textu ustálený význam a vyskytují se natolik často, že jsou pro ně zavedeny speciální značky a názvy:

$\&$	=	a	*konjunkce*
$\vee$	=	nebo	*disjunkce* (nevylučovací)
$\neg$	=	není pravda, že …	*negace*
$\to$	=	jestliže …, pak …	*implikace*
$\leftrightarrow$	=	právě když	*ekvivalence*
$(\forall x)$	=	pro každé x platí, že …	*univerzální kvantifikátor*
$(\exists x)$	=	existuje x takové, že …	*existenční kvantifikátor*

Dosah těchto symbolů je nutno vyznačovat závorkami, např. $(x > 1 \;\&\; x < 2) \vee x = 0$. Pro ušetření některých závorek obvykle předpokládáme, že symboly $\to, \leftrightarrow$ vážou méně silně než ostatní. Místo znaku $\neg$ často jen škrtáme příslušný symbol, např. $\neg(x = 5)$ píšeme $x \neq 5$.

Příklady zápisů pomocí logických symbolů:

- Větu „Jestliže $x^2 = 1$, pak $x = 1$ nebo $x = -1$“ lze psát: $x^2 = 1 \to (x = 1 \vee x = -1)$.
- Zápis $(\forall a)(a + a = 3a)$ vyjadřuje nepravdivé tvrzení (jaké?), kdežto $(\exists a)(a + a = 3a)$ pravdivé (proč?).
- Tvrzení „ke každému číslu existuje číslo větší“ lze zapsat jako $(\forall x)(\exists y)(y > x)$. Tvrzení „existuje nejmenší číslo“ lze zapsat jako $(\exists x)(\forall y)(x \leq y)$.

  Pozorujte: pro posouzení pravdivosti je třeba mít určen obor proměnných – např. posledně uvedené tvrzení je pravdivé v oboru čísel přirozených, ale nepravdivé v reálných.

Informace k množinové části kurzu: `libor.behounek.online/lotem`

(LOTEM 2018/19, handout k §1.2)

1.2 Množiny a jejich prvky

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: $-1 \notin \mathbb{N}$, $\sqrt{2} \notin \mathbb{Q}$.

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

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

Za množiny tedy nepovažujeme např. neurčitě 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: množina $\mathbb{N}$ všech přirozených čísel je rovna množině všech celých čísel z intervalu $(-\frac{1}{2}, +\infty)$.

Komprehenzní termy.

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

  Jsou-li prvky členy pravidelné posloupnosti, lze použíy trojtečku, např. $\mathbb{N} = \{0, 1, 2, \ldots\}$.

- Množinu právě těch prvků x, které mají vlastnost Φ, značíme $\{x \mid \Phi\}$; např.:

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

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

  Podobně $(\exists x \in A)\Psi$ a $(\forall x \in A)\Psi$ jsou zkratky za časté zápisy tvaru $(\exists x)(x \in A \,\&\, \Psi)$ resp. $(\forall x)(x \in A \rightarrow \Psi)$. Příklady: $(\exists n \in \mathbb{N})(n^2 = 4)$, $(\forall x \in \mathbb{R})(x^2 \geq 0)$.

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

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.

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

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

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

$$A \cup B = \{x \mid x \in A \vee x \in B\},$$
$$A \cap B = \{x \mid x \in A \,\&\, x \in B\},$$
$$A \setminus B = \{x \mid x \in A \,\&\, x \notin B\}.$$

Příklad: Množina všech iracionálních čísel je definována jako $\mathbb{R} \setminus \mathbb{Q}$.

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 $\mathbb{R} \setminus \mathbb{Q}$.

(LOTEM 2018/19, handout k §2.1)

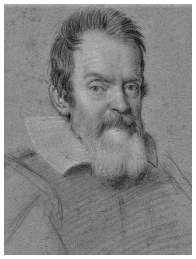
2. Mohutnosti množin

2.1 Inkluze a ekvivalence množin

Galileův paradox. Sudých přirozených čísel je zjevně *méně* než všech přirozených čísel (sudé je jen každé druhé). Lze je však se všemi přirozenými čísly vzájemně jednoznačně spárovat – tedy zároveň je jich vlastně *stejně mnoho:*

$$\begin{array}{cccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & \cdots \end{array}$$

Galilei uvedl tento paradox v dialogu O dvou nových vědách (1638); usoudil z něj, že porovnávat nekonečná množství není možné. Cantorova teorie množin jej řeší rozlišením dvou způsobů porovnání nekonečných množin – pomocí *inkluze* a *ekvivalence.*



Galileo Galilei

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:

$$A \subseteq B \equiv_{\text{def}} (\forall x)(x \in A \to x \in B).$$

Vztah $\subseteq$ nazýváme *inkluze.* Zápis $\neg(A \subseteq B)$ zkracujeme $A \not\subseteq B$. Vztah $A \subseteq B \;\&\; A \neq B$ zapisujeme $A \subset B$ či $A \subsetneq B$ a hovoříme o *ostré inkluzi* a *vlastní podmnožině.*

Příklady: $[0, \pi) \subset \mathbb{R}$; krychle je (vlastní) částí koule jí opsané; $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Vlastnosti inkluze:

1. $A \subseteq B \;\&\; B \subseteq C \to A \subseteq C$
2. $A \subseteq B \;\&\; B \subseteq A \to A = B$
3. $\emptyset \subseteq A, \quad A \subseteq A$

(Pozn.: Nejsou-li v tvrzeních uvedeny kvantifikátory, je míněna obecná platnost pro všechny hodnoty proměnných, tj. jako by byly kvantifikovány univerzálně. Poslední tvrzení tedy znamená $(\forall A)(A \subseteq A)$.)

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 $\pi \notin \mathbb{R}$. (Je ovšem $\{\pi\} \subseteq \mathbb{R}$, zatímco $\{\pi\} \notin \mathbb{R}$.)
- 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 $\mathbb{N} \notin \mathbb{Z}$.

Inkluze a velikost množin. Velikosti množin sice můžeme srovnávat inkluzí, mnoho dvojic množin je v ní ale neporovnatelných – např. $\{1,3,5\} \not\subseteq \{5,\pi,\sqrt{2}\}$ a ani naopak, $\{5,\pi,\sqrt{2}\} \not\subseteq \{1,3,5\}$, přestože obě množiny jsou trojprvkové, tedy „stejně velké“. Lepším způsobem porovnávání velikostí množin je vzájemně jednoznačné párování jejich prvků jako v Galileově paradoxu; to vede k pojmům bijekce a množinové ekvivalence.

Bijekce. *Bijekcí* mezi množinami A a B rozumíme vzájemně jednoznačné přiřazení mezi prvky obou množin – tj. když každému prvku množiny A je přiřazen právě jeden prvek množiny B a každý prvek množiny B je přiřazen právě jednomu prvku množiny A.

Příklad: Přiřazení $F\colon n \mapsto 2n$ (pro každé $n \in \mathbb{N}$) je bijekcí mezi množinou $\mathbb{N}$ všech přirozených čísel a množinou $\{2n \mid n \in \mathbb{N}\}$ všech sudých přirozených čísel.

Značení: Je-li přiřazení F bijekcí mezi A a B, píšeme $F\colon A \leftrightarrow B$. Bijekcím se též říká *vzájemně jednoznačná zobrazení.* (Definici bijekce později zpřesníme.)

Ekvivalence množin. Existuje-li bijekce $F\colon A \leftrightarrow B$, říkáme, že množiny A a B jsou *ekvivalentní* a píšeme $A \approx B$. (Terminologie též: A, B jsou *ekvipotentní, ekvipolentní, stejné mohutnosti* či *stejné kardinality*).

Příklady:

- $\{5,\pi,\sqrt{2}\} \approx \{1,2,3\}$. Důkaz: bijektivní přiřazení je např.: $5 \mapsto 1$, $\pi \mapsto 2$, $\sqrt{2} \mapsto 3$.
- $\mathbb{N} \approx \{2n \mid n \in \mathbb{N}\}$, např. přiřazením $F\colon n \mapsto 2n$ pro všechna $n \in \mathbb{N}$.
- $[0,1] \approx [0,5]$, např. bijekcí $G\colon x \mapsto 5x$ pro všechna $x \in [0,1]$.

Řešení Galileova paradoxu. Sudých přirozených čísel je méně než všech přirozených čísel *ve smyslu inkluze,* ale je jich stejně jako všech přirozených čísel *ve smyslu ekvivalence:*

$$\{2n \mid n \in \mathbb{N}\} \subset \mathbb{N}, \text{ ale } \{2n \mid n \in \mathbb{N}\} \approx \mathbb{N}.$$

Je to přitom pojem ekvivalence, který lépe než inkluze vystihuje velikost množin – např. konečné množiny jsou ekvivalentní, právě když mají týž počet prvků. (Nacházení bijekcí mezi množinami, a tedy důkazy ekvivalence různých množin, procvičíme v příkladech na cvičení.)

(LOTEM 2018/19, handout k §2.2)

2.2 Spočetné a nespočetné množiny

Ve cvičeních jsme si ukázali ekvivalenci mnoha nekonečných množin, např. $\mathbb{N} \approx \mathbb{Z}$, $\mathbb{R} \approx [0,1]$ atd. Vzniká otázka, zda nejsou všechny nekonečné množiny vzájemně ekvivalentní. Ukazuje se, že nikoli: např. $\mathbb{N} \not\approx \mathbb{R}$. Elegantní metodou, jak neexistenci bijekce mezi některými množinami dokázat, je tzv. Cantorova diagonálizace:

Věta: $\mathbb{N} \not\approx \mathbb{R}$.

Důkaz Cantorovou diagonální metodou: 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 bijekce, spor. □

Důsledek: Tedy také $\mathbb{Z} \not\approx \mathbb{R}$, neboť $\mathbb{Z} \approx \mathbb{N}$; podobně $\mathbb{N} \not\approx [0,1]$, neboť $[0,1] \approx \mathbb{R}$; atp.

Množina $\mathbb{R}$ tak má jinou nekonečnou mohutnost než množiny $\mathbb{N}$ či $\mathbb{Z}$. Reálných čísel je přitom (ve smyslu mohutnosti) očividně *více* než čísel přirozených: Cantorova diagonalizace ukázala, že $\mathbb{N}$ lze bijektivně zobrazit na vlastní část $\mathbb{R}$, ale nikdy ne na celé $\mathbb{R}$. Tato vlastnost je vhodným kritériem porovnávání konečných i nekonečných mohutností:

Subvalence. Říkáme, že množina A je *subvalentní* množině B, pokud existuje bijekce množiny A na nějakou podmnožinu množiny B. Značení: $A \preceq B$. (Bijekcím A na podmnožinu B se též říká *injekce* či *prostá zobrazení* A do B.)

Zápis $A \prec B$ (striktní subvalence) znamená, že $A \preceq B$, ale $A \not\approx B$. Pokud $A \prec B$, říkáme též, že A má *menší mohutnost* či *menší kardinalitu* než B. Příklady:

- Cantorova diagonalizace ukazuje, že $\mathbb{N} \prec \mathbb{R}$. (Tudíž také $\mathbb{Z} \prec \mathbb{R}$, $\mathbb{N} \prec [0,1]$ atp.)
- Každá konečná množina je striktně subvalentní libovolné nekonečné (rozmyslete).
- Pro konečné množiny platí, že m-prvková je subvalentní n-prvkové, právě když $m \leq n$ (rozmyslete). Speciálně $\emptyset$ je subvalentní každé množině (má nejmenší kardinalitu).

Nejmenší nekonečná mohutnost. Mohutnost množiny $\mathbb{N}$ je nejmenší (ve smyslu subvalence) mezi všemi nekonečnými množinami, jak plyne z tohoto tvrzení:

Tvrzení: Je-li množina A nekonečná, pak $\mathbb{N} \preceq A$.

Důkaz: Protože A je nekonečná, můžeme postupně vybírat její prvky, vždy různé od všech předchozích, a přiřazovat je po řadě všem přirozeným číslům $0, 1, 2, \ldots$ (Kdyby v n-tém kroku žádný nezbýval, znamenalo by to, že A má jen $n-1$ prvků, tedy že je konečná – spor s předpokladem.) Tím postupně zkonstruujeme bijekci $\mathbb{N}$ na část množiny A, tedy $\mathbb{N} \preceq A$. □

Spočetné množiny. Množiny ekvivalentní s $\mathbb{N}$ tedy mají nejmenší nekonečnou mohutnost. Jsou to přitom právě ty množiny, jejichž prvky lze vzájemně jednoznačně očíslovat všemi přirozenými čísly, neboli je seřadit do nekonečné posloupnosti (rozmyslete podle definice ekvivalence s $\mathbb{N}$). To motivuje následující pojem:

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

Příklady:

- Množiny $\mathbb{N}$, $\mathbb{Z}$ a všechny jim ekvivalentní množiny (např. všechny jejich nekonečné podmnožiny, množina $\mathbb{Z} \cup \{\mathrm{e}, \pi, \sqrt{2}\}$ apod.) a také všechny konečné množiny jsou *spočetné.*

  Poznámka: Někteří autoři nazývají spočetnými pouze nekonečné spočetné množiny. Spočetným včetně konečných pak říkají „nejvýše spočetné".

- Jak ukazuje Cantorova diagonalizace, $\mathbb{R}$ a všechny množiny jí ekvivalentní (např. všechny reálné intervaly, množina všech bodů úsečky či přímky atp.) jsou *nespočetné.*

Nespočetné množiny. Vzniká další přirozená otázka, zda jsou všechny nespočetné množiny ekvivalentní $\mathbb{R}$ – jinak řečeno zda existují jen dvě nekonečné mohutnosti (spočetná a nespočetná). Variantou Cantorova diagonálního důkazu lze ukázat, že nikoli: např. množina všech reálných funkcí reálné proměnné, kterou je zvykem značit $\mathbb{R}^{\mathbb{R}}$, má větší mohutnost než $\mathbb{R}$:

Tvrzení: $\mathbb{R} \prec \mathbb{R}^{\mathbb{R}}$.

Důkaz: Nechť je každému $r \in \mathbb{R}$ přiřazena nějaká reálná funkce reálné proměnné $f_r \in \mathbb{R}^{\mathbb{R}}$. Sestrojíme funkci $g \in \mathbb{R}^{\mathbb{R}}$, která není přiřazena žádnému $r \in \mathbb{R}$, takto: pro každé $r \in \mathbb{R}$ buď $g(r) = f_r(r) + 1$. Pro žádné $r \in \mathbb{R}$ není $g = f_r$, neboť g se liší od f_r aspoň v bodě r. Každé přiřazení funkcí z $\mathbb{R}^{\mathbb{R}}$ reálným číslům tedy vždy nějakou funkci vynechává, proto $\mathbb{R} \not\approx \mathbb{R}^{\mathbb{R}}$. Triviálně ovšem $\mathbb{R} \preceq \mathbb{R}^{\mathbb{R}}$, např. přiřazením příslušné konstantní funkce každému $r \in \mathbb{R}$. □

Existují tedy nejméně dvě nespočetné mohutnosti (později uvidíme, že je jich mnohem více). Pro jejich rozlišení říkáme, že:

- Množina A má *mohutnost kontinua,* pokud $A \approx \mathbb{R}$.
- Množina A má mohutnost *potence kontinua,* pokud $A \approx \mathbb{R}^{\mathbb{R}}$.

Nekonečná kardinální čísla. Mohutnosti konečných množin označujeme přirozenými čísly, vyjadřujícími počet jejich prvků. Pro označení počtů prvků (mohutností) nekonečných množin potřebujeme nová, nekonečná čísla:

- Mohutnost nekonečných spočetných množin značíme $\aleph_0$ (alef nula). Mohutnost kontinua značíme $\mathfrak{c}$ (gotické c). Mohutnost potence kontinua značíme $2^{\mathfrak{c}}$ (dvě na kontinuum).
- Mohutnost množiny A značíme obecně $|A|$.
  Příklady: $|\emptyset| = 0$, $\left|\{x \in \mathbb{R} \mid x^2 = 1\}\right| = 2$, $|\mathbb{N}| = |\mathbb{Z}| = \aleph_0$, $|\mathbb{R}| = |(0,1)| = \mathfrak{c}$, $|\mathbb{R}^{\mathbb{R}}| = 2^{\mathfrak{c}}$.

Čísla označující konečné i nekonečné mohutnosti se nazývají *kardinální čísla* či krátce *kardinály* (z lat. *numerus cardinalis* = číslovka základní = „kolik?"). Konečné kardinály jsou prostě čísla přirozená, z nekonečných známe zatím tři: $\aleph_0$, $\mathfrak{c}$, $2^{\mathfrak{c}}$. Podle velikosti (tj. subvalencí) je lze seřadit takto:

$$0 < 1 < 2 < 3 < \cdots < \aleph_0 < \mathfrak{c} < 2^{\mathfrak{c}}.$$

Později poznáme mnoho dalších (zejména větších) kardinálů a naučíme se je sčítat a násobit.

(LOTEM 2018/19, handout k §2.3)

2.3 Cantorova-Bernsteinova věta

Věta spojovaná se jmény Cantora, Bernsteina a Schrödera, poprvé však zřejmě dokázaná Dedekindem, umožňuje dokázat ekvivalenci množin A a B nalezením dvou injekcí, z A do B a naopak. To je často výrazně jednodušší než přímá konstrukce bijekce mezi A a B.


Ernst Schröder


Felix Bernstein


Richard Dedekind

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

V důkazu využijeme standardní značení:

- Obraz množiny X v zobrazení F, tj. množinu všech prvků přiřazených zobrazením F prvkům množiny X, značíme $F[X]$.
- Pro zobrazení F a G značí $F \circ G$ jejich složení, tj. přiřazení $F \circ G\colon x \mapsto z$, pokud $F\colon x \mapsto y$ a $G\colon y \mapsto z$. (Pozorujte: složení bijekcí je bijekce.)

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:

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

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

Důsledek: Pokud $A \subseteq B$ a $B \preceq A$, pak již $A \approx B$.

Důkaz: Je-li $A \subseteq B$, pak samozřejmě také $A \preceq B$, neboť přiřazení $x \mapsto x$ pro každé $x \in A$ je injekcí A do B. □

Víme-li tedy, že A je podmnožinou B, stačí pro důkaz ekvivalence $A \approx B$ najít injekci B do A.

(LOTEM 2018/19, handout k §2.4)

2.4 Kartézské součiny

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

$$A \times B = \{\langle a, b\rangle \mid a \in A \,\&\, b \in B\}$$
$$A_1 \times \cdots \times A_n = \{\langle a_1, \ldots, a_n\rangle \mid a_1 \in A_1 \,\&\, \ldots \,\&\, a_n \in A_n\}$$

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

René Descartes (Cartesius)

Bijekce a injekce. Pomocí pojmu kartézského součinu lze mj. upřesnit definici bijekce a injekce. Bijektivní či injektivní zobrazení mezi množinami A a B lze chápat jako množinu uspořádaných dvojic vzor–obraz, tedy jako podmnožinu kartézského součinu $A \times B$, splňující příslušné podmínky jednoznačného přiřazení prvků.

Upřesněná definice: *Bijekcí* mezi množinami A a B rozumíme kteroukoli podmnožinu F kartézského součinu $A \times B$ takovou, že:

$$(\forall x \in A)(\exists!\, y \in B)\big(\langle x, y\rangle \in F\big) \,\&\, (\forall y \in B)(\exists!\, x \in A)\big(\langle x, y\rangle \in F\big).$$

Injekcí z A do B rozumíme bijekci mezi A a některou podmnožinou $C \subseteq B$. Místo $\langle x, y\rangle \in F$ obvykle píšeme $F(x) = y$.

Mohutnosti kartézských součinů. Pro konečné množiny $|A| = n$, $|B| = n$ je samozřejmě $|A \times B| = m \cdot n$. Pro nekonečné množiny dokážeme několik tvrzení.

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

Důkaz: Cantorova párovací funkce $\pi(m, n) = \frac{1}{2}(m + n)(m + n + 1) + n$ je bijekcí $\pi\colon \mathbb{N}^2 \leftrightarrow \mathbb{N}$. Protože $\mathbb{Z} \approx \mathbb{N}$ (viz §2.1), je také $\mathbb{Z}^2 \approx \mathbb{N}^2 \approx \mathbb{N}$. 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: $\mathbb{R}^2 \approx \mathbb{R}$.

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 injektivní (zdůvodněte). □

Důsledek: Tedy také např. $\mathbb{N} \approx \mathbb{Q}^2 \approx \mathbb{N}^3 \approx \mathbb{Z}^4$; $\mathbb{R} \approx \mathbb{C} \approx \mathbb{R}^3$; úsečka je ekvivalentní čtverci, kruhu, krychli, hyperboloidu; atp. (Ujasněte si proč.)

Tvrzení:

1. Jsou-li A, B spočetné, pak také $A \cup B$, $A \times B$ jsou spočetné.
2. Mají-li A, B mohutnost kontinua, pak také $A \cup B$, $A \times B$ mají mohutnost kontinua.

Důkaz:

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 $\mathbb{R} \preceq A \cup B \preceq [0,1) \cup [1,2) = [0,2) \approx \mathbb{R}$, $A \times B \approx \mathbb{R} \times \mathbb{R} \approx \mathbb{R}$. □

Důsledek: Množina $\mathbb{R} \setminus \mathbb{Q}$ všech iracionálních čísel je nespočetná.

Důkaz: Kdyby byla spočetná, byla by dle předchozích tvrzení spočetná i $(\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q} = \mathbb{R}$, ta však je nespočetná; spor. (Složitějším důkazem lze ukázat i to, že $\mathbb{R} \setminus \mathbb{Q} \approx \mathbb{R}$.) □

(LOTEM 2018/19, handout k §2.5)

2.5 Množiny množin

Množiny jako prvky množin. Podle Cantorovy definice (§1.2) 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 reálných intervalů, množina všech trojúhelníků v rovině, množina všech podmnožin $\mathbb{R}$ 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.
- Rozlišujte: $\emptyset \neq \{\emptyset\} \neq \{\{\emptyset\}\}$. (Zdůvodněte!)

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:

$$x \in \bigcup \mathscr{A} \leftrightarrow (\exists A)(A \in \mathscr{A} \,\&\, x \in A), \quad \text{tj. } \bigcup \mathscr{A} = \{x \mid (\exists A \in \mathscr{A})(x \in A)\}$$
$$x \in \bigcap \mathscr{A} \leftrightarrow (\forall A)(A \in \mathscr{A} \to x \in A), \quad \text{tj. } \bigcap \mathscr{A} = \{x \mid (\forall A \in \mathscr{A})(x \in A)\}$$

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

Pozorujte: $\bigcup\{A,B\} = A \cup B$, $\bigcap\{A,B\} = A \cap B$.

Tvrzení:

1. Sjednocení spočetně mnoha spočetných množin je spočetné.
2. Sjednocení spočetně mnoha množin mohutnosti kontinua má mohutnost kontinua.

Důkaz: Bez újmy na obecnosti můžeme předpokládat, že uvažované množiny jsou vzájemně disjuktní. (Nejsou-li, mohutnost se nezvětší – rozmyslete.)

1. 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 $\bigcup_{i\in\mathbb{N}} A_i$.
2. Mějme vzájemně disjunktní $A_i \approx \mathbb{R} \approx [i, i+1)$ pro každé $i \in \mathbb{N}$. Pak $\bigcup_{i\in\mathbb{N}} A_i \approx \bigcup_{i\in\mathbb{N}} [i, i+1) \approx [0, +\infty) \approx \mathbb{R}$. □

Důsledek: Množina $\mathbb{A}$ všech algebraických čísel je spočetná. (Rozmyslete: celočíselných polynomů stupně n je spočetně mnoho a každý má nejvýše n kořenů.) Tedy množina $\mathbb{R} \setminus \mathbb{A}$ všech reálných transcendentních čísel je nespočetná (lze ukázat, že má mohutnost kontinua).

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

Příklady:

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

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 přiřazení jsou zjevně injektivní (zdůvodněte). □

Tvrzení: $\mathscr{P}(\mathbb{R}) \approx \mathbb{R}^{\mathbb{R}}$. (Pro definici $\mathbb{R}^{\mathbb{R}}$ viz §2.2.)

Důkaz: Je $\mathscr{P}(\mathbb{R}) \preceq \mathbb{R}^{\mathbb{R}}$, neboť každé podmnožině $A \subseteq \mathbb{R}$ lze injektivně přiřadit její *charakteristickou funkci* $\chi_A \in \mathbb{R}^{\mathbb{R}}$, kde $\chi_A(x) = 1$ pro $x \in A$ a $\chi_A(x) = 0$ pro $x \notin A$. Obráceně také $\mathbb{R}^{\mathbb{R}} \preceq \mathscr{P}(\mathbb{R})$, neboť každá reálná funkce $F \in \mathbb{R}^{\mathbb{R}}$ má injektivně přiřazen svůj *graf* $\{\langle x, F(x)\rangle \mid x \in \mathbb{R}\} \subseteq \mathbb{R}^2$, takže $\mathbb{R}^{\mathbb{R}} \preceq \mathscr{P}(\mathbb{R}^2) \approx \mathscr{P}(\mathbb{R})$. □

Vidíme, že $\mathscr{P}(\mathbb{N})$ má mohutnost kontinua a $\mathscr{P}(\mathbb{R})$ má mohutnost potence kontinua (viz §2.2). V obou případech je tedy mohutnost potenční množiny větší než mohutnost původní množiny: $\mathscr{P}(\mathbb{N}) \approx \mathbb{R} \succ \mathbb{N}$ a $\mathscr{P}(\mathbb{R}) \approx \mathbb{R}^{\mathbb{R}} \succ \mathbb{R}$. To není náhoda – později uvidíme, že $\mathscr{P}(A)$ má vždy větší mohutnost než A.

(LOTEM 2018/19, handout k §2.6)

2.6 Podmnožiny kontinua

Viděli jsme, že mnohé zdánlivě velké množiny reálných čísel (např. $\mathbb{Q}$, $\mathbb{A}$) jsou pouze spočetné. Naopak některé na pohled „téměř prázdné“ množiny mají mohutnost kontinua:

Cantorovo diskontinuum. Odstraňme z intervalu $[0,1]$ jeho otevřenou prostřední třetinu $(\frac{1}{2},\frac{2}{3})$; z obou zbývajících intervalů odstraňme jejich otevřené prostřední třetiny; ze všech čtyř zbývajících intervalů odstraňme jejich otevřené prostřední třetiny; atd. do nekonečna. Sjednocení intervalů zbývajících v n-tém kroku označme D_n a vezměme jejich průnik $\mathbb{D} = \bigcap_{n\in\mathbb{N}} D_n$, zvaný *Cantorovo diskontinuum.*

Všimněte si: po n-tém kroku zbývá sjednocení 2^n uzavřených intervalů délky $1/3^n$, odstranili jsme tedy intervaly celkové délky $1-(2/3)^n$. Po provedení všech kroků jsou tak odstraněny intervaly celkové délky 1, tj. $\mathbb{D}$ má míru 0. Přesto $\mathbb{D}\neq\emptyset$, naopak $\mathbb{D}$ má mohutnost kontinua:

Tvrzení: $\mathbb{D}\approx\mathbb{R}$.

Důkaz: Pozorujte, že $\mathbb{D}$ obsahuje právě ta reálná čísla z intervalu $[0,1]$, která mají trojkový rozvoj neobsahující číslici 1: v n-tém kroku jsme totiž odstranili právě čísla s cifrou 1 na n-tém místě trojkového rozvoje. (Rozvoje s koncovou periodou 2 tentokrát povolujeme, takže např. $1/3\in\mathbb{D}$ díky trojkovému rozvoji 0,02222…) Sestrojíme injekci $F\colon [0,1)\to\mathbb{D}$ tak, že číslu $r\in[0,1)$ s binárním rozvojem $r=\sum_{n=1}^{\infty} b_i\cdot 2^{-n}$ přiřadíme číslo $F(r)=\sum_{n=1}^{\infty} 2b_i\cdot 3^{-n}$; jinak řečeno, v jednoznačném *dvojkovém* rozvoji r nahradíme všechny výskyty číslice 1 číslicí 2 a výsledek chápeme jako *trojkový* rozvoj čísla $F(r)$. Ujasněte si, že $F(r)\in\mathbb{D}$, že F je injektivní, a že tudíž $\mathbb{R}\approx[0,1)\preceq\mathbb{D}\subseteq\mathbb{R}$, tedy $\mathbb{D}\approx\mathbb{R}$ díky Cantorově-Bernsteinově větě. □

Poučení: Mohutnosti množin reálných čísel nelze snadno poznat „od pohledu“ – je nutno poctivě sestrojovat bijekce (či injekce).

Mohutnost a míra. Určování mohutností množin by bylo samoúčelné, kdyby mohutnost neměla žádné podstatné matematické důsledky. Jedním z takových důsledků je ale např. fakt, že všechny *spočetné* podmnožiny $\mathbb{R}$ mají *nulovou míru,* tj. lze je pokrýt sjednocením intervalů libovolně malé délky:

Tvrzení: Každá spočetná podmnožina $\mathbb{R}$ má míru 0.

Důkaz: Buď $A\subseteq\mathbb{R}$ spočetná a buď ε libovolně malé kladné reálné číslo. Pokryjeme prvky A intervaly celkové délky nepřevyšující ε. Množina A je spočetná, její prvky lze tedy seřadit do posloupnosti $a_0,a_1,a_2,\ldots$ Každý prvek $a_n\in A$ pokryjeme intervalem $(a_n-\varepsilon/2^{n+2}, a_n+\varepsilon/2^{n+2})$. Pozorujte, že jejich celková délka je $\varepsilon/2+\varepsilon/4+\varepsilon/8+\cdots=\varepsilon$ a pokrývají všechny prvky A. □

Důsledek: $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{A}$ mají míru 0. (Naopak tedy např. $[0,1]\setminus\mathbb{Q}$ má míru $1-0=1$.) Ne každá množina míry 0 však musí být spočetná, jak ukazuje např. Cantorovo diskontinuum.

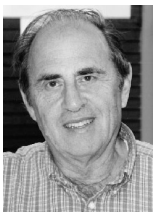
Hypotéza kontinua. Všechny dosud uvažované podmnožiny $\mathbb{R}$ byly buď spočetné, nebo měly mohutnost kontinua. To vedlo Cantora (1878) k formulaci hypotézy, kterou se léta marně snažil dokázat:

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.


David Hilbert


Kurt Gödel


Paul Cohen

Algoritmicky vyčíslitelná čísla. Ujasněte si:

1. Kolik je všech možných řetězců délky n v dané konečné abecedě, např. ASCII či Unicode?
2. Kolik je tudíž všech možných konečných řetězců v této abecedě? (Použijte tvrzení o mohutnosti spočetného sjednocení spočetných množin.)
3. Kolik je tedy všech možných programů ve vašem oblíbeném programovacím jazyce?
4. Kolik je tudíž reálných čísel, jejichž nekonečné desetinné rozvoje lze postupně vypisovat počítačovým programem?

Vidíme, že *algoritmicky vyčíslitelných* reálných čísel je pouze spočetně – drtivou většinu reálných čísel tedy nejen nelze zapsat, ale ani algoritmicky popsat. Většina reálných čísel je tak našimi konečnými prostředky neuchopitelná – nemělo by nás tedy příliš udivovat, že některá tvrzení o množinách reálných čísel (jako CH) nelze v teorii množin dokázat ani vyvrátit.

(LOTEM 2018/19, handout k §2.7)

2.7 Dodatečné množinové principy

CH jako dodatečný množinový princip. V předchozím oddílu jsme viděli, že Cantorovu hypotézu kontiua (CH) nelze v teorii množin dokázat ani vyvrátit. Můžeme tudíž dle chuti buď ji, nebo její negaci přijmout jako dodatečný *množinový princip* (viz §2.1), upřesňující jinak neurčené chování množin reálných čísel.

Další volitelné množinové principy. Jsou i další množinové principy, které můžeme buď přijmout, nebo odmítnout, a tím upřesnit Cantorův pojem množiny. Zmíníme stručně několik nejdůležitějších. V předchozích oddílech jsme již tiše používali dva explicitně neuvedené principy, dnes běžně přijímané, ale v minulosti kontroverzní (aktuální nekonečno, nekonstruktivní vymezení výběrové množiny):

Princip nekonečna: Obor všech přirozených čísel tvoří množinu.

Odmítnutí principu nekonečna by vedlo 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 nepráznych množin). Stejně jako v případě CH, princip výběru nelze dokázat ani vyvrátit z ostatních principů teorie množin (nevyvratitelnost Gödel 1940, nedokazatelnost Cohen 1963 jako u CH).

Pozor: princip výběru *není* tvrzením, že z neprázdné množiny lze vybrat nějaký prvek (to je z ostatních principů dokazatelné). Podstatná je v něm možnost výběru *třeba i nekonečně mnoha nijak nespecifikovaných* prvků zároveň.

Pro jeho nekonstruktivní povahu bývá zvykem použití principu výběru (či některé z jeho mnoha ekvivalentních variant) explicitně zmiňovat a vyznačovat. V tomto kurzu byl zatím použit pro důkaz těchto tvrzení (ve všech případech podstatně, tj. jeho použití nelze obejít):

- Je-li A nekonečná, pak $\mathbb{N} \preceq A$ (§2.2): důkaz vybíral v nekonečně mnoha krocích vždy další nespecifikovaný prvek.
- Sjednocení spočetně mnoha spočetných množin je spočetné; sjednocení spočetně mnoha množin mohutnosti kontinua má mohutnost kontinua (§2.5): náš důkaz tiše vybral pro každý prvek spočetné množiny množin vždy *jednu* ze všech bijekcí na $\mathbb{N}$ resp. $[0, 1)$.

Nefundované množiny. Může být množina svým vlastním prvkem, např. $X = \{X\}$ či $Y = \{5, \pi, \sqrt{2}, Y\}$? 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.*

(LOTEM 2018/19, handout k §2.8 a začátku §2.9)

2.8 Cantorova věta

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

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

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:

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

  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 (§1.2) je množina „souhrn objektů v jeden celek“. Cantorův paradox lze chápat jako důkaz, že *není možné* shrnout všechny množiny v jeden celek; tedy že *neexistuje* množina všech množin.

Vlastní třídy. Obor všech množin tedy 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 a ve cvičeních uvidíme další vlastní třídy.)

Protože vlastní třídy nemohou být chápány jako konkrétní, definitivně vytvořené matematické objekty, nemohou se stávat prvky množin (srv. Cantorovu definici z §1.2: „*konkrétních* rozlišených *objektů*“). Definici náležení lze sice rozšířit i na náležení prvků do vlastních tříd, např. $\emptyset \in \mathrm{V}$, vlastní třídy ale nemohou stát na levé straně vztahu náležení (tj. lze psát např. $A \in \mathrm{V}$, nikoli však $\mathrm{V} \in A$).

Podobně lze na vlastní třídy rozšířit i množinové pojmy, v jejichž definici se vlastní třídy nevyskytnou na levé straně vztahu náležení – např. inkluzi či elementární množinové operace. Příklady: $\mathscr{P}(A) \subseteq \mathrm{V}$, neboť $\mathscr{P}(A)$ má za prvky pouze množiny, tj. prvky V; průnik $A \cap \mathrm{V}$ je množina všech prvků A, které jsou množinami; atp.

2.9 Kardinální čísla

Kardinální čísla. *Kardinální čísla* (či 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 (čili konečné kardinály) ztotožňujeme s přirozenými čísly: pro m-prvkovou množinu A píšeme $|A| = m$. Pro význačné nekonečné kardinality zavádíme zvláštní symboly:

- $|\mathbb{N}| = \aleph_0$, $|\mathbb{R}| = \mathfrak{c}$, $|\mathscr{P}(\mathbb{R})| = 2^{\mathfrak{c}}$. (Viz §2.2.)
- Vzájemně různé (viz §2.8) 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: $\beth_0 = \aleph_0$, $\beth_1 = \mathfrak{c}$, $\beth_2 = 2^{\mathfrak{c}}$, $\beth_3 = |\mathscr{P}(\mathscr{P}(\mathbb{R}))|$, atd.

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

- $\kappa \leq \lambda$, právě když $A \preceq B$ (čili $\kappa < \lambda$, právě když $A \prec B$)
- $\kappa + \lambda = |A \cup B|$
- $\kappa \cdot \lambda = |A \times B|$
  Součin $\kappa \cdot \kappa \cdot \ldots \cdot \kappa$ (n činitelů, pro $n \in \mathbb{N}$) zkracujeme κ^n, přičemž klademe $\kappa^0 = 1$.
- $2^\kappa = \big|\mathscr{P}(A)\big|$

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 $A' \preceq B'$.)
- $0 < 1 < 2 < 3 < \cdots < \aleph_0 < \mathfrak{c} < \beth_2 < \beth_3 < \beth_4 < \cdots$
- Aritmetika konečných kardinalit souhlasí s aritmetikou přirozených čísel.
- $\aleph_0 + 1 = \aleph_0$, $\aleph_0 + \aleph_0 = \aleph_0$, $\mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$, $2^{\aleph_0} = \mathfrak{c}$ atd. (podrobněji viz dále).
  Důkazy: $\mathbb{N} \cup \{-1\} \approx \mathbb{N}$, $\mathbb{N} \cup \mathbb{Z}^- = \mathbb{Z} \approx \mathbb{N}$, $\mathbb{R} \times \mathbb{R} \approx \mathbb{R}$, $\mathscr{P}(\mathbb{N}) \approx \mathbb{R}$. (Viz §2.2–§2.5.)
- $2^{\beth_n} = \beth_{n+1}$ pro každé $n \in \mathbb{N}$.

(LOTEM 2018/19, handout #2 k §2.9)

Zákony kardinální aritmetiky.

1. *Komutativita a asociativita sčítání a násobení:*

$$\kappa + \lambda = \lambda + \kappa \qquad \kappa \cdot \lambda = \lambda \cdot \kappa$$
$$(\kappa + \lambda) + \mu = \kappa + (\lambda + \mu) \qquad (\kappa \cdot \lambda) \cdot \mu = \kappa \cdot (\lambda \cdot \mu)$$

2. *Chování 0 a 1:* $\kappa + 0 = \kappa$, $\kappa \cdot 0 = 0$, $\kappa \cdot 1 = \kappa$

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

4. *Monotonie:* Pokud $\kappa_1 \leq \kappa_2$, pak: $\kappa_1 + \lambda \leq \kappa_2 + \lambda$, $\kappa_1 \cdot \lambda \leq \kappa_2 \cdot \lambda$, $2^{\kappa_1} \leq 2^{\kappa_2}$.

5. *Zákony mocnění:* $2^{\kappa+\lambda} = 2^\kappa \cdot 2^\lambda$, $(2^\kappa)^\lambda = 2^{\kappa\cdot\lambda}$

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

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

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 později v §6.1), 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 $A \preceq A'$). Důkazy tvrzení 5–6 přesahují rámec kurzu. □

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	n	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\beth_3$	$\cdots$
2^κ	2^n	$\mathfrak{c}$	$\beth_2$	$\beth_3$	$\beth_4$	$\cdots$

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 $n \in \mathbb{N}$. Označme $\beth_\omega = \big|\mathscr{P}\big(\bigcup_{n\in\mathbb{N}} A_n\big)\big|$. Pak $\beth_n < \beth_\omega$ 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 2018/19, handout k §3.1 a §3.2)

3. Ordinální čísla a dobrá uspořádání

3.1 Ordinální čísla

Iterováním operací potence a sjednocení jsme v §2.9 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 prvků?“), 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 (potencí nebo sjednocením – viz §2.9) nejblíže větší prvek této posloupnosti. Posloupnost ordinálních čísel, jimiž chceme takto vytvářené kardinály indexovat, 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:

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

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

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

Definice: Ordinál je *izolovaný,* pokud má bezprostředního předchůdce (tj. je *následníkem*) či je roven 0; jinak je *limitní.* Ordinál je konečný (spočetný), pokud má konečnou (spočetnou) množinu předchůdců. Nekonečným ordinálům se též říká *transfinitní.*

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

3.2 Dobře uspořádané množiny

Tvrzení: Každá neprázdná množina ordinálů má nejmenší prvek.

Důkaz: Buď A neprázdná množina ordinálů. Ukážeme, že nejmenší následník γ množiny ordinálů $B = \{\beta \in \mathrm{Ord} \mid (\forall \alpha \in A)(\beta < \alpha)\}$, jenž existuje dle vytvořujícího principu z §3.1, je i nejmenším prvkem A. Dle definice B jsou prvky A striktními majorantami B a ze všech striktních majorant množiny B je γ nejmenší. 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). □

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

1. V dobrém uspořádání jsou každé dva prvky porovnatelné. (Důkaz: uvažte nejmenší prvek $\{a, b\}$.)
2. V dobrém uspořádání neexistuje nekonečná klesající posloupnost $a_0 > a_1 > a_2 > \cdots$ (Důkaz: množina $\{a_0, a_1, a_2, \ldots\}$ by neměla nejmenší prvek.) S principem výběru platí i obráceně.
3. Prvky dobře uspořádaných množin lze vzestupně číslovat po řadě ordinálními čísly. (Nástin důkazu: na nejmenším prvku, kde by to nebylo možné, bychom dostali spor.)
4. Tvrzení o dobrých uspořádáních lze 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.) Důkazy transfinitní indukcí v praxi často rozlišují případy pro nulu, následníky a limitní ordinály.

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 množiny A, dokud všechny prvky množiny A nevyčerpáme. (Důkaz používá princip výběru, srv. §2.7.) □

Ernst Zermelo

Důsledky Zermelovy věty:

1. Princip výběru. (Důkaz: v dobrém uspořádání lze vždy vybírat nejmenší prvky množin.)
   Zermelova věta je tedy s principem výběru ekvivalentní – vzájemně ze sebe vyplývají.
2. Uspořádání kardinálních čísel podle velikosti je dobré. (Nástin důkazu: kardinálu κ přiřaďme nejmenší ordinál ι_κ takový, že množinu mohutnosti κ lze očíslovat předchůdci čísla ι_κ. Každý kardinál κ tak lze ztotožnit s ordinálem ι_κ – tzv. *iniciálním ordinálem* kardinality κ.)
   Důsledek: Vždy $A \preceq B$ nebo $B \preceq A$.
3. Za předpokladu platnosti principu výběru lze tedy všechny nekonečné kardinály očíslovat po řadě ordinálními čísly. Nekonečný kardinál číslovaný podle velikosti ordinálem α se značí $\aleph_\alpha$:
   $$\aleph_0 < \aleph_1 < \aleph_2 < \cdots < \aleph_\omega < \aleph_{\omega+1} < \cdots < \aleph_{\omega\cdot 2} < \cdots$$
   Cantorovu hypotézu pak lze formulovat i jako tvrzení, že $\beth_1 = \aleph_1$, čili že $2^{\aleph_0} = \aleph_1$.
   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 opět Gödel 1940 a nedokazatelnost Cohen 1963).

(LOTEM 2018/19, handout k §3.3)

3.3 Ordinální aritmetika

Typy dobrých uspořádání. Transfinitní indukcí lze ukázat (viz §3.2), že prvky každé dobře uspořádané množiny je možno vzestupně očíslovat právě všemi ordinály z intervalu $[0,\alpha) = \{\beta \in \mathrm{Ord} \mid \beta < \alpha\}$ pro nějaké ordinální číslo α. Toto α je přitom pro každou dobře uspořádanou množinu jednoznačně určeno a nazývá se *typ* jejího dobrého uspořádání. Přesněji:

Definice: Ordinál α je *typem* dobrého uspořádání $\trianglelefteq$ na množině A, pokud existuje bijekce $F\colon [0,\alpha) \leftrightarrow A$ taková, že pro všechny ordinály $\beta,\gamma < \alpha$ platí: $F(\beta) \trianglelefteq F(\gamma)$, právě když $\beta \le \gamma$.

Příklady:

- Množina $\{\sqrt{2},\pi,5\} \subseteq \mathbb{R}$ je dobře uspořádaná podle typu 3, neboť její prvky $\sqrt{2} < \pi < 5$ lze vzestupně očíslovat ordinály $0 < 1 < 2$ z ordinálního intervalu $[0,3) = \{0,1,2\}$.
- Množina $A = \{2 - 10^{-n} \mid n \in \mathbb{N}\} \cup \{2\} = \{1, 1.9, 1.99, 1.999, \ldots, 2\}$ má typ $\omega+1$, neboť prvkům ordinálního intervalu $[0,\omega+1) = \{0,1,2,\ldots,\omega\}$ lze přiřadit prvky množiny A vzestupně takto: $n \mapsto 2 - 10^{-n}$ pro $n \in \mathbb{N}$ a $\omega \mapsto 2$.

Aritmetika ordinálních čísel. Podobně jako pro čísla kardinální, i pro ordinály se zavádějí aritmetické operace součtu, součinu, mocniny aj. Pro konečné ordinály tyto operace souhlasí s aritmetikou konečných kardinálů, tj. přirozených čísel. Pro nekonečné ordinály se však jejich definice i vlastnosti výrazně liší, přestože pro ně používáme stejné znaky $+$, $\cdot$ atd.: například pro nekonečné kardinály platí $\kappa+1 = \kappa$, zatímco pro ordinály je vždy $\alpha+1 > \alpha$. V nekonečné aritmetice je tudíž třeba zřetelně uvádět, zda máme na mysli operace kardinální, nebo ordinální (zvláště proto, že v literatuře se někdy kardinál $\aleph_0$ rovněž označuje ω).

Ordinální součet. Součet ordinálů $\alpha+\beta$ je definován jako typ dobrého uspořádání, které vznikne, položíme-li dobrá uspořádání typů α a β (v tomto pořadí) „za sebe“. Přesněji:

Definice: Nechť A a B jsou disjunktní množiny s dobrým uspořádáním $\le$ typu α resp. β. Součet ordinálů $\alpha+\beta$ je definován jako typ dobrého uspořádání $\le$ na množině $A \cup B$, které souhlasí s uspořádáním $\le$ na A i na B a navíc $a < b$, kdykoli $a \in A$ a $b \in B$.

Příklady:

- $2 + 3 = 5$

  Dáme-li za sebe posloupnosti 2 a 3 prvků, lze výslednou posloupnost očíslovat ordinály z intervalu $[0,5) = \{0,\ldots,4\}$. Pozorujte: prvek očíslovaný ordinálem γ je $\gamma+1$. v řadě, zatímco γ je typ množiny všech jeho předchůdců; tak je tomu i u transfinitních posloupností prvků.

- $1 + \omega = \omega$

  Návod: např. pro $A = \{-1\}$, $B = \mathbb{N}$ najděte vzestupné očíslování $A \cup B$ ordinály z $[0,\omega) = \mathbb{N}$.

- $\omega + 1 \neq \omega$

  Návod: Uvažte, že množiny uspořádané podle typu ω, např. $\mathbb{N}$, nemají poslední prvek, kdežto množiny typu $\omega+1$, např. $\mathbb{N} \cup \{+\infty\}$, poslední prvek mají. Ujasněte si, že tudíž nemůže existovat *vzestupné* očíslování množiny typu $\omega+1$ právě všemi ordinály z $[0,\omega) = \mathbb{N}$.

  Ordinálními čísly z $[0,\omega)$ lze ovšem očíslovat *počáteční úsek* množiny typu $\omega+1$ (kdežto naopak nikoli), proto $\omega + 1 > \omega$.

Ordinální součin. Ordinální součin $\alpha \cdot \beta$ je typ dobrého uspořádání, které vznikne, když v dobrém uspořádání typu β nahradíme každý prvek dobrým uspořádáním typu α. (Pozor na pořadí činitelů: vhodné čtení ordinálního součinu $\alpha \cdot \beta$ je „α β-krát“.)

Ekvivalentně řečeno, $\alpha \cdot \beta$ je typem dobrého uspořádání kartézského součinu množiny typu β s množinou typu α v pořadí „po sloupcích“, tj. seřazeného podle první složky a v jejím rámci podle druhé složky (tzv. *lexikografické uspořádání*). Formálněji:

Definice: Nechť A a B jsou množiny s dobrým uspořádáním $\leq$ typu α resp. β. Součin ordinálů $\alpha \cdot \beta$ je definován jako typ dobrého uspořádání kartézského součinu $B \times A$, v němž klademe $\langle a, b\rangle < \langle a', b'\rangle$, právě když $a < a' \vee (a = a' \,\&\, b < b')$ pro všechna $a, a' \in A$, $b, b' \in B$.

Příklady:

- $\omega \cdot 2 = \omega + \omega$, kdežto $2 \cdot \omega = \omega$ (rozmyslete podle definice).
- $(\omega + 1) \cdot 2 = \omega \cdot 2 + 1$, kdežto $2 \cdot (\omega + 1) = \omega + 2$.

  Pozorujte: $(\omega + 1) \cdot 2 = (\omega + 1) + (\omega + 1) = \omega + (1 + \omega) + 1 = \omega + \omega + 1 = \omega \cdot 2 + 1$; oproti tomu $2 \cdot (\omega + 1) = 2 \cdot \omega + 2 \cdot 1 = \omega + 2$.

Zákony ordinální aritmetiky. Vyšetřením typu příslušné množiny nebo transfinitní indukcí lze dokázat např. tyto obecné vlastnosti ordinálních operací:

1. *Asociativita:* $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$, $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$

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

2. *Distributivita zleva:* $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$

   Distributivita zprava neplatí: $(1 + 1) \cdot \omega = 2 \cdot \omega = \omega \neq \omega + \omega = \omega \cdot (1 + 1)$.

3. *Monotonie:* Pokud $\alpha < \alpha'$, pak:

   $$\alpha + \beta \leq \alpha' + \beta \qquad \beta + \alpha < \beta + \alpha'$$
   $$\alpha \cdot \beta \leq \alpha' \cdot \beta \qquad \beta \cdot \alpha < \beta \cdot \alpha'$$

   Levé monotonie nelze zesílit na striktní, např. $1 + \omega = 2 + \omega$ a $1 \cdot \omega = 2 \cdot \omega$.

(LOTEM 2018/19, handout k §6.1)

6. Teorie množin a logika

6.1 Formální důkazy tvrzení o množinách

Množinové pojmy z pohledu formální logiky:

- Symbol $\in$ je binárním predikátem (zvaným *predikát náležení*).
- Zápis $x \in A$ je *atomickou formulí* predikátové logiky. (Predikát náležení zapisujeme infixově, tj. mezi jeho dva argumenty, podobně jako predikát rovnosti $=$.)
- Zápisy množinových tvrzení pomocí logických symbolů (§1.1), např. $(\exists A)(\forall x)\neg(x \in A)$, jsou formulemi predikátové logiky.

  Připomeňme zkratky (§1.1–2): zápis $x \notin A$ je zkratkou za $\neg(x \in A)$, zápis $(\forall x \in A)\varphi$ zkratkou za $(\forall x)(x \in A \to \varphi)$ a $(\exists x \in A)\varphi$ za $(\exists x)(x \in A \,\&\, \varphi)$.
- Symboly $\subseteq, \approx, \preceq$ jsou binární predikáty; $\cup, \cap, \setminus, \times$ jsou binární a $\mathscr{P}, \bigcup, \bigcap$ unární funkční symboly; $\emptyset$ je objektová konstanta (nulární funkční symbol).
- Proměnné $(x, A, \mathcal{A}, \dots)$, konstanty $(\emptyset, 5, \mathbb{N}, \dots)$ a aplikace funkčních symbolů (např. $A \cap B, \mathscr{P}(A \times B), \bigcup \mathcal{A}$ apod.) jsou *termy,* tj. výrazy označující objekty teorie množin.

  Také zápis uspořádané dvojice $\langle x, y\rangle$ lze chápat jako term, jehož argumenty píšeme dovnitř binárního funkčního symbolu značeného pouhými špičatými závorkami $\langle\dots\rangle$. Podobně lze chápat n-ární komprehenzní termy $\{x \mid \varphi(x_1, \dots, x_n)\}$ pro každou formuli φ (viz §1.2).

Formule s definovanými množinovými pojmy lze vesměs chápat jako zkratky za formule obsahující pouze predikáty náležení a rovnosti, např.:

- $A \subseteq B$ jako zkratku za $(\forall x)(x \in A \to x \in B)$, srv. §2.1,
- $X \in \bigcup \mathcal{A}$ jako zkratku za $(\exists A)(A \in \mathcal{A} \,\&\, X \in A)$, srv. §2.5, atp.

Teorii množin tak lze chápat jako formální teorii v predikátové logice s rovností a s jazykem obsahujícím jediný primitivní predikát $\in$. Vlastnosti množinových pojmů lze pak dokazovat z jejich definic pomocí pravidel predikátové logiky (§5). Jako dodatečné předpoklady (axiomy) lze přitom používat formule vyjadřující přijaté množinové principy (např. extenzionalitu, viz §2.1). Příklady takových důkazů uvedeme níže a na cvičeních.

Důkazy rovnosti a inkluze množin. Pozorujte: k důkazu rovnosti množin $A = B$ stačí dokázat formuli $x \in A \leftrightarrow x \in B$. Z ní totiž pravidlem generalizace (§5) odvodíme formuli $(\forall x)(x \in A \leftrightarrow x \in B)$, odkud z principu extenzionality (§2.1) odvodíme $A = B$ pravidlem modus ponens (§4). Podobně k důkazu inkluze $A \subseteq B$ stačí dokázat $x \in A \to x \in B$.

Důkazy logickými úpravami formulí. Formální důkazy množinových tvrzení vedeme v praxi většinou spíše ekvivalentními logickými úpravami (či řetězcem logicky platných implikací) než přímým odvozováním v kalkulu predikátové logiky (§5). Používáme přitom odvozené zákony predikátové logiky (De Morganovy, prenexaci, distributivitu spojek atp.), včetně odvoditelných důkazových metod (sporem, rozborem případů, kontrapozicí apod.). Pro řetězce logicky platných ekvivalencí a implikací budeme používat znaky $\longleftrightarrow, \longrightarrow$.

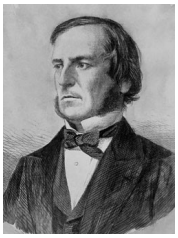
Vlastnosti elementárních množinových operací. Elementární množinové operace $\cup, \cap, \setminus$ dědí vlastnosti výrokových spojek, pomocí nichž jsou definovány (viz §1.2). Z platných výrokových ekvivalencí či implikací plynou odpovídající množinové identity a inkluze.

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

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

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

Jednoduché inkluze a identity elementárních množinových operací se tak redukují na výrokový počet, a tím trivializují: lze je ověřovat např. *tabulkovou metodou* (§4) nebo *Vennovými diagramy.* (Ujasněte si, jak políčka Vennových diagramů odpovídají jednotlivým řádkům pravdivostních tabulek pro výroky $p \equiv x \in A$, $q \equiv x \in B$, $r \equiv x \in C$, $s \equiv x \in D$.) V důsledku toho tvoří elementární množinové operace $(\cup, \cap, \setminus)$ i výrokové spojky $(\vee, \&, \neg)$ tutéž algebraickou strukturu – *Boolovu algebru.*


George Boole


John Venn

Příklady formálních důkazů. Vennovy diagramy dostačují pouze pro důkazy identit a inkluzí elementární teorie množin. Složitější tvrzení je možno dokazovat buď neformálními úvahami (jako v §1–3), nebo pomocí formálních kroků predikátové logiky. Důvody formalizace důkazů jsou mj. strojová ověřitelnost, explicitnost předpokladů a možnost metamatematického zkoumání (důkazů o dokazatelnosti). Uvedeme pouze dva příklady formálních důkazů množinových tvrzení (další ve cvičeních):

Tvrzení: $A \cap \bigcup \mathscr{B} = \bigcup \{A \cap B \mid B \in \mathscr{B}\}$.

Důkaz: Dle úvahy uvedené výše stačí dokázat formuli $x \in A \cap \bigcup \mathscr{B} \leftrightarrow x \in \bigcup \{A \cap B \mid B \in \mathscr{B}\}$. Rozepíšeme definice a provedeme ekvivalentní úpravy podle zákonů predikátové logiky (viz §5):

$x \in A \cap \bigcup \mathscr{B} \longleftrightarrow x \in A \wedge x \in \bigcup \mathscr{B}$	dle definice $\cap$	(§1.2)
$\longleftrightarrow x \in A \,\&\, (\exists B)(B \in \mathscr{B} \,\&\, x \in B)$	dle definice $\bigcup$	(§2.5)
$\longleftrightarrow (\exists B)(x \in A \,\&\, B \in \mathscr{B} \,\&\, x \in B)$	prenexace	(§5)
$\longleftrightarrow (\exists B)(B \in \mathscr{B} \,\&\, x \in A \,\&\, x \in B)$	komutativita &	(§4)
$\longleftrightarrow (\exists B)(B \in \mathscr{B} \,\&\, x \in A \cap B)$	dle definice $\cap$	(§1.2)
$\longleftrightarrow x \in \bigcup \{A \cap B \mid B \in \mathscr{B}\}$	dle definice $\bigcup$	(§2.5)

(V praxi je u podobných důkazů vhodné rozepisovat definice „od obou konců“ a snažit se výsledné formule upravit na vzájemně ekvivalentní tvary.) □

Tvrzení: $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Důkaz: Jednotlivé kroky zdůvodněte sami podle definic množinových pojmů a platných ekvivalencí výrokové logiky:

$\langle a, q \rangle \in A \times (B \cup C) \longleftrightarrow a \in A \,\&\, q \in B \cup C \longleftrightarrow a \in A \,\&\, (q \in B \vee q \in C) \longleftrightarrow (a \in A \,\&\, q \in B) \vee (a \in A \,\&\, q \in C) \longleftrightarrow \langle a, q \rangle \in A \times B \vee \langle a, q \rangle \in A \times C \longleftrightarrow \langle a, q \rangle \in (A \times B) \cup (A \times C)$. □

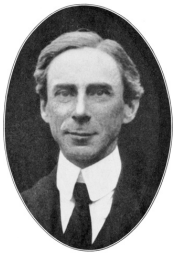
(LOTEM 2018/19, handout k §6.2)

6.2 Axiomatická teorie množin

Naivní princip komprehenze: Každá 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 (§2.8) vyděluje vlastní třídy: předpoklad, že vyděluje množinu, vedl ke sporu s Cantorovou větou.
Jednodušší důkaz – tzv. *Russellův paradox:* Třída $\mathcal{R} = \{X \mid X \notin X\}$ je vlastní – dle její definice je $\mathcal{R} \in \mathcal{R} \leftrightarrow \mathcal{R} \notin \mathcal{R}$, spor. □



Bertrand Russell

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

Matematici si časem všimli, že některé množinové konstrukce (např. sjednocení, potence, záměna prvků či princip nekonečna) je zatím 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 $A \cup B$, $A \cap B$, $A \setminus B$, $A \times B$ 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 problému: 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: $z = \{q \in x \mid \varphi(q)\}$, $x \cap y =_{\mathrm{df}} \{q \in x \mid q \in y\}$.
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 (§1.2); 9 = princip fundovanosti (ekvivalentní formulace, §2.7); 10 = princip výběru (§2.7); 6 = princip nekonečna (§2.7), 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.
- ZFC zná jen jeden druh objektů – množiny. Ostatní matematické objekty (uspořádané dvojice, čísla, kardinály atp.) se v ní modelují pomocí vhodných množin.

(LOTEM 2017/18, 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.

Řešení:

- *Uspořádané dvojice* (Kuratowského definice):

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

  Platí (dokažte): $\langle x_1, y_1\rangle = \langle x_2, y_2\rangle \leftrightarrow x_1 = x_2 \,\&\, y_1 = y_2$.

- *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 $\mathbb{N}$.)

Kazimierz Kuratowski

John von Neumann

- *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 s iniciálními ordinály, tj. takovými $\alpha \in \mathrm{Ord}$, že ordinální interval $[0, \alpha)$ nelze bijektivně zobrazit na ordinální interval $[0, \beta)$ pro žádné $\beta < \alpha$, Konečné kardinály jsou tedy ztotožněny s konečnými ordinály (čili přirozenými čísly), $\aleph_0 = \omega$, $\aleph_1 = \omega_1$ 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.