Množiny velké a větší

Alexander „Olin“ Slávik

Úvod

Co jsou to množiny? Kdy jsou dvě množiny stejně velké a kdy je naopak jedna větší než druhá? A co vlastně jsou čísla? Tyto otázky si začali klást matematici na přelomu 19. a 20. století, kdy už sice byly mnohé partie matematiky značně rozvinuté, k množinám (a nejen jim) se však stále přistupovalo spíše intuitivně, bez solidního matematického podkladu. Účelem této přednášky je pokusit se na tyto otázky odpovědět nebo alespoň odpověď naznačit.

Paradoxy aneb Kde je chyba?

Následujících několik myšlenkových postupů mělo poměrně zásadní význam pro rozvoj teorie množin a matematické logiky. Vžilo se pro ně poněkud nesprávné označení *paradoxy*, ačkoliv jde o sporná tvrzení.

Paradox. (Russelův) Nechť m je množina všech množin takových, že nejsou svým vlastním prvkem, tedy $m = \{x : x \notin x\}$. Platí $m \in m$?

Paradox. (Cantorův) Označme $\mathbf{V}$ množinu všech množin. Dle Cantorovy věty platí $\mathbf{V} \prec \mathcal{P}(\mathbf{V})$, ovšem zároveň snadno nahlédneme, že $\mathcal{P}(\mathbf{V}) \subseteq \mathbf{V}$, tedy by mělo platit i $\mathbf{V} \succcurlyeq \mathcal{P}(\mathbf{V})$ (pro vysvětlení symbolů viz dále).

Paradox. Jak vypadá množina $\check{c}$ definovaná jako množina všech čísel, které lze popsat nejvýše dvaceti českými slovy? Množina $\check{c}$ je určitě konečná, protože českých slov je konečně mnoho, tedy má největší prvek. Patří do množiny $\check{c}$ číslo definované jako „největší prvek množiny čísel sestávající z prvků, které lze popsat dvaceti českými slovy, zvýšený o jedna“?

Současná všeobecně používaná teorie množin (Zermelova-Fraenkelova teorie s axiomem výběru, ZFC) se s těmito nepříjemnými skutečnostmi vyrovnává tak, že jednoduše žádný z výše uvedených objektů neuznává jako množinu. Předně je hlavním rysem této teorie, že není nijak založena na přirozeném jazyce, pouze na jazyce matematické logiky. V tomto jazyce je zformulováno několik axiomů, které popisují, co vlastně množiny jsou (přesněji jak lze vytvořit množiny z jiných množin) a ostatní objekty se za množiny nepovažují. Rozbor těchto „základních kamenů“ moderní teorie množin je nad rámec tohoto příspěvku.

Mohutnost množin

Uvažme následující situaci: na lekci tanečních se sešlo mnoho chlapců a dívek – tolik, že kdybychom je chtěli spočítat, tak bychom se při tom skoro určitě „sekli“.

Přesto můžeme poměrně snadno zjistit, které pohlaví je v sále více zastoupeno. Jednoduše vyhlásíme volenku (v tuto chvíli nezáleží na tom, zda pánskou, či dámskou) a jakmile párování ustane, všimneme si, jestli „na ocet“ zůstali nějací hoši, nebo děvčata[6]. Pokud všichni tančí, je jasné, že je chlapců i dívek stejně mnoho.

Tyto úvahy snadno přepíšeme do formálních definic, hovořících o mohutnostech množin.

Definice. *Řekneme, že množiny x, y* mají stejnou mohutnost, *pokud existuje prosté zobrazení množiny x na množinu y (píšeme $x \approx y$). Řekneme, že množina x má* mohutnost menší nebo rovnu mohutnosti *y, pokud existuje prosté zobrazení množiny x do množiny y (zapisujeme $x \preccurlyeq y$). Řekneme, že množina x má* mohutnost menší než *y, pokud existuje prosté zobrazení množiny x do množiny y a neexistuje prosté zobrazení množiny y do množiny x (zapisujeme $x \prec y$). Analogicky definujeme vztahy $x \succcurlyeq y$, $x \succ y$.*

Jaké problémy nastanou, pokud se podíváme na nekonečné množiny, tj. když připustíme, že se v tanečních sešlo nekonečně mnoho lidí? Mohlo by se nám třeba stát, že chlapci i dívky budou očíslování (všemi) přirozenými čísly. Při pánské volence si pak hoch 1 vyvolí jako partnerku dívku 2, hoch 2 dívku 4, obecně hoch n dívku $2n$ – všichni hoši tančí, ale „polovina“ děvčat zůstala sedět! Totéž se nám může stát při dámské volence: kdyby třeba dívka n šla na parket s chlapcem 2^n, je patrné, že z chlapců „téměř nikdo“ netančí. Přesto je patrné, že by mohli tančit všichni (třeba když bude n tančit s n). Tento problém řeší následující věta:

Věta. (Cantor-Bernsteinova) *Pokud pro nějaké dvě množiny x, y platí zároveň $x \preccurlyeq y$ a $x \succcurlyeq y$, tak platí i $x \approx y$.*

Jak je to s mohutnostmi běžných množin čísel? Následující tvrzení se může zdát překvapující – vždyť racionálních čísel je o tolik víc než přirozených!

Tvrzení. $\mathbb{N} \approx \mathbb{Z} \approx \mathbb{Q}$ *a* $\mathbb{R} \approx \mathbb{C}$, *ale* $\mathbb{N} \prec \mathbb{R}$.

Definice. *Řekneme, že nekonečná množina x je* spočetná, *pokud $x \approx \mathbb{N}$. V opačném případě je* nespočetná.

Příklad. Historicky zajímavá je otázka existence transcendentních čísel, tedy reálných čísel, která nejsou řešením žádné rovnice tvaru

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

kde $a_0, a_1, \ldots, a_n \in \mathbb{Z}$. S prostředky teorie množin lze rozhodnout snadno – stačí ukázat, že doplněk této množiny (množina tzv. algebraických čísel) je spočetná množina.[7]

[6] Zde mlčky předpokládáme, že všichni přítomní jsou opravdu „tancechtiví“, a tedy si nenechají ujít žádnou příležitost k tanci.

[7] Lze ukázat, že např. e nebo π jsou transcendentní čísla.

Definice. Potenční množinou *množiny x nazveme množinu všech podmnožin množiny x, značíme $\mathcal{P}(x)$.*

Věta. (Cantorova) *Pro každou množinu x platí $x \prec \mathcal{P}(x)$.*

Cantorova věta nám říká, že škála mohutností množin není omezená – kdykoliv si vezmeme nějakou množinu, jsme schopni k ní najít množinu s větší mohutností. To však není všechno. Uvažme posloupnost množin

$$\mathbb{N}, \quad \mathcal{P}(\mathbb{N}), \quad \mathcal{P}(\mathcal{P}(\mathbb{N})), \quad \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))), \quad \ldots.$$

Sjednotíme-li všechny tyto množiny, dostaneme množinu, která má mohutnost větší než kterákoliv z množin v posloupnosti.

Dále nás může zajímat, „o kolik“ je potenční množina větší než původní množina. Řečeno přesněji a konkrétněji, ptáme se, zda existuje taková množna x, že platí

$$\mathbb{N} \prec x \prec \mathcal{P}(\mathbb{N}).$$

Tato otázka po dlouhá léta zaměstnávala matematiky, až se nakonec ukázala překvapivá skutečnost – jde o tzv. *nerozhodnutelné tvrzení*, tedy v teorii ZFC nejsme schopni tento výrok ani dokázat, ani vyvrátit.

Přirozená čísla

Axiomy teorie množin hovoří pouze o množinách, o číslech není nikde zmínka – chceme-li tedy pracovat s objekty, jako jsou přirozená čísla či $\mathbb{N}$, musíme je nadefinovat jako množiny. Konstrukci přirozených čísel provedeme tak, že za přirozené číslo prohlásíme množinu všech menších přirozených čísel. Nula[8] je tedy prázdná množina, jednička je $\{0\}$, dvojka $\{0,1\} = \{0,\{0\}\}$, $3 = \{0,1,2\} = \{0,\{0\},\{0,\{0\}\}\}$ atd.

Snadno nahlédneme, že obecně platí[9] $n+1 = n \cup \{n\}$. Dále nám tato definice přirozeným způsobem generuje známé uspořádání přirozených čísel: $n < m$, právě když $n \in m$, a $n \leq m$, právě když $n \subseteq m$. Na tomto místě raději precizujme pojem uspořádání:

Definice. *Relaci $\trianglelefteq$ na množině u nazveme* (částečným) uspořádáním, *pokud pro všechna $x, y, z \in m$ platí:*

(i) $x \trianglelefteq x$,
(ii) $(x \trianglelefteq y \wedge y \trianglelefteq x) \Rightarrow x = y$,
(iii) $(x \trianglelefteq y \wedge y \trianglelefteq z) \Rightarrow x \trianglelefteq z$.

[8] V teorii množin zpravidla nulu za přirozené číslo považujeme.

[9] Toto tvrzení není úplně správně, jelikož je v něm použito sčítání, které zatím není nijak definováno. Zpravidla se množina $n \cup \{n\}$ značí $s(n)$ a nazývá se *následník* n.

Platí-li navíc pro každé $x, y \in u$ alespoň jedna z možností $x \trianglelefteq y$, $x \trianglerighteq y$, hovoříme o lineárním uspořádání. *Pokud ještě k tomu platí, že každá podmnožina $v \subseteq u$ má v uspořádání $\trianglelefteq$ nejmenší prvek (tedy existuje takové $x \in v$, že pro všechna $y \in v$ platí $x \trianglelefteq y$), jde o* dobré uspořádání.

Poznámka. Každé uspořádání přirozeně existuje ve dvou verzích – neostré a ostré. Neostrá verze je definovaná výše, ostrá verze zakazuje rovnost. Příkladem takové dvojice je např. $\leq$ a $<$ na přirozených číslech.

Běžné uspořádání přirozených čísel je dobré, oproti tomu uspořádání celých čísel dobré není, stejně tak třeba uspořádání reálných čísel v intervalu $\langle 0, 1\rangle$. Každé lineární uspořádání konečné množiny je nutně dobré.

Všimněme si následující (prakticky zřejmé) vlastnosti přirozených čísel: pokud libovolnou konečnou množinu lineárně uspořádáme, je toto uspořádání stejné jako uspořádání nějakého přirozeného čísla (tedy množiny po sobě jdoucích přirozených čísel) pomocí $\in$. Přirozená čísla jsou tedy jakési modelové příklady uspořádání konečných množin. Chtěli bychom vytvořit podobné reprezentatny i pro dobrá uspořádání nekonečných množin. Těmito reprezentanty budou ordinální čísla (krátce ordinály).

Ordinální čísla

Definice. *Množinu u nazveme* ordinálním číslem, *pokud je na ní $\in$ ostré dobré uspořádání a pro všechna $x \in u$ platí $x \subseteq u$.*

Příklad. Všechna přirozená čísla jsou ordinální čísla, množina $\mathbb{N}$ je také ordinálním číslem (v této souvislosti ji zpravidla značíme ω).

Jaká jsou další ordinální čísla? Např. $\omega \cup \{\omega\}$, což velmi připomíná konstrukci přirozených čísel. Toto ordinální číslo odpovídá uspořádání přirozených čísel, ke kterým ještě navíc přidáme „nekonečno“, tedy prvek, který je větší než všechna přirozená čísla. Vlastnosti ordinálních čísel čísel shrneme v následující větě:

Věta. (Vlastnosti ordinálních čísel)

(i) *Prvky ordinálního čísla jsou opět ordinální čísla.*
(ii) *$\in$, resp. $\subseteq$ je ostré, resp. neostré dobré uspořádání (značíme $<$, resp. $\leq$) na třídě*[10] *všech ordinálních čísel (kterou značíme* **On***).*
(iii) **On** *není množina.*
(iv) *Každé dobré uspořádání nějaké množiny je isomorfní*[11] *uspořádání právě jednoho ordinálního čísla (tzv. ordinální typ uspořádání).*

[10] *Třída* je v ZFC soubor všech množin, které splňují nějaký zadaný výrok. Může, ale nemusí jít o množinu (pak hovoříme o *vlastní třídě*).

[11] Jsou-li dvě uspořádané množiny *isomorfní*, znamená to, že mezi nimi existuje *isomorfismus*, tedy bijekce, která zachovává uspořádání.

(v) *Sjednocení a průnik množiny (souboru) ordinálních čísel je opět ordinální číslo. Navíc pro množinu ordinálních čísel u je její sjednocení $\alpha = \bigcup u$ supremem této množiny, tedy jde o nejmenší*[12] *ordinální číslo, pro které platí, že pro všechna $\beta \in u$ je $\beta \leq \alpha$. Analogicky průnik je infimem této množiny.*

Definice. *Ordinální číslo α nazveme* izolované, *jestliže existuje takové ordinální číslo β, že $\alpha = \beta \cup \{\beta\}$. Ordinální číslo, které není izolované, nazveme* limitní.

Příklad. Všechna přirozená čísla jsou izolovanými ordinály, oproti tomu ω je limitní ordinál.

Stejně jako na přirozených číslech, i na ordinálních číslech můžeme zavést základní aritmetické operace.

Definice. (Aritmetika ordinálních čísel)

(i) Součet *ordinálních čísel α, β (značíme $\alpha+\beta$) definujeme jako ordinální typ tzv. lexikografického uspořádání na množině $(\{0\} \times \alpha) \cup (\{1\} \times \beta)$, tedy uspořádání, které se v rámci α i β „chová stejně“ jako $\leq$ a všechny prvky z β jsou větší než všechny prvky z α.*[13]

(ii) Součin *ordinálních čísel α, β (značíme $\alpha \cdot \beta$) definujeme jako ordinální typ lexikografického uspořádání na množině $\beta \times \alpha$.*[14]

(iii) Ordinální mocninu *definujeme rekurzivně:*

(a) $\alpha^0 = 1$,

(b) $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$,

(c) $\alpha^\beta = \bigcup\{\alpha^\gamma : 0 < \gamma < \beta\}$ *pro β limitní.*

Poznámka. Ordinální součet i součin jsou asociativní, nejsou však obecně komutativní: např. $1 + \omega = \omega \neq \omega + 1$, $2 \cdot \omega = \omega \neq \omega \cdot 2$. Platí však distributivita zleva: $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

Poznámka. Ordinální mocnina je pro nekonečné exponenty téměř nemožná na představu. Není možné např. představovat si ω^ω jako lexikografické uspořádání nekonečných posloupností přirozených čísel, protože toto uspořádání není dobré a navíc je množina těchto posloupností nespočetná, zatímco ω^ω je spočetná množina.

[12] Ve smyslu uspořádání $<$, neboli $\in$.

[13] Přesnější popis „technického provedení“ je tento: z prvků $\gamma \in \alpha$ „vyrobíme“ uspořádané dvojice $(0, \gamma)$ a z prvků $\delta \in \beta$ zase $(1, \delta)$. Vzniklé množiny sjednotíme a výsledné uspořádání se nejprve „dívá“ na první složky uspořádaných dvojic. Pokud jsou stejné, rozhodne se podle druhých složek. Dvojice jsou tedy uspořádány „jako ve slovníku“ – nejprve podle prvního písmena, pak podle druhého, odtud pojem lexikografické uspořádání.

[14] Opačné pořadí v kartézském součinu je z historických důvodů.

Kardinální čísla

Zatímco ordinální čísla popisují uspořádání množin, kardinální čísla (krátce kardinály) popisují mohutnosti. Zkonstruujeme je jednoduše tak, že pro každou mohutnost vezmeme ze všech ordinálů dané mohutnosti ten nejmenší (ve smyslu uspořádání ordinálů).

Definice. *Řekneme, že ordinální číslo κ je* kardinální číslo, *pokud pro všechna $\alpha < \kappa$ platí $\alpha \prec \kappa$.*

Příkladem kardinálních čísel jsou opět přirozená čísla a ω. Avšak $\omega + 1$ již není kardinální číslo, jelikož $\omega + 1 \approx \omega$. Třídu všech ordinálních čísel značíme $\mathbf{Cn}$, třídu všech nekonečných ordinálních čísel $\mathbf{Cn}^\infty$.

Tvrzení. *Třída $\mathbf{Cn}$ je dobře uspořádána $\in$ (ostře) i $\subseteq$ (neostře).*

Definice. *Pro libovolnou množinu u definujeme* mohutnost *či* kardinalitu *jako kardinální číslo κ splňující $u \approx \kappa$ (značíme $|u|$).*

Definice. (Aritmetika kardinálních čísel)

(i) Součet *kardinálních čísel κ, λ (značíme $\kappa + \lambda$) definujeme jako mohutnost množiny* $(\{0\} \times \kappa) \cup (\{1\} \times \lambda)$.
(ii) Součin *kardinálních čísel κ, λ (značíme $\kappa \cdot \lambda$) definujeme jako mohutnost množiny $\kappa \times \lambda$.*
(iii) Kardinální mocninu κ^λ *definujeme jako mohutnost množiny všech funkcí z λ do κ.*

Věta. *Pro nekonečná kardinální čísla κ, λ platí $\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda)$.*

Je vidět, že sčítání a násobení kardinálů se chová poměrně „nudně“. Oproti tomu kardinální mocnina je velmi divoká – obecně jsme o ní schopni říct jen velmi málo. Tato skutečnost není dána tím, že by tvrzení o kardinální mocnině byla obtížně dokazatelná, ale tím, že jsou mnohá z nich z povahy teorie ZFC prostě nedokazatelná (viz otázka mohutnosti potenční množiny výše).

Věta. *Existuje právě jeden třídový isomorfismus tříd $\mathbf{On}$ a $\mathbf{Cn}^\infty$, značíme ho $\aleph$.*

Platí $\aleph_0 = \omega$, $\aleph_1$ je první nespočetný ordinál (kardinál). Je jasné, že $\aleph$ je rostoucí funkce, navíc se zdá být enormně rychle rostoucí (vždyť už $\aleph_\omega$ je nepředstavitelně velká množina). Následující tvrzení je tedy téměř šokující:

Tvrzení. *Funkce $\aleph$ má (vlastní) třídu pevných bodů (tj. takových ordinálních čísel, pro která platí $\aleph_\alpha = \alpha$), která je isomorfní s $\mathbf{On}$.*

Literatura a zdroje

[1] Bohuslav Balcar, Petr Štěpánek: *Teorie množin*, Academia, Praha, 2000.
[2] Vojtěch Jarník: *Diferenciální počet II*, Academia, Praha, 1984.
[3] Josef Mlček: *Poznámky k přednášce Úvod do teorie množin*
[4] Martin Tancer: *Teorie množin*, sborníkový příspěvek, Olšanka, 2006.
[5] Robert Šámal: *Ordinály, kardinály – taková zvláštní čísla*, sborníkový příspěvek, Jablonná, 1999.