Přírodovědecká fakulta

TEORIE MNOŽIN

pro učitele

Eduard FUCHS

MASARYKOVA UNIVERZITA Brno, 2000

OBSAH

PŘEDMLUVA

Množinově-logický jazyk matematiky je dnes již zcela běžný od 1. třídy základní školy. Proto musí být pro budoucí učitele matematiky jeho dokonalé zvládnutí — včetně nezbytného nadhledu — naprostou samozřejmostí.

Cíle tohoto textu lze shrnout následovně:

1. vysvětlit nutnost formalizace matematických teorií a nastínit základní metody této formalizace;

2. vyložit základní pojmy teorie množin, především pak popsat základní vlastnosti kardinálních a ordinálních čísel;

3. popsat vývoj teorie množin a vliv této teorie na matematiku 20. století.

K pochopení probírané látky není potřeba žádných hlubších předběžných znalostí. (Stručný přehled nejpotřebnějších elementárně-množinových pojmů je uveden v dodatku na konci této části CD).

Řada těchto pojmů je dnes již součástí středoškolské matematiky a všechny jsou podrobně probírány v základních matematických přednáškách. Jejich dokonalé zvládnutí — a to v rozsahu výrazně převyšujícím zmíněný dodatek — je proto možno považovat za samozřejmé.

Teorie množin sehrála ve vývoji matematiky roli zcela zásadní. Proto je historii teorie množin a důsledkům této teorie pro matematiku 20. století věnována celá 4. kapitola. V této kapitole jsou rovněž uvedeny autentické ukázky z klíčových textů B. Bolzana a G. Cantora.

Zvláštní pozornost si zaslouží ta část 4. kapitoly, která je věnována dílu K. Gödela. Význam jeho „věty o neúplnosti“ dnes již přesahuje rámec matematiky samotné. Přesné odvození této věty a charakterizace jejích důsledků přitom není součástí učitelského studia matematiky, neboť k tomu nemají vybudován dostatečný logický aparát. Forma zpracování této problematiky ve 4. kapitole by však měla čtenářům umožnit alespoň pochopení základních idejí Gödelova důkazu.

Symbolika užívaná v textu je běžná a význam všech symbolů je v textu (respektive v připojeném dodatku) definován. Upozorněme pouze, že — na rozdíl od středoškolské praxe — rozlišujeme inkluzi $\subseteq$ a $\subset$. Symbol $A \subset B$ tak značí, že A je *vlastní* podmnožinou množiny B.

Běžné množiny čísel označujeme následovně:

$\mathbb{N}$ ... množina všech přirozených čísel
$\mathbb{Z}$ ... množina všech celých čísel
$\mathbb{Q}$ ... množina všech racionálních čísel
$\mathbb{R}$ ... množina všech reálných čísel.

Kapitola 1

Formální výstavba matematiky

1 Axiomatická teorie a její model

Cítíte-li se skvěle,
budťe bez obav.
To přejde.
BOLINGŮV POSTULÁT.

S rychlým rozvojem matematiky — zejména pak matematické analýzy — vznikla v 19. století naléhavá potřeba řádné výstavby základů matematických teorií. Vhodnou základnou se stala **teorie množin**, kterou počal v 70. letech minulého století systematicky budovat německý matematik Georg Cantor. (Podrobně historii vzniku teorie množin popíšeme ve 4. kapitole.)

Základní množinové pojmy jsou natolik jednoduché, názorné a pro matematiku potřebné, že dnes už pronikly i do školské matematiky na té nejzákladnější úrovni. I malé děti snadno chápou „množiny“ jako označení toho, co se v běžné řeči nazývá „soubor“, „souhrn“ a podobně a bez problémů zvládají základní množinovou algebru.

Na první pohled jistě není zřejmé, že by se v takto budované teorii mohly objevit těžkosti zásadního rázu. Velmi snadno však lze ukázat, že nelze beztrestně předpokládat, že **každý** souhrn nějakých objektů vytváří množinu. Stačí připustit, že existuje množina všech množin, které nejsou svým vlastním prvkem, tj. množina

$$\mathcal{A} = \{X;\ X \text{ je množina, } X \notin X\}.$$

Z definice množiny $\mathcal{A}$ okamžitě vyplývá, že nemůže platit ani vztah $\mathcal{A} \in \mathcal{A}$ (podle definice množiny $\mathcal{A}$ odtud totiž plyne $\mathcal{A} \notin \mathcal{A}$), ani vztah $\mathcal{A} \notin \mathcal{A}$ (odtud zase naopak plyne $\mathcal{A} \in \mathcal{A}$, neboť právě z takových množin jsme množinu $\mathcal{A}$ vytvořili). V tomto okamžiku jsme se však ocitli v neřešitelné situaci, neboť z intuitivní představy množiny je okamžitě zřejmé, že pro

každý objekt x a každou množinu A **nutně** platí **právě jeden** ze vztahů $x \in A$, respektive $x \notin A$. (I když samozřejmě nemusíme vždy vědět, **která** z těchto situací v daném případě nastává.)

Právě jsme zformulovali nejznámější z tzv. **antinomií teorie množin**, *antinomii* Russellovu. Antinomií, tj. tvrzení vedoucích ke sporu, se na přelomu 19. a 20. století objevila celá řada; podrobně o nich budeme hovořit v kapitole IV, §3. Jejich důsledky pro moderní matematiku byly dalekosáhlé, neboť přesvědčivě prokázaly, že **celou matematiku** je nutno budovat jinými metodami, když dosavadní postupy totálně selhaly. V teorii množin samotné pak antinomie ukázaly, že je neudržitelné Cantorovo původní stanovisko, že totiž **množina je souhrn jakýchkoliv objektů, chápaných jakožto jeden celek**. (Takto pojímané teorii se dnes říká *naivní* nebo *intuitivní* teorie množin.)

Nalezení východisek z této situace nebylo vůbec jednoduché a jak uvidíme, nebylo všeobecně přijaté řešení vlastně nalezeno dodnes. Nejobvyklejším způsobem výstavby matematických teorií je dnes **axiomatická metoda**.

Čtenář jistě dobře ví, v čem tato metoda spočívá. Každou matematickou teorii lze chápat jako systém nějakých tvrzení o objektech z určité oblasti. Například aritmetika je v tomto smyslu množinou výroků o číslech, geometrie množinou výroků o „vhodných“ podmnožinách daného prostoru a podobně.

Je zřejmé, že při deduktivní výstavbě (a matematika je ve své podstatě nesporně deduktivní vědou) není možné *každé* tvrzení odvodit z tvrzení jednodušších a *každý* pojem definovat pomocí jednodušších pojmů. Proto je nutné o některých nedefinovaných pojmech, tzv. *primitivních pojmech* dané teorie, vyslovit tvrzení — *axiómy*, považované za pravdivé bez důkazu. Podle předem stanovených odvozovacích pravidel se pak z těchto tvrzení odvozují další.

V této kapitole se budeme zabývat formální stránkou takto budovaných matematických teorií.

V závěru tohoto paragrafu si však vyjasněme ještě jednu věc. Uvedli jsme, že Cantorova intuitivní teorie množin je ve světle antinomií neudržitelná. Přitom však i dnes učíme děti ve školách, že množina je totéž jako souhrn, systém, soubor a podobně. Znamená to tedy, že na školách vědomě učíme „špatnou“ teorii?

Uvedli jsme, že při axiomatické výstavbě se o jistých nedefinovaných objektech (například v eukleidovské geometrii jsou to pojmy „bod“, „přímka“ atd.) vysloví nedokazovaná tvrzení (v eukleidovské geometrii je to 5 známých postulátů). Podle předem dohodnutých pravidel se pak na tomto základě deduktivně buduje celá teorie. Takto budovanou teorii (například geometrii) může chápat a rozumět jí každý, kdo užívá stejná odvozovací pravidla jako tvůrce dané teorie, i když si nedefinované pojmy může představovat zcela jinak (nebo si je eventuálně nepředstavuje vůbec). (Axiomatickou geometrii tedy může zvládnout i ten, kdo si *vůbec nic* konkrétního nedovede představit pod pojmy „bod“, „přímka“ apod.) Jakmile si takovou představu vytvoříme, jakmile si nedefinované pojmy nějak interpretujeme, vytváříme tím tzv. *model*

dané axiomatické teorie. I když je zřejmé, že tento model si nelze vytvořit zcela libovolně, je snad jasné, že obecně lze k dané teorii vytvořit modelů více.

V tomto smyslu se například učíme na školách pouze jeden z možných modelů eukleidovské geometrie. Je to ovšem model vytvořený tisíciletou zkušeností lidstva, model, který nejvěrněji odráží náš makrosvět. (Čtenář se však jistě setkal i s jinými modely, které jsou zvlášť výhodné při výkladu neeukleidovské geometrie.)

A jak je to tedy s teorií množin? Standardní model axiomatické teorie množin obdržíme tak, že si primitivní, tj. nedefinovaný pojem „množina“ interpretujeme jakožto synonymum slova soubor. Intuitivní teorie množin — lépe řečeno její jistá modifikace — se tak stává modelem axiomatické teorie množin. (Později uvidíme, že ve školách učíme model tzv. *teorie Zermelo-Fraenkelovy*). V modelu dané teorie lze ovšem, na rozdíl od intuitivní teorie, provádět jen ty konstrukce a zavádět jen ty pojmy, které jsou odrazem konstrukcí a pojmů přípustných v axiomatické teorii.

Proto například nemůže být množinou *jakýkoliv* souhrn nějakých objektů (například souhrn všech množin) a proto nemůžeme dospět k antinomiím, které se objevily v Cantorově teorii.

2 Jazyk matematických teorií

Všechno lze udělat snáz.
ILESŮV ZÁKON

Při popisu matematických jazyků záhy vypozorujeme řadu analogií s jazyky přirozenými (hovorovými). I s nematematiky se jistě shodneme na následujících skutečnostech:

(a) K popisu každého jazyka (češtiny, ruštiny, angličtiny apod.) se užívá jistých znaků, jejichž souhrn nazvěme *abecedou*.

(b) Z prvků této abecedy se tvoří větší celky, nazývané *slova*, respektive *věty*. Přitom jen některá formálně utvořená „slova“ z daných znaků jsou slovy daného jazyka. Tak například slovo „vhpaimple“ je sice utvořena ze znaků české abecedy, zcela jistě to však není české slovo, „window“ sice není české slovo, ale je to slovo anglického jazyka a podobně.

(c) Jen některé v předcházejícím smyslu „správně“ vytvořené věty mají smysl, respektive jsou pravdivé. Například „věta“ „Jan a slunce včera prší“ je gramaticky správně utvořena, jistě se však shodneme, že je to naprostý nesmysl. Věta „Molekula každého prvku je složena z pěti atomů“ je utvořena gramaticky správně, je smysluplná, avšak každý, kdo má alespoň minimální znalosti chemie ví, že je nepravdivá.

Slova daného jazyka (ať přirozeného nebo matematického) můžeme posuzovat ze dvou hledisek. Studujeme-li jazyk, aniž přihlížíme k tomu, co jednotlivé znaky, slova atd. znamenají, studujeme-li tedy pouze zákonitost sdružování znaků, závislosti tvaru slov apod. na tvaru jejich

částí a podobně, říkáme, že jazyk studujeme z hlediska *syntaktického*. Jestliže nám jde o to, jaký je význam jednotlivých znaků, slov atd., studujeme jazyk z hlediska *sémantického*.

V této kapitole nám půjde téměř výhradně o studium matematických jazyků z hlediska *syntaktického*.

Konečně si ujasněme poslední věc, než budeme hovořit o matematických jazycích podrobněji. Zadáváme-li určitý jazyk S, užíváme při tvoření tohoto jazyka nějaký jiný jazyk, odlišný od S. Tento jazyk nazýváme *metajazykem*[1] jazyka S. Prvky abecedy tohoto metajazyka nazýváme *metaznaky*, tuto abecedu nazýváme *metaabecedou* a podobně.

Konečně zdůrazněme, že hlavním cílem této kapitoly je popsat formalizaci matematických teorií, vyjasnit základní principy této formalizace a na některých příkladech ji ilustrovat, nikoliv provedení formální výstavby jako takové.

★ ★ ★

Symboly, které již nedělíme na symboly jednodušší, nazvěme *znaky*. Za znaky obvykle volíme písmena (latinská, řecká), číslice, závorky, čárky, ale často i jiné symboly, jako například $\cup$, $\cap$, $\vee$, $\wedge$, $+$, $\forall$, $\exists$ a podobně. Přitom předpokládáme, že poznáme, kdy jsou dva znaky totožné (kdy je například na dvou místech napsán stejný znak). Neobsahuje-li abeceda žádný znak, nazývá se *prázdná*. My však v dalším, kdykoliv řekneme abeceda, budeme mít na mysli abecedu neprázdnou.

Skupinám znaků napsaným zleva doprava budeme říkat *slova* (vytvořená v dané abecedě). Je-li například dána abeceda

$$a \qquad b \qquad * \qquad \wedge \qquad +$$

jsou slova například nápisy

$$*ab \wedge \wedge \qquad \text{nebo} \qquad * * + *b \wedge a$$

nikoliv však nápis $a * \vee b \wedge \wedge c$ (symbol $\vee$ nepatří do naší abecedy). Účelné je definovat tzv. *prázdné slovo*, které není tvořeno žádným znakem. Prázdné slovo je zřejmě slovem v každé abecedě. Za slovo považujeme také jednotlivé znaky.

Nyní je rovněž zřejmé, co rozumíme *posloupností slov*. Doplníme-li zvolenou abecedu o nový znak, který nazveme *oddělujícím znakem*, nazýváme každé slovo v této rozšířené abecedě posloupností slov v abecedě původní. Často oddělující znak nepíšeme a místo něho uděláme mezi slovy mezeru.

Abychom si nyní usnadnili popis studovaného jazyka, zvolíme si nějaké znaky, kterými budeme označovat slova vytvořená v naší abecedě. Čtenáři je jistě zřejmé, že to nemohou být

[1] *Meta* (z řečtiny), v složených slovech první část s významem „za“, „po“. Například *metateorie* je teorie zkoumající jinou teorii. Podrobně je studována zejména *metamatematika*.

znaky naší abecedy, ale že to budou *metaznaky*. Dohodněme se, že za metaznaky označující slova, zvolíme malá písmena řecké abecedy (eventuálně s indexy; tyto indexy však nepovažujeme za samostatný znak).

Označují-li α, β totéž slovo, napíšeme $\alpha \sim \beta$. Je-li například φ znak označující slovo $*ba+$, píšeme $\varphi \sim *ba+$. Prázdné slovo označíme symbolem ω.

Jsou-li α, β dvě slova a napíšeme-li je bez oddělovacího znaku těsně za sebou, dostaneme opět slovo, které nazýváme slovem *složeným* ze slov α,β a značíme je $\alpha\beta$.

V dalším budeme běžně užívat řady zřejmých tvrzení následujícího typu, z nichž některá ani nebudeme výslovně formulovat.

2.1. Věta.

(a) *Pro libovolné slovo φ platí $\omega\varphi \sim \varphi$, $\varphi\omega \sim \varphi$.*

(b) *Pro libovolná slova α, β, γ je slovo složené ze slov $\alpha\beta$, γ totožné se slovem složeným ze slov α, $\beta\gamma$ (tj. skládání slov je* asociativní*).*

2.2. Definice. Slovo α se nazývá *podslovem* slova β, jestliže existují slova γ, δ taková, že $\beta \sim \gamma\alpha\delta$.

2.3. Poznámka. (Je zřejmé, že prázdné slovo je podslovem každého slova a každé slovo je podslovem sebe sama. (Stačí totiž, aby $\gamma \sim \omega$, $\delta \sim \omega$ v definici 2.2).

2.4. Příklad. Je-li 3098114 slovo v nějaké abecedě, jsou například 309, 811 nebo 4 jeho podslova, avšak slovo 814 není jeho podslovem.

Poněvadž znaky považujeme za slova, je zřejmá následující definice:

2.5. Definice. Řekneme, že znak ξ *se vyskytuje* ve slově α (nebo že slovo α *obsahuje* znak ξ), je-li ξ podslovem slova α.

I laik při pozorování matematikovy činnosti brzy postřehne, že matematik podle nějakých pravidel umí některá slova nahrazovat slovy jinými. Výuka počtů na základní škole například spočívá v tom, naučit děti nahrazovat slova utvořená v abecedě $0123456789 + \times$ slovy jinými. (Slovo „4 + 17“ nahradíme slovem „21“, slovo „4 $\times$ 9“ slovem „36“ a podobně.)

Nyní si tento případ zobecníme.

Pojem *funkce* je nám znám. Je tedy zřejmé, že když udáme předpis, jak slova utvořená v dané abecedě nahrazujeme jednoznačně slovy jinými, zadáváme tím nějakou funkci na slovech této abecedy.

Je-li f taková funkce a α slovo, značí $f(\alpha)$ slovo, které funkce f přiřazuje slovu α. ($f(\alpha)$ musí být tedy určeno jednoznačně; je přitom zřejmé, že f je opět metaznak.)

Mezi funkcemi definovanými na slovech však mohou být podstatné rozdíly v tom, jak obtížné je nalézt k danému slovu slovo přiřazené. Dokumentujme to na následujících příkladech.

2.6. Příklad. Buď dána abeceda

$$123456789 + .$$

Definujme na slovech této abecedy funkce f, g, h takto:

Buď α slovo vytvořené v této abecedě. Nechť $\alpha \sim \beta + \gamma$, kde β ani γ není prázdné a obě označují nějaké přirozené číslo. Pak je:

(a) $f(\alpha)$ slovo označující součet slov β, γ (například $f(2 + 3) \sim 5$).

(b) $g(\alpha)$ slovo, které získáme takto: číslo π umocníme na racionální exponent, jehož čitatelem je přirozené číslo označené slovem β, jmenovatelem číslo označené slovem γ, v dekadickém rozvoji takto vzniklého čísla vezmeme cifru stojící na 10^k-tém místě, kde k je přirozené číslo, které je součinem čísel označených slovy β a γ. Tato cifra je pak slovem, které označíme $g(\alpha)$. (Například $g(2 + 3)$ je miliontá cifra dekadického rozvoje čísla $\pi^{2/3}$.)

(c) $h(\alpha)$ je slovo, které označuje průměrnou teplotu v Praze ve °C zaokrouhlenou na celé stupně φ-tý den po 1. 1. 2100, kde $\varphi \sim f(\alpha)$ (například $h(2 + 3)$ je průměrná teplota ve °C dne 6. 1. 2100).

Není-li α slovo uvedeného tvaru, položme $f(\alpha) \sim \omega$, $g(\alpha) \sim \omega$, $h(\alpha) \sim \omega$.

Je zřejmé, že funkce f a g se výrazně liší od funkce h. U funkcí f, g lze popsat návod, podle něhož zcela mechanicky dovede ke slovu α přiřadit slovo $f(\alpha)$ (alespoň teoreticky) i stroj. Takové funkce nazveme *algoritmizovatelné*. Funkce h však zcela prokazatelně algoritmizovatelná není.

I algoritmizovatelné funkce se však mohou podstatně lišit. Máme-li zadánu nějakou funkci a udáme-li stroji slovo α, vypočítá stroj příslušnou funkční hodnotu až po nějaké době. Čas, který stroj k výpočtu potřebuje, však nedovedeme vždycky předem odhadnout. U funkce f z příkladu 2.6 nám hodnotu $f(\alpha)$ — alespoň v „běžných“ případech — udává i kapesní kalkulačka prakticky okamžitě. Hodnotu $g(\alpha)$ by asi i ten nejvýkonnější počítač počítal obecně velmi dlouho. Je tedy jasný smysl následující definice[2].

[2] Ani tato definice není zcela výstižná. Kdybychom u nějaké funkce sice potřebný čas uměli odhadnout, byl by však řádově v milionech roků — nebo snad ještě delší — vyhovovala by příslušná funkce právě vyslovené definici, evidentně by však nesplňovala požadavek jisté „jednoduchosti“, kterou chceme touto definicí postihnout. Spíše než o „předem odhadnutelný“ čas nám jde o výpočet v „rozumném“ čase. Tento pojem je však nemožné precizovat. Čtenáři je současně jistě zřejmé, že právě definovaný pojem *mechanické počitatelnosti* se v čase výrazně mění.

2.7. Definice. Řekneme, že funkce f je *mechanicky počitatelná*, je-li algoritmizovatelná a obdržíme-li pro každé slovo α hodnotu $f(\alpha)$ v čase, který lze předem odhadnout.

Uveďme si nyní některé jednoduché mechanicky počitatelné funkce.

2.8. Definice. Buď ξ nějaký znak. Definujme funkce f, g takto

$$f(\alpha) = \xi\alpha, \qquad g(\alpha) = \alpha\xi.$$

Funkci f nazýváme *připsáním znaku ξ zleva*, funkci g *připsáním znaku ξ zprava*.

2.9. Definice. Buď α libovolný znak, β libovolné slovo. Buď f funkce, splňující následující tři požadavky:
(i) pro každá dvě slova φ, ψ platí

$$f(\varphi\psi) \sim f(\varphi)\, f(\psi),$$

(ii) $f(\alpha) \sim \beta$,
(iii) je-li ξ znak, který není totožný se znakem α, je $f(\xi) \sim \xi$.
Pak se f nazývá *substituce* slova β za znak α. Tuto substituci označíme symbolem

$$[\alpha \to \beta].$$

Zcela analogický smysl má označení

$$[\alpha_1 \to \beta_1, \ldots, \alpha_n \to \beta_n].$$

Rozumíme jím substituci slov β_i za znaky α_i, $i = 1, \ldots, n$ (viz následující příklady).

2.10. Příklad. Zvolme abecedu jako v příkladu 2.6. Nechť f je substituce:
(a) $[1 \to 04]$
(b) $[1 \to 2,\ 2 \to 3,\ + \to \omega]$
(c) $[+ \to 1,\ 0 \to 2,\ 9 \to +]$.
Pak f přiřazuje slovu „21 + 4890“ slovo:
(a) 204 + 4890
(b) 324890
(c) 21148 + 2.

Prozatím jsme popisovali víceméně mechanicky práci se znaky. Dobře však víme, že v matematickém jazyce — stejně jako v jazycích přirozených — nepovažujeme za slovo každé seskupení znaků ze zvolené abecedy a slova neskládáme do posloupností zcela nahodile. Víme, že například při sčítání čísel uvažujeme slova typu „48 + 290“ a nikoliv slova „+ + +01“ nebo „28 + 42+“ a podobně. Při odvozování nějakého vzorce nepíšeme za sebou slova namátkou, ale podle jistých předem stanovených pravidel.

Souhrnu pravidel, kterými se matematik řídí ve své činnosti, říkáme *kalkul*. Pojem kalkulu zde však nebudeme definovat. Je snad ale jasné, že kalkulů je celá řada; každá matematická teorie má svůj specifický kalkul. Prakticky všechny kalkuly však mají „něco“ společného. V následujících dvou paragrafech budeme precizovat výrokový kalkul, který v intuitivním smyslu běžně užíváme.

3 Výrokový kalkul

Dobrý úsudek si vytvoříme díky špatné zkušenosti.
Zkušenost nabudeme díky špatnému úsudku.
HIGDONŮV ZÁKON

3.1. Definice. *Abeceda výrokového kalkulu* je tvořena následujícími znaky:

1. Velkými písmeny latinské abecedy $A, B, \ldots, X, Y, Z$ případně opatřenými indexy. Tyto znaky nazýváme *výrokovými proměnnými* (nebo též *proměnnými pro výroky*).
2. Znaky $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$ nazývanými *logické spojky*.
3. Znaky (a) (levá a pravá závorka).

3.2. Poznámka. Označíme-li proměnnou pro výroky symbolem A_1, P_3, Z_{10} a podobně, *neznamená* to, že naši abecedu de facto rozšiřujeme o znaky označující přirozená čísla. Na uvedené znaky, jednoduše řečeno, pohlížíme jako na *jediný* symbol.

Při počítání s výroky samozřejmě nebereme v úvahu všechna slova, která lze v dané abecedě vytvořit. Za správně utvořené slovo jistě nepovažujeme slovo $A\neg \vee B$ nebo $(A)\neg(B) \vee (C\neg)$. Na první pohled ovšem není jasné, jak popsat ta slova, která ve výrokovém kalkulu budeme považovat za správně utvořená. Správná slova, která popíšeme následující definicí, budeme nazývat *výrokové formule* nebo stručně jen *formule*, pokud nebude moci dojít k nedorozumění. (Ve shodě s §2 budeme k označování formulí a obecně slov v abecedě výrokového kalkulu užívat metaznaků $\alpha, \beta, \gamma, \ldots$, eventuálně s indexy.)

3.3. Definice.

(1) Každá výroková proměnná je výrokovou formulí.

(2) Jsou-li φ, ψ výrokové formule, je každé ze slov $\neg(\varphi)$, $(\varphi)\vee(\psi)$, $(\varphi)\wedge(\psi)$, $(\varphi)\Rightarrow(\psi)$, $(\varphi)\Leftrightarrow(\psi)$ výrokovou formulí.

(3) Žádné slovo, které nelze získat pomocí (1) a (2) není výrokovou formulí.

3.4. Poznámka. Definice 3.3 samozřejmě není a nemůže být výčtem všech výrokových formulí, neboť těch je evidentně nekonečně mnoho. Definice je pouze rekurentním návodem ke tvorbě výrokových formulí. Ukažme alespoň na několika příkladech, jak lze podle definice 3.3 konstruovat komplikovanější formule a jak poznáme, zda zadané slovo je nebo není výrokovou formulí.

Jsou-li například A, B, C, D výrokové proměnné, jsou podle (2) slova

$$(A)\Rightarrow(B),\qquad (C)\vee\big(\neg(D)\big)$$

výrokovými formulemi. Opět podle (2) jsou pak výrokovými formulemi i slova

$$\Big(\neg\big((A)\Rightarrow(B)\big)\Big)\Leftrightarrow(D),\qquad (A)\wedge\Big((C)\vee\big(\neg(D)\big)\Big),$$

takže je výrokovou formulí i slovo

$$\Big(\Big(\neg\big((A)\Rightarrow(B)\big)\Big)\Leftrightarrow(D)\Big)\Rightarrow\Big((A)\wedge\Big((C)\vee\big(\neg(D)\big)\Big)\Big) \qquad (*)$$

atd.

Je vidět, že definice 3.3 nám umožňuje vytvářet dostatečně komplikované formule.

Zcela analogicky postupujeme, když chceme zjistit, zda je dané slovo výrokovou formulí. Nechť například je

$$\varphi\sim\Big(\neg\big(\neg(A)\big)\Big)\Rightarrow\Big(\big(\neg(B)\vee(C)\big)\Leftrightarrow\Big((D)\vee\big(\neg(A)\big)\Big)\Big).$$

Zjišťujeme, zda φ je formule.

K tomu, aby φ byla formule, je podle 3.3 nutné, aby slova

$$\neg\big(\neg(A)\big)\quad\text{a}\quad\big(\neg(B)\vee(C)\big)\Leftrightarrow\Big((D)\vee\big(\neg(A)\big)\Big)$$

byla formulemi. Aby druhé z těchto slov bylo formulí, je nutné, aby byla formulemi slova

$$\neg(B)\vee(C)\qquad\text{a}\qquad(D)\vee\big(\neg(A)\big).$$

Nyní již vidíme, že φ není formule, neboť $\neg(B) \vee (C)$ není formule. V tomto slovu totiž chybí jedny závorky; správně by měla vypadat takto:

$$\big(\neg(B)\big) \vee (C) \quad \text{nebo} \quad \neg\big((B) \vee (C)\big)\,.$$

Podle definice 3.3 tedy poznáme, zda dané slovo je nebo není formulí a současně nám tato definice umožňuje z jednodušších formulí vytvářet formule složitější. (Později uvidíme, že dovedeme v jistém slova smyslu sestavit libovolně komplikovanou formuli – viz větu 3.19.)

I z několika mála dosud uvedených formulí je však zřejmé, že zápisy výrokových formulí jsou leckdy příliš komplikované, zejména pokud jde o užívání závorek. Například slova $\neg A \vee B$, respektive $A \wedge B$ nejsou podle definice 3.3 formule, i když je nám naprosto zřejmé, jaký smysl těmto slovům přikládáme. Proto uzavřeme následující dohodu, která nám umožní zjednodušení zápisů výrokových formulí.

3.5. Úmluva. Zápisy výrokových formulí lze zjednodušit pomocí následujících tří pravidel. Jejich dodržování však nebudeme striktně vyžadovat, budeme se řídit tím, jaký z povolených zápisů bude v dané situaci nejúčelnější.

1. Je-li podslovem slova φ slovo (ψ), kde ψ je libovolná výroková proměnná, budeme místo (ψ) psát pouze znak ψ.

2. U logických spojek stanovíme následující pořadí „předností“:

   (a) znak $\neg$ má přednost před všemi ostatními logickými spojkami;

   (b) znaky $\wedge$, $\vee$ jsou rovnocenné a mají přednost před rovnocennými znaky $\Rightarrow$, $\Leftrightarrow$.

   Závorky, které nám zajišťují realizaci uvedených předností, při psaní formulí vynecháme.

3. Při kumulaci většího počtu závorek užijeme i závorek hranatých [,], resp. složených {, }, které však nezmění význam formule.

3.6. Příklad.

(a) Slovo $\big((A) \vee (B)\big) \Rightarrow (C)$ lze podle (1) zapsat ve tvaru $(A \vee B) \Rightarrow C$. Podle (2) lze toto slovo ještě zjednodušit na tvar $A \vee B \Rightarrow C$.

(b) Slovo

$$\big(\neg(A)\big) \vee \Big(\neg\big(\neg\big((C) \wedge (D)\big)\big)\Big)$$

lze podle (1) a (2) zjednodušit takto:

$$\neg A \vee \neg\neg(C \wedge D).$$

Podle (4) však můžeme totéž slovo napsat také například takto:

$$\neg A \vee \neg\big(\neg(C \wedge D)\big)$$

nebo

$$(\neg A) \vee \Big[\neg\big(\neg(C \wedge D)\big)\Big].$$

(c) Formuli ($\star$) v poznámce 3.4 lze přepsat takto:

$$\big[(\neg A \Rightarrow B) \Leftrightarrow D\big] \Rightarrow \big[A \wedge (C \vee \neg D)\big].$$

Při konstrukci výrokových formulí lze s výhodou často využívat následujícího tvrzení, které vyplývá bezprostředně z definice výrokové formule.

3.7. Věta. *Buďte α, β výrokové formule, ξ libovolná výroková proměnná. Buď f substituce $[\xi \to \beta]$. Pak je $f(\alpha)$ výroková formule. (Tzn., že když ve výrokové formuli nahradíme proměnnou formulí, dostaneme opět formuli).*

3.8. Příklad. Buď f substituce $\big[A \to \neg(B \vee C) \Rightarrow D \wedge C\big]$ a

$$\varphi \sim A \Rightarrow (B \wedge \neg C) \vee (\neg A \wedge B).$$

Pak je φ zřejmě formule a podle 3.7 je výrokovou formulí slovo

$$\big(\neg(B \vee C) \Rightarrow D \wedge C\big) \Rightarrow \Big\{(B \wedge \neg C) \vee \Big[\neg\big(\neg(B \vee C) \Rightarrow D \wedge C\big) \wedge B\Big]\Big\}.$$

Ve výrokovém kalkulu nám ovšem nejde o to, psát výrokové formule nebo zjišťovat, zda dané slovo je výrokovou formulí. Dobře víme, co rozumíme výrokem; smyslem námi popisovaných výrokových formulí je to, že pokud výrokové proměnné chápeme jako označení pro výroky, pak jsou výrokové formule rovněž zápisy (složených) výroků. Víme také, že charakteristickou vlastností výroků je jejich **pravdivost**, respektive **nepravdivost**. Hlavním cílem výrokového kalkulu je právě studium toho, jak pravdivost či nepravdivost složeného výroku závisí na pravdivosti či nepravdivosti výroků, z nichž byl tento výrok pomocí logických spojek utvořen[3].

[3] V této chvíli je čtenáři jistě zcela zřejmý rozdíl mezi **sémantickým** přístupem k výstavbě výrokového kalkulu, jak ho zná například ze střední školy, a **syntaktickým** přístupem, který demonstrujeme nyní. Při středoškolské výuce se nejdříve zavede, či — lépe řečeno — vysvětlí pojem *výrok* jako označení pro tvrzení, o němž má smysl prohlásit, že je pravdivé, respektive nepravdivé a pak se intuitivně budují další potřebné pojmy. Při syntaktické výstavbě se pojem *výrok* vůbec nedefinuje, je to primitivní pojem. Zato jsme však přesně popsali, jak vypadají formule, což při sémantické výstavbě pouze mimochodem vyplývá z toho, jak zavádíme formální označení. Při sémantické výstavbě je tedy pravdivost či nepravdivost výroku zabudována přímo v jeho „definici“, my však tímto atributem musíme výrokový kalkul teprve opatřit.

Výrokový kalkul nám neumožní zjistit, zda jednoduché tvrzení nějaké teorie je pravdivé či nikoli; to jsme nuceni zjišťovat jiným způsobem. (Pomocí výrokového kalkulu například nejsme schopni zjistit, zda je pravdivé tvrzení „$2^{13}-1$ je prvočíslo“; že je toto tvrzení pravdivé, je možno dokázat v teorii čísel.) Výrokový kalkul nám jen upřesní, jak správně tvořit z výroků jednodušších výroky složitější a jak pravdivost těchto složitějších výroků závisí na pravdivosti příslušných výroků jednodušších. (Z výrokového kalkulu lze například zjistit, kdy je pravdivé tvrzení: „Je-li $2^{13}-1$ prvočíslo, je také $2^{17}-1$ prvočíslo“.)

Výrokový kalkul je tedy natolik obecný, že *nepostačuje* k vytvoření speciálních matematických teorií. Na druhé straně je ovšem natolik univerzální, že je součástí prakticky každého matematického jazyka. Proto věnujeme výrokovému kalkulu takovou pozornost.

3.9. Definice. Rozšiřme abecedu výrokového kalkulu o znaky 0, 1. Buď p funkce na slovech utvořených v této rozšířené abecedě taková, že platí:

(1) není-li slovo φ výrokovou formulí ve smyslu definice 3.3, je $p(\varphi) \sim \omega$ (prázdné slovo);

(2) je-li slovo φ výrokovou formulí, je $p(\varphi) \sim 0$ nebo $p(\varphi) \sim 1$;

(3) jsou-li φ,ψ libovolné výrokové proměnné, pak jsou hodnoty $p(\neg\varphi)$, $p(\varphi \vee \psi)$, $p(\varphi \wedge \wedge \psi)$, $p(\varphi \Rightarrow \psi)$, $p(\varphi \Leftrightarrow \psi)$ zadány následující tabulkou.

$p(\varphi)$	$p(\psi)$	$p(\neg\varphi)$	$p(\varphi \wedge \psi)$	$p(\varphi \vee \psi)$	$p(\varphi \Rightarrow \psi)$	$p(\varphi \Leftrightarrow \psi)$
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

Pak se funkce p nazývá *pravdivostní hodnota* a hodnota $p(\varphi)$ se nazývá *pravdivostní hodnota slova* φ. Je-li $p(\varphi) \sim 1$, říkáme, že *výrok označený formulí* φ *je pravdivý* (nebo stručně *výrok* φ *je pravdivý*), je-li $p(\varphi) \sim 0$, říkáme, že *výrok označený formulí* φ *je nepravdivý* (nebo stručně *výrok* φ *je nepravdivý*).

3.10. Poznámka.

(a) Podmínky (1) a (2) nám zaručují, že funkce p přiřadí hodnotu 0 nebo 1 jen výrokovým formulím. Uvědomme si přitom, že žádná výroková formule neobsahuje znak 0 ani znak 1. Z podmínky (2) současně plyne, že každé výrokové proměnné je přiřazena hodnota 0 nebo 1.

(b) Funkce p *není* mechanicky počitatelná, dokonce ani algoritmizovatelná, neboť pro výrokovou proměnnou φ nemůžeme čistě syntakticky určit, zda je $p(\varphi) \sim 0$ nebo $p(\varphi) \sim 1$.

$p(A)$	$p(B)$	$p(C)$	$p(D)$	$p(\neg A)$	$p(\alpha)$	$p(\beta)$	$p(\neg D)$	$p(\gamma)$	$p(\delta)$	$p(\varphi)$
1	1	1	1	0	1	1	0	1	1	1
1	1	1	0	0	1	0	1	1	1	1
1	1	0	1	0	1	1	0	0	0	0
1	0	1	1	0	1	1	0	1	1	1
0	1	1	1	1	1	1	0	1	0	0
1	1	0	0	0	1	0	1	1	1	1
1	0	1	0	0	1	0	1	1	1	1
1	0	0	1	0	1	1	0	0	0	0
0	1	1	0	1	1	0	1	1	0	1
0	1	0	1	1	1	1	0	0	0	0
0	0	1	1	1	0	0	0	1	0	1
1	0	0	0	0	1	0	1	1	1	1
0	1	0	0	1	1	0	1	1	0	1
0	0	1	0	1	0	1	1	1	0	0
0	0	0	1	1	0	0	0	0	0	1
0	0	0	0	1	0	1	1	1	0	0

Tabulka 1.1:

(c) Podmínka (3) v definici 3.9 nám zaručuje, že logické spojky ve výrokovém kalkulu mají běžný[4] význam.

(d) Z definic 3.3 a 3.9 plyne, že když φ je libovolná výroková formule, lze určit hodnotu $p(\varphi)$ zcela mechanicky, pokud jsou určeny pravdivostní hodnoty $p(\alpha)$ všech výrokových proměnných α, které slovo φ obsahuje.

3.11. Příklad. Určeme pravdivostní hodnotu formule

$$\varphi \sim \big[(\neg A \Rightarrow B) \Leftrightarrow D\big] \Rightarrow \big[A \wedge (C \vee \neg D)\big]$$

z příkladu 3.6(c).

Označme pro jednoduchost $\alpha \sim \neg A \Rightarrow B$, $\beta \sim \alpha \Leftrightarrow D$, $\gamma \sim C \vee \neg D$, $\delta \sim A \wedge \gamma$. Pak je $\varphi \sim \beta \Rightarrow \delta$. Hodnoty $p(\varphi)$ jsou uvedeny v tabulce 1.1:

[4] Slovem „běžný“ samozřejmě rozumíme běžný v matematice. Dobře víme, že tyto spojky, byť jsou do matematiky přeneseny z hovorového jazyka, mají v matematice přece jen význam odlišný. Vzhledem k tomu je proto zásadně **nevhodné** při výuce těchto partií demonstrovat smysl logických spojek na *příkladech ze života*.

3.12. Příklad. Určíme pravdivostní hodnotu formule

$$\varphi \sim (P \Rightarrow Q) \Leftrightarrow \neg(P \wedge \neg Q).$$

(Viz tabulku 1.2)

$p(P)$	$p(Q)$	$p(\neg Q)$	$p(P \wedge \neg Q)$	$p(\neg(P \wedge \neg Q))$	$p(P \Rightarrow Q)$	$p(\varphi)$
1	1	0	0	1	1	1
1	0	1	1	0	0	1
0	1	0	0	1	1	1
0	0	1	0	1	1	1

Tabulka 1.2:

Mezi formulemi, jejichž pravdivostní hodnoty jsme zjišťovali v příkladech 3.11 a 3.12, je na první pohled zřejmý jeden rozdíl. Zatím co pro formuli z příkladu 3.11 je někdy $p(\varphi) \sim 0$ a někdy $p(\varphi) \sim 1$, je výrok označený formulí φ z příkladu 3.12 vždycky pravdivý. Uvidíme, že takové výroky budou hrát v dalších úvahách důležitou roli.

3.13. Definice. Výroková formule φ se nazývá *tautologie*, jestliže $p(\varphi) \sim 1$ při jakékoliv volbě pravdivostních hodnot výrokových proměnných, které se vyskytují ve formuli φ.

Tzn., že formule φ z příkladu 3.11 není tautologií, formule z příkladu 3.12 je tautologií.

Tautologií výrokového počtu je nekonečně mnoho. My zde uvedeme jen nejběžnější. Ještě před tím si však uveďme jedno tvrzení, které nám umožňuje z jakékoliv tautologie vytvářet řadu dalších tautologií.

3.14. Věta. *Buď f libovolná substituce výrokových formulí za výrokové proměnné. Je-li φ libovolná tautologie, je $f(\varphi)$ rovněž tautologie.*

Důkaz. Je-li f substituce a φ tautologie, je podle věty 3.7 $f(\varphi)$ výroková formule. Že je však $f(\varphi)$ tautologie, je okamžitě zřejmé. •

Nyní tedy uveďme přehled nejznámějších tautologií výrokového počtu, nazývaných též *zákony výrokového počtu*. Důkaz tvrzení, že všechny uvedené formule jsou tautologiemi, přenecháme čtenáři.

3.15. Věta. *Všechny formule (1) až (15) jsou tautologiemi výrokového počtu:*

(1)	$\neg(P \wedge \neg P)$	
(2)	$P \vee \neg P$	*(zákon vyloučeného třetího)*
(3)	$P \Leftrightarrow P$	*(zákon totožnosti)*
(4)	$\neg\neg P \Leftrightarrow P$	*(zákon dvojí negace)*
(5)	$(\neg P \Rightarrow P) \Rightarrow P$ $(P \Rightarrow \neg P) \Rightarrow \neg P$	*(zákon Claviův, též reductio ad absurdum)*
(6)	$(P \wedge P) \Leftrightarrow P; (P \vee P) \Leftrightarrow P$	
(7)	$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$	
(8)	$[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$	*(zákon hypotetického sylogismu)*
(9)	$[(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)] \Rightarrow (P \Rightarrow R)$	
(10)	$(P \wedge \neg P) \Rightarrow Q$	*(zákon Dunse Scota)*
(11)	$(P \wedge Q) \Rightarrow P$	
(12)	$\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$	*(de Morganovo pravidlo)*
(13)	$\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$	*(de Morganovo pravidlo)*
(14)	$[(P \Rightarrow Q) \Rightarrow P] \Rightarrow P$	*(Peirceův zákon)*
(15)	$P \Rightarrow [Q \Rightarrow (P \wedge Q)]$	

V poznámce 3.10(d) jsme uvedli, že pro libovolnou výrokovou formuli lze mechanicky sestrojit tabulku pravdivostních hodnot této formule, tj. tabulku, která udává závislost hodnoty $p(\varphi)$ na hodnotách $p(\alpha)$ výrokových proměnných, které se ve formuli φ vyskytují.

Nyní se pokusme zodpovědět opačnou otázku, zda k předem zadané tabulce pravdivostních hodnot lze sestrojit výrokovou formuli, jejíž tabulka pravdivostních hodnot je totožná s touto předem zvolenou tabulkou. Přesně si tento problém zformulujeme následovně.

3.16. Problém. Buď n přirozené číslo. Pak existuje 2^n navzájem různých n-členných posloupností utvořených z nul a jedniček. Uspořádejme všechny tyto posloupnosti do tabulky o 2^n řádcích a n sloupcích a přidejme k takto vzniklé tabulce ještě jeden sloupec utvořený z nul a jedniček. Znak stojící v průsečíku i-tého řádku a j-tého sloupce označme α_{ij}. (Je tedy $\alpha_{ij} \sim 0$ nebo $\alpha_{ij} \sim 1$ pro $i = 1, 2, \ldots, 2^n$ a $j = 1, \ldots, n+1$).

Nyní chceme zjistit, zda:

(1) existuje výroková formule φ, v níž se vyskytuje právě n výrokových proměnných $A_1, \ldots, A_n$ taková, že pro každé $i = 1, 2, \ldots, 2^n$ platí: je-li $p(A_j) = \alpha_{ij}$ pro $j = 1, \ldots, n$, pak $p(\varphi) = \alpha_{i,n+1}$;

(2) v případě, že taková formule φ existuje, je určena jednoznačně.

3.17. Příklad. Pro $n = 1$ je situace jednoduchá, neboť výchozí tabulku je možno zadat pouze čtyřmi způsoby:

Je však evidentní, že lze volit například v případě (a) formuli $\varphi \sim A \vee \neg A$, v případě (b) formuli $\varphi \sim A$, v případě (c) formuli $\varphi \sim \neg A$ a v případě (d) formuli $\varphi \sim A \wedge \neg A$. V každém z těchto čtyř případů však bez obtíží lze zkonstruovat i jiné výrokové formule se stejnou pravdivostní tabulkou, například takto:

A	φ
1	1
0	1

(a)

A	φ
1	1
0	0

(b)

A	φ
1	0
0	1

(c)

A	φ
1	0
0	0

(d)

Tabulka 1.3:

A	B	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6	φ_7	φ_8
1	1	1	1	1	1	0	1	1	1
1	0	1	1	1	0	1	1	0	0
0	1	1	1	0	1	1	0	1	0
0	0	1	0	1	1	1	0	0	1

A	B	φ_9	φ_{10}	φ_{11}	φ_{12}	φ_{13}	φ_{14}	φ_{15}	φ_{16}
1	1	0	0	0	1	0	0	0	0
1	0	1	1	0	0	1	0	0	0
0	1	1	0	1	0	0	1	0	0
0	0	0	1	1	0	0	0	1	0

Tabulka 1.4:

(a) $\varphi \sim \neg(A \wedge \neg A)$
(b) $\varphi \sim \neg\neg A$
(c) $\varphi \sim A \Rightarrow \neg A$
(d) $\varphi \sim \neg(\neg\neg A \Leftrightarrow A)$.

Dokázali jsme tak, že v případě $n = 1$ je odpověď na problém 3.16 (1) kladná, na problém 3.16(2) záporná.

3.18. Příklad. Buď $n = 2$. Pak lze tabulku podle 3.16 sestavit celkem 16 způsoby, které jsou souhrnně uvedeny v tabulce 1.4.
Porovnáním s tabulkou v definici 3.9 je okamžitě vidět, které sloupce v tabulce 1.4 odpovídají tabulkám logických spojek. Zřejmě lze volit $\varphi_2 \sim A \vee B$, $\varphi_4 \sim A \Rightarrow B$, $\varphi_8 \sim A \Leftrightarrow B$, $\varphi_{12} \sim A \wedge B$.

Evidentní je však skutečnost, že lze velmi jednoduše zkonstruovat výrokovou formuli s požadovanou vlastností v každém ze zbývajících dvanácti případů. Za φ_1 lze například zvolit libovolnou tautologii ve dvou proměnných (například formuli (7), (10), (11), (12), (13), (14) ve

větě 3.15), za φ_{16} negaci libovolné z těchto tautologií. Určit zbývající formule je jednoduchým cvičením pro čtenáře. Mechanický návod pro jejich konstrukci však plyne z důkazu věty 3.19.

3.19. Věta. *Buď n libovolné přirozené číslo. Pak lze v každém případě zkonstruovat výrokovou formuli s vlastnostmi požadovanými v problému 3.16(1), přičemž tato výroková formule není určena jednoznačně.*

Důkaz provedeme indukcí vzhledem k počtu výrokových proměnných, které se v hledané výrokové formuli vyskytují.

Pro $n = 1$ jsme tvrzení dokázali v příkladu 3.17. K důkazu dalšího indukčního kroku využijeme výrokové formule

$$\tau \sim (\neg A \wedge B) \vee (A \wedge C) \, .$$

Sestrojme tabulku pravdivostních hodnot formule τ:

$p(A)$	$p(B)$	$p(C)$	$p(\neg A \wedge B)$	$p(A \wedge C)$	$p(\tau)$
1	1	1	0	1	1
1	1	0	0	0	0
1	0	1	0	1	1
0	1	1	1	0	1
1	0	0	0	0	0
0	1	0	1	0	1
0	0	1	0	0	0
0	0	0	0	0	0

Tabulka 1.5:

Z tabulky 1.5 je ihned vidět, že platí následující tvrzení.

Lemma. Je-li $p(A) \sim 1$, je $p(\tau) \sim p(C)$, je-li $p(A) \sim 0$, je $p(\tau) \sim p(B)$.

Předpokládejme nyní, že pro přirozené n je věta 3.19 dokázána. Dokážeme, že tvrzení platí i pro $n + 1$. Nechť tedy je zadána tabulka o 2^{n+1} řádcích a $n + 2$ sloupcích. Rozdělme nyní tuto tabulku na dvě části následovně: vyškrtněme z tabulky předposlední sloupec (odpovídající pravdivostním hodnotám $p(A_{n+1})$) a do první části zařaďme ty řádky, v nichž je ve vyškrtnutém sloupci 0, do druhé části zařaďme zbývající řádky. Každá část je nyní tabulkou pravdivostních hodnot nějaké výrokové formule, v níž se vyskytují pouze výrokové proměnné $A_1, \ldots, A_n$. Podle předpokladu však dovedeme zkonstruovat výrokové formule φ_1, φ_2 tak, že první část naší tabulky je tabulkou pravdivostních hodnot formule φ_1 a druhá část tabulkou pravdivostních hodnot formule φ_2.

Definujme nyní

$$\varphi \sim (\neg A_{n+1} \wedge \varphi_1) \vee (A_{n+1} \wedge \varphi_2).$$

Výroková formule φ vznikla z formule τ substitucí

$$[A \to A_{n+1},\, B \to \varphi_1,\, C \to \varphi_2]\,.$$

Z lemmatu však nyní plyne:

Je-li $p(A_{n+1}) \sim 0$, je $p(\varphi) \sim p(\varphi_1)$, je-li $p(a_{n+1}) \sim 1$, je $p(\varphi) \sim p(\varphi_2)$, takže naše tabulka je skutečně tabulkou pravdivostních hodnot výrokové formule φ.

Dokázali jsme tedy, že pro každé přirozené n lze mechanicky zkonstruovat k předem zadané tabulce pravdivostních hodnot příslušnou výrokovou formuli. Nejednoznačnost této konstrukce plyne z toho, že již pro $n = 1$ lze ke každé tabulce pravdivostních hodnot najít více výrokových formulí (viz příklad 3.17). Tím je věta dokázána. •

3.20. Příklad. Zkonstruujme formule φ_3 a φ_{14} z příkladu 3.18.

(a) Tabulku pro $p(\varphi_3)$ si zapíšme následovně:

$p(A)$	$p(B)$	$p(\varphi_3)$
1	0	1
0	0	1
1	1	1
0	1	0

Tabulka 1.6:

Nyní vyškrtneme sloupec $p(B)$ a zbývající sloupce rozdělíme do dvou tabulek takto:

1	1
0	1

první část

1	1
0	0

druhá část

Tabulka 1.7:

K těmto pravdivostním tabulkám však dovedeme zkonstruovat příslušné výrokové formule podle 3.17 například takto:

$$\varphi_1 \sim A \vee \neg A, \qquad \varphi_2 \sim A.$$

Podle důkazu věty 3.19 je nyní

$$\varphi_3 \sim \big[\neg B \wedge (A \vee \neg A)\big] \vee (B \wedge A).$$

Podle příkladu 3.17 však lze k tabulkám 8 zvolit formule φ_1, φ_2 i takto:

$$\varphi_1 \sim \neg(A \wedge \neg A), \qquad \varphi_2 \sim \neg\neg A$$

a pak lze φ_3 přepsat do tvaru

$$\varphi_3 \sim \big[\neg B \wedge \neg(A \wedge \neg A)\big] \vee (B \wedge \neg\neg A).$$

(b) Pravdivostní tabulku pro φ_{14} rozdělíme na dvě části takto:

1	1
0	1

první část

1	1
0	0

druhá část

Tabulka 1.8:

Podle příkladu 3.17 lze nyní volit

$$\varphi_1 \sim A \wedge \neg A, \qquad \varphi_2 \sim \neg A,$$

takže

$$\varphi_{14} \sim \big[\neg B \wedge (A \wedge \neg A)\big] \vee (B \wedge \neg A).$$

Zvolíme-li však (opět podle příkladu 3.17)

$$\varphi_1 \sim \neg(\neg\neg A \Leftrightarrow A), \qquad \varphi_2 \sim A \Rightarrow \neg A,$$

dostaneme

$$\varphi_{14} \sim \big[\neg B \wedge \neg(\neg\neg A \Leftrightarrow A)\big] \vee \big[B \wedge (A \Rightarrow \neg A)\big].$$

3.21. Poznámka. Z věty 3.19 plyne, že logické spojky $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$ nám umožňují zkonstruovat libovolně komplikované výrokové formule. Nevyřešena je prozatím otázka, zda není možné vybudovat výrokový kalkul s menším počtem logických spojek; toho by bylo možno dosáhnout jednak vypuštěním některé z pěti uvedených spojek (dobře víme, že to fakticky možné je, neboť například spojku $\Leftrightarrow$ lze vyjádřit pomocí spojek $\Rightarrow$, $\wedge$), jednak zavedením nových spojek, které by eventuálně mohly být při tvorbě výrokového kalkulu výhodnější.

K tomuto účelu je vhodné zavést pojem logické ekvivalence výrokových formulí, jehož užitečnost vyplývá bezprostředně z věty 3.19, podle které ke každé tabulce pravdivostních hodnot existuje více výrokových formulí.

3.22. Definice. Řekneme, že výrokové formule φ, ψ jsou *logicky ekvivalentní*, když platí:

(a) Každá výroková proměnná, která se vyskytuje ve φ, se vyskytuje i v ψ a každá výroková proměnná, která se vyskytuje v ψ, se vyskytuje i ve φ.

(b) Zadáme-li libovolně pravdivostní hodnoty všech výrokových proměnných, které se ve formulích φ, ψ vyskytují, platí $p(\varphi) \sim p(\psi)$.

Jsou-li formule φ, ψ logicky ekvivalentní, píšeme $\varphi \equiv \psi$ ($\equiv$ je zřejmě metaznak).

3.23. Poznámka. (a) Zřejmě tedy $\varphi \equiv \psi$ platí právě tehdy, když mají formule φ, ψ stejnou tabulku pravdivostních hodnot.

(b) Zřejmě je $\varphi \equiv \psi$ právě tehdy, když formule $\varphi \Leftrightarrow \psi$ je tautologie.

Přímo z definice 3.22 plyne

3.24. Věta. *Budťe α, β, γ libovolné výrokové formule. Pak platí:*

(i) $\alpha \equiv \alpha$,

(ii) *je-li* $\alpha \equiv \beta$, *pak je* $\beta \equiv \alpha$,

(iii) *je-li* $\alpha \equiv \beta$ *a* $\beta \equiv \gamma$, *pak je* $\alpha \equiv \gamma$.

Nyní si ukážeme, že místo pěti logických spojek $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$ vystačíme pouze s vhodnými dvojicemi.

3.25. Věta. *Buď φ libovolná výroková formule. Pak existují formule α, β, γ takové, že $\varphi \equiv$ $\equiv \alpha \equiv \beta \equiv \gamma$ a přitom platí:*

(a) *ve formuli α se nevyskytují jiné logické spojky než $\wedge$, $\neg$;*

(b) *ve formuli β se nevyskytují jiné logické spojky než $\vee$, $\neg$;*

(c) *ve formuli γ se nevyskytují jiné logické spojky než $\Rightarrow$, $\neg$.*

Důkaz této věty nebudeme podrobně provádět. (Je například v [3]). Ukážeme si pouze, jak lze nalézt například formuli α. V následující definici zadáme rekurentně *mechanicky počitatelnou funkci h* na slovech výrokového kalkulu, která nám umožní k libovolné výrokové formuli najít logicky ekvivalentní výrokovou formuli, v níž se nevyskytují jiné logické spojky než $\wedge$ a $\neg$. •

3.26. Definice. Funkci h na slovech výrokového kalkulu definujeme takto: není-li slovo φ výrokovou formulí, klademe $h(\varphi) \sim \omega$ (prázdné slovo). Jsou-li φ, ψ libovolné výrokové formule, klademe:

(i) $h(\varphi) \sim \varphi$, je-li φ výroková proměnná;

(ii) $h(\neg\varphi) \sim \neg h(\varphi)$;

(iii) $h(\varphi \wedge \psi) \sim h(\varphi) \wedge h(\psi)$;

(iv) $h(\varphi \vee \psi) \sim \neg\big[\neg h(\varphi) \wedge \neg h(\psi)\big]$;

(v) $h(\varphi \Rightarrow \psi) \sim \neg\big[h(\varphi) \wedge \neg h(\psi)\big]$;

(vi) $h(\varphi \Leftrightarrow \psi) \sim \neg\big[h(\varphi) \wedge \neg h(\psi)\big] \wedge \neg\big[h(\psi) \wedge \neg h(\varphi)\big]$.

3.27. Poznámka. Z definice výrokové formule plyne, že definice 3.26 nám vskutku umožňuje převést libovolnou výrokovou formuli postupně na tvar, v němž se nevyskytují znaky $\vee$, $\Rightarrow$ a $\Leftrightarrow$. Přitom je opravdu zřejmé, že funkce h je mechanicky počitatelná.

Nyní bychom, přesně vzato, měli dokázat, že formule, kterou obdržíme postupným užitím definice 3.26, je logicky ekvivalentní s výchozí výrokovou formulí. Důkaz však ponecháme čtenáři. (Je vcelku zřejmé, že podmínky (i) – (iii) zajišťují, že funkce h nemění formuli, která je již napsána ve vhodném tvaru a podmínky (iv) – (vi) využívají vhodných elementárních tautologií. Tak například (iv) zřejmě využívá de Morganova pravidla.)

3.28. Příklad. Najděte k formuli φ z příkladu 3.11 logicky ekvivalentní formuli, v níž se nevyskytují znaky $\vee, \Rightarrow, \Leftrightarrow$.

Je tedy

$$\varphi \sim \big[(\neg A \Rightarrow B) \Leftrightarrow D\big] \Rightarrow \big[A \wedge (C \vee \neg D)\big].$$

Pak:

$$h(\neg A \Rightarrow B) \sim \neg\big[h(\neg A) \wedge \neg h(B)\big] \sim \neg(\neg A \wedge \neg B)$$
$$h(C \vee \neg D) \sim \neg\big[\neg h(C) \wedge \neg h(\neg D)\big] \sim \neg(\neg C \wedge \neg\neg D)$$
$$h\big[A \wedge (C \vee \neg D)\big] \sim h(A) \wedge h(C \vee \neg D) \sim A \wedge \neg(\neg C \wedge \neg\neg D)$$
$$h\big[(\neg A \Rightarrow B) \Leftrightarrow D\big] \sim \neg\big[h(\neg A \Rightarrow B) \wedge \neg h(D)\big] \wedge \neg\big[h(D) \wedge \neg h(\neg A \Rightarrow B)\big] \sim$$
$$\sim \neg\big[\neg(\neg A \wedge \neg B) \wedge \neg D\big] \wedge \neg\big[D \wedge \neg\neg(\neg A \wedge \neg B)\big]$$
$$h(\varphi) \sim \neg\Big\{h\big[(\neg A \Rightarrow B) \Leftrightarrow D\big] \wedge \neg h\big[A \wedge (C \vee \neg D)\big]\Big\} \sim$$
$$\sim \neg\Big\{\neg\big[\neg(\neg A \wedge \neg B) \wedge \neg D\big] \wedge \neg\big[D \wedge \neg\neg(\neg A \wedge \neg B)\big] \wedge \neg\big[A \wedge \neg(\neg C \wedge \neg\neg D)\big]\Big\}.$$

3.30. Definice. Definujme logické spojky „|“ a „↓“ následujícími tabulkami pravdivostních hodnot:

$p(\varphi)$	$p(\psi)$	$p(\varphi \mid \psi)$	$p(\varphi \downarrow \psi)$
1	1	0	0
1	0	1	0
0	1	1	0
0	0	1	1

Tabulka 1.9:

(Spojka | se nazývá *Shefferova*).

3.29. Poznámka. Z věty 3.25 tedy plyne, že výrokový kalkul lze vybudovat pomocí tří různých dvojic logických spojek. Již v 3.21 jsme se však zmínili, že je otázkou, zda nelze najít jiné logické spojky, které by byly „efektivnější“, než jsou logické spojky běžně užívané. Ukážeme, že to opravdu možné je. Uvedeme dvě logické spojky, z nichž každá sama o sobě nám umožňuje vybudovat výrokový kalkul.

3.31. Věta. *Budťe A, B libovolné výrokové proměnné. Pak platí:*

(1) $A|B \equiv \neg(A \wedge B)$

(2) $A|A \equiv \neg A$

(3) $A|B \equiv \neg A \vee \neg B$

(4) $A \downarrow B \equiv \neg(A \vee B)$

(5) $A \downarrow B \equiv \neg A \wedge \neg B$

Důkaz je triviální a přenecháme jej čtenáři. •

Z vět 3.25 a 3.31 plyne

3.32. Důsledek. *Buď φ libovolná formule výrokového kalkulu. Pak existují formule α, β takové, že $\varphi \equiv \alpha \equiv \beta$ a formule α neobsahuje jinou logickou spojku než | a formule β jinou logickou spojku než $\downarrow$.*

4 Predikátový kalkul

Některé věci nelze vědět —
nevíme však, o které věci jde.
JAFFOVA POUČKA

Výrokový kalkul, který jsme podrobně probrali v §3, zkoumá závislost pravdivosti složených výroků na pravdivosti či nepravdivosti jednodušších výroků, z nichž je složen.

Uvedli jsme však již, že v jeho obecnosti je současně i jeho omezení. Pravidly výrokového kalkulu by se měly řídit úvahy v matematice stejně jako v biologii, v lingvistice stejně jako v meteorologii.

Výrokový kalkul je však v jistém slova smyslu jen prvním přiblížením k našemu cíli, tj. k popisu formalizace matematických teorií. Víme již, že výrokový kalkul nám vůbec neumožňuje rozhodovat, zda jednoduché — atomární — výroky dané teorie jsou pravdivé či nikoliv, ani nám neumožňuje rozhodnout, které formule v dané teorii jsou správně utvořené a podobně.

V tomto paragrafu nám půjde pouze o syntaktický popis studované problematiky. Na rozdíl od výrokového kalkulu nám však predikátový kalkul umožní i syntaktický popis atomárních výroků.

Víme již, že různé matematické teorie mají navzájem odlišné jazyky, užívají různých symbolů, tvoří se v nich formule odlišnými způsoby. Přesto však mají mnoho věcí společných. A právě tento „společný základ“ nyní popíšeme.

V jistém slova smyslu budeme postupovat obdobně jako v §3. Nejprve popíšeme *abecedu*, pak určíme, která slova v této abecedě budeme považovat za správně utvořená (ta budeme nazývat *predikátové formule*), budeme definovat *tautologie* predikátového kalkulu a podobně.

Nejprve tedy k abecedě predikátového kalkulu. Vzhledem k tomu, že již budeme studovat i syntaktickou strukturu atomárních výroků, musí naše abeceda nutně obsahovat znaky, které jsou specifické pro danou teorii (například v teorii množin je to znak $\in$, v aritmetice znaky $+$, $\leq$ apod.). Kromě logických spojek je do naší abecedy nutno zařadit i znaky $\forall$ a $\exists$ (kvantifikátory). Samozřejmě abecedu vytvoříme tak, aby neobsahovala metaznaky, jichž budeme užívat analogicky jako v §§2 – 3.

4.1. Definice. *Abeceda predikátového kalkulu* je tvořena následujícími znaky:

1. Znaky pro *proměnné pro objekty* (obvykle jsou to písmena latinské abecedy, případně s indexy).
2. Znaky $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$, $\forall$, $\exists$ *pro logické spojky a kvantifikátory.*
3. *Specifické znaky* pro popisovanou teorii (například v teorii množin znak $\in$).
4. Závorky (a).

4.2. Poznámka. V tomto paragrafu budeme proměnné pro objekty označovat malými písmeny $a, b, c, \ldots, x, y, z$ atd. Velká písmena si prozatím rezervujeme pro výrokové proměnné, které budeme ještě potřebovat k zápisu výrokových formulí. O užití indexů v naší abecedě platí totéž, co jsme již uvedli v poznámce 3.2.

4.3. Definice. Řekneme, že proměnná x je *vázána* ve slově φ, je-li slovo $\forall x$ nebo slovo $\exists x$ podslovem slova φ.
Každá proměnná, která ve slově φ není vázána, se nazývá *volná proměnná* ve slově φ.
Proměnná, která se ve slově φ vyskytuje a je volnou proměnnou ve φ, se nazývá *podstatně volná* ve φ.

4.4. Příklad. Buď

$$\varphi \sim \big(x \vee (y \Rightarrow \exists z)\big) \Leftrightarrow (\forall t \vee w)$$

Pak jsou zřejmě:
x, y, w podstatně volné proměnné ve φ
z, t vázané proměnné ve φ
$u, v, p, r, \ldots$ volné proměnné ve φ.

4.5. Definice. Řekneme, že slova φ, ψ jsou *slučitelná*, jestliže žádná podstatně volná proměnná v jednom z těchto slov není vázaná ve druhém slově.

4.6. Příklad. Nechť

$$\varphi \sim \exists x(y \Rightarrow z) \vee \forall t$$

$$\psi \sim \forall x u(\vee w)$$

$$\varrho \sim t \Leftrightarrow (\exists x \vee z).$$

Pak jsou slova φ, ψ slučitelná, slova ψ, ϱ jsou také slučitelná, ale slova φ, ϱ slučitelná nejsou.

Je zřejmé, že v žádné teorii nemá smysl uvažovat všechna možná slova vytvořená v abecedě definované v 4.1. „Správně“ vytvořená slova budeme, podobně jako v §3, opět definovat rekurentně; udáme návod, jak lze ze slov jednodušších vytvářet slova složitější. K tomu je však především nutné mít k dispozici „základní“, nejjednodušší formule, které již nevznikají z formulí jednodušších. Ve výrokovém kalkulu roli těchto formulí plnily přímo výrokové proměnné. V predikátovém kalkulu tuto úlohu zastávají tzv. **primitivní predikáty**.

Definovat primitivní predikáty však v této chvíli nemůžeme. Čtenář si již jistě uvědomil, že každá matematická teorie nutně má své vlastní primitivní predikáty. (Představíme-li si totiž, co po primitivních predikátech požadujeme, snadno si uvědomíme, že to zřejmě budou formule, z nichž se po dosazení konstant za proměnné stanou atomární výroky dané teorie; v aritmetice jsou to například slova „$x < y$“, „$x + y < z$“ apod., v teorii množin slovo „$x \in y$“ atd.).

Shrneme-li tedy uvedené úvahy, znamená to, že při budování každé teorie je nutno, kromě jiného, po zadání abecedy stanovit primitivní predikáty, přesněji řečeno: **prohlásit některá slova za primitivní predikáty**. V každé teorii jsou přitom tyto primitivní predikáty stanoveny jinak a je tak do značné míry na vůli toho, kdo teorii tvoří, která slova za primitivní predikáty prohlásí. Při jejich volbě je však užitečné dodržovat jistá pravidla.

Především je vhodné, aby primitivních predikátů bylo co nejméně. Poněvadž primitivní predikáty hrají roli nejjednodušších formulí, nesmí se v nich vyskytovat logické spojky a z mnoha důvodů předpokládáme, že se v nich nevyskytují ani kvantifikátory. (Později uvidíme, že teorii množin lze vybudovat pomocí jediného primitivního predikátu „$x \in y$“.) Často jsou primitivní predikáty stanoveny tak, že jsou za primitivní predikáty prohlášena jistá slova, z nichž lze všechny ostatní primitivní predikáty obdržet substitucí proměnných za proměnné.

Vlastnosti *primitivních predikátů* shrneme do následující úmluvy.

4.7. Dohoda.

1. Je-li φ primitivní predikát, pak se ve φ nevyskytuje žádný ze znaků $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$, $\forall$, $\exists$.

2. Je-li φ primitivní predikát a f libovolná substituce tvaru $[\xi \to \eta]$, kde ξ, η jsou proměnné pro objekty, pak je $f(\varphi)$ primitivní predikát.

Nyní již můžeme přistoupit k definici formulí.

4.8. Definice.

1. Každý primitivní predikát je *predikátovou formulí*.

2. Je-li φ predikátová formule, je také slovo $\neg(\varphi)$ predikátová formule.

3. Jsou-li φ, ψ slučitelné predikátové formule, jsou také slova $(\varphi) \vee (\psi)$, $(\varphi) \wedge (\psi)$, $(\varphi) \Rightarrow (\psi)$ a $(\varphi) \Leftrightarrow (\psi)$ predikátovými formulemi.

4. Je-li φ predikátová formule a proměnná x není ve slově φ vázaná, jsou slova $(\exists x)(\varphi)$ a $(\forall x)(\varphi)$ predikátovou formulí.

5. Slovo, které nelze vytvořit pomocí (1) – (4), není predikátovou formulí.

4.9. Příklad. V teorii množin je slovo $x \in y$ primitivním predikátem. Podle definice 4.8 jsou tedy následující slova predikátovými formulemi:

(a) $(x \in y) \vee (y \in z)$,

(b) $\neg\big((x \vee y) \vee (y \vee z)\big)$,

(c) $(x \in z) \Leftrightarrow \Big(\neg\big((x \in y) \vee (y \in z)\big)\Big)$,

(d) $(\forall x)\Big((x \in z) \Leftrightarrow \Big(\neg\big((x \in y) \vee (y \in z)\big)\Big)\Big)$

atd.

Predikátovou formulí však není slovo

$$(\forall x)\Big((x \in y) \Rightarrow \big((\exists x)(x \in z)\big)\Big),$$

neboť ve formuli $(x \in y) \Rightarrow \big((\exists x)(x \in z)\big)$ je proměnná x vázaná a proto nelze této formuli předřadit slovo $\forall x$.

4.10. Poznámka. I v predikátovém kalkulu, pokud to bude možné, budeme zjednodušovat zápis predikátových formulí. Z úmluvy 3.5 převezmeme všechna pravidla, která doplníme navíc o dohodu, že každý z kvantifikátorů $\forall$, $\exists$ má přednost před kteroukoliv z logických spojek $\vee$, $\wedge$, $\neg$, $\Rightarrow$, $\Leftrightarrow$, takže například $(\exists x)\varphi \vee \psi$ značí $\big((\exists x)(\varphi)\big) \vee (\psi)$ a nikoliv $(\exists x)(\varphi \vee \psi)$.

4.11. Definice. Řekneme, že predikátová formule je *uzavřená*, nevyskytuje-li se v ní podstatně volná proměnná.

4.12. Poznámka. Každé dvě uzavřené formule jsou slučitelné. Uvědomme si rovněž, že **každé tvrzení matematické teorie je nutně uzavřenou formulí**, což však zdaleka neznamená, že by každá uzavřená formule měla být pravdivým výrokem. Je-li φ predikátová formule v níž se vyskytují podstatně volné proměnné, není φ zřejmě výrok. Výrok však z φ utvoříme, dosadíme-li za podstatně volné proměnné do φ konstanty, tj. konkrétní objekty dané teorie. Obecně tak můžeme z φ utvořit výrok pravdivý i nepravdivý.

4.13. Definice. Řekneme, že predikátová formule φ je tautologií predikátového kalkulu (nebo stručně jen *tautologií*), jestliže po každém dosazení konstant za podstatně volné proměnné ve φ obdržíme pravdivý výrok. (Triviálně je tedy tautologií každá pravdivá uzavřená formule.)

4.14. Příklad. Tautologií v teorii množin jistě je například formule

$$\varphi \sim (\forall y)\big((x \in y) \vee \neg(x \in y)\big)$$

s jedinou podstatně volnou proměnnou x.

Je evidentní, že vyšetřování tautologií predikátového kalkulu je podstatně komplikovanější než popis tautologií výrokového kalkulu. Nyní však ukážeme šest jednoduchých pravidel, která umožňují vytvářet tautologie predikátového kalkulu. Důležitost těchto pravidel bude zřejmá z definice, kterou uvedeme později (definice 4.29).

4.15. Pravidlo 1. Buď φ libovolná tautologie výrokového kalkulu, buďte $A_1, \dots, A_n$ všechny výrokové proměnné vyskytující se ve φ. Buďte $\psi_1, \dots, \psi_n$ libovolné navzájem slučitelné formule. Buď konečně f substituce

$$[A_1 \to \psi_1, \dots, A_n \to \psi_n]\,.$$

Pak je formule $f(\varphi)$ tautologií predikátového kalkulu.

Důkaz tvrzení, že popsaným způsobem opravdu vždy vznikne tautologie, je jednoduchý a přenecháme jej čtenáři. •

4.16. Poznámka. Je zřejmé, že $f(\varphi)$ je uzavřená formule, pokud jsou všechny formule $\psi_1, \dots, \psi_n$ uzavřené.

4.17. Příklad.

(a) Podle věty 3.15(8) je

$$\big[(P \Rightarrow Q) \wedge (Q \Rightarrow R)\big] \Rightarrow (P \Rightarrow R)$$

tautologie výrokového kalkulu. Slova

$$\psi_1 \sim (x \in y) \Rightarrow (z \in y)$$
$$\psi_2 \sim (\forall t)(x \in t)$$
$$\psi_3 \sim (\exists w)\big[(x \in w) \wedge (w \in z)\big]$$

jsou zřejmě slučitelné formule. Podle pravidla 4.15 je tedy

$$\Big\{\Big\{\big[(x \in y) \Rightarrow (z \in y)\big] \Rightarrow \big[(\forall t)(x \in t)\big]\Big\} \wedge$$
$$\wedge \Big\{\big[(\forall t)(x \in t)\big] \Rightarrow \Big\{(\exists w)\big[(x \in w) \wedge (w \in z)\big]\Big\}\Big\}\Big\} \Rightarrow$$
$$\Rightarrow \Big\{\big[(x \in y) \Rightarrow (z \in y)\big] \Rightarrow \Big\{(\exists w)\big[(x \in w) \wedge (w \in z)\big]\Big\}\Big\}$$

tautologie predikátového kalkulu.

(b) Podle věty 3.15(10) je tautologií formule

$$(P \wedge \neg P) \Rightarrow Q.$$

Je tedy tautologií predikátového kalkulu například formule

$$\big[(x \in y) \wedge \neg(x \in y)\big] \Rightarrow (\forall z)(x \in z)$$

nebo formule

$$\Big\{\big[(x \in y) \Rightarrow (z \in y)\big] \wedge \neg\big[(x \in y) \Rightarrow (z \in y)\big]\Big\} \Rightarrow (\forall t)(x \in t).$$

Z příkladu 4.17 je vidět, že každá tautologie výrokového kalkulu je vlastně návodem k vytváření tautologií predikátového kalkulu. Lehce se však ukáže že pravidlo 4.15 nám ještě neumožňuje odvodit všechny tautologie predikátového kalkulu.

Další pravidlo k získávání tautologií uvedeme nyní.

4.18. Pravidlo 2. Je-li $(\exists x)\varphi$ predikátová formule, jsou formule

1. $(\exists x)\varphi \Leftrightarrow \neg(\forall x)(\neg\varphi)$
2. $(\forall x)\varphi \Leftrightarrow \neg(\exists x)(\neg\varphi)$

tautologie predikátového kalkulu.

Uvedené pravidlo vlastně formalizuje to, jak negujeme výroky s kvantifikátory, což známe již ze střední školy.

4.19. Příklad. Poněvadž $\varphi \sim (\exists x)\big[(x \in y) \Rightarrow (x \in z)\big]$ je predikátová formule, jsou tautologiemi formule

$$\Big\{(\exists x)\big[(x \in y) \Rightarrow (x \in z)\big]\Big\} \Leftrightarrow \neg\Big\{(\forall x)\neg\big[(x \in y) \Rightarrow (x \in z)\big]\Big\}$$

a

$$\Big\{(\forall x)\big[(x \in y) \Rightarrow (x \in z)\big]\Big\} \Leftrightarrow \neg\Big\{(\exists x)\neg\big[(x \in y) \Rightarrow (x \in z)\big]\Big\}.$$

4.20. Pravidlo 3. Buď $(\forall x)\varphi$ predikátová formule, v níž není proměnná y vázaná. Buď f substituce $[x \to y]$. Pak je $(\forall x)\varphi \Rightarrow f(\varphi)$ tautologie.

4.21. Poznámka. Jestliže je formule $(\forall x)\varphi$ nepravdivá, je formule $(\forall x)\varphi \Rightarrow f(\varphi)$ tautologií triviálně. Pravidlo 4.20 rovněž není zajímavé v případě, kdy se proměnná x ve slově φ nevyskytuje. Smysl pravidla 4.20 spočívá v následujícím: vyskytuje-li se ve slovu φ proměnná x a $(\forall x)\varphi$ je pravdivá formule, je φ pravdivou formulí po dosazení libovolné proměnné (která ovšem nesmí být ve φ vázaná) za x.

4.22. Příklad. Podle pravidla 4.20 je tautologií například predikátová formule

$$(\forall x)\big[(x \in y) \vee (x \in z)\big] \Rightarrow \big[(t \in y) \vee (t \in z)\big].$$

4.23. Pravidlo 4. Buď φ predikátová formule, v níž je proměnná x vázaná a v níž se proměnná y nevyskytuje. Buď f substituce $[x \to y]$. Pak je

$$\varphi \Leftrightarrow f(\varphi)$$

tautologie.

4.24. Příklad. Buď $\varphi \sim (\exists x)\big((x \in y) \Leftrightarrow (x \in z)\big)$, f buď substituce $[x \to u]$. Pak je

$$(\exists x)\big[(x \in y) \Leftrightarrow (x \in z)\big] \Leftrightarrow (\exists u)\big[(u \in y) \Leftrightarrow (u \in z)\big]$$

tautologie. Vidíme, že podle pravidla 4.23 nezáleží na označení vázané proměnné.

4.25. Pravidlo 5. Jsou-li následující dvě slova predikátové formule, jsou to tautologie:
(a) $(\forall x)(\varphi \Leftrightarrow \psi) \Rightarrow \big[(\forall x)\varphi \Leftrightarrow (\forall x)\psi\big]$
(b) $(\exists x)(\varphi \Leftrightarrow \psi) \Rightarrow \big[(\exists x)\varphi \Leftrightarrow (\exists x)\psi\big]$.

4.26. Příklad. Formule

$$(\forall x)\big[(x \in y) \Leftrightarrow (x \in z)\big] \Rightarrow \big[(\forall x)(x \in y) \Leftrightarrow (\forall x)(x \in z)\big]$$

$$(\exists x)\big[(x \in y) \Leftrightarrow (x \in z)\big] \Rightarrow \big[(\exists x)(x \in y) \Leftrightarrow (\exists x)(x \in z)\big]$$

jsou tautologie.

4.27. Pravidlo 6. Buď $\big((\exists x)\varphi\big) \wedge \psi$ predikátová formule a nechť se proměnná x nevyskytuje ve slovu ψ. Pak jsou následující formule tautologie:
(a) $\big((\exists x)\varphi\big) \wedge \psi \Leftrightarrow (\exists x)(\varphi \wedge \psi)$
(b) $\big((\forall x)\varphi\big) \wedge \psi \Leftrightarrow (\forall x)(\varphi \wedge \psi)$
(c) $\Big[\big((\forall x)\varphi\big) \Rightarrow \psi\Big] \Leftrightarrow (\forall x)(\varphi \Rightarrow \psi)$.

4.28. Příklad. Buď $\varphi \sim x \in z$, $\psi \sim \neg(y \in z)$. Pak jsou podle pravidla 4.27 všechny následující formule tautologiemi:

(i) $\big[(\exists x)(x \in y) \wedge \neg(y \in z)\big] \Leftrightarrow (\exists x)\big[(x \in y) \wedge \neg(y \in z)\big]$

(ii) $\big[(\forall x)(x \in y) \wedge \neg(y \in z)\big] \Leftrightarrow (\forall x)\big[(x \in y) \wedge \neg(y \in z)\big]$

(iii) $\big[(\forall x)(x \in y) \Rightarrow \neg(y \in z)\big] \Leftrightarrow (\forall x)\big[(x \in y) \Rightarrow \neg(y \in z)\big]$.

4.29. Definice. Tautologie utvořená pomocí některého z pravidel 1 – 6 se nazývá *elementární tautologie* predikátového kalkulu.

Lze dokázat, že existují tautologie, které nejsou elementární. Proto si nyní stanovíme další dvě jednoduchá *doplňující pravidla* pro odvozování tautologií.

4.30. Doplňující pravidla.

(**DP 1**) Jsou-li φ a $\varphi \Rightarrow \psi$ tautologie predikátového kalkulu, je i ψ tautologie predikátového kalkulu.

(**DP 2**) Je-li x volná proměnná v tautologii φ, je $(\forall x)\varphi$ tautologie predikátového kalkulu.

Význam elementárních tautologií a doplňujících pravidel je zřejmý z následující definice.

4.31. Definice. *Důkazem v predikátovém kalkulu* nazýváme takovou posloupnost formulí, že každý člen této posloupnosti je buďto elementární tautologií nebo je odvozen z některých předchozích členů této posloupnosti pomocí pravidel (DP 1) a (DP 2).
Důkazem formule φ je posloupnost, která je důkazem a jejímž posledním členem je formule φ. Řekneme, že formule φ je *dokazatelná v predikátovém kalkulu*, když existuje její důkaz.
Je-li φ dokazatelná, píšeme $\vdash \varphi$. ($\vdash$ je tedy nový metaznak).

4.32. Poznámka. Podle definice 4.31 je každá dokazatelná formule tautologií. Neznamená to však, že najít důkaz dané formule je obecně snadnou záležitostí. Stejně tak je evidentní, že jedna a táž formule může mít několik důkazů.

4.33. Příklad. Ukážeme, že predikátová formule

$$\Big\{(\exists z)\big[(y \in z) \vee (w \in z)\big]\Big\} \Rightarrow \Big\{(\exists x)\Big\{\big[(x \in y) \Rightarrow \neg(x \in y)\big] \Rightarrow \neg(x \in y)\Big\} \Leftrightarrow$$

$$\Leftrightarrow \neg(\forall x)\neg\Big\{\big[(x \in y) \Rightarrow \neg(x \in y)\big] \Rightarrow \neg(x \in y)\Big\}\Big\} \qquad (*)$$

je dokazatelná.

Podle věty 3.15 je výroková formule

$$(P \Rightarrow \neg P) \Rightarrow \neg P$$

tautologie výrokového kalkulu. Podle pravidla 4.15 je tedy predikátová formule

$$\varphi \sim \big[(x \in y) \Rightarrow \neg(x \in y)\big] \Rightarrow \neg(x \in y) \qquad \text{(i)}$$

elementární tautologií predikátového kalkulu. Podle pravidla 4.18(1) je pak ale elementární tautologií predikátového kalkulu i formule

$$\psi \sim (\exists x)\Big\{\big[x \in y) \Rightarrow \neg(x \in y)\big] \Rightarrow \neg(x \in y)\Big\} \Leftrightarrow \neg(\forall x)\neg\Big\{\big[(x \in y) \Rightarrow$$

$$\Rightarrow \neg(x \in y)\big] \Rightarrow \neg(x \in y)\Big\}, \qquad \text{(ii)}$$

tj. $\psi \sim (\exists x)\varphi \Leftrightarrow \neg(\forall x)(\neg\varphi)$. Poněvadž je výroková formule

$$P \Rightarrow (Q \Rightarrow P)$$

zřejmě tautologií výrokového kalkulu, je opět podle pravidla 4.15 formule

$$\psi \Rightarrow \Big\{\Big\{(\exists z)\big[(y \in z) \wedge (w \in z)\big]\Big\} \Rightarrow \psi\Big\} \qquad \text{(iii)}$$

elementární tautologií. Pak ale podle (DP 1) je elementární tautologií i formule

$$\Big\{(\exists z)\big[(y \in z) \wedge (w \in z)\big]\Big\} \Rightarrow \psi,$$

což je ovšem formule ($\star$), kterou chceme dokázat.

Jinak řečeno, posloupnost formulí

$$\varphi, \psi, \psi \Rightarrow \Big\{\Big\{(\exists z)\big[(y \in z) \wedge (w \in z)\big]\Big\} \Rightarrow \psi\Big\}, (\star)$$

je důkaz formule ($\star$).

4.34. Věta. *Budte φ, ψ dokazatelné slučitelné formule predikátového kalkulu. Pak je i formule $\varphi \wedge \psi$ dokazatelná.*

Důkaz. Podle předpokladu existují důkazy formulí φ, ψ. Označme tyto důkazy

$$\varphi_1, \varphi_2, \ldots, \varphi$$
$$\psi_1, \psi_2, \ldots, \psi.$$

Podle pravidla 4.15 a věty 3.15(15) je tedy

$$\sigma \sim \varphi \Rightarrow \big[\psi \Rightarrow (\varphi \wedge \psi)\big]$$

elementární tautologie. Podle (DP 1) je pak elementární tautologií formule

$$\tau \sim \psi \Rightarrow (\varphi \wedge \psi).$$

Opět podle (DP 1) je ale elementární tautologií i formule $\varphi \wedge \psi$.

Tím je tvrzení dokázáno, neboť posloupnost

$$\varphi_1, \varphi_2, \ldots, \varphi, \psi_1, \psi_2, \ldots, \psi, \sigma, \tau, \varphi \wedge \psi$$

je důkazem formule $\varphi \wedge \psi$. •

4.35. Poznámka. Tvrzení 4.34 je dalším návodem na vytváření dokazatelných formulí (a tedy tautologií) predikátového kalkulu. Je přitom zřejmé, že pravidla pro vytváření elementárních tautologií spolu s pravidly (DP 1) a (DP 2) nám umožňují zformulovat takových návodů celou řadu. Čtenář nechť si promyslí, že důkaz dokazatelnosti formule ($\star$) v příkladu 4.33 je založen na následujícím návodu:

Je-li $\vdash \psi$ a slovo $\varphi \Rightarrow \psi$ je formule, je také $\vdash \varphi \Rightarrow \psi$.

5 Axiomatická teorie

Pokusy musí být opakovatelné —
jen tak mohou naprosto stejným způsobem vždy selhat.
PÁTÁ FINAGLOVA ZÁSADA

Ukázali jsme si rozdíl mezi výrokovým a predikátovým kalkulem a víme již, jak užitečný je predikátový kalkul při popisu a zkoumání teorie ze syntaktického hlediska. Predikátový kalkul nám umožnil precizovat syntaktickou strukturu atomárních výroků a definovat dokazatelnost formule (v predikátovém kalkulu). V příkladu 4.33 jsme si ukázali, že pomocí predikátového kalkulu můžeme dokázat i poměrně komplikované formule a je zřejmé, že náš příklad byl přitom zvolen velmi jednoduše. Současně z §4 plyne, že dokazatelných formulí v predikátovém kalkulu je nekonečně mnoho.

Čtenáři je však jistě zřejmé, že ani predikátový kalkul není dostatečným nástrojem k vybudování konkrétní matematické teorie. Víme totiž, že dokazatelné formule v predikátovém kalkulu nemohou vypovídat nic o tom, čím se dvě různé matematické teorie odlišují. Predikátový kalkul je pořád jen „společným základem“ těch teorií, při jejichž výstavbě tohoto kalkulu použijeme. Navíc je podle poznámky 4.32 každá dokazatelná formule predikátového kalkulu tautologií, jinak řečeno, dosadíme-li do dokazatelné formule za podstatně volné proměnné libovolné konstanty dané teorie, obdržíme *vždycky* pravdivé tvrzení. Víme však, že při výstavbě matematické teorie nám nejde o hledání tautologií, ale právě naopak, chceme většinou dokázat **pravdivost** uzavřených formulí, které považujeme za zápisy výroků.

My však již víme, co je nutno v této situaci provést. Jisté formule prohlásíme za pravdivé bez důkazu.Tyto formule nazveme **axiómy** dané teorie a z těchto axiómů pak odvozujeme další tvrzení. Jak lze takto vybudovat nějakou teorii prakticky, uvidíme v §6. Nyní si jen stručně uvedeme některé základní vlastnosti společné všem axiomatickým teoriím.

K vytvoření *axiomatické teorie* je tedy nutno: (a) stanovit konkrétně primitivní predikáty (a tím tedy vlastně zadat predikátový kalkul), (b) udat soupis axiómů.

Při výstavbě axiomatické teorie uvidíme, že axiómy jsou, zhruba řečeno, dvojího druhu. Některé axiómy pouze upřesňují jazyk matematické teorie, nejčastěji tak, že zadávají jisté vztahy mezi primitivními predikáty. Jiné axiómy naopak postulují základní vlastnosti objektů, které v dané situaci studujeme. Po formální stránce je nejjednodušší systém axiómů zadat tak, že udáme jejich soupis. To však není vždycky možné — například proto, že axiómů dané teorie je nekonečně mnoho. (Tak je tomu například u Zermelo-Fraenkelovy teorie množin — viz §6.) V takovém případě je obvykle udáván alespoň tvar formulí, které za axiómy považujeme. V každém případě je však přirozené požadovat, aby bylo o každé formuli možno mechanicky rozhodnout, zda je nebo není axiómem.

Nyní již předpokládejme, že jsme stanovili primitivní predikáty a axiómy teorie $\mathcal{T}$.

5.1. Definice. *Důkazem v teorii* $\mathcal{T}$ nazýváme takovou posloupnost formulí, že každý člen této posloupnosti:

(a) je axiómem teorie $\mathcal{T}$, nebo

(b) je elementární tautologií, nebo

(c) je utvořen z některých předcházejících členů důkazu užitím pravidel (DP 1) a (DP 2).

5.2. Definice. Řekneme, že formule φ je *dokazatelná v teorii* $\mathcal{T}$, existuje-li důkaz v teorii $\mathcal{T}$, jehož posledním členem je formule φ. Je-li φ dokazatelná v $\mathcal{T}$, píšeme $\mathcal{T} \vdash \varphi$. Uzavřená dokazatelná formule φ v teorii $\mathcal{T}$ se nazývá *věta* (nebo *teorém* nebo též v některých případech *lemma*) teorie $\mathcal{T}$.

Bezprostředně z definic 5.1 a 5.2 plyne

5.3. Věta. *Je-li* $\vdash \varphi$, *je také* $\mathcal{T} \vdash \varphi$.

Při axiomatické výstavbě nějaké teorie je obvyklé, že stanovením počátečních axiómů vytvoříme teorii $\mathcal{T}$ a tu pak postupně doplňujeme o další axiómy. Analogií věty 5.3 je pak následující zřejmé tvrzení:

5.4. Věta. *Nechť teorie* $\mathcal{T}_1$ *vznikla z teorie* $\mathcal{T}$ *přidáním dalších axiómů. Pak ze vztahu* $\mathcal{T} \vdash \varphi$ *plyne* $\mathcal{T}_1 \vdash \varphi$.

V dalším bude užitečné přijmout následující označení: teorii $\mathcal{T}_1$, která vznikne z teorie $\mathcal{T}$ přidáním jediného axiómu τ, označíme $(\mathcal{T}, \tau)$. Má-li teorie $\mathcal{T}$ jen konečně mnoho axiómů $\varphi_1, \ldots, \varphi_n$, označíme ji $(\varphi_1, \ldots, \varphi_n)$.

Jednou ze základních vět (přesněji řečeno *metavět*) je následující tvrzení:

5.5. Věta o dedukci. Buďte φ, ψ slučitelné formule, ψ nechť je uzavřená. Pak je formule φ dokazatelná v $(\mathcal{T}, \psi)$ právě tehdy, když je v $\mathcal{T}$ dokazatelná formule $\psi \Rightarrow \varphi$.

Důkaz. Tvrzení je intuitivně zcela zřejmé. Formální důkaz je rovněž poměrně jednoduchý.

Z jedné strany je důkaz triviální: je-li $\mathcal{T} \vdash \psi \Rightarrow \varphi$, existuje v $\mathcal{T}$ důkaz $\varphi_1, \ldots, \psi \Rightarrow \varphi$. Ale ψ je axióm v (T, ψ), takže φ je podle (DP 1) tautologie v $(\mathcal{T}, \psi)$. Posloupnost

$$\varphi_1, \ldots, \psi \Rightarrow \varphi, \psi, \varphi$$

je tedy důkazem formule φ v $(\mathcal{T}, \psi)$.

Důkaz tvrzení, že z $(\mathcal{T}, \psi) \vdash \varphi$ plyne $\mathcal{T} \vdash \psi \Rightarrow \varphi$ nebudeme provádět. Je uveden například v [3]. •

V úvodu tohoto paragrafu jsme uvedli, že axiomatická teorie může obsahovat nekonečně mnoho axiómů. Z následujícího tvrzení však plyne, že k důkazu jednotlivých formulí by stačila teorie s konečně mnoha axiómy. Je totiž zřejmé, že platí

5.6. Věta. *Buď $\mathcal{T} \vdash \varphi$ a budťe $\psi_1, \ldots, \psi_n$ všechny axiómy, které se vyskytují v některém důkazu φ. Pak je*

$$(\psi_1, \ldots, \psi_n) \vdash \varphi.$$

Z následující věty pak plyne, že každou teorii s konečně mnoha axiómy lze považovat za teorii s jediným axiómem.

5.7. Věta. $\big[(\psi_1, \ldots, \psi_n) \vdash \varphi\big] \Leftrightarrow \big[(\psi_1 \wedge \ldots \wedge \psi_n) \vdash \varphi\big]$.

Důkaz. I. Nechť $(\psi_1, \ldots, \psi_n) \vdash \varphi$. Podle pravidla 4.15 a věty 3.15(11) je

$$\alpha_1 \sim \big[\psi_1 \wedge (\psi_2 \wedge \ldots \wedge \psi_n)\big] \Rightarrow \psi_1$$

elementární tautologie. Formule

$$\beta_1 \sim \psi_1 \wedge (\psi_2 \wedge \ldots \wedge \psi_n)$$

je axióm v $(\psi_1 \wedge \ldots \wedge \psi_n)$, takže ψ_1 může být členem důkazu podle (DP 1). Posloupnost

$$\alpha_1, \beta_1, \psi_1$$

je tedy důkazem formule ψ_1 v teorii $(\psi_1 \wedge \ldots \wedge \psi_n)$.

Analogicky lze sestrojit důkazy

$$\alpha_i\,,\ \beta_i\,,\ \psi_i$$

pro $i = 2, \ldots, n$.

Je-li nyní

$$\varphi_1, \varphi_2, \ldots, \varphi$$

důkaz formule φ v teorii $(\psi_1, \ldots, \psi_n)$, je

$$\alpha_1, \beta_1, \psi_1, \ldots, \alpha_n, \beta_n, \psi_n, \varphi_1, \varphi_2, \ldots, \varphi$$

důkaz formule φ v $(\psi_1 \wedge \psi_2 \wedge \ldots \wedge \psi_n)$.

II. Nechť $(\psi_1 \wedge \ldots \wedge \psi_n) \vdash \varphi$. Důkaz formule φ v této teorii je podle věty 4.34 i důkazem v teorii $(\psi_1, \ldots, \psi_n)$. •

Nyní již lehce zformulujeme vztah mezi důkazem formule v $\mathcal{T}$ a důkazem vhodné formule v predikátovém kalkulu.

5.8. Věta. *$\mathcal{T} \vdash \varphi$ právě tehdy, když existují axiómy $\psi_1, \ldots, \psi_n$ v $\mathcal{T}$ takové, že $\vdash (\psi_1 \wedge \ldots \wedge \wedge \psi_n) \Rightarrow \varphi$.*

Důkaz. I. Nechť $\mathcal{T} \vdash \varphi$. Buďte $\psi_1, \ldots, \psi_n$ axiómy, které se vyskytují v důkazu formule φ. Podle 5.6 je $(\psi_1, \ldots, \psi_n) \vdash \varphi$, takže podle 5.7 je $(\psi_1 \wedge \ldots \wedge \psi_n) \vdash \varphi$. Podle 5.5 je pak ale $\vdash (\psi_1, \ldots, \psi_n) \Rightarrow \varphi$.

II. Obrácené tvrzení plyne opět z vět 5.5, 5.6 a 5.7. •

V §1 jsme uvedli, že teorie, v níž se objeví antinomie, je prakticky bezcenná. Nyní již můžeme ukázat z jakého důvodu.

5.9. Definice. Řekneme, že teorie $\mathcal{T}$ je *sporná*, existuje-li taková formule φ, že

$$\mathcal{T} \vdash \varphi \qquad \text{i} \qquad \mathcal{T} \vdash \neg\varphi.$$

Není-li teorie sporná, říkáme, že je *bezesporná*.

5.10. Věta. *Ve sporné teorii je dokazatelná každá formule.*

Důkaz. Nechť v $\mathcal{T}$ platí $\mathcal{T} \vdash \varphi$, $\mathcal{T} \vdash \neg\varphi$ a buď ψ libovolná formule. Je-li $\psi \sim \varphi$, není co dokazovat. Nechť tedy ψ není totožná s φ.

(a) *ψ je slučitelná s φ*: Nechť

$$\alpha_1, \alpha_2, \ldots, \varphi$$

je důkaz φ v $\mathcal{T}$,

$$\beta_1, \beta_2, \ldots, \neg\varphi$$

důkaz $\neg\varphi$ v $\mathcal{T}$. Podle věty 4.34 je $\varphi \wedge \neg\varphi$ v $\mathcal{T}$ dokazatelná. Existuje tedy důkaz

$$\gamma_1, \gamma_2, \ldots, \varphi \wedge \neg\varphi.$$

Podle pravidla 4.15 a věty 3.15(10) je

$$(\varphi \wedge \neg\varphi) \Rightarrow \psi$$

elementární tautologie, takže ψ je dokazatelná podle (DP 1). Důkazem ψ v $\mathcal{T}$ je posloupnost

$$\alpha_1, \alpha_2, \ldots, \varphi, \beta_1, \beta_2, \ldots, \psi, \gamma_1, \gamma_2, \ldots, \varphi \wedge \neg\varphi, (\varphi \wedge \neg\varphi) \Rightarrow \psi, \psi.$$

(b) *Necht' φ, ψ nejsou slučitelné.* Buď τ libovolná formule slučitelná s φ i s ψ. Podle (a) jsou tedy dokazatelné formule τ i $\neg\tau$. Z dokazatelnosti těchto formulí však opět podle (a) plyne dokazatelnost formule ψ. •

Dokázat bezespornost zadané axiomatické teorie je nesmírně komplikovaná záležitost, jejíž rozbor přesahuje naše možnosti. Uveďme si alespoň jedno kritérium bezespornosti.

5.11. Definice. Řekneme že φ je *nerozhodnutelná* formule teorie $\mathcal{T}$, jestliže v $\mathcal{T}$ není dokazatelná ani φ ani $\neg\varphi$.

5.12. Věta. *Existuje-li v teorii $\mathcal{T}$ nerozhodnutelná formule, je $\mathcal{T}$ bezesporná.*

Důkaz. Tvrzení plyne z věty 5.10. •

5.13. Důsledek. *Je-li φ nerozhodnutelná formule teorie $\mathcal{T}$, jsou teorie $(\mathcal{T}, \varphi)$ i $(\mathcal{T}, \neg\varphi)$ bezesporné.*

Důkaz. Buď φ nerozhodnutelná formule v $\mathcal{T}$ a připusťme že $(\mathcal{T}, \varphi)$ je sporná. Podle věty 5.10 je pak $(\mathcal{T}, \varphi) \vdash \neg\varphi$. Podle věty 5.5 je pak ale $\mathcal{T} \vdash (\varphi \Rightarrow \neg\varphi)$. Existuje tedy v $\mathcal{T}$ důkaz

$$\alpha_1, \alpha_2, \ldots, \varphi \Rightarrow \neg\varphi$$

formule $\varphi \Rightarrow \neg\varphi$. Podle pravidla 4.15 a (DP 1) je pak ale

$$\alpha_1, \alpha_2, \ldots, \varphi \Rightarrow \neg\varphi,\ (\varphi \Rightarrow \neg\varphi) \Rightarrow \neg\varphi, \neg\varphi$$

důkaz formule $\neg\varphi$ v $\mathcal{T}$ a to je spor s předpokladem, že φ je nerozhodnutelná. To znamená, že teorie $(\mathcal{T}, \varphi)$ je bezesporná.

Důkaz bezespornosti teorie $(\mathcal{T}, \neg\varphi)$ lze provést zcela analogicky. •

5.14. Definice. Řekneme, že teorie $\mathcal{T}$ je *úplná,* jestliže v $\mathcal{T}$ neexistuje nerozhodnutelná formule (tj. pro každou formuli φ je $\mathcal{T} \vdash \varphi$ nebo $\mathcal{T} \vdash \neg\varphi$).

5.15. Poznámka. Při konstrukci axiomatické teorie se zdá samozřejmý požadavek takové volby axiómů, aby teorie byla bezesporná a úplná. Jak uvidíme v kapitole IV, §5, **nelze** takovou teorii množin sestrojit.

6 Axiomatická teorie množin

Když vše vysvětlíte tak, aby to všichni pochopili,
najde se někdo, kdo to chápat nebude.
DŮSLEDEK KRANSKEHO ZÁKONA

Nyní již můžeme bez potíží hovořit o axiomatických teoriích množin a můžeme předvést, jak je nějaká teorie axiomaticky budována.

První úspěšnou axiomatickou teorii množin předložil v roce 1908 německý matematik Zermelo. Později tuto teorii doplnil Fraenkel a vzniklá axiomatická teorie, tak zvaná *Zermelo-Fraenkelova teorie množin*, patří dodnes k nejužívanějším. (Nadále ji budeme označovat **ZF**.) Podstatným rysem **ZF** teorie je to, že je omezena možnost vytvářet množiny ze *všech* objektů daných vlastností. (Nelze hovořit o množině *všech* množin, o množině *všech* grup a podobně.)

Při zadání množiny všech objektů daných vlastností musí být předem stanoveno, ze které množiny (předem zadané) tyto objekty vybíráme. Nyní je tedy zřejmé, že tak často zdůrazňovaná nutnost vždycky zvolit „základní“ množinu při výuce množinových pojmů na střední škole de facto znamenala, že teorie množin byla na střední škole fakticky budována (i když se o tom nikde nehovořilo) v rámci **ZF** teorie. Přesněji řečeno (ve smyslu §1), na střední škole se vyučuje *model* Zermelo-Fraenkelovy teorie.

V moderní matematice je však dnes častěji než teorie Zermelo-Fraenkelova užívána jiná axiomatická teorie, na jejímž vybudování mají největší podíl J. von Neumann, P. Bernays a K. Gödel. Tato teorie je nazývána *Gödel-Bernaysova teorie množin*. (Budeme ji označovat **GB**). Na první pohled je možná **GB** teorie komplikovanější než teorie **ZF**. (Uvedli jsme však již v §5, že **ZF** teorie obsahuje nekonečně mnoho axiómů, zatím co **GB** teorii lze vybudovat na základě *konečně* mnoha axiómů.)

Hlavním přínosem **GB** teorie je skutečnost, že v ní lze bez obtíží hovořit i o těch systémech, které v **ZF** teorii netvoří množinu. *Primitivním* (tj. nedefinovaným) pojmem v **ZF** teorii je pojem „množina“. Primitivním pojmem **GB** teorie je „třída“, jejíž intuitivní smysl je následující. Třídou nazýváme systém *všech* objektů, patřících do oboru pravdivosti nějaké výrokové formy. **Některé třídy se pak nazvou množiny**, ukáže se však, že **některé třídy množinou nejsou**. Takové třídy se nazývají **vlastní** (to je pak například třída všech množin, třída všech grup a podobně).

V našich možnostech samozřejmě není budovat systematicky nějakou axiomatickou teorii množin. Ukažme si však alespoň, jak lze v rámci poněkud upravené **GB** teorie vybudovat

některé běžné množinové pojmy. Čtenář tím získá představu o postupech užívaných v axiomatické teorii a dovede si zrekonstruovat formalizaci teorie, kterou budeme v kapitolách II a III probírat neformálně.

Přesný popis **ZF** a **GB** teorie pak mohou čtenáři najít například v [4] nebo v [5].

6.1. Definice. *Abecedu* teorie tříd tvoří následující znaky:

1. Velká písmena latinské abecedy (eventuálně s indexy) označující proměnné pro objekty.
2. Znaky $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$, $\forall$, $\exists$ pro logické spojky a kvantifikátory.
3. Specifický znak $\in$.
4. Závorky (a).

6.2. Poznámka. (a) Abecedu definovanou v definici 6.1 nazýváme *základní abecedou teorie tříd*. Později bude vhodné tuto abecedu rozšířit o další znaky.

(b) Definice 6.1 je v naprosté shodě s definicí 4.1.

(c) Objekty naší teorie, označované znaky A, B, C, ..., X, Y, Z a podobně nazýváme *třídy*.

(d) Specifický symbol $\in$ čteme slovy „je prvkem“.

(e) K označování slov v naší abecedě budeme užívat opět metaznaků φ, ψ atd. Z praktických důvodů přitom uzavřeme následující dohodu: když některé slovo naší abecedy označíme metaznakem

$$\varphi(X_1, \ldots, X_n)\,,$$

rozumíme tím skutečnost, že $X_1, \ldots, X_n$ jsou právě všechny podstatně volné proměnné v tomto slově.

Jak jsme již uvedli v §5, lze teorii množin i teorii tříd vybudovat na základě jediného primitivního predikátu. Uvědomme si, že následující definice je ve shodě s dohodou 4.7:

6.3. Definice. *Primitivním predikátem teorie tříd* nazýváme slovo $X \in Y$ a každé slovo, které z něho vznikne substitucí proměnných za proměnné.

6.4. Poznámka. Uvádět definici *formule* v teorii tříd není nutné, neboť to bychom jen opsali definici 4.8. Beze změny lze nyní na teorii tříd aplikovat všechny další pojmy z §4, jako například uzavřená formule, tautologie, slučitelné formule, dokazatelná formule atd. V příkladech v §4 jsme si všechny tyto pojmy na formulích teorie tříd demonstrovali.

Víme již, že pomocí predikátového kalkulu je dokazatelných nekonečně mnoho formulí v teorii tříd. Chceme-li však obdržet výsledky specifické pro teorii tříd, musíme za axiómy prohlásit některé uzavřené formule.

Za první axióm, zvaný *existenční*, zvolíme formuli, která nám zaručí, že se alespoň jednou realizuje vztah, který označujeme symbolem $\in$.

Axióm 1 $(\exists X)(\exists Y)(X \in Y)$

Význam axiómu 1 bude zvláště patrný po vyslovení následující definice:

6.5. Definice. Řekneme, že třída X je *množina*, jestliže existuje třída Y tak, že $X \in Y$.

6.6. Poznámka. Z axiómu 1 plyne, že existuje alespoň jedna množina. Čtenář nyní může namítnout, že definici 6.5 nelze takto vyslovit ve formalizovaném jazyku. Striktně vzato by bylo nutno postupovat následovně: zaveďme nový metaznak $\mathcal{M}$ a dohodněme se, že symbolem $\mathcal{M}(X)$ budeme označovat slovo $(\exists Y)(X \in Y)$, tj.

$$\mathcal{M}(X) \sim (\exists Y)(X \in Y).$$

(Vzhledem k pravidlu 4.23 nám přitom ve slově $\mathcal{M}(X)$ nezáleží na označení vázané proměnné.) Slovo $\mathcal{M}(X)$ pak čteme: *X je množina*.

Metaznak $\mathcal{M}$ nám sice umožňuje stručné vyjádření toho, že daná třída je množinou, přesto si však toto vyjádření ještě zjednodušíme následující dohodou:

6.7. Dohoda o rozšíření základní abecedy. Základní abecedu definovanou v 6.1 doplníme o malá písmena latinské abecedy (event. s indexy), kterými budeme rovněž označovat třídy. Budeme však striktně dodržovat pravidlo, že *malým písmenem označíme jen ty třídy, které jsou množinami*.

6.8. Poznámka. (a) Znak „x“ tedy čteme „množina x“, znak „X“ čteme „třída X“. Může se ovšem stát, že třída X je současně množinou. Podle dohody 6.7 je tak *možno množiny označit malými i velkými písmeny, třídu, která není množinou, však malým písmenem označit nesmíme.*

(b) Stejného faktu by bylo možno ovšem dosáhnout i bez doplnění základní abecedy. Malá písmena bychom mohli považovat za metaznaky a slovo „x“ považovat za jiný zápis formule „$\mathcal{M}(X)$“.

V dalším textu budeme běžně postupovat způsobem uvedeným v poznámce 6.6. Nové pojmy budeme běžně zavádět tak, že je popíšeme nějakou formulí v naší abecedě. K jednoduchému popisu těchto situací zavedeme metaznak :=, který značí, že na levé straně stojí symbol

nebo formule definovaný formulí (nebo slovem) na pravé straně. Na příklad definici množiny můžeme zapsat takto:

$$\mathcal{M}(X) := (\exists Y)(X \in Y)$$

popřípadě

$$x := (\exists Y)(X \in Y).$$

Nyní již můžeme definovat *rovnost tříd*.

6.9. Definice. $X = Y := (\forall Z)(Z \in X \Leftrightarrow Z \in Y)$. Slovy: *dvě třídy se rovnají, když mají stejné prvky*.

Někdy se znak = považuje za znak základní abecedy a slovo $X = Y$ se považuje za primitivní predikát. Aby však rovnost měla smysl, který jí intuitivně připisujeme, je nutné, aby měla následující tři vlastnosti, které nyní z axiómu 1 odvodíme. (Uvědomme si, ze kdybychom slovo $X = Y$ považovali za primitivní predikát, museli bychom následující formule prohlásit za axiómy.)

6.10. Věta. *Platí:*

(1) $(\forall X)(X = X)$

(2) $(\forall X)(\forall Y)\big[(X = Y) \Rightarrow (Y = X)\big]$

(3) $(\forall X)(\forall Y)(\forall Z)\Big\{\big[(X = Y) \wedge (Y = Z)\big] \Rightarrow (X = Z)\Big\}$.

Důkaz. (1) a (2) plyne bezprostředně z definice.

(3) Nechť $(X = Y) \wedge (Y = Z)$ a buď W libovolná třída. Podle definice 6.9 je

$$\big[(W \in X) \Leftrightarrow (W \in Y)\big] \wedge \big[(W \in Y) \Leftrightarrow (W \in Z)\big],$$

tj. $W \in X \Leftrightarrow W \in Z$, tj. $X = Z$. •

6.11. Poznámka. V každé teorii, v níž je zavedena rovnost, lze zavést nový kvantifikátor zpravidla označený symbolem „$\exists!$“, který čteme „*existuje právě jeden*“. Tento intuitivně zcela zřejmý pojem lze formalizovat následovně: Buď φ formule s volnou proměnnou X, v níž se nevyskytuje Y. Buď f substituce $[X \to Y]$. Pak klademe

$$(\exists! X)\varphi := (\exists X)\varphi \wedge (\forall X)(\forall Y)\Big[\big(\varphi \wedge f(\varphi)\big) \Rightarrow (X = Y)\Big]$$

(tato formule znamená: *existuje právě jedno X tak, že φ*).

Symbol $\exists!$ můžeme opět buďto považovat za metaznak nebo o tento symbol můžeme doplnit základní abecedu a odpovídajícím způsobem pak rozšířit definici formule.

Prozatím jsme uvedli jen jeden axióm. Nyní však již budeme nuceni zavést další. Promyslíme-li si totiž, co intuitivně rozumíme rovností dvou objektů, zjistíme, že kromě vlastností (1) – (3) z věty 6.10 musí být splněn požadavek, že dva sobě rovné objekty mají stejné vlastnosti, tj. v jakékoliv situaci lze jeden z nich nahradit druhým. Přesně řečeno, po rovnosti požadujeme, aby bylo splněno následující tvrzení:

6.12. Metavěta. *Buď $\varphi(X_1, \ldots, X_n)$ libovolná formule, v níž se nevyskytují proměnné $Y_1, \ldots, Y_n$. Pak je dokazatelná formule*

$$(\forall X_1)\ldots(\forall X_n)(\forall Y_1)\ldots(\forall Y_n)\Big\{\big[(X_1 = Y_1) \wedge (X_1 = Y_2) \wedge \ldots$$

$$\ldots \wedge (X_n = Y_n) \wedge \varphi(X_1, \ldots, X_n)\big] \Rightarrow \varphi(Y_1, \ldots, Y_n)\Big\}.$$

Prozatím nemůžeme tuto metavětu demonstrovat v teorii tříd. To nám umožní až zavedení tzv. *axiómu invariance*:

Axióm 2. $(\forall X)(\forall Y)(\forall Z)\Big\{\big[(X = Y) \wedge (X \in Z)\big] \Rightarrow (Y \in Z)\Big\}$

6.13. Věta.

$$(\forall X)(\forall Y)(\forall Z)(\forall W)\Big\{\big[(X = Y) \wedge (Z = W) \wedge (X \in Z)\big] \Rightarrow (Y \in W)\Big\}.$$

Důkaz. Tvrzení plyne bezprostředně z definice 6.9 a z axiómu 2. •

6.14. Poznámka. Je zřejmé, že 6.13 je zvláštním případem metavěty 6.12. Stačí totiž do věty 6.13 za formuli $\varphi(X_1, \ldots, X_n)$ dosadit formuli $X \in Y$.

Následující schéma axiómů (tj. obecný návod, které uzavřené formule je nutno považovat za axiómy) činí teorii tříd tak nadmíru v matematice užitečnou. Postuluje nám totiž existenci třídy, jejímiž prvky jsou právě všechny množiny s nějakou předem zvolenou vlastností.
Schéma axiómů 3. Buď $\varphi(x, X_1, \ldots, X_n)$ libovolná formule, v níž se nevyskytuje znak Y. Pak je formule

$$(\forall X_1)(\forall X_2)\ldots(\forall X_n)(\exists Y)(\forall x)\big[(x \in Y) \Leftrightarrow \varphi(x, X_1, \ldots, X_n)\big]$$

axióm.

Uvedené schéma axiómů nám umožňuje uvést následující definici:

6.15. Definice. Buď $\varphi(x, X_1, \ldots, X_n)$ libovolná formule, v níž se nevyskytuje Y. Pak klademe

$$Y = \{x; \varphi(x, X_1, \ldots, X_n)\} := [x \in Y \Leftrightarrow \varphi(x, X_1, \ldots, X_n)].$$

(Slovně: $\{x; \varphi(x, X_1, \ldots, X_n)\}$ je třída všech množin x, pro které platí

$$\varphi(x, X_1, \ldots, X_n)\,,$$

což souhlasí s běžně užívaným označením).

6.16. Definice. Označme

$$V = \{x; x = x\}, \quad \emptyset = \{x; x \neq x\}.$$

Konstantu V nazýváme *univerzální třída*, konstantu $\emptyset$ nazýváme *prázdná třída*.

6.17. Poznámka. Symbol $\neq$ definujeme (zcela obvykle) takto:

$$X \neq Y := \neg(X = Y).$$

Analogicky

$$X \notin Y := \neg(X \in Y).$$

6.18. Věta.

(1) $(\forall X)[(X \in V) \Leftrightarrow \mathcal{M}(X)]$

(2) $(\forall x)(x \notin \emptyset)$.

Důkaz. (1) (a) $\neg\mathcal{M}(X) \Rightarrow \neg[(\exists Y)(X \in Y)] \Rightarrow X \notin V$

(b) Podle věty 6.10 je $(\forall x)(x = x)$, tj. $x \in V$.

(2) $(\forall x)\neg(x \neq x) \Rightarrow x \notin \emptyset$. •

Podle věty 6.18 je univerzální třída V právě *třídou všech množin*.

6.19. Definice.

$X \cup Y := \{x; x \in X \vee x \in Y\}$
$X \cap Y := \{x; x \in X \wedge x \in Y\}$
$X - Y := \{x; x \in X \wedge x \notin Y\}$
$X' := \{x; x \notin X\}$
$X \subseteq Y := (\forall Z)[(Z \in X) \Rightarrow (Z \in Y)]$
$X \subset Y := (X \subseteq Y) \wedge (X \neq Y)$
$\mathcal{P}(X) := \{x; x \subseteq X\}$.

6.20. Poznámka. Na základě schématu axiómů 3 je definice 6.19 korektní. Důkaz obvyklých vlastností operací $\cup, \cap, -$ je jednoduchým cvičením.

Třída $\mathcal{P}(X)$ se nazývá *potenční třída třídy* X. Pozor na to, že prvky $\mathcal{P}(X)$ jsou *množiny*! Axiomatika nám nedovoluje definovat objekt $\{X; X \subseteq Y\}$!!

6.21. Poznámka. Definovali jsme tedy pro třídy operace sjednocení, průniku a rozdílu. Zřejmě lze bez obtíží definovat i symetrickou diferenci. Pro tyto operace evidentně platí všechna běžná tvrzení. Nejasná zůstává pouze následující otázka. *Jsou-li* X*,*Y *množiny, je i* $X \cup Y$ (a analogicky $X \cap Y$, $X - Y$, $\mathcal{P}(X)$) *množina*? Intuitivně se zdá samozřejmé, že odpověď na tuto otázku je *kladná*. Vcelku bez potíží však lze ukázat, že tomu tak *není*; přesněji řečeno, *bez dodatečných axiómů nelze dokázat, že sjednocení dvou množin je množina* a podobně pro další operace. Proto jsou v **GB** teorii axiómy následujícího typu:

Axióm 4. $(\forall x)(\forall y)(\exists Z)(x \cup y \in Z)$

Pomocí metaznaku $\mathcal{M}$ lze tento axióm stručně napsat takto:

$$\mathcal{M}(x \cup y).$$

Analogický smysl mají axiómy
Axióm 5. $\mathcal{M}(x \cap y)$

Axióm 6. $\mathcal{M}(x - y)$

Axióm 7. $\mathcal{M}(\mathcal{P}(x))$

Axióm 8. $\mathcal{M}(\emptyset)$

Schéma axiómů 3 nám umožňuje vyslovit i následující definici:

6.22. Definice.
$\{x\} := \{t; t = x\}$
$\{x, y\} := \{t; t = x \vee t = y\}$.
Třída $\{x\}$ se nazývá *jednoprvková třída*, třída $\{x, y\}$ se nazývá *neuspořádaná dvojice* (nebo stručněji *dvojice*) prvků x, y.

Z analogických důvodů jako u axiómů 4 – 8 je nutno přijmout následující axióm:

Axióm 9. $\mathcal{M}(\{x, y\})$

6.23. Lemma. $(\forall x)\mathcal{M}(\{x\})$.

Důkaz. Tvrzení plyne z axiómu 9 a ze vztahu $\{x, x\} = \{x\}$. •

Řada předcházejících axiómů nám umožňuje prohlásit některé třídy za množiny. Je tedy přirozená otázka, zda nelze přijmout axióm, který by nám zaručoval, že *každá třída je množinou*, tj. axióm

$$(\forall X)(\exists Y)(X \in Y).$$

Z následující věty plyne, *že přijetím tohoto axiómu bychom obdrželi spornou teorii*.

6.24. Věta. *Existuje třída, která není množinou.*

Důkaz. Podle axiómu 3 lze definovat třídu

$$B = \{x; x \notin x\}.$$

Připusťme, že B je množina. Pak je buďto $B \in B$ nebo $B \notin B$. Nechť tedy $B \in B$. Podle definice třídy B to však znamená, že $B \notin B$: spor. Musí tedy platit $B \notin B$. Protože však je B množina, plyne odtud $B \in B$: spor. Výchozí předpoklad, tj. předpoklad, že B je množina, je tedy nesprávný. •

Má tedy smysl následující definice:

6.25. Definice. Třída, která není množinou, se nazývá *vlastní*.

6.26. Poznámka. (a) Lze ukázat, že vlastní třídou je například také univerzální třída V. Diference tříd a množin je tedy v **GB** teorii podstatná.

(b) Čtenář si při důkazu věty 6.24 jistě uvědomil, že vlastně opakujeme *Russellův paradox* z §1. Z tohoto důkazu tedy plyne, že *v* **GB** *teorii nelze Russellův paradox vůbec zformulovat*, neboť množina, která nám tento paradox v intuitivní teorii množin realizovala, je v **GB** teorii vlastní třídou. Zcela analogicky je tomu v axiomatických teoriích množin s ostatními paradoxy intuitivní teorie množin.

(c) Víme již, že bychom dostali spornou teorii, kdybychom připustili, že V je množina (tj. že existuje „množina všech množin“). Nyní je ovšem otázkou, zda nelze analogické antinomie v teorii tříd obdržet, kdybychom uvažovali objekt „třída všech tříd“ a podobně. Uvědomme si však, že takový objekt v naší *teorii vůbec neexistuje*. Ve schématu axiómů 3 je podstatné, že x je *množinová proměnná*. Kdybychom tento axióm „zobecnili“ tak, že bychom znak „x“ nahradili znakem „X“, dostali bychom spornou teorii !!

★ ★ ★

Na tomto místě můžeme demonstraci axiomatické výstavby teorie množin ukončit. Podstata axiomatické teorie je snad nyní jasná. Budeme-li v následujících kapitolách budovat teorii

množin neformálně, dovede si již čtenář jistě zrekonstruovat, jak by se tato teorie formálně precizovala.

Nebudeme-li v dalším ani například důkazy provádět přesně tak, jak jsme je formalizovali v této kapitole (ostatně takto to probíhá téměř ve všech partiích matematiky), neznamená to, že formalizace v této kapitole popisovaná je zbytečná. Podstatné je to, že úvahy, které v dalším budeme provádět, formalizovat **lze** a že **víme, jakým způsobem**.

Cvičení ke kapitole 1

Jestliže pokus vyjde,
stala se někde chyba.
PRVNÍ FINAGLŮV ZÁKON

1. Určete všechna podslova slov „383 + 4081“, „3333“, „1056 − 1056“.

2. Dokažte, že pro každou substituci f platí $f(\omega) \sim \omega$.

3. Dokažte, že když f je nějaká substituce slov za znaky a α je libovolné slovo, stačí k určení slova $f(\alpha)$ znát, jak se transformují znaky, které se ve slově α vyskytují.

4. Buď dána abeceda jako v příkladu 2.6. Najděte nějakou substituci f slov za znaky takovou, že v žádném slovu $f(\alpha)$ se nevyskytují znaky „1“, „2“ a „3“.

5. Dokažte, že následující výrokové formule jsou tautologie:

a) $\big[(P \Rightarrow Q) \wedge \neg Q\big] \Rightarrow \neg P$

b) $(P \wedge Q \Rightarrow R) \Leftrightarrow \big[P \Rightarrow (Q \Rightarrow R)\big]$

c) $\big[P \Rightarrow (Q \Rightarrow R)\big] \Rightarrow \big[(P \Rightarrow Q) \Rightarrow (P \Rightarrow R)\big]$

d) $\big[(P \Rightarrow Q) \wedge P\big] \Rightarrow Q$

e) $\big[(P \vee Q) \wedge \neg P\big] \Rightarrow Q$

f) $\big[(P \Rightarrow Q) \wedge (R \Rightarrow S)\big] \Rightarrow \big[(P \wedge S) \Rightarrow (Q \vee R)\big]$ (Návod: Určete, kdy $p(Q \vee \vee R) \sim 0$, $p(P \wedge S) \sim 1$. Pravdivost implikace pak bude zřejmá.)

6. Dokažte, že následující výrokové formule jsou tautologie:

a) $\big[(P \vee Q) \Rightarrow (P \vee \neg Q)\big] \Rightarrow (\neg P \vee Q)$ (Návod: Vyšetřete případ $p(P) \sim 1$, $p(Q) \sim 0$.)

b) $\Big\{\big[(P \wedge Q) \Rightarrow R\big] \wedge \big[(P \wedge Q) \Rightarrow \neg R\big]\Big\} \Rightarrow (\neg P \wedge \neg Q \wedge \neg R)$
(Návod: Vyšetřete případ $p(P) \sim p(Q) \sim 0$, $p(R) \sim 1$. Uvědomte si, že lze přitom volit pravdivostní hodnoty tak, že $p(P \wedge Q) \sim 0$, $p(R) \sim 1$.)

7. Vyjádřete formule ze cvičení 6 pomocí spojek $\neg$, $\vee$, respektive $\neg$, $\Rightarrow$, respektive $\neg$, $\wedge$.

8. K formulím $A \Rightarrow B$, $A \wedge B$, $(A \Rightarrow B) \vee C$, $(A \Leftrightarrow B) \vee \big[C \wedge (A \Rightarrow B)\big]$ najděte logicky ekvivalentní formule, v nichž se vyskytují pouze logické spojky $|$, respektive $\downarrow$.

Kapitola 2

Základní množinové pojmy

1 Základní operace na systémech množin

Právě o těch nejjednodušších věcech
nevíme vůbec nic.
DE NEVERSŮV ZÁKON SLOŽITOSTI

1.1. Definice. Buď $I \neq \emptyset$ libovolná (tzv. *indexová*) množina. Buď A_i množina pro každé $i \in I$. *Sjednocením* množin A_i, $i \in I$, nazýváme množinu

$$\bigcup_{i \in I} A_i := \{x; \exists i_0 \in I \text{ takové, že } x \in A_{i_0}\}.$$

Průnikem množin a_i, $i \in I$, nazýváme množinu

$$\bigcap_{i \in I} A_i := \{x; \forall i \in I \text{ platí } x \in A_i\}.$$

Je-li $\bigcap_{i \in I} A_i = \emptyset$, říkáme, že systém A_i, $i \in I$, je *disjunktní*. Platí-li pro každé i, $j \in I$, $i \neq j$, $A_i \cap A_j = \emptyset$, říkáme, že množiny A_i, $i \in I$, jsou *po dvo disjunktní*

Nyní ukážeme, že sjednocení a průniky libovolných systémů množin mají zcela analogické vlastnosti jako odpovídající operace s konečně mnoha množinami. Následující tvrzení jsou zřejmá.

1.2. Věta. *Buďte $I \neq \emptyset$, M libovolné množiny, A_i, B_i buďte množiny pro každé $i \in I$. Pak platí:*

(a) $\bigcap_{i\in I} A_i \subseteq A_i \subseteq \bigcup_{i\in I} A_i$ *pro každé* $i \in I$;

(b) $\bigcap_{i\in I}(A_i \cap B_i) = \bigcap_{i\in I} A_i \cap \bigcap_{i\in I} B_i$;

(c) $\bigcup_{i\in I}(A_i \cup B_i) = \bigcup_{i\in I} A_i \cup \bigcup_{i\in I} B_i$;

(d) $\bigcap_{i\in I} A_i \cup \bigcap_{i\in I} B_i = \bigcap_{i,j}(A_i \cup B_j) \subseteq \bigcap_{i\in I}(A_i \cup B_i)$;

(e) $\bigcup_{i\in I} A_i \cap \bigcup_{i\in I} B_i = \bigcup_{i,j}(A_i \cap B_j) \supseteq \bigcup_{i\in I}(A_i \cap B_i)$;

(f) $\bigcap_{i\in I}(M \cup A_i) = M \cup \bigcap_{i\in I} A_i$;

(g) $\bigcup_{i\in I}(M \cap A_i) = M \cap \bigcup_{i\in I} A_i$;

(h) $M \subseteq A_i$ *pro každé* $i \in I \Rightarrow M \subseteq \bigcap_{i\in I} A_i$;

(i) $A_i \subseteq M$ *pro každé* $i \in I \Rightarrow \bigcup_{i\in I} A_i \subseteq M$.

Distributivní zákony (f), (g) ve větě 1.2 lze zobecnit následujícím způsobem.

1.3. Věta. *Buď* $I \neq \emptyset$ *libovolná množina, buď* $T_i \neq \emptyset$ *množina pro každé* $i \in I$. *Položme*

$$M = \bigcup_{i\in I} T_i, \quad K = \{X;\ X \subseteq M \text{ a pro každé } i \in I \text{ platí} X \cap T_i \neq \emptyset\}.$$

Buď konečně A_i *množina pro každé* $t \in T_i$, $i \in I$. *Pak platí:*

(1) $\bigcap_{i\in I}\bigcup_{t\in T_i} A_t = \bigcup_{X\in K}\bigcap_{t\in X} A_t$;

(2) $\bigcup_{i\in I}\bigcap_{t\in T_i} A_t = \bigcap_{X\in K}\bigcup_{t\in X} A_t$.

Důkaz. Dokážeme například tvrzení (2). Důkaz vztahu (1) je zcela analogický.

I. Buď $x \in \bigcup_{i\in I}\bigcap_{t\in T_i} A_t$ libovolný prvek. Pak existuje $i_0 \in I$ tak, že $x \in \bigcap_{t\in T_{i_0}} A_t$, tj. $x \in A_t$ pro každé $t \in T_{i_0}$. Buď $X \in K$ libovolná množina. Podle definice množiny K je $X \cap T_{i_0} \neq \emptyset$, tj. existuje $t_0 \in X \cap T_{i_0}$. Podle předpokladu platí $x \in A_{t_0}$ a tedy tím spíše $x \in \bigcup_{t\in X} A_t$. Protože poslední vztah nastává pro každou množinu $X \in K$, plyne odtud $x \in \bigcap_{X\in K}\bigcup_{t\in X} A_t$. Dokázali jsme tak, že $\bigcup_{i\in I}\bigcap_{t\in T_i} A_t \subseteq \bigcap_{X\in K}\bigcup_{t\in X} A_t$.

II. Nyní zvolme libovolně $x \in \bigcap_{X\in K} \bigcup_{t\in X} A_t$. Pak pro každou množinu $X \in K$ platí $x \in \bigcup_{t\in X} A_t$, takže v každé množině $X \in K$ existuje $t \in X$ tak, že $x \in A_t$. Položme $Y \in \{t; t \in M, x \notin A_t\}$. Pak zřejmě $Y \notin K$, takže existuje $i_0 \in I$ tak, že $Y \cap T_{i_0} = \emptyset$. To však znamená, že pro každé $t \in T_{i_0}$ platí $x \in A_t$, tj. $x \in \bigcap_{t\in T_{i_0}} A_t$ a tím spíše $x \in \bigcup_{i\in I} \bigcap_{t\in T_i} A_t$. Dokázali jsme tak i opačnou inkluzi $\bigcap_{X\in K} \bigcup_{t\in X} A_t \subseteq \bigcup_{i\in I} \bigcap_{t\in T_i} A_t$. •

Formulace zobecněného komutativního i zobecněného asociativního zákona je podstatně jednodušší. Důkazy jsou snadné a proto je přenecháme čtenáři.

1.4. Věta. (Zobecněný komutativní zákon) *Buď $I \neq \emptyset$ libovolná množina, A_i buď množina pro každé $i \in I$. Buď $f: I \to I$ bijekce. Pak platí:*

$$\bigcup_{i\in I} A_i = \bigcup_{i\in I} A_{f(i)}, \qquad \bigcap_{i\in I} A_i = \bigcap_{i\in I} A_{f(i)}.$$

1.5. Věta. (Zobecněný asociativní zákon) *Buď $I \neq \emptyset$ libovolná množina, buď $\{J_k; k \in K\}$ rozklad na množině I. Buď A_i množina pro každé $i \in I$. Pak platí:*

$$\bigcup_{i\in I} A_i = \bigcup_{k\in K} \bigcup_{i\in J_k} A_i, \qquad \bigcap_{i\in I} A_i = \bigcap_{k\in K} \bigcap_{i\in J_k} A_i.$$

Pro systémy množin lze snadno uvést i de Morganova pravidla.

1.6. Věta. (De Morganova pravidla) *Buď A libovolná množina, buď B_i množina pro každé $i \in I$, kde $I \neq \emptyset$. Pak platí:*

(a) $A - \bigcup_{i\in I} B_i = \bigcap_{i\in I} (A - B_i)$;

(b) $A - \bigcap_{i\in I} B_i = \bigcup_{i\in I} (A - B_i)$.

Důkaz. Důkazy obou tvrzení jsou zcela analogické. Dokážeme proto jen tvrzení (a):
$x \in A - \bigcup_{i\in I} B_i \Leftrightarrow \left[x \in A \wedge x \notin \bigcup_{i\in I} B_i\right] \Leftrightarrow \left[x \in A \wedge \text{pro každé } i \in I \text{ je } x \notin B_i\right] \Leftrightarrow \forall i \in \in I: x \in A - B_i \Leftrightarrow x \in \bigcap_{i\in I} (A - B_i)$. •

Ponecháme čtenáři, aby si promyslel, jak právě uvedená de Morganova pravidla souvisejí s pravidly (12) a (13) ve větě 3.15.

Nyní zobecníme pojem kartézského součinu konečného počtu množin.

1.7. Definice. Buď $I \neq \emptyset$ libovolná množina, A_i buď množina pro každé $i \in I$. *Kartézským součinem* množin A_i, $i \in I$, nazýváme množinu

$$\bigotimes_{i\in I} A_i := \{f;\ \ f: I \to \bigcup_{i\in I} A_i,\ \ f(i) \in A_i \quad \text{pro každé} \quad i \in I\}.$$

1.8. Poznámka. (a) Je-li v definici 1.7 I množina všech přirozených čísel, píšeme místo $\bigotimes_{i\in\mathbb{N}} A_i$ symbol $\bigotimes_{i=1}^{\infty} A_i$. Podle definice je tento kartézský součin množina všech *posloupností* $(a_i)_{i=1}^{\infty}$ takových, že $a_i \in A_i$ pro každé $i \in I$.

(b) Nechť $I = \{1, 2\}$. Kartézské součiny $\bigotimes_{i\in I} A_i$ a $A_1 \times A_2$ nejsou formálně totožné, neboť prvky součinu $\bigotimes_{i\in I} A_i$ jsou některá zobrazení množiny I do množiny $A_1 \cup A_2$, prvky $A_1 \times A_2$ jsou všechny uspořádané dvojice $[x, y]$ takové, že $x \in A_1$, $y \in A_2$. Je však zřejmé, že když každému prvku $[x, y] \in A_1 \times A_2$ přiřadíme to zobrazení $f \in \bigotimes_{i\in I} A_i$, pro které platí $f(1) = x$, $f(2) = y$, dostáváme bijekci mezi oběma kartézskými součiny. Rozdíl mezi těmito formálními zápisy kartézského součinu není tedy podstatný a budeme jej nadále zanedbávat.

(c) Nechť jsou si v definici 1.7 všechny množiny A_i navzájem rovny, tj. $A_i = A$ pro každé $i \in I$. Z definice pak plyne, že $\bigotimes_{i\in I} A_i = \bigotimes_{i\in I} A$ je množina všech zobrazení množiny I do množiny A, tj. množina, kterou značíme A^I.

Z definice kartézského součinu je zřejmé, že platí:

1.9. Věta. *Buď $I \neq \emptyset$, A_i buď množina pro každé $i \in I$. Pak je $\bigotimes_{i\in I} A_i = \emptyset$ právě tehdy, když $A_i = \emptyset$ pro některé $i \in I$.*

Důkaz. Vzhledem k tomu, že je důkaz jednoduchý, přenecháme jej čtenáři. Poznamenejme pouze, že k důkazu tvrzení, že z neprázdnosti množin A_i plyne neprázdnost kartézského součinu, je nutno užít axiómu výběru (viz §4). •

1.10. Věta. (Distributivní zákon) *Buď $A \neq \emptyset$ množina, $B_\alpha \neq \emptyset$ buď množina pro každé $\alpha \in A$. Pro každé $\alpha \in A$, $\beta \in B_\alpha$ buď $C_{\alpha\beta}$ množina. Pak platí*

$$\bigotimes_{\alpha\in A} \bigcup_{\beta\in B_\alpha} C_{\alpha\beta} = \bigcup_{\gamma\in\Gamma} \bigotimes_{\alpha\in A} C_{\alpha\gamma(\alpha)},$$

kde $\Gamma = \bigotimes_{\alpha\in A} B_\alpha$.

Důkaz. $\varphi \in \bigotimes_{\alpha\in A} \bigcup_{\beta\in B_\alpha} C_{\alpha\beta} \iff \big[\varphi\colon A \to \bigcup_{\alpha\in A}\bigcup_{\beta\in B_\alpha} C_{\alpha\beta}$ a pro každé $\alpha \in A$ platí $\varphi(\alpha) \in \in \bigcup_{\beta\in B_\alpha} A_{\alpha\beta}\big] \iff \big[\forall\alpha \in A\colon\ \exists\beta \in B_\alpha$ tak, že $\varphi(a) \in C_{\alpha\beta}\big] \iff \big[\forall\alpha \in A\colon \varphi(\alpha) \in C_{\alpha\gamma(\alpha)}$, kde $\gamma \in \Gamma = \bigotimes_{\alpha\in A} B_\alpha$ je to zobrazení A do $\bigcup_{\alpha\in A} B_\alpha$, pro které $\gamma(\alpha) = \beta$ je některý prvek, pro který $\varphi(\alpha) \in C_{\alpha\beta}\big] \iff \exists\gamma \in \Gamma$ takové, že $\varphi \in \bigotimes_{\alpha\in A} C_{\alpha\gamma(\alpha)} \iff \varphi \in \bigcup_{\gamma\in\Gamma} \bigotimes_{\alpha\in A} C_{\alpha\gamma(\alpha)}$. •

Cvičení k §1

Nevěř na zázraky —
spoléhej na ně.
ŠESTÁ FINAGLOVA ZÁSADA

1. Buďte X, Y, T množiny, $F{:}T \to \mathcal{P}(X)$, $f{:}X \to Y$. Dokažte, že platí:

a) $f\left(\bigcup_{t\in T} F(t)\right) = \bigcup_{t\in T} f\big[F(t)\big]$;

b) $f\left(\bigcap_{t\in T} F(t)\right) \subseteq \bigcap_{t\in T} f\big[F(t)\big]$.

2. Dokažte, že když je zobrazení f injektivní, lze ve cvičení 1(b) psát místo inkluze rovnost.

2 Dobře uspořádané množiny

Nikdy předem nezdůrazňujte,
že se chystáte říci něco významného.
ROSSŮV ZÁKON

Jak v dalším uvidíme, budou hrát dobře uspořádané množiny v dalším textu významnou roli.

2.1. Definice. Uspořádaná množina se nazývá *dobře uspořádaná*, když každá její neprázdná podmnožina obsahuje nejmenší prvek.

2.2. Věta. *Buď A dobře uspořádaná množina. Pak platí:*

(a) *A je řetězec;*

(b) *je-li $A \neq \emptyset$, obsahuje A nejmenší prvek;*

(c) *je-li $B \subseteq A$, je B (s indukovaným uspořádáním) dobře uspořádaná;*

(d) *je-li $B \cong A$, je B dobře uspořádaná;*

(e) *buď $x \in A$ libovolný prvek. Není-li x největší prvek v A, existuje v A prvek y, který pokrývá prvek x (tj. y je bezprostřední následovník prvku x).*

Důkaz.

(a) Buďte $x, y \in A$ libovolné. Podle definice obsahuje množina $\{x, y\}$ nejmenší prvek, takže prvky x, y jsou srovnatelné.

(b) Tvrzení plyne z definice 2.1.

(c) Buď $B \subseteq A$ libovolná. Je-li $\emptyset \neq X \subseteq B$ libovolná, je $X \subseteq A$ a podle definice X obsahuje nejmenší prvek. Je tedy B dobře uspořádaná.

(d) Tvrzení je zřejmé.

(e) Pro libovolný prvek $x \in A$ označme $E(x) = \{t; t \in A,\ t > x\}$. Není-li x největší prvek v A, je $E(x) \neq \emptyset$ (neboť podle (a) je A řetězec), takže $E(x)$ obsahuje nejmenší prvek t_0. Nyní je zřejmé, že prvek t_0 pokrývá prvek x.

•

2.3. Věta. *Řetězec A je dobře uspořádaný právě tehdy, když každý jeho klesající řetězec je konečný, tj. každá množina $\{x_1, x_2, \dots\} \subseteq A$ taková, že $x_1 > x_2 > \cdots > x_n > \dots$, je konečná.*

Důkaz. I. Nechť každý klesající řetězec v A je konečný. Ukážeme, že A je dobře uspořádaná.

Buď $\emptyset \neq B \subseteq A$ libovolná. Potřebujeme dokázat, že B obsahuje nejmenší prvek. Zvolme $x_1 \in B$ libovolně. Je-li x_1 nejmenší prvek B, je důkaz hotov. Není-li x_1 nejmenší, existuje $x_2 \in B$, $x_2 < x_1$, neboť A je řetězec. Není-li x_2 nejmenší v B, existuje $x_3 \in B$, $x_3 < x_2$ atd. Indukcí lze takto v B definovat klesající řetězec $x_1 > x_2 > x_3 > \dots$, který však podle předpokladu musí být konečný. Odtud již plyne, že B obsahuje nejmenší prvek.

II. Nechť v řetězci A existuje nekonečný klesající řetězec $x_1 > x_2 > \dots$. Pak množina $\emptyset \neq \{x_1, x_2, \dots x_n, \dots\} \subseteq A$ neobsahuje nejmenší prvek, takže A není dobře uspořádaná množina. •

Z věty 2.3 okamžitě plyne

2.4. Důsledek. *Každý konečný řetězec je dobře uspořádaný.*

2.5. Věta. *Buď A dobře uspořádaná množina, buď $B \subseteq A$ taková, že existuje izomorfismus $f\colon A \to B$. Pak pro každý prvek $x \in A$ platí $x \leq f(x)$.*

Důkaz. Označme $K = \{x; x \in A,\ f(x) < x\}$ a připusťme, že $K \neq \emptyset$. Pak K obsahuje nejmenší prvek x_0. Položme $x_1 = f(x_0)$. Protože je $x_0 \in K$, je $f(x_0) = x_1 < x_0$. Protože je f izomorfismus, je $f(x_1) < f(x_0) = x_1$, tj. $x_1 \in K$. To je však spor, neboť x_0 je nejmenší prvek množiny K. Je tedy $K = \emptyset$. •

2.6. Definice. Buď A libovolná uspořádaná množina. Množina $X \subseteq A$ se nazývá *začátek* množiny A, když pro každý prvek $t \in X$ platí

$$\{u;\ u \in A,\ u \leq t\} \subseteq X.$$

Začátek $X \subseteq A$ se nazývá *vlastní začátek* množiny A, je-li $X \neq A$.

2.7. Věta. *Dobře uspořádaná množina není izomorfní s žádným svým vlastním začátkem ani s jeho žádnou podmnožinou.*

Důkaz. Buď A dobře uspořádaná množina, B buď vlastní začátek v A. Pak je $B \subset A$, takže $A - B \neq \emptyset$. Množina $A - B$ obsahuje nejmenší prvek a_0. Je zřejmé, že a_0 je horní závora množiny B, $a_0 \notin B$. Připusťme, že existuje $X \subseteq B$ tak, že $A \cong X$. Buď $f\colon A \to X$ izomorfismus. Pak je $f(a_0) \in X \subseteq B$, tj. $f(a_0) < a_0$, což podle věty 2.5 není možné. •

2.8. Důsledek. *Buď A dobře uspořádaná množina, budte B, C začátky v A. Je-li $B \cong C$, pak je $B = C$.*

Důkaz. Je-li $B = A$, $B \cong C$, je $B = C$ podle věty 2.7. Buďte B, C vlastní začátky v A. Je-li $B \neq C$, je buďto B vlastní začátek v C nebo C vlastní začátek v B. Pak ale B, C nemohou být podle věty 2.7 izomorfní. •

2.9. Označení. Buď A uspořádaná množina, $x \in A$ buď libovolný. Klademe

$$A(x) = \{t;\ t \in A,\ t < x\}.$$

Je zřejmé, že pro každý prvek $x \in A$ je $A(x) \neq A$ a $A(x)$ je začátek v A. Dále je zřejmé, že platí:

2.10. Lemma. Buď A dobře uspořádaná množina, $B \subseteq A$ buď vlastní začátek v A. Pak existuje $x \in A$ tak, že $B = A(x)$.

2.11. Věta. *Buďte A, B dobře uspořádané množiny. Je-li $A \cong B$, existuje právě jeden izomorfismus $f\colon A \to B$.*

Důkaz. Buďte $f\colon A \to B$, $g\colon A \to B$ izomorfismy a připusťme, že $f \neq g$. Pak existuje $x_0 \in A$ tak, že $f(x_0) \neq g(x_0)$. Protože je f izomorfismus, je $A(x_0) \cong B\big(f(x_0)\big)$; protože je g izomorfismus, je $A(x_0) \cong B\big(g(x_0)\big)$, takže $B\big(f(x_0)\big) \cong B\big(g(x_0)\big)$. Podle důsledku 2.8 je pak ale $B\big(f(x_0)\big) = B\big(g(x_0)\big)$, tj. $f(x_0) = g(x_0)$: spor. •

2.12. Poznámka. Z předcházejícího je již zřejmé, že dobře uspořádané množiny jsou řetězce s jistými vlastnostmi. Podle důsledku 2.4 je každý **konečný** řetězec dobře uspořádaný, nekonečný řetězec je však dobře uspořádaný jen v některých případech. Například řetězec $\mathbb{N}$ všech přirozených čísel je dobře uspořádaný, ale řetězce $\mathbb{Z}$, $\mathbb{Q}$, respektive $\mathbb{R}$ dobře uspořádané nejsou.

Následující věta udává, že struktura dobře uspořádaných řetězců je dokonce v jistém slova smyslu jednoznačně předepsána.

2.13. Věta. *Budte A, B dobře uspořádané množiny. Pak nastane právě jedna z následujících možností:*

(1) $A \cong B$*;*

(2) $A \cong B(x)$ *pro vhodný prvek* $x \in B$*;*

(3) $B \cong A(x)$ *pro vhodný prvek* $x \in A$*.*

Důkaz. Buďte A, B dobře uspořádané množiny. Řekneme, že prvek $x \in A$ je *normální*, jestliže existuje prvek $y \in B$ takový, že $A(x) \cong B(y)$. Označme $G = \{x;\ x \in A,\ x \text{ je normální}\}$. Zcela analogicky definujeme množinu $H = \{x;\ x \in B,\ x \text{ je normální}\}$.

Je-li $A = \emptyset$ nebo $B = \emptyset$, je tvrzení věty triviální. Nechť tedy $A \neq \emptyset \neq B$. Pak je také $G \neq \emptyset \neq H$, neboť nejmenší prvek množiny A, respektive B je evidentně normální. Dále je zřejmé, že G je začátek v A a H je začátek v B. Podle lemmatu 2.10 to však znamená, že je $G = A$ nebo $G = A(a_0)$ pro vhodný prvek $a_0 \in A$ a analogicky $H = B$ nebo $H = B(b_0)$ pro vhodný prvek $b_0 \in B$.

Nyní dokážeme, že je $G \cong H$. Definujme zobrazení $f\colon G \to H$ takto: pro $x \in G$ buď $f(x) = y$ ten prvek v H, pro který platí $A(x) \cong B(y)$. Pak je zřejmě f izomorfismus G na H. Nyní mohou nastat čtyři možnosti.

(a) $G = A$, $H = B$. Pak je však $A \cong B$, takže platí (1).

(b) $G = A$, $H = B(b_0)$. Pak je $A \cong B(b_0)$, tj. platí (2).

(c) $G = A(a_0)$, $H = B$. Pak je $B \cong A(a_0)$, tj. platí (3).

(d) $G = A(a_0)$, $H = B(b_0)$.

Je však zřejmé, že poslední případ ve skutečnosti nastat nemůže. Ze vztahu $G \cong H$ totiž plyne $A(a_0) \cong B(b_0)$, takže $a_0 \in G$, $b_0 \in H$ a to není možné. •

2.14. Poznámka. Je-li A konečná množina, lze na ní jednoduše definovat uspořádání $\leq$ tak, aby $(A, \leq)$ byla dobře uspořádaná. Podle důsledku 2.4 stačí za relaci $\leq$ zvolit jakékoliv úplné uspořádání. Je tedy přirozená otázka, zda lze dobré uspořádání definovat na každé množině. Odpověď na tuto otázku dal Ernst ZERMELO (viz věta 4.7). Vzhledem k potížím spojeným s důkazem Zermelova tvrzení tento stav objasníme v §4.

V závěru tohoto paragrafu uveďme jednu z nejdůležitějších aplikací dobře uspořádaných množin, tak zvaný *princip transfinitní indukce*.

Ze střední školy známe důkazovou metodu nazývanou *úplná indukce* (nebo též *matematická indukce*). Touto metodou se nejčastěji dokazují vzorce, formule apod., které mají být pravdivé pro všechna přirozená čísla. Připomeňme si, že důkaz úplnou indukcí spočívá v tom, že důkaz výroku $(\forall n \in \mathbb{N})V(n)$ se provede ve dvou krocích:

(1) $V(1)$,
(2) $(\forall n \in \mathbb{N})\big(V(n) \Rightarrow V(n+1)\big)$.

Poněvadž množina $\mathbb{N}$ všech přirozených čísel je dobře uspořádaná, je zřejmé, že úplná indukce je speciálním případem následujícího tvrzení.

2.15. Věta. (Princip transfinitní indukce) *Buď W dobře uspořádaná množina s nejmenším prvkem x_0. Buď $P(x)$ výroková funkce o jedné proměnné s definičním oborem W. Nechť platí:*

(1) *$P(x_0)$ je pravdivý výrok;*

(2) *pro každý prvek $x \in W$ platí: je-li $P(t)$ pravdivý výrok pro každý prvek $t \in W$, $t < x$, je také $P(x)$ pravdivý výrok.*

Pak je $P(x)$ pravdivý výrok pro každý prvek $x \in W$.

Důkaz. Nechť jsou splněny předpoklady věty. Připusťme, že množina $W' = \{x;\ x \in W,\ P(x)$ je nepravdivý výrok$\}$ je neprázdná. Protože W je dobře uspořádaná, obsahuje W' nejmenší prvek y_0. Je $y_0 > x_0$, neboť $P(x_0)$ je pravdivý výrok. Pro každé $t \in W$, $t < y_0$, je $P(t)$ pravdivý výrok, takže podle předpokladu je také $P(y_0)$ pravdivý výrok: spor. Je tedy $W' = \emptyset$. •

2.16. Poznámka. V kapitole III uvidíme, že množina W při transfinitní indukci je obvykle nějaká množina tzv. ordinálních čísel. Uvědomme si také, že transfinitní indukci lze užít nejen k důkazům, ale i v definicích, respektive při popisu konstrukcí apod. Chceme-li totiž definovat objekt $f(\alpha)$ pro každé $\alpha \in W$ (W je dobře uspořádaná množina s nejmenším prvkem x_0), stačí podle věty 2.15 definovat objekt $f(x_0)$ a udat předpis, jak objekt $f(\alpha)$ definovat pomocí všech $\beta \in W$, $\beta < \alpha$.

3 Aritmetika uspořádaných množin

I ta nejjednodušší myšlenka
se dá vyjádřit složitě.
MALEKŮV ZÁKON

Nyní jednoduše zavedeme početní operace pro uspořádané množiny.

3.1. Definice. Buďte $(G, \leq_G)$, $(H, \leq_H)$ disjunktní uspořádané množiny. Jejich *součtem* $G + H$ nazýváme uspořádanou množinu $(G \cup H, \leq)$, na níž je uspořádání $\leq$ definováno takto: Pro $x, y \in G \cup H$ platí $x \leq y$ právě tehdy, když nastane jedna z možností:
(1) $x, y \in G$, $x \leq_G y$;
(2) $x, y \in H$, $x \leq_H y$;
(3) $x \in G$, $y \in H$.

Relaci $\leq$ definovanou v 3.1 můžeme vyjádřit takto:

$$\leq = \leq_G \cup \leq_H \cup (G \times H).$$

Je však třeba dokázat, že uvedená definice je správná, tj. že $G + H$ je vskutku uspořádaná množina.

3.2. Věta. *Relace $\leq$ definovaná v 3.1 je uspořádání na množině $G \cup H$.*

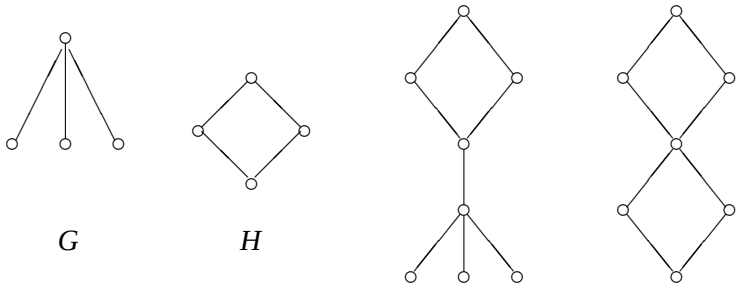
Důkaz. Musíme dokázat, že relace $\leq$ je reflexivní, antisymetrická a tranzitivní.

(a) **Reflexivita**: Buď $x \in G \cup H$ libovolný. Je-li $x \in G$, platí $x \leq_G x$, neboť $\leq_G$ je uspořádání na G a tedy je reflexivní. Podle definice relace $\leq$ však odtud plyne $x \leq x$. Podobně postupujeme v případě $x \in H$.

(b) **Antisymetrie**: Buďte $x, y \in G \cup H$ libovolné takové, že $x \leq y \wedge y \leq x$. Je-li $x \in G$, $y \in G$, platí $x \leq_G y \wedge y \leq_G x$. Protože je $\leq_G$ antisymetrická, plyne odtud $x = y$. Podobně obdržíme $x = y$ i v případě, že $x \in H$, $y \in H$. Přitom není možné, aby například $x \in G$, $y \in H$, neboť v tomto případě nemůže platit $y \leq x$ (vzhledem k předpokladu, že $G \cap H = \emptyset$). Tím je antisymetrie relace $\leq$ dokázána.

(c) **Tranzitivita**: Buďte $x, y, z \in G \cup H$ libovolné takové, že $x \leq y$ a $y \leq z$. Je-li $x, y, z \in G$, respektive $x, y, z \in H$, vyplývá platnost vztahu $x \leq z$ okamžitě z tranzitivity relace $\leq_G$, respektive $\leq_H$. Nechť tedy neleží všechny prvky x, y, z v G, respektive v H. Vzhledem ke (3) v definici 3.1 je okamžitě zřejmé, že nutně platí $x, y \in G$, $z \in H$ nebo $x \in G$, $y, z \in H$. V obou těchto případech však podle (3) platí $x \leq z$ a relace $\leq$ je tranzitivní. •

3.3. Příklad. Na obrázku 1 jsou hasseovské diagramy uspořádaných množin G, H a součtů $G + H$ a $H + G$.



Obr. 1

3.4. Poznámka. Z příkladu 3.3 je zřejmé, že operace + definovaná v 3.1 obecně **není komutativní**. Komutativní zákon neplatí ani v zeslabeném tvaru $G + H \cong H + G$. V dalším však ukážeme, že operace + je asociativní.

Definici 3.1 nyní zobecníme následujícím způsobem:

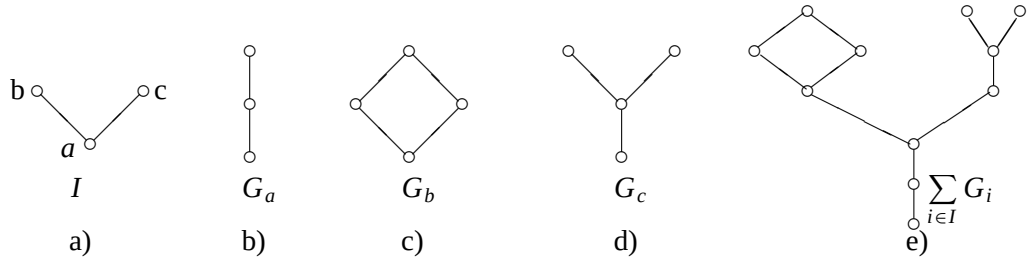
3.5. Definice. Buď $I \neq \emptyset$ uspořádaná množina, buď G_i uspořádaná množina pro každé $i \in I$. Nechť jsou množiny G_i, $i \in I$, po dvou disjunktní. *Součtem* $\sum_{i\in I} G_i$ množin G_i přes množinu I rozumíme uspořádanou množinu $(\bigcup_{i\in I} G_i, \leq)$ s uspořádáním $\leq$ definovaným takto: pro $x, y \in \bigcup_{i\in I} G_i$ platí $x \leq y$ právě tehdy, když nastane jedna z následujících možností:
(1) existuje $i_0 \in I$ tak, že $x \in G_{i_0}$, $y \in G_{i_0}$ a $x \leq y$ v G_{i_0};
(2) $x \in G_i$, $y \in G_j$ a $i < j$ v I.

Podobně jako ve větě 3.2 bychom nyní měli dokázat, že relace $\leq$ definovaná v 3.5 je uspořádání na množině $\bigcup_{i\in I} G_i$. Vzhledem k tomu, že důkaz věty 3.2 lze snadno přeformulovat i pro tento obecnější případ, přenecháme jeho provedení čtenáři.

3.6. Příklad.

(a) Součet definovaný v 3.1 je zřejmě speciálním případem definice 3.5; odpovídá případu, kdy I je dvouprvkový řetězec.

(b) Buď $I = \{a, b, c\}$ uspořádaná množina s hasseovským diagramem na obrázku 2a, G_a, G_b, G_c buďte uspořádané množiny s diagramy na obrázcích 2b, 2c, 2d. Na obrázku 2e je hasseovský diagram množiny $\sum_{i\in I} G_i$.



Obr. 2

3.7. Věta. *(*Asociativní zákon*) Buď $I \neq \emptyset$ uspořádaná množina, buďte G_i, $i \in I$, po dvou disjunktní uspořádané množiny. Nechť $I = \sum_{k\in K} J_k$. Pak platí:*

$$\sum_{i\in I} G_i = \sum_{k\in K} \sum_{i\in J_k} G_i .$$

Důkaz. Množinová rovnost obou stran dokazovaného vztahu plyne z věty 1.4. Dokážeme rovnost uspořádání.

Nechť tedy $x, y \in \sum_{i\in I} G_i$. Existuje-li $i_0 \in I$, tak, že $x \in G_{i_0}$, $y \in G_{i_0}$, je zřejmě $x \le y$ v $\sum_{i\in I} G_i$ právě tehdy, když $x \le y$ v $\sum_{k\in K}\sum_{i\in J_k} G_i$. Nechť tedy $x \in G_i$, $y \in G_j$, $i < j$ v I. Existuje-li $k_0 \in K$ tak, že $i, j \in J_{k_0}$, je tvrzení zřejmé. Nechť tedy $i \in J_k$, $j \in J_\ell$, $k < \ell$ v K. Pak je $x \le y$ v $\sum_{i\in I} G_i$ právě tehdy, když $i < j$. Avšak $i < j$ v I právě tehdy, když $k < \ell$ v K, tj. $x \le y$ v $\sum_{k\in K}\sum_{i\in J_k} G_i$. Tím je věta dokázána. •

Zvolíme-li ve větě 3.7 za I speciálně tříprvkový řetězec, plyne z ní

3.8. Důsledek. *Buďte A, B, C libovolné po dvou disjunktní uspořádané množiny. Pak platí:*

$$(A + B) + C = A + (B + C).$$

3.9. Definice. Buďte $(G, \le_G)$, $(H, \le_H)$ uspořádané množiny. Jejich *součinem* $G \cdot H$ rozumíme uspořádanou množinu $(G \times H, \le)$ s uspořádáním $\le$ definovaným takto:

$$[x_1, y_1] \le [x_2, y_2] \quad \text{v} \quad G \cdot H \iff \begin{array}{ll} (1) & y_1 <_H y_2 \quad \text{nebo} \\ (2) & y_1 = y_2,\ x_1 \le_G x_2. \end{array}$$

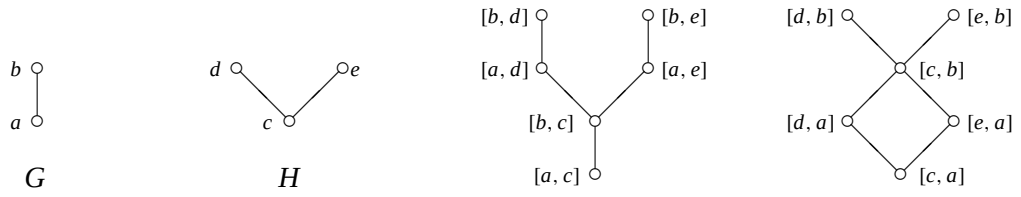
3.10. Věta. *Relace $\le$ definovaná v 3.9 je uspořádání na množině $G \times H$.*

Důkaz. (a) Reflexivita relace $\le$ je zřejmá z definice.

(b) Nechť $[x_1, y_1] \le [x_2, y_2]$ a současně $[x_2, y_2] \le [x_1, y_1]$. Vzhledem k antisymetrii relace $\le_H$ není možné, aby $y_1 \ne y_2$. Pro $y_1 = y_2$ však z antisymetrie relace $\le_G$ okamžitě plyne $x_1 = x_2$. To znamená, že i relace $\le$ je antisymetrická.

(c) Nechť $[x_1, y_1] \le [x_2, y_2]$ a $[x_2, y_2] \le [x_3, y_3]$. Je-li $y_1 < y_2 < y_3$, plyne vztah $[x_1, y_1] \le$ $\le [x_3, y_3]$ z tranzitivity relace $\le_H$. Je-li $y_1 = y_2 = y_3$, plyne uvedený vztah z tranzitivity relace $\le_G$. Je-li $y_1 = y_2$, $y_2 < y_3$, platí $y_1 < y_3$ a tedy $[x_1, y_1] \le [x_3, y_3]$. Podobně v případě $y_1 < y_2$, $y_2 = y_3$. Žádný další případ evidentně nastat nemůže, takže relace $\le$ je tranzitivní. •

3.11. Příklad. Na obrázku 3 jsou hasseovské diagramy uspořádaných množin G, H a jejich součinů $G \cdot H$ a $H \cdot G$.



G H $G \cdot H$ $H \cdot G$

a) b) c) d)

Obr. 3

3.12. Poznámka. Z příkladu 3.11 plyne, že ani násobení uspořádaných množin *není obecně komutativní*, a to ani v zeslabeném tvaru $G \cdot H \cong H \cdot G$. Podobně jako pro operaci + však i pro násobení platí asociativní zákon.

3.13. Věta. *Budťe G, H, K libovolné uspořádané množiny. Pak platí*

$$(G \cdot H) \cdot K = G \cdot (H \cdot K).$$

Důkaz. Množinová rovnost obou stran dokazovaného vztahu je zřejmá. Podle definice 3.9 platí $[x_1, y_1, z_1] \leq [x_2, y_2, z_2]$ v $(G \cdot H) \cdot K$ právě tehdy, když je $z_1 < z_2$ nebo $z_1 = z_2$, $[x_1, y_1] \leq [x_2, y_2]$. Avšak $[x_1, y_1] \leq [x_2, y_2]$ v $G \cdot H$ právě tehdy, když je $y_1 < y_2$ nebo $y_1 = y_2$, $x_1 \leq x_2$. Přesně tytéž vztahy však platí, jestliže je $[x_1, y_1, z_1] \leq [x_2, y_2, z_2]$ v $G \cdot (H \cdot K)$. Odtud plyne, že v obou množinách $(G \cdot H) \cdot K$ a $G \cdot (H \cdot K)$ je definováno stejné uspořádání. •

3.14. Věta. (Levý distributivní zákon). *Bud'$I \neq \emptyset$ uspořádaná množina, budťe G, H_i $(i \in I)$ uspořádané množiny. Necht'jsou množiny H_i po dvou disjunktní. Pak platí*

$$G \cdot \sum_{i \in I} H_i = \sum_{i \in I} G \cdot H_i.$$

Důkaz. Množinová rovnost obou stran dokazovaného vztahu je zřejmá. Dokážeme rovnost uspořádání v obou množinách.

Nechť tedy platí $[x_1, y_1] \leq [x_2, y_2]$ v $G \cdot \sum H_i$. Pak nastane jedna z následujících dvou možností:

(1) $y_1 < y_2$ v $\sum H_i$;

(2) $y_1 = y_2 \wedge x_1 \leq x_2$ v G.

Nechť nastane případ (1). Pak buď

(1a) existuje $i_0 \in I$ tak, že $y_1, y_2 \in H_{i_0}$ a $y_1 < y_2$ v H_{i_0}, nebo

(1b) $y_1 \in H_i$, $y_2 \in H_j$ a $i < j$ v I.

V obou případech (1a) i (1b) však dostáváme tvrzení ekvivalentní s tím, že $[x_1, y_1] < < [x_2, y_2]$ v $\sum G \cdot H_i$.

Nechť tedy nastane případ (2). Pak existuje $i_0 \in I$ tak, že $y_1, y_2 \in H_{i_0}$. Tvrzení $[x_1, y_1] \leq$ $\leq [x_2, y_2]$ v $G \cdot \sum H_i$ je však nyní ekvivalentní s tím, že $[x_1, y_1] \leq [x_2, y_2]$ v $G \cdot H_{i_0}$ a tedy i v $\sum G \cdot H_i$. Tím je věta dokázána. •

3.15. Důsledek. *Budte G, H, K, $H \cap K = \emptyset$, libovolné uspořádané množiny. Pak platí*

$$G \cdot (H + K) = G \cdot H + G \cdot K.$$

3.16. Poznámka. *Pravý distributivní zákon,* tj. tvrzení $(\sum H_i) \cdot G = \sum (H_i \cdot G)$ obecně neplatí. Položíme-li například $G = \{a\}$, $H = \{b\}$, pak $G + H$ je řetězec $\{a < b\}$. Zvolíme-li nyní $K = \{c, d, e\}$ tak, že hasseovský diagram uspořádané množiny $(K, \leq)$ je na obrázku 3b, je zřejmě na obrázku 3c diagram množiny $(G + H) \cdot K$ a na obrázku 3d diagram množiny $G \cdot K + H \cdot K$. Tyto dvě množiny však nejsou ani izomorfní.

3.17. Věta. *Buď $I \neq \emptyset$ uspořádaná množina, budte A_i $i \in I$, po dvou disjunktní uspořádané množiny. Necht' existuje množina A tak, že $A_i \cong A$ pro každé $i \in I$. Pak platí*

$$\sum_{i \in I} A_i \cong A \cdot I.$$

Důkaz. Nechť pro každé $i \in I$ je $g_i \colon A_i \to A$ izomorfismus. Definujme zobrazení $f \colon \bigcup_{i \in I} A_i \to$ $\to A \times I$ takto: buď $x \in \bigcup_{i \in I} A_i$ libovolný prvek. Pak $f(x) = \big[g_i(x), i\big]$, kde $i \in I$ je ten prvek, pro který platí $x \in A_i$. Pak je zřejmě f hledaný izomorfismus. •

3.18. Věta. *Buď $I \neq \emptyset$ dobře uspořádaná množina. Budte A_i, $i \in I$, po dvou disjunktní dobře uspořádané množiny. Pak je $\sum_{i \in I} A_i$ dobře uspořádaná množina.*

Důkaz. Buď $\emptyset \neq B \subseteq \sum_{i \in I} A_i$ libovolná. Označme $I_B = \{i;\ i \in I,\ B \cap A_i \neq \emptyset\}$. Pak je $\emptyset \neq I_B \subseteq I$, takže I_B obsahuje nejmenší prvek i_0. $B \cap A_{i_0}$ je nyní neprázdná podmnožina v A_{i_0}, takže $B \cap A_{i_0}$ obsahuje nejmenší prvek b. Je však zřejmé, že b je nejmenší prvek množiny B. •

3.19. Důsledek. *Budte A, B disjunktní dobře uspořádané množiny. Pak je $A + B$ dobře uspořádaná množina.*

Z věty 3.18 a důsledku 3.19 plyne

3.20. Věta. *Budte G, H dobře uspořádané množiny. Pak je také množina $G \cdot H$ dobře uspořádaná.*

3.21. Důsledek. *Budte G, H konečné řetězce. Necht' má řetězec G m prvků, a řetězec H necht' má n prvků. Pak je $G \cdot H$ řetězec obsahující $m \cdot n$ prvků.*

4 Axióm výběru a věty s ním ekvivalentní

Neodpovídají-li fakta vaší teorii,
je třeba se jich co nejrychleji zbavit.
MAIERŮV ZÁKON

V kapitole I jsme viděli, jak se postupuje při axiomatické výstavbě teorie množin a jak vypadají axiómy. V různých axiomatických teoriích jsou samozřejmě za axiómy volena odlišná tvrzení, vesměs jsou však axiómy vcelku jednoduchá tvrzení a proti jejich volbě nejsou vznášeny žádné principiální výhrady. Jedinou výjimkou je právě tak zvaný *axióm výběru*, někdy též nazývaný *Zermelův axióm*. V tomto paragrafu si ukážeme některé těžkosti s tímto axiómem spojené. Podrobněji budeme o axiómu výběru hovořit ještě v kapitole IV, §4.

Nejprve si však ukažme, jaké důvody vedly k formulaci tohoto axiómu.

4.1. Příklad. (a) Buďte A, B, C, D následující množiny: $A = \{a, b, c\}$, $B = \{a, f, g, h\}$, $C = \{c, d, e, f\}$, $D = \{a, f, k\}$.

Potřebujeme-li sestrojit množinu M takovou, že $M \subseteq A \cup B \cup C \cup D$ a průnik množiny M s každou z množin A, B, C, D je jednoprvkový, můžeme zvolit například $M = \{b, e, g, k\}$ nebo $M = \{a, e\}$ a podobně.

(b) Buď $I \neq \emptyset$ libovolná množina, buďte $A_i \neq \emptyset$, $i \in I$, po dvou disjunktní dobře uspořádané množiny. Pak můžeme bez potíží definovat množinu M s následujícími vlastnostmi:

(i) $M \subseteq \bigcup_{i \in I} A_i$,

(ii) pro každé $i \in I$ je $M \cap A_i$ jednoprvková množina.

Lze to udělat například tak, že množinu M utvoříme z nejmenších prvků všech množin A_i.

Množina M je v obou případech definována tak, že jsme z každé ze zadaných množin vybrali jeden prvek.

4.2. Příklad. Definujme na množině $\mathbb{R}$ všech reálných čísel relaci ϱ takto:

$$\varrho := \{[x, y];\ x \in \mathbb{R},\ y \in \mathbb{R},\ x - y \text{ je racionální číslo}\}.$$

Pak je zřejmě ϱ ekvivalence na $\mathbb{R}$. Utvoříme-li faktormnožinu $\mathbb{R}/\varrho$, je ihned vidět, že $\mathbb{R}/\varrho$ je nekonečná množina a každá třída rozkladu $\mathbb{R}/\varrho$ je rovněž nekonečná množina.

Chceme-li nyní sestrojit množinu M analogicky jako v příkladech 4.1, je ihned vidět, že **nelze** vůbec podat konstrukci této množiny. Chceme-li vůbec tvrdit, že existuje množina M taková, že

(i) $M \subseteq \mathbb{R}$,

(ii) pro každý prvek $x \in \mathbb{R}/\varrho$ je $M \cap X$ jednoprvková množina,

nelze toto tvrzení v běžných axiomatických systémech vůbec odvodit bez axiómu výběru.

Nyní tedy axióm výběru zformulujeme. Nebudeme uvádět jeho symbolický zápis, pouze budeme tento zápis slovy interpretovat.

Axióm výběru. *Buď $A \neq \emptyset$ libovolná množina, buď $\{M_\alpha, \alpha \in A\}$ systém neprázdných množin, které jsou po dvou disjunktní. Pak existuje množina M taková, že:*

1. $M \subseteq \bigcup_{\alpha \in A} M_\alpha$,
2. *$M \cap M_\alpha$ je jednoprvková množina pro každé $\alpha \in A$.*

Z axiómu výběru lze lehce odvodit následující tvrzení:

4.3. Věta. (Zobecněný axióm výběru) *Buď $\mathcal{M} = \{M_\alpha;\ \alpha \in A\}$ neprázdný systém neprázdných množin. Pak existuje zobrazení*

$$f\colon \mathcal{M} \to \bigcup_{\alpha \in A} M_\alpha$$

takové, že $f(M_\alpha) \in M_\alpha$ pro každé $\alpha \in A$.

Důkaz. Pro každou množinu $M_\alpha \in \mathcal{M}$ položme

$$M'_\alpha = \{[M_\alpha, m_\alpha];\ m_\alpha \in M_\alpha\},$$

tj. $M'_\alpha = \{M_\alpha\} \times M_\alpha$. Definujeme-li zobrazení $g\colon M'_\alpha \to M_\alpha$ takto:

$$g\big([M_\alpha, m_\alpha]\big) = m_\alpha \quad \text{pro každý prvek} \quad [M_\alpha, m_\alpha] \in M'_\alpha,$$

je zřejmě g bijekce. Označme $\mathcal{M}' = \{M'_\alpha;\ \alpha \in A\}$. Množiny ze systému $\mathcal{M}'$ jsou zřejmě neprázdné a po dvou disjunktní, takže lze na $\mathcal{M}'$ aplikovat axióm výběru. Z každé množiny M'_α lze tedy vybrat jeden prvek $[M_\alpha, m_\alpha]$. Definujeme-li nyní pro každé $M_\alpha \in \mathcal{M}$ prvek $f(M_\alpha)$ tak, že $f(M_\alpha) = m_\alpha$, je důkaz hotov. •

4.4. Poznámka. Stručně lze tedy axióm výběru zformulovat takto: *Buď $\mathcal{M}$ libovolný neprázdný systém neprázdných množin. Pak lze z každé množiny systému $\mathcal{M}$ vybrat jeden prvek.*

4.5. Poznámka. Axióm výběru je v „běžných“ axiomatických teoriích množin (například v **ZF** nebo v **GB**) nezávislým axiómem. Principiálně lze tedy vybudovat teorii množin i bez užití axiómu výběru. Je však vcelku zřejmé, že bychom se tak velmi rychle dostali do značných a mnohdy nepřekonatelných potíží. Již v důkazu věty 1.9 jsme uvedli, že teprve s užitím axiómu výběru můžeme tvrdit, že $\bigotimes_{i\in I} A_i \neq \emptyset$, pokud je $I \neq \emptyset$ a $A_i \neq \emptyset$ pro každé $i \in I$. Bez užití axiómu výběru nelze dokázat ani řadu jiných, stejně zdánlivě evidentních tvrzení (a to nejen v teorii množin, ale i například v analýze a podobně).

Prozatím však asi není jasné, proč by proti přijetí axiómu výběru měly být vznášeny nějaké výhrady. (Tvrzení axiómu se samo o sobě zdá jistě vcelku samozřejmé.)

Hlavní potíže spojené s přijetím axiómu výběru si demonstrujme opět na příkladu 4.2. Užijeme-li axióm výběru, lze „zkonstruovat“ množinu M tak, že z každé třídy rozkladu $\mathbb{R}/\varrho$ vybereme jeden prvek. Přesněji řečeno, axióm výběru nám zaručí **existenci** takové množiny M, přesto však neznáme žádné pravidlo, které by nám umožnilo **sestrojit** konkrétní příklad takové množiny. Právě v tomto tkví zásadní potíž spojená s axiómem výběru: lze-li existenci nějakého objektu dokázat pouze užitím axiómu výběru, nelze tento objekt zkonstruovat. To si ostatně budeme ještě několikrát demonstrovat.

S axiómem výběru je ekvivalentní řada tvrzení. Ve větě 4.7 uvedeme některá z nich. K jejich formulaci však potřebujeme následující definici.

4.6. Definice. Buď A uspořádaná množina. Řekneme, že $X \subseteq A$ je *maximální řetězec* v A, když platí:
(1) X je řetězec,
(2) je-li $Y \subseteq A$ takový řetězec, že $X \subseteq Y$, pak je $X = Y$.

Z celé řady tvrzení, která jsou s axiómem výběru ekvivalentní, uvedeme pouze *Zermelovu větu*, *Hausdorffovu větu* a *Zornovo lemma*.

4.7. Věta. *Následující tvrzení jsou ekvivalentní s axiómem výběru:*

(a) **Zermelova věta:** *Na každé množině existuje dobré uspořádání.*[1]

(b) **Hausdorffova věta:** *Každý řetězec uspořádané množiny je podmnožinou některého maximálního řetězce této množiny.*

(c) **Zornovo lemma:** *Je-li každý řetězec uspořádané množiny A shora ohraničený, existuje ke každému prvku $x \in A$ maximální prvek $m_x \in A$ takový, že $x \leq m_x$.*

[1] Obvykle je Zermelova věta formulována tak, že *každou množinu lze dobře uspořádat*. Tato formulace je však značně nepřesná a — pro toho, kdo se v popisované problematice nevyzná — matoucí, neboť jak již víme, konstrukci onoho dobrého uspořádání alespoň v těch případech, kdy opravdu užijeme axiómu výběru, popsat **nelze**.

Důkaz věty 4.7 lze nalézt například v [7], kapitola I, §6. My zde provedeme na ukázku alespoň důkaz tvrzení, že z axiómu výběru plyne Zermelova věta. Důkaz tohoto tvrzení lze sice provést stručněji; z původního Zermelova důkazu, který zde jen s nepatrnými úpravami provedeme, je však lépe vidět roli axiómu výběru. •

Nejprve však některé potřebné pojmy.

4.8. Definice. Buď A řetězec, buďte G, H neprázdné podmnožiny v A. Řekneme, že uspořádaná dvojice $[G, H]$ je *řez* v množině A, když platí:
(a) $G \cup H = A$,
(b) $G \cap H = \emptyset$,
(c) pro libovolné $x \in G$, $y \in H$ platí $x < y$.
Je-li $[G, H]$ řez v A, nazývá se G *dolní třída* a H *horní třída* tohoto řezu.

4.9. Lemma. Řetězec $A \neq \emptyset$ je dobře uspořádaný právě tehdy, když obsahuje nejmenší prvek a horní třída každého řezu v A obsahuje nejmenší prvek.

Důkaz. I. Buď A dobře uspořádaná množina, $[G, H]$ buď řez v A. Protože je $H \neq \emptyset$, obsahuje H nejmenší prvek.

II. Nechť horní třída každého řezu v A obsahuje nejmenší prvek a 0_A je nejmenší prvek v A. Buď $\emptyset \neq B \subseteq A$ libovolná podmnožina. Označme

$$C = \{x;\ x \in A, \text{existuje } t \in B \text{ takové, že } x \geq t\ \}.$$

Pak je zřejmě $C = A$ nebo je $[A - C, C]$ řez v A. V obou případech však C obsahuje nejmenší prvek, který je zřejmě nejmenším prvkem množiny B. Je tedy množina A dobře uspořádaná. •
Důkaz Zermelovy věty.

Buď M libovolná množina. Je-li M konečná, lze ji podle poznámky 2.14 dobře uspořádat, takže není co dokazovat.

Buď tedy M nekonečná. Označme

$$\mathcal{M} = \{X;\ X \subseteq M,\ X \neq \emptyset\}.$$

Podle věty 4.3 vybereme z každé množiny $X \in \mathcal{M}$ jeden prvek $f(X)$. Tento prvek nazveme *vyznačený* prvek množiny X. Je-li $A \subset M$ libovolná, nazveme *připojeným* prvkem k množině A vyznačený prvek množiny $M - A$ a označíme jej p_A. (Tj. $p_A = f(M - A)$.) Konečně pro každou $A \subset M$ nazveme množinu

$$A^+ = A \cup \{p_A\}$$

následovníkem množiny A. Protože je $p_A \notin A$, je $A \subset A^+$.

Nyní zavedeme následující označení: systém $\mathcal{A} \subseteq \mathcal{P}(M)$ podmnožin v M nazveme *řetězem* v M, když platí:

(1) $\emptyset \in \mathcal{A}$;

(2) je-li $\emptyset \neq \mathcal{B} \subseteq \mathcal{A}$ libovolná podmnožina v $\mathcal{A}$, je $\bigcup_{X \in \mathcal{B}} X \in \mathcal{A}$;

(3) je-li $A \in \mathcal{A}$, $A \subset M$, je $A^+ \in \mathcal{A}$.

Alespoň jeden řetěz v M existuje — například $\mathcal{P}(M)$. Dále je zřejmé, že průnik libovolného neprázdného systému řetězů v M je opět řetěz v M. Odtud však plyne, že množina všech řetězů v M, uspořádaná inkluzí, obsahuje nejmenší prvek $\mathcal{A}_0$ — průnik všech řetězů v M.

Buď tedy $\mathcal{A}_0$ nejmenší řetěz v M. Řekneme, že množina $A \in \mathcal{A}_0$ je *normální*, jestliže je srovnatelná s každou množinou $X \in \mathcal{A}_0$ (tj. platí $A \subseteq X$ nebo $X \subseteq A$). Dokážeme nyní následující tvrzení:

(α) *Buď $A \in \mathcal{A}_0$, $A \subset M$. Je-li A normální, je také A^+ normální.*

Potřebujeme dokázat, že když je A normální, pak pro libovolnou množinu $X \in \mathcal{A}_0$ platí $X \subseteq A^+$ nebo $A^+ \subseteq X$. Dokážeme však víc než to: dokážeme, že pro libovolnou $X \in \mathcal{A}_0$ je $X \subseteq A$ nebo $A^+ \subseteq X$.

Označme

$$\mathcal{A}_0(A) = \{X;\ X \in \mathcal{A}_0,\ X \subseteq A \quad \text{nebo} \quad A^+ \subseteq X\}.$$

Pak je $\mathcal{A}_0(A) \subseteq \mathcal{A}_0$. Dokážeme-li nyní, že $\mathcal{A}_0(A)$ je řetěz v M, je nutně $\mathcal{A}_0(A) = \mathcal{A}_0$, neboť $\mathcal{A}_0$ je nejmenší řetěz v M. Tím však bude dokázáno tvrzení (α).

Je zřejmé, že $\emptyset \in \mathcal{A}_0(A)$, takže $\mathcal{A}_0(A)$ splňuje podmínku (1).

Buď $\emptyset \neq \mathcal{B} \subseteq \mathcal{A}_0(A)$ libovolná podmnožina. Jestliže pro každou množinu $X \in \mathcal{B}$ platí $X \subseteq A$, pak také $\bigcup_{X \in \mathcal{B}} X \subseteq A$, takže $\bigcup_{X \in \mathcal{B}} X \in \mathcal{A}_0(A)$. Existuje-li $X_0 \in \mathcal{B}$ tak, že $A^+ \subseteq X_0$, je tím spíše $A^+ \subseteq \bigcup_{X \in \mathcal{B}} X$. To však znamená, že $\mathcal{A}_0(A)$ splňuje i podmínku (2).

Zbývá již dokázat jen to, že $\mathcal{A}_0(A)$ splňuje i podmínku (3). Buď tedy $K \in \mathcal{A}_0(A)$, $K \subset M$, libovolná. Pak je buďto $K \subseteq A$ nebo $A^+ \subseteq K$. Je-li však $A^+ \subseteq K$, je tím spíše $A^+ \subseteq K^+$, takže $K^+ \in \mathcal{A}_0(A)$. Nechť je tedy $K \subseteq A$. Je-li $K = A$, je $K^+ = A^+$, takže $A^+ \subseteq K^+$ a opět je $K^+ \in \mathcal{A}_0(A)$. Zbývá tedy již jen případ $K \subset A$. Dokážeme, že pak platí $K^+ \subseteq A$.

Podle předpokladu je A normální, takže je $K^+ \subseteq A$ nebo $A \subseteq K^+$. Je-li $K^+ \subseteq A$, není co dokazovat. Nechť tedy $A \subseteq K^+ = K \cup \{p_K\}$. Protože podle podle předpokladu je $K \subset A$, je zřejmě $A = K^+$, tj. $K^+ \subseteq A$. Opět tak platí $K^+ \in \mathcal{A}_0(A)$.

Je tedy $\mathcal{A}_0(A)$ řetěz v M a tvrzení (α) je dokázáno.

Nyní dokážeme následující tvrzení:

(β) $(\mathcal{A}_0, \subseteq)$ *je řetězec.*

Zřejmě stačí dokázat, že každá množina $X \in \mathcal{A}_0$ je normální, neboť pak jsou každé dvě

množiny $X, Y \in \mathcal{A}_0$ srovnatelné. K tomu však stačí dokázat, že množina

$$N(\mathcal{A}_0) = \{X;\ X \in \mathcal{A}_0,\ X \text{ je normální}\}$$

je řetěz v M, neboť je $N(\mathcal{A}_0) \subseteq \mathcal{A}_0$ a $\mathcal{A}_0$ je nejmenší řetěz v M.

Zřejmě je $\emptyset \in N(\mathcal{A}_0)$, takže $N(\mathcal{A}_0)$ splňuje podmínku (1).

Buď $\emptyset \neq \mathcal{B} \subseteq N(\mathcal{A}_0)$ libovolná podmnožina. Pak se vztah $\bigcup_{X \in \mathcal{B}} X \in N(\mathcal{A}_0)$ dokáže analogicky jako obdobný vztah v důkazu tvrzení (α). Splňuje tedy $N(\mathcal{A}_0)$ i podmínku (2).

Tvrzení (α) znamená však právě ten fakt, že $N(\mathcal{A}_0)$ splňuje i podmínku (3).

Tím je dokázáno i tvrzení (β).

Nyní dokážeme, že:

(γ) *Řetězec* $(\mathcal{A}_0, \subseteq)$ *je dobře uspořádaný.*

Je zřejmé, že $\emptyset$ je nejmenší prvek v $\mathcal{A}_0$. Podle lemmatu 4.9 stačí dokázat, že horní třída každého řezu v množině $\mathcal{A}_0$ obsahuje nejmenší prvek.

Buď tedy $[\mathcal{S}, \mathcal{T}]$ řez v $\mathcal{A}_0$. Položme $S = \bigcup_{X \in \mathcal{S}} X$. Poněvadž je $\mathcal{A}_0$ řetěz v M, plyne z podmínky (2) v definici řetězu, že $S \in \mathcal{A}_0$. To však znamená, že je $S \in \mathcal{S}$ nebo $S \in \mathcal{T}$. Je-li $S \in \mathcal{S}$, platí pro každou množinu $X \in \mathcal{T}$ vztah $S \subset X$, přičemž je $\mathcal{T} \neq \emptyset$. Je tedy $S \subset M$. Pak ale $S \subset S^+$, takže $S^+ \in \mathcal{T}$. Nyní je však zřejmé, že S^+ je nejmenší prvek v $\mathcal{T}$, neboť množina $S^+ - S$ je jednoprvková, takže nemůže existovat $W \in \mathcal{A}_0$ tak, že $S \subset W \subset S^+$.

Nechť tedy je $S \in \mathcal{T}$. Pak je ale zřejmé, že S je nejmenší prvek množiny $\mathcal{T}$. Pro libovolnou množinu $Y \in \mathcal{T}$ totiž platí

$$X \subset Y \quad \text{pro každou množinu} \quad X \in \mathcal{S} \quad \text{(podle definice 4.8(c))},$$

takže také $S = \bigcup_{X \in \mathcal{S}} X \subseteq Y$.

Tím je tvrzení (γ) dokázáno.

Konečně dokážeme tvrzení:

(δ) *Existuje bijekce množiny* $\mathcal{A}_0 - \{M\}$ *na množinu* M.

Definujme zobrazení g: $(\mathcal{A}_0 - \{M\}) \to M$ takto: $g(A) = p_A$ pro každou množinu $A \in \mathcal{A}_0$, $A \subset M$. Ukážeme, že zobrazení g je bijekce.

Buďte $A, B \in \mathcal{A}_0 - \{M\}$ libovolné takové, že $A \neq B$. Pak je $A \subset B$ nebo $B \subset A$.

Nechť tedy je například $A \subset B$. Pak je nutně $A^+ \subseteq B$ (neboť A^+, B jsou srovnatelné a nemůže platit $B \subset A^+$), tj. $p_A \in B$. Protože však $p_B \notin B$, je $g(A) = p_A \neq p_B = g(B)$, takže g je injekce.

Buď nyní $a \in M$ libovolný. Položme

$$A = \bigcup \{X;\ X \in \mathcal{A}_0,\ a \notin X\}.$$

Alespoň jedna taková množina $X \in \mathcal{A}_0$ existuje — například $\emptyset$. Protože je $\mathcal{A}_0$ řetěz, je $A \in \mathcal{A}_0$. Nyní dokážeme, že je $a = p_A$.

Připusťme, že je $a \neq p_A$. Pak je $a \notin A^+ \supset A$, přičemž $A^+ \in \mathcal{A}_0$: spor, neboť A je sjednocení *všech* množin z $\mathcal{A}_0$, které neobsahují prvek a. Je tedy $a = p_A$, tj. $a = g(A)$, takže g je surjekce.

Tím je tvrzení (δ) dokázáno.

Definujeme-li nyní na množině M relaci $\leq$ takto:

$$x, y \in M,\ x \leq y \iff g^{-1}(x) \subseteq g^{-1}(y),$$

je zřejmé, že $(M, \leq)$ je dobře uspořádaná, neboť g je evidentně izomorfismus.

Dokázali jsme tedy, že pomocí axiómu výběru lze dokázat Zermelovu větu. •

4.10. Poznámka. V důkazu Zermelovy věty jsme uvedli „konstrukci“ dobrého uspořádání na libovolné množině M. Ve skutečnosti však obecně nedovedeme každou množinu dobře uspořádat (nelze například udat konkrétní dobré uspořádání množiny $\mathbb{R}$ všech reálných čísel, byť podle Zermelovy věty takové dobré uspořádání existuje). Víme již, že potíž tkví v podstatě axiómu výběru. Tohoto axiómu jsme užili jen v počátku důkazu, když jsme v každé množině $\emptyset \neq X \subseteq M$ vybírali jeden prvek. Právě tato okolnost však způsobila to, že důkaz Zermelovy věty je pouze „existenční“ a nikoliv „konstruktivní“.

Kapitola 3

Kardinální a ordinální čísla

1 Kardinální číslo. Spočetné množiny

Věda má vždycky pravdu.
Nenechte se zmást fakty.
FINAGLOVO KRÉDO

1.1. Definice. Řekneme, že množiny A, B jsou *ekvivalentní* a píšeme $A \sim B$, jestliže existuje bijekce $f\colon A \to B$.

1.2. Poznámka. Je zřejmé, že když A je konečná množina, platí $A \sim B$ právě tehdy, když i B je konečná množina a obě množiny mají stejný počet prvků.

1.3. Příklad.

(a) Množina $\mathbb{N}$ všech přirozených čísel je ekvivalentní s množinou S všech sudých čísel, neboť zobrazení $f\colon \mathbb{N} \to S$ definované vztahem $f(x) = 2x$ je zřejmě bijekce.

(b) Buďte $a_1 < a_2$, $b_1 < b_2$ libovolná reálná čísla. Pak jsou intervaly (a_1, a_2), (b_1, b_2) ekvivalentní, neboť zobrazení $f\colon (a_1, a_2) \to (b_1, b_2)$ definované vztahem

$$f(x) = \frac{b_2 - b_1}{a_2 - a_1}(x - a_1) + b_1$$

je zřejmě bijekce.

1.4. Věta. *Buďte A, B, C libovolné množiny. Pak platí:*

(1) $A \sim A$;

(2) $A \sim B \Rightarrow B \sim A$;

(3) $A \sim B \wedge B \sim C \Rightarrow A \sim C$.

Důkaz. Tvrzení jsou zřejmá, neboť id_A je bijekce, je-li $f\colon A \to B$ bijekce, je také $f^{-1}\colon B \to A$ bijekce, a konečně, jsou-li $f\colon A \to B$, $g\colon B \to C$ bijekce, je $g \circ f\colon A \to C$ bijekce. •

1.5. Věta. *Buď $I \neq \emptyset$ množina, A_i, B_i $(i \in I)$, A, B, C budťe libovolné množiny. Pak platí:*

1. *Je-li $f\colon I \to I$ bijekce, pak $\bigotimes_{i\in I} A_i \sim \bigotimes_{i\in I} A_{f(i)}$, zejména $(A \times B) \sim (B \times A)$.*
2. *Nechť pro každé $i \in I$ platí $A_i \sim B_i$. Pak $\bigotimes_{i\in I} A_i \sim \bigotimes_{i\in I} B_i$.*
3. *$A \sim B \Rightarrow \mathcal{P}(A) \sim \mathcal{P}(B)$.*
4. *Jsou-li množiny A_i i množiny B_i po dvou disjunktní a platí-li $A_i \sim B_i$ pro každé $i \in I$, platí $\bigcup_{i\in I} A_i \sim \bigcup_{i\in I} B_i$.*
5. *Jsou-li množiny A_i po dvou disjunktní, pak $A^{\bigcup_{i\in I} A_i} \sim \bigotimes_{i\in I} A^{A_i}$; zejména pro disjunktní množiny B, C platí $A^{B\cup C} \sim (A^B \times A^C)$.*
6. *$A^{B\times C} \sim (A^B)^C$*
7. *$(\bigotimes_{i\in I} A_i)^B \sim \bigotimes_{i\in I} A_i^B$, zejména $(A \times B)^C \sim (A^C \times B^C)$.*

Důkaz. Důkazy vztahů (1) – (4) jsou jednoduché a proto je nebudeme uvádět.

(5) Pro každý prvek $\varphi \in A^{\bigcup_{i\in I} A_i}$, tj. $\varphi\colon \bigcup_{i\in I} A_i \to A$, označme φ_i restrikci zobrazení φ na množinu A_i. Pak je $\varphi_i \in A^{A_i}$. Definujme zobrazení

$$F\colon A^{\bigcup_{i\in I} A_i} \to \bigotimes_{i\in I} A^{A_i}$$

takto: pro $\varphi \in A^{\bigcup A_i}$ je $F(\varphi) = f$ to zobrazení množiny I do množiny $\bigcup A^{A_i}$, pro které platí $f(i) = \varphi_i$. Pak je zřejmě F požadovaná bijekce.

(6) Buď $f \in A^{B\times C}$ libovolný prvek. Pro každý prvek $c \in C$ definujme zobrazení $g_c\colon B \to$ $\to A$, tj. prvek množiny A^B, takto: $g_c(x) = f(x, c)$ pro každý prvek $x \in B$. Definujeme-li nyní $F(y) = g_y$ pro každý prvek $y \in C$, je $F\colon C \to A^B$, tj. $F \in (A^B)^C$. Nyní je však zřejmé, že

zobrazení, které každému prvku $f \in A^{B\times C}$ přiřadí takto zkonstruované zobrazení F, je bijekce množiny $A^{B\times C}$ na množinu $(A^B)^C$.

(7) Buď $f \in (\bigotimes_{i\in I} A_i)^B$ libovolný prvek. Pro každý prvek $b \in B$ je $f(b)$ prvek množiny $\bigotimes_{i\in I} A_i$, tj. $f(b) = f_b\colon I \to \bigcup_{i\in I} A_i$, přičemž $f_b(i) \in A_i$ pro každé $i \in I$. Definujme nyní zobrazení $f_i\colon B \to A_i$ takto: $f_i(b) = f_b(i)$ pro každý prvek $b \in B$. Zobrazení $F\colon (\bigotimes A_i)^B \to \bigotimes A_i^B$ definované vztahem $F(f)(i) = f_i$ je pak evidentně bijekce. •

1.6. Definice. Řekneme, že množina je *spočetná*, je-li ekvivalentní s množinou všech přirozených čísel. Množina, která je konečná nebo spočetná, se nazývá *nejvýše spočetná*.

1.7. Poznámka. Je-li A spočetná množina, existuje podle definice 1.1 bijekce $f\colon \mathbb{N} \to A$. Takové funkce f, pro něž je Dom $f = \mathbb{N}$, se nazývají *posloupnosti*. Lze tedy říci, že množina A je spočetná, lze-li její prvky uspořádat do posloupnosti.

1.8. Věta. *Každá podmnožina spočetné množiny je nejvýše spočetná.*

Důkaz. Buď A spočetná množina. Podle poznámky 1.7 je tedy $A = (a_n)_{n=1}^{\infty}$. Buď $B \subseteq A$ libovolná podmnožina. Buď n_1 nejmenší přirozené číslo takové, že $a_{n_1} \in B$, n_2 nejmenší přirozené číslo takové, že $n_2 > n_1$ a $a_{n_2} \in B$ atd. Posloupnost (a_{n_k}) je buďto konečná a tedy B je konečná, nebo je nekonečná a to znamená, že B je spočetná. •

1.9. Věta. *Buď I nejvýše spočetná množina, buď A_i nejvýše spočetná množina pro každé $i \in I$. Pak je množina $\bigcup_{i\in I} A_i$ nejvýše spočetná.*

Důkaz. Je zřejmé, že stačí dokázat, že když je I spočetná a všechny A_i jsou spočetné, pak je také $\bigcup_{i\in I} A_i$ spočetná. V tomto případě můžeme bez újmy na obecnosti předpokládat, že $I = \mathbb{N}$. Každou z množin A_i lze podle předpokladu uspořádat do posloupnosti takto:

$$\begin{aligned} A_1 &= \{a_{11}, a_{12}, \dots, a_{1n}, \dots\} \\ A_2 &= \{a_{21}, a_{22}, \dots, a_{2n}, \dots\} \\ &\vdots \\ A_n &= \{a_{n1}, a_{n2}, \dots, a_{nn}, \dots\} \\ &\vdots \end{aligned}$$

Pak je ale $\bigcup_{i\in I}^{\infty} A_i = \{a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, a_{14}, a_{23}, a_{32}, a_{41}, \dots\}$, takže množina $\bigcup_{i\in I}^{\infty} A_i$ je spočetná. •

1.10. Důsledek. *Množina všech celých čísel je spočetná.*

1.11. Věta. *Každá nekonečná množina A obsahuje spočetnou podmnožinu B takovou, že množina $A - B$ je opět nekonečná.*

Důkaz. Je-li množina A nekonečná, existují prvky $a_1, b_1 \in A$, $a_1 \neq b_1$. Protože je $A - \{a_1, b_1\}$ nekonečná, existují prvky $a_2, b_2 \in A - \{a_1, b_1\}$, $a_2 \neq b_2$ atd. Indukcí lze zřejmě v A sestrojit dvě disjunktní spočetné podmnožiny

$$B = (a_n)_{n=1}^{\infty}, \qquad C = (b_n)_{n=1}^{\infty}.$$

Tím je tvrzení dokázáno. (Pozorný čtenář však jistě postřehl, že jsme v důkazu využili axiómu výběru.) •

1.12. Věta. *Kartézský součin dvou spočetných množin je spočetná množina.*

Důkaz. Podle věty 1.5(2) víme, že když $A \sim C$, $B \sim D$, pak je $A \times B \sim C \times D$. Stačí tedy dokázat, že $\mathbb{N}^2$ je spočetná množina.

Pro každý prvek $[p, q] \in \mathbb{N}^2$ nazveme výškou tohoto prvku číslo $p + q$. Je zřejmé, že pro každé $n \in \mathbb{N}$, $n > 1$, existuje $n - 1$ dvojic výšky n: $[1, n-1], [2, n-2], \ldots, [n-1, 1]$. Označme $P_n = \{[p, q];\ [p, q] \in \mathbb{N}^2$, výška $[p, q]$ je $n\}$. Pak je $\mathbb{N}^2 = \bigcup_{n=2}^{\infty} P_n$ podle věty 1.9 spočetná. •

1.13. Důsledek. *Kartézský součin konečného (nenulového) počtu spočetných množin je spočetná množina.*

1.14. Důsledek. *Množina $\mathbb{Q}$ všech racionálních čísel je spočetná.*

Důkaz. Víme, že každé kladné racionální číslo r lze jednoznačně vyjádřit jako podíl $\frac{p}{q}$ nesoudělných přirozených čísel. Těchto podílů je nejvýše tolik, jako všech dvojic $[p, q] \in \mathbb{N}^2$, tj. nejvýše spočetně mnoho. Odtud a z věty 1.9 nyní plyne tvrzení. •

1.15. Věta. *Buď A spočetná množina. Pak je množina K všech konečných posloupností prvků množiny A spočetná.*

Důkaz. Buď $n \in \mathbb{N}$ libovolné. Podle důsledku 1.13 je množina A^n všech uspořádaných n-tic z prvků množiny A spočetná. Podle věty 1.9 je i množina $K = \bigcup_{n=1}^{\infty} A^n$ spočetná. •

1.16. Důsledek. *Množina všech polynomů (jedné proměnné) s racionálními koeficienty je spočetná.*

Důkaz. Každému polynomu $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ ($a_0 \neq 0$) stačí přiřadit prvek $[a_0, a_1, \ldots, a_n] \in \mathbb{Q}^{n+1}$. •

1.17. Poznámka. Nyní si můžeme uvést jeden z prvních dokladů toho, jak teorie množin umožnila zodpovědět problém jiné matematické disciplíny, v tomto případě teorie čísel.

Reálné číslo se nazývá *algebraické*, je-li kořenem nějakého polynomu s racionálními koeficienty. Reálné číslo, které není algebraické, se nazývá *transcendentní*. Je okamžitě zřejmé, že každé racionální číslo je algebraické, stejně tak jako například čísla $\sqrt{2}$, $\sqrt{3}$, $\sqrt{26}$ atd.

Teprve v 19. století se však podařilo dokázat, že například číslo π je transcendentní. Otázkou však bylo, kolik vlastně transcendentních čísel existuje. Teorie množin tuto otázku jednoduše vyřešila. Z faktu, že každý polynom n-tého stupně má nejvýše n reálných kořenů a z důsledku 1.16 okamžitě plyne, že *množina všech algebraických čísel je spočetná*. V dalším uvidíme, že to znamená, že transcendentních čísel je „více“ než čísel algebraických — viz důsledek 2.11.

1.18. Poznámka. Při formální výstavbě teorie množin lze přesně popsat, jak lze *každé* množině A přiřadit objekt card A, nazývaný *kardinální číslo množiny* A. Přitom pro každé dvě množiny A, B platí

$$\text{card } A = \text{ card } B \iff A \sim B. \qquad (*)$$

Poněvadž zde nebudeme tuto formalizovanou konstrukci uvádět, spokojíme se s konstatováním, že každé množině A lze přiřadit symbol card A tak, že je splněna výše uvedená podmínka ($\star$).

Kardinální číslo množiny A se často také nazývá *mohutnost* množiny A. Podle poznámky 1.2 mají dvě konečné množiny stejné kardinální číslo právě tehdy, když mají stejný počet prvků. Má tedy smysl přijmout následující označení:
má-li konečná množina A n prvků, označíme card $A = n$. Zejména tedy card $\emptyset = 0$. Kardinální číslo spočetných množin značíme symbolem $\aleph_0$ ($\aleph$ — čti „alef“ — je první písmeno hebrejské abecedy). (Důvod tohoto označení uvidíme v §6 – viz poznámka 6.9.)

Cvičení k §1

Pouze v jediném případě si můžeme být neomylně jisti:
jsme-li si jisti, že se mýlíme.
HOLTENOVA POUČKA

1. Dokažte následující tvrzení:

a) Množina všech intervalů v $\mathbb{R}$, jejichž koncové body jsou racionální, je spočetná.

b) Buď $\mathcal{A}$ nějaká množina po dvou disjunktních intervalů v $\mathbb{R}$. Pak je $\mathcal{A}$ nejvýše spočetná. (Návod: Vyberte v každém intervalu jedno racionální číslo.)

2. Buď f reálná funkce jedné reálné proměnné. Dokažte, že množina všech bodů, v nichž má funkce f ostrý lokální extrém, je nejvýše spočetná. (Návod: Využijte výsledku cvičení 1(a).)

3. Dokažte, že množina všech bodů nespojitosti monotonní reálné funkce jedné reálné proměnné je nejvýše spočetná. (Návod: Využijte cvičení 1(b) a faktu, že monotonní funkce má v každém bodě limitu zleva i limitu zprava.)

2 Nerovnost mezi kardinálními čísly

Jde-li to s věcmi do háje,
nikdo netuší, jak je hluboký.
HANEŮV ZÁKON

Následující *Cantor-Bernsteinova věta* patří k základním tvrzením teorie množin.

2.1. Cantor-Bernsteinova věta. Buďte A, B libovolné množiny. Existují-li množiny $A_1 \subseteq A$, $B_1 \subseteq B$ takové, že $A \sim B_1$, $B \sim A_1$, platí $A \sim B$.

Důkaz. Je-li některá z množin A, B konečná, je tvrzení triviální. Buď tedy A nekonečná, $f\colon B \to A_1$ buď bijekce. Je-li $A_1 = A$, není co dokazovat. Nechť tedy je $A_1 \subset A$ a analogicky $B_1 \subset B$. Označme $A_2 = f(B_1)$. Pak platí:

$$A_2 \subset A_1 \subset A,\ A \sim A_2,\ B \sim A_1. \tag{2.1.}$$

Stačí tedy dokázat, že je $A \sim A_1$, neboť z tranzitivity relace $\sim$ pak plyne $A \sim B$.

Podle (1) existuje bijekce $g\colon A \to A_2$. Pak platí:

$$\begin{aligned} A_1 \subset A &\Longrightarrow A_3 := g(A_1) \subset A_2, \\ A_2 \subset A_1 &\Longrightarrow A_4 := g(A_2) \subset A_3, \\ A_3 \subset A_2 &\Longrightarrow A_5 := g(A_3) \subset A_4, \end{aligned}$$

$$\vdots$$

Přitom platí

$$\begin{aligned} g(A - A_1) &= A_2 - A_3 \\ g(A_1 - A_2) &= A_3 - A_4 \\ g(A_2 - A_3) &= A_4 - A_5 \end{aligned}$$

$$\vdots$$

Protože je g bijekce, plyne odtud ekvivalence následujících množin:

$$(A - A_1) \cup (A_2 - A_3) \cup (A_4 - A_5) \cup \ldots \cup (A_n - A_{n+1}) \cup \ldots$$
$$(A_2 - A_3) \cup (A_4 - A_5) \cup (A_5 - A_6) \cup \ldots \cup (A_{n+1} - A_{n+2}) \cup \ldots \qquad (2.2.)$$

Označme

$$D := A \cap \bigcap_{i \in I}^{\infty} A_i .$$

Pak je zřejmé, že platí:

$$A = D \cup (A - A_1) \cup (A_1 - A_2) \cup (A_2 - A_3) \cup (A_3 - A_4) \cup \ldots$$
$$A_1 = D \cup (A_1 - A_2) \cup (A_2 - A_3) \cup (A_3 - A_4) \cup \ldots \qquad (2.3.)$$

Protože pro sjednocení množin platí asociativní a komutativní zákon, lze vztahy (2.3) přepsat na tvar

$$A = \big[D \cup (A_1 - A_2) \cup (A_3 - A_4) \cup \ldots\big] \cup \big[(A - A_1) \cup (A_2 - A_3) \cup \ldots\big]$$
$$A_1 = \big[D \cup (A_1 - A_2) \cup (A_3 - A_4) \cup \ldots\big] \cup \big[(A_2 - A_3) \cup (A_4 - A_5) \cup \ldots\big]$$

V prvních závorkách množin A i A_1 však stojí tytéž množiny, množiny ve druhých závorkách jsou podle (2.2) ekvivalentní. To však znamená, že $A \sim A_1$, což jsme chtěli dokázat. •

2.2. Definice. Buďte a, b libovolná kardinální čísla, A, B libovolné takové množiny, že $a = \operatorname{card} A$, $b = \operatorname{card} B$. Pak klademe:

$$a \leq b \iff \text{existuje injektivní zobrazení} \quad f\colon A \to B.$$

2.3. Poznámka. (a) Relaci $\leq$ mezi kardinálními čísly jsme definovali pomocí množin o příslušných mohutnostech. Analogicky budeme postupovat i později například při definici aritmetických operací. To však znamená, že je nutno dokázat, že platnost vztahu $a \leq b$ nezávisí na konkrétní volbě množin A, B, přesněji řečeno, je nutno dokázat, že

když je $A \sim A_1$, $B \sim B_1$, pak injekce A do B existuje právě tehdy,
když existuje injekce A_1 do B_1.

Toto tvrzení je však evidentní a zformulování jednoduchého důkazu přenecháme čtenáři. V dalším pak tvrzení tohoto typu většinou nebudeme uvádět.

(b) Definici 2.2 jsme mohli zformulovat i jinak. Uvědomíme-li si totiž, že zřejmě

injekce A do B existuje právě tehdy, když existuje $B_1 \subseteq B$ tak, že $A \sim B_1$,

můžeme říci, že

$$a \leq b \iff \text{existuje } B_1 \subseteq B \quad \text{taková, že} \quad A \sim B_1.$$

Nyní je však nutno dokázat, že relace $\leq$ definovaná v 2.2 je uspořádání. Vzhledem k tomu, že později uvidíme, že *neexistuje množina všech kardinálních čísel* (tj. systém všech kardinálních čísel tvoří vlastní třídu), je nutno toto tvrzení zformulovat následovně:

2.4. Věta. *Buď $\mathcal{A}$ libovolná množina kardinálních čísel. Pak je $(\mathcal{A}, \leq)$ uspořádaná množina.*

Důkaz. Reflexivita a tranzitivita relace $\leq$ je zřejmá, neboť id_A je injekce pro každou množinu A a složení dvou injekcí je opět injekce.

Antisymetrie relace $\leq$ plyne z Cantor-Bernsteinovy věty 6.10. •

Následující tvrzení je dalším ekvivalentem axiómu výběru.

2.5. Věta. *Pro každá dvě kardinální čísla a, b platí $a \leq b$ nebo $b \leq a$.*

Důkaz. Buďte A, B libovolné takové množiny, že card $A = a$, card $B = b$. Podle Zermelovy věty 4.7 lze množiny A, B dobře uspořádat. Tvrzení nyní plyne z věty 2.13 v kapitole II. •

2.6. Poznámka. Podle věty 2.5 tvoří každá množina kardinálních čísel řetězec. Zejména platí

$$0 < 1 < 2 < \cdots < n < \cdots < \aleph_0.$$

Z věty 1.11 plyne, že $\aleph_0$ *je nejmenší nekonečné kardinální číslo*. Prozatím však nevíme, zda existují nekonečná kardinální čísla různá od $\aleph_0$. V následující větě dokážeme, že taková kardinální čísla existují. Jinými slovy, existují nekonečné množiny, které nejsou spočetné. Takové množiny se nazývají *nespočetné*.

2.7. Cantorova věta. Buďte $X \neq \emptyset \neq Y$ libovolné množiny, card $Y \geq 2$. Pak platí

$$\text{card } Y^X > \text{ card } X.$$

Důkaz. Nejprve dokážeme, že platí card $X \leq$ card Y^X.

Podle předpokladu existují prvky $y_1, y_2 \in Y$, $y_1 \neq y_2$. Pro každý prvek $x \in X$ definujme zobrazení $f_x\colon X \to Y$ takto:

$$f_x(t) = \begin{cases} y_1 & \text{pro } t = x \\ y_2 & \text{pro } t \in X,\ t \neq x. \end{cases}$$

Pak je pro $x_1, x_2 \in X$, $x_1 \neq x_2$, zřejmě $f_{x_1} \neq f_{x_2}$, neboť například $f_{x_1}(x_1) = y_1$, $f_{x_2}(x_1) = y_2$. Zobrazení $F\colon X \to Y^X$ definované vztahem $F(x) = f_x$ pro každý prvek $x \in X$ je tedy injekce, což jsme chtěli dokázat.

Nyní dokážeme, že je card $X \neq$ card Y^X.

Připusťme, že existuje bijekce $\varphi\colon X \to Y^X$. Definujme zobrazení $f\colon X \to Y$ následovně:

$$f(x) = \begin{cases} y_1, & \text{jestliže } \varphi(x)(x) \neq y_1 \\ y_2, & \text{jestliže } \varphi(x)(x) = y_1. \end{cases}$$

Pak je $f \in Y^X$ a pro každé $x \in X$ je $\varphi(x) \neq f$, takže φ není surjekce: spor.

Dokázali jsme tak, že card $X <$ card Y^X. •

2.8. Poznámka. Dokázali jsme právě, že *ke každému kardinálnímu číslu existuje kardinální číslo větší*. Proto existují kardinální čísla větší než $\aleph_0$, tj. existují nespočetné množiny. Uvědomme si však, že z věty 2.7 okamžitě plyne, že kardinálních čísel větších než je $\aleph_0$ je *nekonečně mnoho*. Zejména to znamená, že **dvě nespočetné množiny ani zdaleka nemusí mít stejné kardinální číslo!**

Metoda, kterou jsme dokázali, že v důkazu věty 2.7 neexistuje surjekce $\varphi\colon X \to Y^X$, je tzv. *Cantorova diagonální metoda*. Jejím speciálním případem je důkaz následujícího tvrzení.

2.9. Věta. *Množina všech reálných čísel x, $0 < x < 1$ je nespočetná.*

Důkaz. Buď $x \in (0,1)$ libovolné. Pak lze x napsat pomocí dekadického rozvoje ve tvaru $0{,}a_1a_2a_3\ldots$, přičemž tento rozvoj je určen jednoznačně, vyloučíme-li rozvoje, v nichž se od jistého indexu počínaje vyskytuje pouze devítka. (Takže například číslo $0{,}320\overline{9}$ zapíšeme ve tvaru $0{,}321$.)

Předpokládejme nyní, že množina reálných čísel z intervalu $(0,1)$ je spočetná. Pak lze tato čísla uspořádat do posloupnosti $(r_n)_{n=1}^{\infty}$ a každé číslo r_i lze jednoznačně vyjádřit pomocí dekadického rozvoje takto:

$$\begin{aligned} r_1 &= 0{,}a_{11}a_{12}a_{13}a_{14}\ldots \\ r_2 &= 0{,}a_{21}a_{22}a_{23}a_{24}\ldots \\ r_3 &= 0{,}a_{31}a_{32}a_{33}a_{34}\ldots \\ &\vdots \\ r_n &= 0{,}a_{n1}a_{n2}a_{n3}a_{n4}\ldots \\ &\vdots \end{aligned}$$

Zkonstruujme nyní číslo $r = 0{,}a_1a_2a_3a_4\ldots$ takto: pro $i = 1, 2, \ldots, n, \ldots$ je

$$a_i = \begin{cases} 1 & \text{je-li } a_{ii} \neq 1 \\ 2 & \text{je-li } a_{ii} = 1. \end{cases}$$

Pak je $r \in (0,1)$ a pro každé $n \in \mathbb{N}$ přitom $r \neq r_n$: spor. Interval $(0,1)$ tedy není spočetný. •

2.10. Důsledek. *Množina $\mathbb{R}$ všech reálných čísel je nespočetná a platí $\mathbb{R} \sim (0,1)$.*

Důkaz. Zobrazení $f(x) = \operatorname{arctg} x$ je bijekce $\mathbb{R}$ na interval $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$. Podle příkladu 1.3(b) jsou však intervaly $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ a $(0, 1)$ ekvivalentní. •

2.11. Důsledek.

(a) *Množina $\mathbb{I}$ všech iracionálních čísel je nespočetná.*

(b) *Množina všech transcendentních čísel je nespočetná.*

Důkaz. (a) Je $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$ a $\mathbb{Q}$ je podle důsledku 1.14 spočetná. Kdyby byla množina $\mathbb{I}$ spočetná, byla by $\mathbb{R}$ spočetná podle věty 1.9: spor. Je tedy $\mathbb{I}$ nespočetná.
(b) Analogicky (z 1.9, 1.17 a 2.10). •

2.12. Věta. *Buď X libovolná množina. Pak platí*

$$\operatorname{card} \mathcal{P}(X) > \operatorname{card} X.$$

Důkaz. Je-li $X = \emptyset$, je $\operatorname{card} X = 0$ a $\operatorname{card} \mathcal{P}(X) = \operatorname{card} \{\emptyset\} = 1 > 0$. Nechť tedy $X \neq \emptyset$. Zvolme ve větě 2.7 $Y = \{0, 1\}$. Definujme nyní zobrazení $F\colon Y^X \to \mathcal{P}(X)$ takto:

$$\text{pro každé } f\colon X \to Y \text{ je } F(f) = \{x;\ x \in X,\ \ f(x) = 0\}.$$

Pak je zřejmě F bijekce a tvrzení věty nyní plyne z věty 2.7, neboť

$$\operatorname{card}\mathcal{P}(X) = \operatorname{card} Y^X > \operatorname{card} X.$$

•

2.13. Věta. *Buď M nespočetná množina, A nejvýše spočetná podmnožina množiny M. Pak je $\operatorname{card} M = \operatorname{card}(M - A)$.*

Důkaz. Je $M = (M - A) \cup A$. Protože je A nejvýše spočetná množina, plyne z věty 1.9, že $M - A$ je nespočetná. Podle věty 1.11 existuje spočetná množina $A_1 \subseteq M - A$. Označme $P = (M - A) - A_1$. Pak je $M - A = A_1 \cup P$, tj. $M = (A \cup A_1) \cup P$. Protože je množina $A \cup A_1$ spočetná, existuje bijekce $f\colon A_1 \to A \cup A_1$. Položme pro každé $x \in M - A$

$$g(x) = \begin{cases} f(x) & \text{pro } x \in A_1 \\ x & \text{pro } x \in P. \end{cases}$$

Pak je $g\colon (M - A) \to M$ bijekce a věta je dokázána. •

2.14. Důsledek. *Buď A libovolná nekonečná množina, B nejvýše spočetná množina. Pak* $\operatorname{card}(A \cup B) = \operatorname{card} A$.

Důkaz. Je-li A spočetná, plyne tvrzení z věty 1.9. Je-li A nespočetná, plyne tvrzení z věty 2.13. •

Zásadní důležitost v teorii nekonečných množin má následující tvrzení:

2.15. Věta. *Množina A je nekonečná právě tehdy, když obsahuje vlastní podmnožinu $B \subset A$ takovou, že $A \sim B$.*

Důkaz. I. Je-li A konečná, není podle poznámky 1.2 ekvivalentní s žádnou svou vlastní podmnožinou.

II. Nechť je A nekonečná. Je-li spočetná, plyne tvrzení z věty 1.11, je-li nespočetná, plyne tvrzení z věty 2.13. •

2.16. Poznámka. Dosud jsme neuvedli, jak lze při axiomatické výstavbě teorie množin formalizovat intuitivně zřejmý pojem konečné a nekonečné množiny. Nyní vidíme, že nám to umožňuje věta 2.15. Při axiomatické výstavbě lze podle této věty říci, že *množina je nekonečná, je-li ekvivalentní s nějakou svou vlastní podmnožinou*. Přitom je snad evidentní, že to, zda nekonečné množiny v axiomatické teorii existují nebo ne, závisí na tom, zda přijmeme nebo nepřijmeme axióm, který nám jejich existenci postuluje. (V **ZF** a **GB** samozřejmě takový axióm je.)

Cvičení k §2

Nejméně vysilující je
spolehnout se na vlastní síly.
MURPHYHO PARADOX

1. Buďte $(a_n)_{n=1}^{\infty}$, $(b_n)_{n=1}^{\infty}$ rostoucí posloupnosti reálných čísel. Řekneme, že posloupnost (b_n) roste než posloupnost (a_n), když platí $\lim_{n\to\infty} \frac{a_n}{b_n} = 0$. Dokažte:

a) Ke každé rostoucí posloupnosti existuje posloupnost, která roste rychleji.

b) Je-li $\mathcal{A} \neq \emptyset$ taková množina rostoucích posloupností, že s každou posloupností obsahuje všechny posloupnosti, které rostou rychleji, pak je množina $\mathcal{A}$ nespočetná. (Návod: Důkaz provádějte sporem. Předpokládejte, že $\mathcal{A}$ je nejvýše spočetná a Cantorovou diagonální metodou sestrojte posloupnost, která roste rychleji než všechny posloupnosti z $\mathcal{A}$.)

3 Aritmetika kardinálních čísel

Pokud vycházejí matematické poučky ze skutečnosti,
nejsou spolehlivé.
Pokud jsou spolehlivé, nevycházejí ze skutečnosti.
EINSTEINŮV POSTŘEH

Aby byl název kardinální **číslo** oprávněný, je přirozené požadovat, abychom pro kardinální čísla zavedli obvyklé spolehlivé a ze skutečnosti vycházející aritmetické operace. V tomto paragrafu ukážeme, jak je definován součet, součin a mocnina kardinálních čísel. Ponecháme na čtenáři, aby si promyslel, že pro konečná kardinální čísla budou uváděné definice odpovídat obvyklým aritmetickým operacím v množině nezáporných celých čísel.

Poznamenejme ještě, že definici součtu a součinu dvou kardinálních čísel (a tedy i libovolného konečného počtu kardinálních čísel) lze zformulovat bez užití axiómu výběru. Pro definici součtu,qf respektive součinu nekonečného systému kardinálních čísel se však užití axiómu výběru nelze vyhnout. (Přesněji řečeno, bez axiómu výběru nelze dokázat, že každá množina kardinálních čísel má součet a součin.)

3.1. Definice. Buďte a, b libovolná kardinální čísla, A, B buďte libovolné takové množiny, že card $A = a$, card $B = b$, $A \cap B = \emptyset$. *Součtem* kardinálních čísel a, b rozumíme kardinální číslo

$$a + b := \text{ card } (A \cup B).$$

Obecněji: Buď $K \neq \emptyset$ libovolná množina, buď a_k kardinální číslo pro každé $k \in K$. Buďte A_k, $k \in K$ po dvou disjunktní množiny takové, že pro každé $k \in K$ platí card $A_k = a_k$. Pak definujeme

$$\sum_{k \in K} a_k := \text{ card } \bigcup_{k \in K} A_k.$$

3.2. Poznámka. Nyní bychom při formálně přesném postupu měli dokázat, že:

(a) pro každý systém a_k, $k \in K$, kardinálních čísel součet $\sum_{k \in K} a_k$ existuje;

(b) tento součet nezávisí na volbě množin A_k, tj. jsou-li A_k, respektive B_k po dvou disjunktní systémy množin takové, že pro každé $k \in K$ platí $A_k \sim B_k$, pak card $\bigcup_{k \in K} A_k =$ $=$ card $\bigcup_{k \in K} B_k$.

Dokázat bod (a) značí dokázat, že když $K \neq \emptyset$ je množina a a_k, $k \in K$, jsou libovolná kardinální čísla, pak existují po dvou disjunktní množiny A_k, $k \in K$, takové, že card $A_k = a_k$

pro každý index $k \in K$. Zvolme tedy libovolné množiny B_k, $k \in K$, tak, že card $B_k = a_k$. Položíme-li $A_k := \{k\} \times B_k$, je zřejmě $A_k \sim B_k$, tj. card $A_k = a_k$ a množiny A_k jsou evidentně po dvou disjunktní.

Tvrzení (b) vyplývá z věty 1.5(4).

Ve shodě s tím, co jsme uvedli již v poznámce 2.3, nebudeme v dalším úvahy tohoto typu opakovat a ponecháme ověření platnosti analogických vztahů u dalších aritmetických operací čtenáři.

3.3. Věta. (Komutativní zákon) *Buď $K \neq \emptyset$ libovolná množina, buď a_k kardinální číslo pro každé $k \in K$. Buď f permutace množiny K. Pak platí*

$$\sum_{k\in K} a_k = \sum_{k\in K} a_{f(k)}.$$

Důkaz. Tvrzení plyne z věty 1.4. •

3.4. Důsledek. *Pro každá dvě kardinální čísla a, b platí*

$$a + b = b + a.$$

Z věty 1.5 okamžitě plyne

3.5. Věta. *Buď $K \neq \emptyset$ libovolná množina, a_k buď kardinální číslo pro každé $k \in K$. Buď $\{K_x;\ x \in X\}$ rozklad množiny K. Pak platí*

$$\sum_{k\in K} a_k = \sum_{x\in X} \sum_{k\in K_x} a_k.$$

3.6. Důsledek. *Pro každá tři kardinální čísla a, b, c platí*

$$(a + b) + c = a + (b + c).$$

3.7. Příklad. (a) Z věty 1.9 plyne, že:

(i) $\aleph_0 + n = \aleph_0$ pro každé konečné kardinální číslo n;

(ii) $\aleph_0 + \aleph_0 = \aleph_0 + \aleph_0 + \aleph_0 = \cdots = \underbrace{\aleph_0 + \aleph_0 + \cdots + \aleph_0 + \ldots}_{\aleph_0\text{–krát}} = \aleph_0$;

(iii) je-li pro každé přirozené číslo n: $1 \leq a_n \leq \aleph_0$, pak $\sum_{n=1}^{\infty} a_n = \aleph_0$, například $1 + 2 + 3 \cdots = \sum_{n=1}^{\infty} n = \aleph_0$.

(b) Je-li $a > \aleph_0$ libovolné, pak pro každé konečné n podle 2.14 platí

$$a + n = a + \aleph_0 = a.$$

3.8. Definice. Buďte a, b libovolná kardinální čísla, A, B buďte libovolné takové množiny, že card $A = a$, card $B = b$. *Součin* kardinálních čísel a, b definujeme takto:

$$a \cdot b := \text{ card } (A \times B).$$

Obecněji: Buď $K \neq \emptyset$ množina, a_k buď kardinální číslo pro každé $k \in K$. Buďte A_k, $k \in K$, libovolné takové množiny, že card $A_k = a_k$ pro každý index $k \in K$. Pak

$$\prod_{k \in K} a_k := \text{ card } \bigotimes_{k \in K} A_k.$$

3.9. Věta. (Komutativní zákon) *Buď' $K \neq \emptyset$, a_k buď'pro každé $k \in K$ kardinální číslo, f buď' permutace množiny K. Pak*

$$\prod_{k \in K} a_k = \prod_{k \in K} a_{f(k)}.$$

Důkaz. Potřebujeme dokázat, že pro libovolný systém množin A_k, $k \in K$ a pro libovolnou bijekci $f\colon K \to K$ platí $\bigotimes_{k \in K} A_k \sim \bigotimes_{k \in K} A_{f(k)}$. Buď $\varphi \in \bigotimes_{k \in K} A_k$ libovolný prvek. Pak je $\varphi\colon K \to \bigcup_{k \in K} A_k$ a platí $\varphi(k) \in A_k$. Je-li $f\colon K \to K$ bijekce, pak pro každé $k \in K$ platí $(\varphi \circ f)(k) = \varphi[f(k)] \in A_{f(k)}$, takže $(\varphi \circ f) \in \bigotimes_{k \in K} A_{f(k)}$. Definujeme-li zobrazení $F\colon \bigotimes_{k \in K} A_k \to$ $\to \bigotimes_{k \in K} A_{f(k)}$ takto: $F(\varphi) = \varphi \circ f$ pro každé $\varphi \in \bigotimes_{k \in K} A_k$, je F zřejmě požadovaná bijekce. •

3.10. Důsledek. *Pro každá dvě kardinální čísla a, b platí*

$$a \cdot b = b \cdot a.$$

3.11. Věta. (Asociativní zákon) *Buďte a_k, $k \in K$ ($\neq \emptyset$), kardinální čísla.*
Buď'$\{K_y;\ y \in Y\}$ rozklad množiny K. Pak platí

$$\prod_{k \in K} a_k = \prod_{y \in Y} \prod_{k \in K_y} a_k.$$

Důkaz. Potřebujeme dokázat, že (při odpovídajícím označení)

$$\bigotimes_{k\in K} A_k \sim \bigotimes_{y\in Y}\bigotimes_{k\in K_y} A_k.$$

Buď tedy $\varphi \in \bigotimes_{k\in K} A_k$ libovolný prvek. Pak je $\varphi\colon K \to \bigcup_{k\in K} A_k$ takové, že pro každý index $k \in K$ platí $f(k) \in A_k$. Pro každé $y \in Y$ nyní položme $\varphi_y := \varphi|K_y$. Definujeme-li zobrazení $\Phi\colon \bigotimes_{k\in K} A_k \to \bigotimes_{y\in Y}\bigotimes_{k\in K_y} A_k$ vztahem $[\Phi(\varphi)](y) = \varphi_y$ pro každé $y \in Y$, je zřejmě Φ potřebná bijekce. •

3.12. Důsledek. *Pro každá tři kardinální čísla a, b, c platí*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Pro praktické počítání s kardinálními čísly je obzvlášť důležitý následující distributivní zákon, který plyne bezprostředně z věty 1.10.

3.13. Věta. (Distributivní zákon) *Buď $A \neq \emptyset$ libovolná množina. Nechť $B_\alpha \neq \emptyset$ je množina pro každé $\alpha \in A$. Pro každé $\alpha \in A$ a každé $\beta \in B_\alpha$ buď $a_{\alpha\beta}$ kardinální číslo. Nechť $\Gamma = \bigotimes_{\alpha\in A} B_\alpha$. Pak platí*

$$\prod_{\alpha\in A}\sum_{\beta\in B_\alpha} a_{\alpha\beta} = \sum_{\gamma\in\Gamma}\prod_{\alpha\in A} a_{\alpha\gamma(\alpha)}.$$

3.14. Důsledek. *Pro každá tři kardinální čísla a, b, c platí*

$$a \cdot (b + c) = a \cdot b + a \cdot c; \qquad (a + b) \cdot c = a \cdot c + b \cdot c.$$

3.15. Věta. *Buď $A \neq \emptyset$ množina,* card $A = a$ *a $b_\alpha = b$ buď kardinální číslo pro každé $\alpha \in A$. Pak platí*

$$\sum_{\alpha\in A} b_\alpha = \sum_{\alpha\in A} b = a \cdot b.$$

Důkaz. Buďte B_α po dvou disjunktní množiny takové, že card $B_\alpha = b$ pro každé $\alpha \in A$. Nechť card $B = b$. Dokážeme, že $\bigcup_{\alpha\in A} B_\alpha \sim (A \times B)$.

Pro každé $\alpha \in A$ existuje podle předpokladu bijekce $f_\alpha\colon B_\alpha \to B$. Pro každý prvek $x \in \bigcup_{\alpha\in A} B_\alpha$ existuje právě jeden index $\alpha_x \in A$ takový, že $x \in B_{\alpha_x}$, neboť množiny B_α jsou po dvou disjunktní. Položíme-li $f(x) = [\alpha_x, f_{\alpha_x}(x)]$, je zřejmě f bijekce množiny $\bigcup_{\alpha\in A} B_\alpha$ na množinu $A \times B$. •

3.16. Příklad.

(a) $1 \cdot a = a$ pro každé kardinální číslo a;

(b) $2 \cdot \aleph_0 = \aleph_0 + \aleph_0 = \aleph_0$;

(c) $n \cdot \aleph_0 = \aleph_0 + \aleph_0 + \cdots + \aleph_0 = \aleph_0$;

(d) $\aleph_0 \cdot \aleph_0 = \aleph_0 + \cdots + \aleph_0 + \cdots = \aleph_0$.

3.17. Poznámka. V příkladu 3.7 jsme viděli, že pro libovolné nekonečné kardinální číslo a a libovolné kardinální číslo $b \leq \aleph_0$ platí

$$a + b = a \ (= \max(a, b)).$$

Podle příkladu 3.16 platí

$$a \cdot \aleph_0 = \aleph_0 \quad (= \max(a, \aleph_0)) \qquad \text{pro každé} \qquad 0 \neq a \leq \aleph_0.$$

V §6 odvodíme , že tyto vztahy jsou speciálním případem tzv. *pohlcovacích zákonů*: pro libovolná dvě kardinální čísla a, b, z nichž *alespoň jedno je nekonečné* (v případě součinu samozřejmě musí být obě nenulová) platí

$$a + b = a \cdot b = \max(a, b).$$

Aritmetika nekonečných kardinálních čísel je proto velmi jednoduchá.

Nyní ještě musíme definovat mocniny kardinálních čísel.

3.18. Definice. Buďte a, b kardinální čísla, A, B buďte takové množiny, že card $A = a$, card $B = b$. Pak definujeme

$$a^b := \text{ card } A^B.$$

První otázkou, kterou nyní musíme rozřešit, je to, zda operace umocňování souvisí „běžným“ způsobem s násobením. Že tomu tak opravdu je, uvidíme v následujícím tvrzení.

3.19. Věta. *Buď B libovolná množina,* card $B = b$. *Budte a_β kardinální čísla pro všechna $\beta \in B$. Jsou-li si všechna čísla a_β navzájem rovna, tj. platí-li $a_\beta = a$ pro všechna $\beta \in B$, pak*

$$\prod_{\beta \in B} a_\beta = \prod_{\beta \in B} a = a^b.$$

Důkaz. Potřebujeme dokázat, že když A_β, $\beta \in B$, jsou takové množiny, že $A_\beta \sim A$ pro všechna $\beta \in B$, pak $\bigotimes_{\beta\in B} A_\beta \sim A^B$.

Buď tedy $f_\beta\colon A \to A_\beta$ bijekce pro každé $\beta \in B$. Pro každé $\varphi \in \bigotimes_{\beta\in B} A_\beta$ buď $F(\varphi)\colon B \to A$ zobrazení definované takto: $\big[F(\varphi)\big](\beta) = f_\beta\big[\varphi(\beta)\big]$ $(= (f_\beta \circ \varphi)(\beta))$. Pak je zřejmě F bijekce $\bigotimes_{\beta\in B} A_\beta$ na A^B. •

3.20. Příklad.

(a) $\aleph_0^2 = \aleph_0 \cdot \aleph_0 = \aleph_0$;

(b) $\aleph_0^n = \aleph_0 \cdot \aleph_0 \ldots \aleph_0 = \aleph_0$ pro každé $1 \le n < \aleph_0$;

(c) $a^0 = 1$ pro každé kardinální číslo a, zejména tedy $0^0 = 1$;

(d) $0^a = 0$ pro každé $a > 0$.

Cantorovu větu 2.7 nyní můžeme přeformulovat takto:

3.21. Věta. *Buďte a, b libovolná kardinální čísla, $a \ge 2$. Pak $a^b > b$.*

Z důkazu věty 2.12 a z věty 3.21 okamžitě plyne

3.22. Věta. *Buď A libovolná množina,* card $A = a$. *Pak* card $\mathcal{P}(A) = 2^a$, *zejména tedy* card $\mathcal{P}(A) >$ card$A$.

3.23. Věta. *Buď $I \neq \emptyset$ libovolná množina, $a, b, c, a_i (i \in I)$ buďte kardinální čísla. Pak platí:*

(1) $a^{\sum a_i} = \prod_{i\in I} a^{a_i}$, *zejména* $a^{b+c} = a^b \cdot a^c$;

(b) $(a^b)^c = a^{b\cdot c}$;

(c) $(\prod_{i\in I} a_i)^b = \prod_{i\in I} a_i^b$, *zejména* $(a \cdot b)^c = a^c \cdot b^c$.

Důkaz. Tvrzení věty plyne bezprostředně z věty 1.5(5) – (7). •

O počítání s nerovnostmi mezi kardinálními čísly nás informuje následující tvrzení.

3.24. Věta. *Buď $A \neq \emptyset$ množina, buďte m_α, n_α taková kardinální čísla, že pro každé $\alpha \in A$ platí $m_\alpha \le n_\alpha$. Pak:*

(1) $\sum_{\alpha\in A} m_\alpha \le \sum_{\alpha\in A} n_\alpha$;

(2) $\prod_{\alpha\in A} m_\alpha \le \prod_{\alpha\in A} n_\alpha$.

Důkaz. (1) Buďte M_α a N_α takové po dvou disjunktní systémy množin, že pro každé $\alpha \in A$ platí card $M_\alpha = m_\alpha$, card $N_\alpha = n_\alpha$. Ze vztahu $m_\alpha \le n_\alpha$ plyne, že $M_\alpha \sim N'_\alpha \subseteq N_\alpha$. Pak ale podle věty 1.5(4) platí $\bigcup_{\alpha\in A} M_\alpha \sim \bigcup_{\alpha\in A} N'_\alpha \subseteq \bigcup_{\alpha\in A} N_\alpha$, tj. $\sum_{\alpha\in A} m_\alpha \le \sum_{\alpha\in A} n_\alpha$.

Tvrzení (2) se dokáže analogicky. •

Z vět 3.24 a 3.19 okamžitě plyne

3.25. Důsledek. *Pro každá kardinální čísla m, n, p platí:*

(1) $n \le p \Rightarrow m^n \le m^p$;

(2) $m \le n \Rightarrow m^p \le n^p$.

3.26. Poznámka. Protože z věty 3.24 zejména plyne, že pro každá kardinální čísla m, n, p taková, že $m \le n$, platí $m + p \le n + p$ a rovněž $m \cdot p \le n \cdot p$, vidíme, že pro počítání s nerovností $\le$ platí v aritmetice kardinálních čísel tatáž pravidla jako v aritmetice čísel přirozených. Je však zřejmé, že **při počítání s ostrou nerovností $<$ analogická pravidla neplatí:** ačkoliv například $2 < 3$, přesto $2 + \aleph_0 = 3 + \aleph_0$ (a nikoliv $2 + \aleph_0 < 3 + \aleph_0$) nebo $5 \cdot \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$ (a nikoliv $5 \cdot \aleph_0 < \aleph_0 \cdot \aleph_0$).

4 Mohutnost kontinua

Odborník je člověk, který úzkostlivě dbá na to,
aby se vyvaroval drobných chyb,
zatím co se nezadržitelně řítí k jednomu velkému omylu.
WEINBERGŮV DŮSLEDEK ALLISONOVY ZÁSADY

Již ve větě 2.10 jsme odvodili, že množina $\mathbb{R}$ všech reálných čísel je nespočetná. Poněvadž číslo card $\mathbb{R}$ hraje v řadě úvah důležitou roli, budeme se jím nyní zabývat podrobněji.

4.1. Definice. Kardinální číslo $\mathbf{c} := 2^{\aleph_0}$ nazýváme *mohutností kontinua*.

Z věty 3.21 víme, že $\mathbf{c} = 2^{\aleph_0} > \aleph_0$. Nyní uvedeme další vlastnosti čísla $\mathbf{c}$.

4.2. Věta. *Buď n libovolné přirozené číslo (tj. $1 \le n < \aleph_0$). Pak platí:*

(1) $n + \mathbf{c} = \aleph_0 + \mathbf{c} = \mathbf{c} + \mathbf{c} = \mathbf{c}$;

(2) $n \cdot \mathbf{c} = \aleph_0 \cdot \mathbf{c} = \mathbf{c} \cdot \mathbf{c} = \mathbf{c}$;

(3) $\mathbf{c}^n = \mathbf{c}$*;*

(4) *pro* $n > 1$ *platí* $n^{\aleph_0} = \aleph_0^{\aleph_0} = \mathbf{c}^{\aleph_0} = \mathbf{c}$.

Důkaz.
(1) Platí: $\mathbf{c} \le n + \mathbf{c} \le \aleph_0 + \mathbf{c} \le \mathbf{c} + \mathbf{c} = 2 \cdot \mathbf{c} = 2 \cdot 2^{\aleph_0} = 2^{1+\aleph_0} = 2^{\aleph_0} = \mathbf{c}$.
(2) Platí: $\mathbf{c} \le n \cdot \mathbf{c} \le \aleph_0 \cdot \mathbf{c} \le \mathbf{c} \cdot \mathbf{c} = 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0+\aleph_0} = 2^{\aleph_0} = \mathbf{c}$.
(3) Plyne indukcí z (2).
(4) $\mathbf{c} = 2^{\aleph_0} \le n^{\aleph_0} \le \aleph_0^{\aleph_0} \le \mathbf{c}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = \mathbf{c}$. •

4.3. Věta. *Následující množiny mají mohutnost kontinua:*

(a) množina $\mathbb{R}$ *všech reálných čísel;*

(b) interval $(0, 1)$*;*

(c) každý (netriviální) interval reálných čísel;

(d) množina všech iracionálních čísel;

(e) množina všech transcendentních čísel;

(f) množina všech posloupností přirozených čísel;

(g) množina $\mathbb{R}^n$ *(n přirozené) všech uspořádaných n-tic reálných čísel;*

(h) množina $\mathcal{P}(\mathbb{N})$ *všech podmnožin množiny přirozených čísel.*

Důkaz. Dokážeme nejprve, že card $(0, 1) = \mathbf{c}$.

Podle věty 4.2(4) je $10^{\aleph_0} = \mathbf{c}$. Podle definice mocniny kardinálních čísel je $10^{\aleph_0} = \text{card } A^{\mathbb{N}}$, kde card $A = 10$. Zvolíme-li $A = \{0, 1, 2, \ldots, 9\}$, je $F = A^{\mathbb{N}}$ množina všech posloupností utvořených z cifer $0, 1, \ldots, 9$. Označme G množinu těch posloupností, v nichž se od jistého indexu počínaje opakuje pouze devítka, tj.

$$G = \left\{ f \in F;\ \ f = (a_n)_{n=1}^{\infty},\ \text{existuje } k \in \mathbb{N} \text{ tak, že } a_i = 9 \text{ pro všechna } i \ge k \right\}.$$

Podle věty 1.15 je G spočetná, takže podle věty 2.13 platí card $(F - G) = \text{card} F = \mathbf{c}$. Přiřadíme-li nyní každému prvku $f = (a_n)_{n=1}^{\infty} \in F - G$ číslo $0, a_1 a_2 \ldots a_n \ldots$, obdržíme zřejmě bijekci množiny $F - G$ na interval $(0, 1)$. Dokázali jsme tak, že card $(0, 1) = \mathbf{c}$.

Z důsledku 2.10 okamžitě plyne, že i card $\mathbb{R} = \mathbf{c}$.

Vzhledem k tomu, že card $\mathbb{Q} = \aleph_0$ (důsledek 1.14) a rovněž množina algebraických čísel je spočetná (poznámka 1.17), plyne z předchozího okamžitě tvrzení (d) i (e). Tvrzení (c) plyne z příkladu 1.3(b). (Uvědomme si, že podle věty 4.2 na mohutnost intervalu reálných čísel nemá vliv, zda koncové body do tohoto intervalu patří či nikoliv.)

Množina všech posloupností přirozených čísel je množina $\mathbb{N}^{\mathbb{N}}$. Její mohutnost $\aleph_0^{\aleph_0}$ je však **c** podle věty 4.2(4), tj. platí (f).

Tvrzení (g) plyne z věty 4.2(3), tvrzení (h) z věty 3.22. •

4.4. Příklad. V příkladu 3.7(iii) jsme odvodili, že

$$1 + 2 + 3 + \cdots = \sum_{n\in\mathbb{N}} n = \aleph_0.$$

Nyní ukážeme, že

$$\prod_{n\in\mathbb{N}} n = 1 \cdot 2 \cdot 3 \cdot \cdots = \mathbf{c}.$$

Platí totiž

$$1 \cdot 2 \cdot 3 \cdot \ldots \le \underbrace{\aleph_0 \cdot \aleph_0 \cdot \aleph_0 \cdot \ldots}_{\aleph_0\text{–krát}} = \aleph_0^{\aleph_0} = \mathbf{c},$$

avšak současně

$$1 \cdot 2 \cdot 3 \cdot \cdots = 2 \cdot 3 \cdot 4 \cdot \ldots \ge \underbrace{2 \cdot 2 \cdot 2 \cdot \ldots}_{\aleph_0\text{–krát}} = 2^{\aleph_0} = \mathbf{c}.$$

4.5. Poznámka. Jak jsme uvedli již v §2, systém všech kardinálních čísel tvoří vlastní třídu. (Toto tvrzení dokážeme v §6, důsledek 6.15.) V definici 2.2 jsme na této třídě definovali uspořádání a z věty 2.5 víme, že vzhledem k tomuto uspořádání tvoří každá množina kardinálních čísel řetězec. Víme například, že $\aleph_0$ je nejmenší nekonečné kardinální číslo (poznámka 2.6) a že ke každému kardinálnímu číslu existuje číslo větší (poznámka 2.8), avšak prakticky žádné další informace o struktuře řetězce kardinálních čísel nemáme. Víme například, že $\aleph_0 < 2^{\aleph_0}$, nevíme však, existuje-li kardinální číslo m takové, že $\aleph_0 < m < 2^{\aleph_0}$. (Předpoklad, že takové číslo m *neexistuje*, tzv. *hypotéza kontinua*, patří k nejznámějším matematickým problémům 20. století. O jeho vyřešení viz poznámku 6.23.) V této chvíli neumíme ani rozhodnout, zda má každé kardinální číslo svého bezprostředního následníka či nikoliv.

Tyto a další informace získáme pomocí tzv. *ordinálních čísel*.

Cvičení k §4

Hlavní příčinou problémů
jsou jejich řešení.
SEVAREIDŮV ZÁKON

1. Dokažte, že když je $2^a \ge \aleph_0$, pak je $2^a \ge c$.

2. Dokažte následující tvrzení: *Množina všech spojitých funkcí* $f\colon \mathbb{R} \to \mathbb{R}$ *má mohutnost kontinua*.

(Návod: Buď $(a_n)_{n=1}^{\infty}$ posloupnost všech racionálních čísel. Přiřaďte každé spojité funkci $f\colon \mathbb{R} \to \mathbb{R}$ posloupnost $(f(a_n))_{n=1}^{\infty}$. Dokažte, že $f \neq g$ právě tehdy, když $(f(a_n)) \neq (g(a_n))$. Tvrzení pak lze již snadno odvodit.)

3. Dokažte, že množina všech funkcí $f\colon \mathbb{R} \to \mathbb{R}$ má mohutnost $2^{\mathfrak{c}}$.

5 Ordinální typy a ordinální čísla

Pokrok neznamená,
že se chybná teorie nahradí správnou.
Pokrok spočívá v tom, že se chybná teorie nahradí takovou,
na které to není tolik znát.
HAWKINSOVA TEORIE POKROKU

V §1 jsme každé množině A přiřadili její kardinální číslo. Nyní analogicky každé *uspořádané* množině přiřadíme její *ordinální typ*. Tak jako podstata kardinálních čísel spočívala v tom, že $\operatorname{card} A = \operatorname{card} B$ právě tehdy, když $A \sim B$, spočívá smysl ordinálních typů ve skutečnosti, že stejný ordinální typ mají právě jen izomorfní uspořádané množiny.

5.1. Definice. Řekneme, že uspořádané množiny A, B mají stejný *ordinální typ* a píšeme $\overline{A} = \overline{B}$, je-li $A \cong B$.

5.2. Poznámka. Pro ordinální typy některých často se vyskytujících množin je výhodné zavést si standardní označení. Tak například ordinální typ prázdné množiny značíme symbolem 0, ordinální typ řetězce o n prvcích (n libovolné přirozené) značíme symbolem n, ordinální typ množiny $\mathbb{N}$ všech přirozených čísel s obvyklým uspořádáním značíme ω, ordinální typ množiny $\mathbb{N}^*$ značíme ω^* a podobně[1]. (Značíme tedy stejnými symboly konečná kardinální čísla i ordinální typy konečných řetězců. K omylu však v dalším nedojde, neboť z kontextu bude vždy zřejmé, v jakém významu budeme těchto symbolů užívat.)

[1] Připomeňme, že pro uspořádanou množinu A značí A^* množinu uspořádanou *duálně*, tj. $(A, \leq)^* = (A, \geq)$. Typ ω^* má tedy například množina všech celých záporných čísel s obvyklým uspořádáním.

Z definice izomorfismu také plyne, že když $\overline{A} = \overline{B}$, pak také card A = card B (pozor: ne naopak!). Má tedy smysl mluvit o mohutnosti daného ordinálního typu. (Například typy ω i ω^* mají mohutnost $\aleph_0$.)

Pomocí aritmetických operací mezi uspořádanými množinami, které jsme definovali v kapitole II, §3, nyní snadno zavedeme aritmetické operace mezi ordinálními typy.

Poznamenejme ještě, že zápisem $\overline{A} = \alpha$ rozumíme fakt, že ordinální typ uspořádané množiny A jsme označili symbolem α (například $\overline{\mathbb{N}} = \omega$).

5.3. Definice. Buďte α, β ordinální typy. Zvolme disjunktní uspořádané množiny A, B tak, že $\overline{A} = \alpha$, $\overline{B} = \beta$. Pak *součet* typů α, β definujeme vztahem:

$$\alpha + \beta := \overline{A + B}.$$

Obecněji: Buď $I \neq \emptyset$ uspořádaná množina, buď α_i ordinální typ pro každé $i \in I$. Buďte A_i, $i \in I$, po dvou disjunktní uspořádané množiny takové, že $\overline{A_i} = \alpha_i$ pro každé $i \in I$. Pak definujeme

$$\sum_{i \in I} \alpha_i := \overline{\sum_{i \in I} A_i}.$$

5.4. Poznámka. Podobně jako u početních operací s kardinálními čísly i operace mezi ordinálními typy definujeme pomocí množin o příslušných ordinálních typech. U každé operace je pak ale nutno dokázat, že výsledek nezávisí na konkrétní volbě těchto množin. K definici 5.3 je tedy nutno dokázat, že když A_i, B_i, $i \in I$ jsou po dvou disjunktní systémy uspořádaných množina takové, že $A_i \cong B_i$ (tj. $\overline{A_i} = \overline{B_i}$) pro každé $i \in I$, pak také $\sum_{i \in I} A_i \cong \sum_{i \in I} B_i$. Důkaz tohoto tvrzení je však jednoduchý a proto ho přenecháme čtenáři. V dalším pak již úvahy tohoto typu nebudeme opakovat.

Z věty 3.11 v II. kapitole okamžitě plyne:

5.5. Věta. (Asociativní zákon) *Buď $I \neq \emptyset$ uspořádaná množina, buď α_i ordinální typ pro každé $i \in I$. Nechť $I = \sum_{k \in K} I_k$. Pak platí*

$$\sum_{i \in I} \alpha_i = \sum_{k \in K} \sum_{i \in I_k} \alpha_i.$$

5.6. Důsledek. *Buďte α, β, γ libovolné ordinální typy. Pak platí*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma).$$

5.7. Poznámka. Z příkladu 3.3 v II. kapitole plyne, že sečítání ordinálních typů obecně není komutativní.

5.8. Příklad.

(a) $\omega + 1 \neq 1 + \omega$, neboť je zřejmé, že $1 + \omega = \omega$ avšak $\omega + 1 \neq \omega$;

(b) $1 + 2 + 3 + \cdots + n + \cdots = \omega$.

5.9. Definice. Buďte α, β libovolné ordinální typy. Buďte A, B libovolné uspořádané množiny takové, že $\overline{A} = \alpha$, $\overline{B} = \beta$. Pak definujeme

$$\alpha \cdot \beta := \overline{A \cdot B}.$$

Z věty 3.13 v II. kapitole plyne

5.10. Věta. *Buďte α, β, γ libovolné ordinální typy. Pak platí*

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma).$$

Z věty 3.14 v II. kapitole plyne levý distributivní zákon.

5.11. Věta. *Buď $I \neq \emptyset$ uspořádaná množina, buď α_i ordinální typ pro každé $i \in I$. Pak pro libovolný ordinální typ α platí*

$$\alpha \cdot \sum_{i \in I} \alpha_i = \sum_{i \in I} (\alpha \cdot \alpha_i).$$

5.12. Důsledek. *Buďte α, β, γ libovolné ordinální typy. Pak platí*

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

5.13. Věta. *Buď $I \neq \emptyset$ uspořádaná množina, $\overline{I} = \beta$. Buď $\alpha_i = \alpha$ ordinální typ pro každé $i \in I$. Pak platí*

$$\sum_{i \in I} \alpha_i = \sum_{i \in I} \alpha = \alpha \cdot \beta.$$

Důkaz plyne z věty 3.17 v II. kapitole. •

5.14. Příklad.

(a) $2 \cdot \omega = 2 + 2 + 2 + \cdots + 2 + \cdots = \omega$;

(b) $\omega \cdot 2 = \omega + \omega \neq \omega$;

(c) $\omega \cdot \omega = \omega + \omega + \omega + \cdots + \omega + \ldots$.

5.15. Definice. Buď α libovolný ordinální typ. Mocninu s konečným exponentem definujeme indukcí takto:

$$\alpha^0 = 1, \qquad a^{n+1} = \alpha^n \cdot \alpha.$$

5.16. Příklad. (a) $\omega^2 = \omega \cdot \omega = \omega + \omega + \cdots + \omega + \ldots$
(b) $\omega + \omega^2 = \omega(1 + \omega) = \omega \cdot \omega = \omega^2$
(c) $\omega^2 + \omega = \omega \cdot (\omega + 1) \neq \omega^2$
(d) $(\omega + \omega) \cdot \omega = (\omega \cdot 2) \cdot \omega = \omega \cdot (2 \cdot \omega) = \omega^2$
(e) $\omega \cdot (\omega + \omega) = \omega \cdot (\omega \cdot 2) = (\omega \cdot \omega) \cdot 2 = \omega^2 + \omega^2$

Uvědomme si, že všechny ordinální typy v příkladu 5.16 jsou spočetné.

5.17. Definice. Ordinální typ dobře uspořádané množiny se nazývá *ordinální číslo*.

5.18. Příklad. 0, 1, 2, 3, . . . , ω, $\omega + 1$, $\omega + 2$, $\omega + \omega$ atd. jsou ordinální čísla, ω^* není ordinální číslo, $\overline{\mathbb{R}}$ není ordinální číslo atd.

Z věty 3.18 v kapitole II. plyne

5.19. Věta. *Buď $I \neq \emptyset$ dobře uspořádaná množina, buď α_i ordinální číslo pro každé $i \in I$. Pak je $\sum_{i \in I} \alpha_i$ ordinální číslo.*

Z vět 3.19 a 3.20 v II. kapitole plyne

5.20. Věta. *Buďte α, β libovolná ordinální čísla. Pak jsou $\alpha + \beta$, $\alpha \cdot \beta$ rovněž ordinální čísla.*

Nyní budeme definovat mezi ordinálními čísly *nerovnost*.

5.21. Definice. Buďte α, β ordinální čísla. Nechť A, B jsou takové uspořádané množiny, že $\overline{A} = \alpha$, $\overline{B} = \beta$. Pak definujeme $\alpha < \beta$ právě tehdy, když existuje $x \in B$ tak, že $A \cong B(x)$. Je-li $\alpha < \beta$ nebo $\alpha = \beta$, píšeme $\alpha \leq \beta$.

5.22. Věta. *Buď $\mathcal{A}$ libovolná množina ordinálních čísel. Pak je $(\mathcal{A}, \leq)$ řetězec.*

Důkaz. Je zřejmé, že relace $\leq$ je reflexivní a tranzitivní. Antisymetrická je podle věty 2.7, úplnost plyne z věty 2.13. •

5.23. Poznámka. Později uvidíme, že podobně jako kardinální čísla tvoří i všechna ordinální čísla vlastní třídu. (Viz §6.)

5.24. Definice. Buď α libovolné ordinální číslo. Symbolem $W(\alpha)$ označíme množinu všech ordinálních čísel β takových, že $\beta < \alpha$.

5.25. Příklad.

$W(0) = \emptyset$	$\overline{W(0)} = \overline{\emptyset} = 0$
$W(1) = \{0\}$	$\overline{W(1)} = \overline{\{0\}} = 1$
$W(2) = \{0, 1\}$	$\overline{W(2)} = \overline{\{0, 1\}} = 2$
$W(\omega) = \{0,1, 2, \dots\}$	$\overline{W(\omega)} = \omega$

To, co naznačují uvedené příklady, dokážeme zcela obecně.

5.26. Věta. *Buď α libovolné ordinální číslo. Pak platí*

$$\overline{W(\alpha)} = \alpha,$$

tj. $W(\alpha)$ je dobře uspořádaná množina a má typ α.

Důkaz. Buď α ordinální číslo, A taková uspořádaná množina, že $\overline{A} = \alpha$. Pro každé $x \in A$ označme $\varphi(x)$ ordinální typ množiny $A(x)$. Pak je zřejmě $\varphi\colon A \to W(\alpha)$. Dokážeme, že φ je izomorfismus.

Buď $\beta \in W(\alpha)$ libovolné ordinální číslo. Pak je $\beta < \alpha$. Podle definice 6.7 existuje ke každé množině B, $\overline{B} = \beta$, prvek $x \in A$ takový, že $B \cong A(x)$, tj. $\beta = \varphi(x)$. Je tedy φ surjekce.

Pro $x, y \in A$, $x < y$ je zřejmě $\overline{A(x)} < \overline{A(y)}$, tj. $\varphi(x) < \varphi(y)$, takže φ je izotonní injekce. Pak je $\varphi^{-1}\colon W(\alpha) \to A$ zřejmě také izotonní, takže φ je izomorfismus. •

5.27. Věta. *Každá množina ordinálních čísel je dobře uspořádaná.*

Důkaz. Buď M libovolná množina ordinálních čísel, $N \neq \emptyset$ její libovolná podmnožina. Zvolme $\alpha \in N$ libovolně. Není-li α nejmenší prvek množiny N, je $P = N \cap W(\alpha) \neq \emptyset$. Protože je $\emptyset \neq P \subseteq W(\alpha)$, obsahuje množina P podle věty 5.26 nejmenší prvek β. Je však zřejmé, že β je nejmenší prvek množiny N, takže množina M je dobře uspořádaná. •

5.28. Poznámka. Buď $M \neq \emptyset$ libovolná množina ordinálních čísel. Podle věty 5.27 je $\overline{M} = \mu$ ordinální číslo. Podle věty 5.26 platí $\overline{W(\mu)} = \mu$, tj. $W(\mu) \cong M$. Podle věty 2.11 existuje právě jeden izomorfismus $f\colon M \to W(\mu)$. Tzn., že množinu M lze jednoznačně psát jako řetězec

$$M = \{\alpha_0 < \alpha_1 < \dots < \alpha_\xi < \dots\}_{\xi<\mu}.$$

5.29. Věta. *Každé ordinální číslo α má svého bezprostředního následovníka, kterým je číslo $\alpha + 1$.*

Důkaz. Nechť $\overline{A} = \alpha$. Buď $b \notin A$ libovolný prvek (například $\{A\}$). Položme $B = A + \{b\}$. Pak $\overline{B} = \alpha + 1$. Protože $A \cong B(b)$, platí $\alpha < \alpha + 1$. Buď nyní $\beta < \alpha + 1$ libovolné ordinální číslo. Podle definice uspořádání je β typ některého začátku množiny B, takže zřejmě platí $\beta \leq \alpha$. Neexistuje tedy β takové, že $\alpha < \beta < \alpha + 1$. •

Z věty 5.29 neplyne, že by každé ordinální číslo muselo mít svého bezprostředního předchůdce! (Víme, že bezprostředního předchůdce nemá například číslo ω). Má tedy smysl následující definice:

5.30. Definice. Ordinální číslo, které má bezprostředního předchůdce, se nazývá *izolované*. Číslo, které není izolované, se nazývá *limitní*.

5.31. Příklad. Čísla $1, 2, \ldots, n, \omega + 1, \omega + 2, \ldots, \omega + \omega + 1$ jsou izolovaná, čísla $0, \omega, \omega \cdot 2, \ldots, \omega \cdot n$ jsou limitní.

5.32. Věta. *Buďte α, β, γ libovolná ordinální čísla. Pak platí:*

(1) $\alpha < \beta \Rightarrow \gamma + \alpha < \gamma + \beta$;

(2) $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$.

Důkaz. (1) Buďte A, B, C po dvou disjunktní uspořádané množiny, $\overline{A} = \alpha$, $\overline{B} = \beta$, $\overline{C} = \gamma$. Protože je $\alpha < \beta$, existuje $x \in B$ takový, že $A \cong B(x)$. Označme $C + A = D$, $C + B = E$. Pak je zřejmě $D \cong E(x)$, tj. $\gamma + \alpha < \gamma + \beta$.

(2) Je-li $\alpha = \beta$, je $\alpha + \gamma = \beta + \gamma$, tj. $\alpha + \gamma \leq \beta + \gamma$. Nechť tedy $\alpha < \beta$. Nechť A, B, C jsou množiny s vlastnostmi jako v (1). Protože $A \cong B(x)$ pro vhodný prvek x, existuje izomorfismus $A + C$ do $B + C$. Tvrzení je nyní zřejmé. •

5.33. Důsledek. *Buďte α, β libovolná ordinální čísla. Pak platí:*

(1) *je-li $\beta \neq 0$, pak $\alpha + \beta > \alpha$;*

(2) $\alpha + \beta \geq \beta$.

Důkaz. (1) Je-li $\beta > 0$, je podle věty 5.32(1) $\alpha + 0 < \alpha + \beta$, tj. $\alpha < \alpha + \beta$.

(2) Protože $0 \leq \alpha$, je $0 + \beta \leq \alpha + \beta$, tj. $\beta \leq \alpha + \beta$ podle věty 4.2(2). •

5.34. Věta. *Buď' $M \neq \emptyset$ množina ordinálních čísel neobsahující největší prvek. Nechť' $M = \{\alpha_0 < \alpha_1 < \cdots < \alpha_\xi < \ldots\}_{\xi < \overline{M}}$. Pak pro každý prvek $\alpha_\varrho \in M$ platí*

$$\alpha_\varrho < \sum_{\xi < \overline{M}} \alpha_\xi .$$

Důkaz. Připusťme, že existuje $\alpha_\varrho \in M$ takový, že $\alpha_\varrho \geq \sum_{\xi<\overline{M}} \alpha_\xi$. Protože α_ϱ není největší prvek v M, existuje $\alpha_{\varrho+1} \in M$, $\alpha_{\varrho+1} > \alpha_\varrho \geq \sum_{\xi<\overline{M}} \alpha_\xi$. Buďte A_ξ, $\xi < \overline{M}$, po dvou disjunktní uspořádané množiny takové, že pro každé $\xi < \overline{M}$ platí $\overline{A_\xi} = \alpha_\xi$. Označme $A = \sum_{\xi<\overline{M}} A_\xi$. Protože $\sum_{\xi<\overline{M}} \alpha_\xi < \alpha_{\varrho+1}$, existuje $x \in A_{\varrho+1}$ takový, že $A \cong A_{\varrho+1}(x)$. Protože $A_{\varrho+1} \subset A$, plyne odtud, že $A_{\varrho+1}$ je izomorfní s vlastní podmnožinou svého vlastního začátku, což je spor s větou 2.7. •

V definici 5.15 jsme definovali mocninu libovolného ordinálního typu v případě, že exponentem bylo konečné ordinální číslo. Transfinitní indukcí nyní tuto definici zobecníme.

5.35. Definice. Buď α libovolné ordinální číslo. Pak definujeme:

1. $\alpha^0 = 1$;
2. $\alpha^{\xi+1} = \alpha^\xi \cdot \alpha$;
3. $\alpha^\xi = \sum_{\varrho<\xi} \alpha^\varrho$ pro $\xi \neq 0$ limitní.

5.36. Příklad. $\omega^\omega = \sum_{\varrho<\omega} \omega^\varrho = 1 + \omega + \omega^2 + \dots$.

Z věty 5.34 okamžitě plyne, že pro každé přirozené n platí $\omega^n < \omega^\omega$. Dále víme, že ω^n je spočetný ordinální typ, takže i ω^ω je spočetný ordinální typ.

6 Třída všech ordinálních čísel. Alefy

Po složitém řešení vždy přichází
jednoduché vysvětlení.
LUNSFORDOVO PRAVIDLO

6.1. Věta. *Buď $M \neq \emptyset$ libovolná množina ordinálních čísel. Pak existuje ordinální číslo α takové, že pro každý prvek $\varrho \in M$ platí $\varrho < \alpha$.*

Důkaz. Obsahuje-li M největší prvek ξ, stačí položit $\alpha = \xi + 1$. Nechť tedy M neobsahuje největší prvek. Podle poznámky 5.28 lze psát

$$M = \{\alpha_0 < \dots < \alpha_\xi < \dots\}_{\xi<\overline{M}}$$

a podle věty 5.34 stačí položit $\alpha = \sum_{\xi<\overline{M}} \alpha_\xi$. •

6.2. Důsledek. *Neexistuje množina všech ordinálních čísel (tj. třída všech ordinálních čísel je vlastní).*

Důkaz. Připusťme, že existuje množina M všech ordinálních čísel. Podle 6.1 existuje ordinální číslo α takové, že $\alpha > \xi$ pro každé $\xi \in M$. Protože však $\alpha \in M$, plyne odtud $\alpha > \alpha$: spor. •

6.3. Věta. *Buď M libovolná množina ordinálních čísel. Pak mezi ordinálními čísly, která nepatří do M, existuje nejmenší.*

Důkaz. Podle věty 6.1 existuje ordinální číslo $\alpha \notin M$. Pokud α není nejmenší číslo nepatřící do M, je $W(\alpha) - M \neq \emptyset$. Hledaný prvek je nyní nejmenší prvek množiny $W(\alpha) - M$. •

6.4. Poznámka. Je-li m konečné kardinální číslo, existuje právě jedno ordinální číslo mohutnosti m. Pro nekonečné kardinální číslo je však situace nepoměrně složitější. Podívejme se například, jak vypadá množina Z_1 všech spočetných ordinálních čísel.

Nejmenším prvkem množiny Z_1 je prvek ω. Je-li totiž α ordinální číslo, $\alpha < \omega$, je α typ množiny izomorfní s některou množinou $\mathbb{N}(x)$, $x \in \mathbb{N}$, takže α je konečné ordinální číslo.

Když využijeme odvozených vlastností aritmetických operací mezi ordinálními čísly, vidíme, že množina Z_1 vypadá následovně (čtenář nechť si promyslí, že všechna uváděná ordinální čísla jsou opravdu spočetná):

$\omega,\ \omega+1,\ \omega+2,\ \ldots,\ \omega+n,\ldots,\ \omega+\omega=\omega\cdot 2,\ \omega\cdot 2+1,\ \ldots,\ \omega\cdot 2+n,\ \ldots,$
$\omega\cdot 2+\omega=\omega\cdot 3,\ \ldots,\ \omega\cdot 4,\ \ldots,\ \omega\cdot n,\ \ldots,\ \omega\cdot\omega=\omega^2,\ \omega^2+1,\ \ldots,\ \omega^2+n,\ldots\omega^2+\omega,$
$\omega^2+\omega+1,\ \ldots,\ \omega^2+\omega+\omega=\omega^2+\omega\cdot 2,\ \omega^2+\omega\cdot 2+1,\ \ldots,\ \omega^2+\omega\cdot 2+\omega=\omega^2+\omega\cdot 3,\ \ldots,$
$\omega^2+\omega\cdot 4,\ldots,\omega^2+\omega\cdot\omega=\omega^2+\omega^2=\omega^2\cdot 2,\omega^2\cdot 2+1,\ldots,\omega^2\cdot 2+\omega,\ldots,\omega^2\cdot 2+\omega+\omega=\omega^2\cdot 2+\omega\cdot 2,$
$\ldots,\omega^2\cdot 2+\omega\cdot 3,\ldots,\omega^2\cdot 2+\omega^2=\omega^2\cdot 3,\ldots,\omega^2\cdot 4,\ldots,\omega^2\cdot\omega=\omega^3,\omega^3+1,\ldots,\omega^3+\omega,\ldots,$
$\omega^3+\omega\cdot 2,\ldots,\omega^3+\omega\cdot 3,\ldots,\omega^3+\omega^2,\ldots,\omega^3+\omega^2+\omega,\ldots,\omega^3+\omega^2+\omega\cdot 2,\ldots,\omega^3+\omega^2\cdot 2,$
$\ldots,\omega^3+\omega^2\cdot 3,\ldots,\omega^3+\omega^3=\omega^3\cdot 2,\ldots,\omega^3\cdot 3,\ldots,\omega^3\cdot\omega=\omega^4,\ldots,\omega^5,\ldots,\omega^6,\ldots,$
$\omega^\omega=\sum_{n<\omega}\omega^n,\omega^\omega+1,\ldots,\omega^\omega+\omega,\ldots,\omega^\omega+\omega\cdot 2,\ldots,\omega^\omega+\omega\cdot\omega=\omega^\omega+\omega^2,\ldots,\omega^\omega+\omega^2+\omega,$
$\ldots,\omega^\omega+\omega^2+\omega\cdot 2,\ldots,\omega^\omega+\omega^2+\omega\cdot 3,\ldots,\omega^\omega+\omega^2\cdot 2,\ldots,\omega^\omega+\omega^3,\ldots,\omega^\omega+\omega^\omega=\omega^\omega\cdot 2,$
$\ldots,\omega^\omega\cdot 3,\ \omega^\omega\cdot 3+1,\ \omega^\omega\cdot 3+2,\ \ldots,\ \omega^\omega\cdot 3+\omega,\ \ldots,\ \omega^\omega\cdot 3+\omega\cdot 2,\ldots,\omega^\omega\cdot 3+\omega^2,\ \ldots,$
$\omega^\omega\cdot 4,\ldots,\omega^\omega\cdot\omega=\omega^{\omega+1},\ldots,\omega^{\omega+1}\cdot 2,\ldots,\omega^{\omega+2},\ldots,\omega^{\omega+3},\ldots,\omega^{\omega+\omega}=\omega^{\omega\cdot 2},\ldots,\omega^{\omega\cdot\omega}=\omega^{\omega^2},$
$\ldots,\omega^{\omega^3},\ldots,\omega^{\omega^4},\ldots,\omega^{\omega^\omega},\ldots,\omega^{\omega^{\omega^\omega}},\ldots,\omega^{\omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}}:=\omega^\omega+\omega^{\omega^\omega}+\omega^{\omega^{\omega^\omega}}+\cdots+\omega^{\omega^{\cdot^{\cdot^{\cdot^{\omega}}}}}+\cdots=:\varepsilon,$
$\varepsilon+1,\ \varepsilon+2,\ \ldots,\ \varepsilon+\omega,\ \ldots$ atd., atd.

Nyní je samozřejmá otázka, zda je množina Z_1 spočetná nebo nespočetná. Najít odpověď na tuto otázku je však velmi jednoduché. Podle Zermelovy věty 4.7 existují nespočetné dobře uspořádané množiny, tj. existují nespočetná ordinální čísla. Podle věty 6.3 existuje *nejmenší* nespočetné ordinální číslo; označme toto číslo ω_1. Podle věty 5.26 je $\overline{W(\omega_1)} = \omega_1$, takže $W(\omega_1) = \{0\} \cup \mathbb{N} \cup Z_1$ je nespočetná. Protože $\mathbb{N}$ je spočetná, je Z_1 nutně nespočetná. Číslo $\operatorname{card} Z_1 \neq \aleph_0$ označme $\aleph_1$.

Nyní zobecníme postup, který jsme prováděli pro kardinální číslo $\aleph_0$.

6.5. Definice. Buď m libovolné nekonečné kardinální číslo. Označme $Z(m)$ množinu všech ordinálních čísel mohutnosti m. Nejmenší prvek množiny $Z(m)$ označme $\omega(m)$. Číslo $\omega(m)$ nazýváme *počáteční ordinální číslo mohutnosti* m.

6.6. Poznámka. Uvědomme si, že definice 6.5 je naprosto regulérní. Z Zermelovy věty 4.7 plyne, že $Z(m)$ je vždy neprázdná množina. Zvolíme-li totiž libovolné nekonečné kardinální číslo m a libovolnou množinu M této mohutnosti, existuje podle Zermelovy věty 4.7 na této množině dobré uspořádání. Ordinální typ takto vzniklé uspořádané množiny je tedy **ordinální číslo** zvolené mohutnosti m, takže existují ordinální čísla každé mohutnosti. Existence čísla $\omega(m)$ plyne z věty 5.27. Číslo $\omega(m)$ *je přitom vždy limitní*. Kdyby totiž platilo $\omega(m) = \alpha + 1$ pro některé α, bylo by $\alpha \in Z(m)$, $\alpha < \omega(m)$, což není možné.

6.7. Věta. *Buď m libovolné nekonečné kardinální číslo. Pak je $\overline{Z(m)}$ limitní ordinální číslo.*

Důkaz. Označme $\xi = \overline{Z(m)}$. Podle věty 5.27 je ξ ordinální číslo. Množina $Z(m)$ neobsahuje největší prvek, neboť $\alpha \in Z(m) \Rightarrow \alpha+1 \in Z(m)$. Odtud však plyne, že $Z(m) \subset \bigcup_{\alpha \in Z(m)} W(\alpha) = W$. Je-li $\beta \in W$ libovolný prvek a $\gamma \leq \beta$ libovolné ordinální číslo, je také $\gamma \in W$ (neboť $\beta \in W(\alpha) \Rightarrow \gamma \in W(\alpha) \subseteq W$). To znamená, že $W = W(\varrho)$, kde ϱ je nejmenší ordinální číslo takové, že $\varrho \notin W$. Podle věty 5.26 platí $\overline{W(\varrho)} = \varrho$, tj. $\overline{W} = \varrho$ a číslo ϱ je limitní ordinální číslo podle poznámky 6.6. Nyní však platí

$$W = W(\varrho) = W\big[\omega(m)\big] + Z(m),$$

tj. $\varrho = \omega(m) + \xi$. Protože je ϱ limitní, je nutně i ξ limitní. (Kdyby totiž platilo $\xi = \zeta + 1$, platilo by $\varrho = \omega(m) + (\zeta + 1) = (\omega(m) + \zeta) + 1$ a ϱ by nebylo limitní.) •

6.8. Definice. Buď m libovolné nekonečné kardinální číslo. Označme

$$A(m) := \{\omega(n);\ \aleph_0 \leq n < m\}.$$

Nechť $\overline{A(m)} = \alpha$. Pak číslo $\omega(m)$ označíme ω_α a kardinální číslo m označíme $\aleph_\alpha$.

6.9. Poznámka. Protože je $A(m)$ množina ordinálních čísel, je dobře uspořádaná, tj. $\overline{A(m)} = \alpha$ je ordinální číslo. Protože $\overline{W(\alpha)} = \alpha$, je $A(m) \cong W(\alpha)$. Platí například

$$A(\aleph_0) = \{\omega(n);\ \aleph_0 \leq n < \aleph_0\} = \emptyset,$$

tj. $\overline{A(\aleph_0)} = 0$. Nejmenší ordinální číslo o mohutnosti $\aleph_0$, tj. číslo ω, máme tedy podle 6.8 označit ω_0. Značení čísla $\aleph_0$ je přitom ve shodě s touto definicí.

Z definic 6.5 a 6.8 okamžitě plyne následující tvrzení:

6.10. Věta. *Každé nekonečné číslo je některým alefem.*

Z uvedené konstrukce plyne, že každé počáteční ordinální číslo i každá mohutnost je ω_α, respektive $\aleph_\alpha$, kde α je nějaké ordinální číslo. Nyní postupně ukážeme, že naopak každé ordinální číslo je indexem některého počátečního ordinálního čísla a tedy i některého alefu.

6.11. Věta. *Budťe ω_α, ω_β libovolná počáteční ordinální čísla. Pak $\omega_\alpha < \omega_\beta$ právě tehdy, když $\alpha < \beta$.*

Důkaz. Podle poznámky 6.9 platí $A(m) \cong W(\alpha)$, kde $\alpha = \overline{A(m)}$, $A(n) \cong W(\beta)$, kde $\beta = \overline{A(n)}$. Platí:

$$\begin{aligned} \alpha < \beta \quad &\Longleftrightarrow \quad W(\alpha) \text{ je vlastní začátek v množině } W(\beta) \Longleftrightarrow \\ &\Longleftrightarrow \quad A(m) \text{ je vlastní začátek v } A(n) \Longleftrightarrow \omega(m) < \omega(n) \Longleftrightarrow \\ &\Longleftrightarrow \quad \omega_\alpha < \omega_\beta. \end{aligned}$$

•

6.12. Věta. *Každé ordinální číslo je indexem některého alefu.*

Důkaz. Připusťme, že existuje ordinální číslo α, které není indexem žádného alefu a tedy ani žádného počátečního ordinálního čísla. Pak lze předpokládat, že α je nejmenší takové ordinální číslo.

Mohou nastat dva případy:

(a) *α je izolované číslo*, tj. $\alpha = \beta + 1$. Podle předpokladu tedy existuje počáteční ordinální číslo ω_b a $\aleph_\beta = \text{card } \omega_\beta$. Označme $\varphi = \overline{Z(\aleph_\beta)}$. Podle věty 6.7 je φ limitní ordinální číslo. Označíme-li $\varrho = \omega_\beta + \varphi$, platí (viz důkaz věty 6.7)

$$W(\varrho) = W(\omega_\beta) + Z(\aleph_\beta) = W(\omega_\beta) + \{\gamma;\ \text{card } \gamma = \aleph_\beta\}.$$

Odtud však

$$A(\text{card } \varrho) = \{\omega_\sigma;\ \sigma < \omega_\beta\} + \omega_\beta,$$

takže index počátečního ordinálního čísla mohutnosti card ϱ je roven $\beta + 1 = \alpha$: spor.

(b) *α je limitní číslo*. Platí $\alpha > 0$, neboť 0 je indexem alefu. Podle předpokladu je každé ordinální číslo $\xi < \alpha$ indexem některého počátečního ordinálního čísla ω_ξ. Toto číslo ω_ξ je přitom podle věty 6.11 jednoznačně určeno. Položme nyní

$$Z = \bigcup_{\omega_0 \le \xi < \alpha} Z(\text{card } \xi), \qquad W = \bigcup_{\xi \in Z} W(\xi).$$

Pak je $\varphi = \overline{W}$ opět počáteční ordinální číslo a zřejmě $\varphi = \omega_\alpha$: spor. •

6.13. Důsledek. *Každé ordinální číslo je indexem právě jednoho alefu, přičemž pro každá ordinální čísla α, β platí*

$$\alpha \leq \beta \quad \text{právě když} \quad \aleph_\alpha \leq \aleph_\beta.$$

Odtud a z věty 5.27 plyne

6.14. Důsledek. *Každá množina kardinálních čísel je dobře uspořádaná.*

Z důsledků 6.13 a 6.2 plyne

6.15. Důsledek. *Neexistuje množina všech kardinálních čísel (tj. třída všech kardinálních čísel je vlastní).*

Z důsledku 6.13 a věty 5.29 plyne

6.16. Důsledek. *Pro každé ordinální číslo α platí $\aleph_\alpha < \aleph_{\alpha+1}$, přičemž neexistuje kardinální číslo m takové, že $\aleph_\alpha < m < \aleph_{\alpha+1}$.*

Již v poznámce 3.17 jsme uvedli, že aritmetika nekonečných kardinálních čísel je jednoduchá vzhledem k platnosti tzv. *pohlcovacích zákonů*. Nyní již můžeme platnost těchto zákonů dokázat. Nejprve však uveďme jedno pomocné tvrzení.

6.17. Lemma. Buďte $\alpha \geq \beta$ libovolná ordinální čísla. Pak existuje právě jedno ordinální číslo γ takové, že $\alpha = \beta + \gamma$.

Důkaz. Buď A libovolná taková uspořádaná množina, že $\overline{A} = \alpha$. Pak v A existuje právě jeden začátek B takový, že $\overline{B} = \beta$. Označíme-li $\gamma = \overline{A - B}$, je $\alpha = \beta + \gamma$. Zbývá tedy dokázat, že toto číslo γ je určeno jednoznačně.

Nechť $\beta + \gamma_1 = \beta + \gamma_2$. Podle věty 5.32(1) nemůže platit $\gamma_1 < \gamma_2$ ani $\gamma_2 < \gamma_1$, takže platí $\gamma_1 = \gamma_2$. •

6.18. Věta. *Pro každé ordinální číslo α platí*

$$\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha.$$

Důkaz. Pro $\alpha = 0$ jsme tvrzení dokázali v příkladu 3.16. Podle principu transfinitní indukce tedy stačí dokázat, že když $\aleph_\xi \cdot \aleph_\xi = \aleph_\xi$ pro každé $\xi < \tau$, pak také $\aleph_\tau \cdot \aleph_\tau = \aleph_\tau$ (při libovolné volbě čísla τ).

Položme tedy $M := W(\omega_\tau) \times W(\omega_\tau)$ (podle definice platí card $W(\omega_\tau) = \aleph_\tau$). Pro $[\beta, \gamma] \in$ $\in M$ platí $\beta < \omega_\tau$, $\gamma < \omega_\tau$. Číslo $\lambda = \beta + \gamma$ nazveme *výškou* prvku $[\beta, \gamma]$. Nejprve ukážeme, že $\lambda = \beta + \gamma < \omega_\tau$.

Označme a = card $W(\beta)$, b = card $W(\gamma)$. Nechť například $a \leq b$. Pak platí $a \leq b < \aleph_\tau$. Nyní mohou nastat tři případy:

(1) β, γ jsou konečná ordinální čísla. Pak je tvrzení $\beta + \gamma < \omega_\tau$ zřejmé.

(2) β je konečné, γ nekonečné. Pak je $a + b = b$, tj. card $(\beta + \gamma)$ = card $\gamma <$ $< \aleph_\tau$, tj. $\beta + \gamma < \aleph_\tau$.

(3) β, γ jsou nekonečná kardinální čísla. Pak jsou a, b některé alefy a podle indukčního předpokladu platí $a \cdot a = a$, $b \cdot b = b$. Pak ale

$$b \leq a + b \leq b + b = 2 \cdot b \leq b \cdot b = b,$$

takže stejně jako v (2) platí $a + b = b$, tj. platí $\beta + \gamma < \omega_\tau$.

Dokázali jsme tak, že výška λ každého prvku množiny M je prvek množiny $W(\omega_\tau)$.
Pro každé $\lambda < \omega_\tau$ nyní položme

$$M_\lambda = \big\{\, [\beta, \gamma] \in M;\ \beta + \gamma = \lambda \big\}, \qquad M = \bigcup_{\lambda < \omega_\tau} M_\lambda.$$

Zvolme nyní $\lambda < \omega_\tau$ libovolně. Podle lemmatu 6.17 existuje pro každé $\beta \leq \lambda$ právě jedno ordinální číslo γ takové, že $\beta + \gamma = \lambda$, tj. existuje právě jeden prvek $[\beta, \gamma] \in M_\lambda$. To však znamená, že $M_\lambda \sim W_{\lambda+1}$, tj. existuje bijekce $f\colon W(\lambda+1) \to M_\lambda$. Definujeme-li nyní uspořádání na M_λ tak, aby f byl izomorfismus, je $M_\lambda \cong W(\lambda + 1)$, tj. $\overline{M_\lambda} = \lambda + 1$. Protože jsou množiny M_λ, $\lambda < \omega_\tau$, po dvou disjunktní, můžeme utvořit jejich součet; jinak řečeno, M lze uspořádat tak, že platí $M = \sum_{\lambda \in W(\omega_\tau)} M_\lambda$. Platí $\overline{M} = \vartheta = \sum_{\lambda \in W(\omega_\tau)} (\lambda + 1)$.

Nyní dokážeme, že $\vartheta = \omega_\tau$. Protože podle věty 5.34 platí $\vartheta \geq \omega_\tau$, stačí dokázat, že nemůže platit $\vartheta > \omega_\tau$. Dokážeme to sporem.

Připusťme tedy, že $\vartheta > \omega_\tau$. Pak ale existuje $\xi_1 = [\beta_1, \gamma_1] \in M$ tak, že pro vlastní začátek $M(\xi_1)$ platí $\overline{M(\xi_1)} = \omega_\tau$. Označme $\lambda_1 = \beta_1 + \gamma_1$. Podle předchozího je $\lambda_1 < \omega_\tau$, tj. card $\lambda_1 < \aleph_\tau$. Pro každé $\xi = [b, \gamma] \in M(\xi_1)$ však platí $\beta + \gamma \leq \lambda_1$, takže tím spíše je $\beta \leq \lambda_1$, $\gamma \leq \lambda_1$. Poněvadž je však card $\lambda_1 < \aleph_\tau$, platí podle indukčního předpokladu

$$\text{card}\, \{[\beta, \gamma] \in M;\ \beta < \lambda_1 + 1,\ \gamma < \lambda_1 + 1\} = \text{ card}\, \lambda_1.$$

Odtud však plyne, že card $M(\xi_1) \leq$ card $\lambda_1 < \aleph_\tau$: spor.

Tím je věta dokázána. •

6.19. Důsledek. (Pohlcovací zákony) *Buďte α, β libovolná ordinální čísla,* max (α, β) *buď větší z nich. Pak platí*

$$\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \aleph_{\max(\alpha,\beta)},$$

tj. součet i součin dvou nekonečných kardinálních čísel je větší z těchto dvou kardinálních čísel.

Důkaz. Nechť například $\beta \leq \alpha$. Pak je $\aleph_\beta \leq \aleph_\alpha$ a platí

$$\aleph_\alpha \leq \aleph_\alpha + \aleph_\beta \leq \aleph_\alpha + \aleph_\alpha = 2 \cdot \aleph_\alpha \leq \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha,$$

tj. $\aleph_\alpha + \aleph_\beta = \aleph_\alpha$.
Podobně

$$\aleph_\alpha \leq \aleph_\alpha \cdot \aleph_\beta \leq \aleph_a \cdot \aleph_\alpha = \aleph_a,$$

tj. $\aleph_\alpha \cdot \aleph_\beta = \aleph_a$. •

Nyní již můžeme snadno určit mohutnost množiny $Z(m)$ pro libovolné nekonečné kardinální číslo m. Platí

6.20. Věta. *Pro každé ordinální číslo α platí*

$$\text{card } Z(\aleph_\alpha) = \aleph_{\alpha+1}.$$

Důkaz. Je zřejmé, že $Z(\aleph_\alpha) = W(\omega_{\alpha+1}) - W(\omega_\alpha)$. Avšak card $Z(\aleph_\alpha)$ je některý alef. Nechť tedy například card $Z(\aleph_\alpha) = \aleph_\gamma$. Protože $W(\omega_{\alpha+1}) = Z(\aleph_\alpha) + W(\omega_\alpha)$, dostáváme $\aleph_{\alpha+1} = \aleph_\gamma + \aleph_\alpha = \aleph_{\max(\gamma,\alpha)}$, tj. $\alpha + 1 = \max(\gamma, \alpha)$. Protože $\alpha < \alpha + 1$, znamená to, že $\gamma = \alpha + 1$. •

Tvrzení věty 6.20 lze ještě zesílit. Podle ní totiž platí card $Z(\aleph_\alpha) = \aleph_{\alpha+1}$ = card $W(\omega_{\alpha+1})$. Ukážeme, že množiny $Z(\aleph_\alpha)$ a $W(\omega_{\alpha+1})$ mají nejen stejné kardinální číslo, ale i stejný ordinální typ.

6.21. Věta. *Buď ω_α libovolné počáteční ordinální číslo. Pak pro každý prvek $\xi \in W(\omega_\alpha)$ platí*

$$\overline{W(\omega_\alpha)} = \overline{W(\omega_\alpha) - W(\xi)}.$$

Důkaz. Označme $B(\xi) = W(\omega_\alpha) - W(\xi)$. Pak $W(\omega_\alpha) = W(\xi) + B(\xi)$. Protože $\overline{W(\xi)} = \xi$, platí card $W(\xi) < \aleph_\alpha$, neboť $\xi < \omega_\alpha$. Dále platí card $W(\omega_\alpha) = \aleph_a$ = card $[W(\xi) + B(\xi)]$, takže card $B(\xi) = \aleph_\alpha$, podle důsledku 6.19. Protože platí $\overline{B(\xi)} \leq \omega_\alpha$ a ω_α je nejmenší ordinální číslo o mohutnosti $\aleph_\alpha$, plyne odtud celkem $\overline{B(\xi)} = \omega_\alpha$. •

6.22. Důsledek. *Pro každé ordinální číslo α platí*

$$\overline{Z(\aleph_\alpha)} = \omega_{\alpha+1}.$$

Důkaz. Platí $Z(\aleph_\alpha) = W(\omega_{\alpha+1}) - W(\omega_\alpha)$. Podle věty 6.21 platí

$$\overline{Z(\aleph_\alpha)} = \overline{W(\omega_{\alpha+1}) - W(\omega_\alpha)} = \overline{W(\omega_{\alpha+1})} = \alpha + 1.$$

•

6.23. Poznámka. Mohutnost kontinua $c = 2^{\aleph_0}$ je podle věty 6.10 některým alefem. Podle věty 3.21 platí $c \geq \aleph_1$. Již Cantor předpokládal, že $c = \aleph_1$. Jak jsme uvedli již v 4.5, nazýval se tento předpoklad **hypotéza kontinua**.

Tato hypotéza patří k nejznámějším matematickým problémům 20. století. Samotný Cantor ji zformuloval již v r. 1878 a dokonce několikrát prohlašoval, že její důkaz v nejbližší době uveřejní. Nikdy se mu však hypotézu nepodařilo rozřešit. Dnes víme, že to bylo vcelku zákonité; hypotéza kontinua byla prostředky, které měl Cantor k dispozici, neřešitelná a odpověď se zcela vymyká představám, které mohli matematikové Cantorovy doby vůbec mít.

Přes značné úsilí mnoha matematiků se tuto hypotézu dlouho nikomu nedařilo ani dokázat ani vyvrátit, ačkoliv řada důvodů stále výrazněji nasvědčovala tomu, že by hypotéza měla být správná. První významný krok učinil až v r. 1940 K. Gödel, který v jím vybudované axiomatické teorii množin[2] dokázal, že **pokud je tato teorie bezesporná, je bezesporná i teorie, která vznikne přidáním axiómu výběru a zobecněné hypotézy kontinua**.[3]

Co z tohoto výsledku plyne? Kdyby bylo například v **ZF** možné hypotézu kontinua vyvrátit, musela by být teorie „**ZF+hypotéza kontinua**“ sporná. Protože však není (pokud není **ZF** sporná sama o sobě, v což samozřejmě doufáme), plyne odtud, že **hypotézu kontinua nelze v ZF vyvrátit**. My však již víme, že to samozřejmě **neznamená, že ji lze v ZF dokázat!**

Stejná situace byla i s axiómem vyběru. Přes četné výhrady k jeho používání Gödelův výsledek znamenal, že axióm výběru nevede ke sporu.[4]

Definitivně byl problém hypotézy kontinua vyřešen v r. 1963, kdy americký matematik P. Cohen dokázal, že **hypotéza kontinua tvoří v Zermelo-Fraenkelově teorii množin nerozhodnutelné tvrzení** (srovnej s definicí 5.11). Téměř současně s Cohenem, v r. 1964, dokázal totéž v teorii Gödel-Bernaysově český matematik P. Vopěnka.

O této problematice se ještě zmíníme v kapitole IV, §5.

Cvičení k §6.

Nic není nemožné,
pokud to nemusíte dělat sami.
WEILERŮV ZÁKON

1. Dokažte následující tvrzení:

[2] V tzv. teorii Σ, která je „hodně blízká“ teorii **ZF**. Zejména bezespornost jedné z těchto teorií implikuje bezespornost druhé.

[3] Hypotéza kontinua je zvláštním případem tzv. *zobecněné hypotézy kontinua* $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ pro každé ordinální číslo α. (Připomeňme si, že z věty 3.21 víme, že vždy platí $2^{\aleph_\alpha} \geq \aleph_{\alpha+1}$.)

[4] Vzájemný vztah mezi axiómem výběru a zobecněnou hypotézou kontinua dokázali W. Sierpiński (1947) a E. Specker (1952), když odvodili, že **ze zobecněné hypotézy kontinua axióm výběru vyplývá.**

Buď $\aleph_\alpha$ nekonečné kardinální číslo. Buď $K \neq \emptyset$ libovolná taková množina, že card $K \leq$ $\leq \aleph_\alpha$. *Budte m_k, $k \in K$, taková kardinální čísla, že $m_k \leq \aleph_\alpha$ pro každé $k \in K$. Pak* $\sum_{k\in K} m_k \leq \aleph_\alpha$.

2. Kardinální číslo $\aleph_\alpha$ se nazývá *iregulární*, jestliže $\aleph_\alpha = \sum_{k\in K} m_k$, kde card $K <$ $< \aleph_\alpha$, $m_k < \aleph_\alpha$ pro každé $k \in K$.

Nekonečné kardinální číslo, které není iregulární, se nazývá *regulární*. Dokažte:

a) *Každé číslo $\aleph_{\alpha+1}$ je regulární.* (Návod: Využijte cvičení 1.)

b) *Číslo $\aleph_{\omega_0}$ je iregulární.* (Návod: Dokažte, že $\aleph_{\omega_0} = \sum_{n<\omega_0} \aleph_n$.)

3. Všechna známá regulární čísla $\aleph_\alpha$ jsou taková, že α je izolované ordinální číslo (považujeme-li nyní 0 za izolované číslo). Dodnes není známo, zda existují regulární kardinální čísla $\aleph_\alpha$, jejichž index α je limitní ordinální číslo; takové kardinální číslo se nazývá *nedosažitelné*.

Promyslete si, že pokud existuje nedosažitelné kardinální číslo $\aleph_\alpha$, musí být nesmírně velké. (Uvažte, že mohutnost jeho indexu α by sama musela být nedosažitelným kardinálním číslem.)

4. Kardinální číslo m se nazývá *měřitelné*, jestliže existuje taková množina A, card $A = m$, a takové zobrazení $f\colon P(A) \to \{0, 1\}$, že platí:

a) $f(A) = 1$;

b) pro každý prvek $a \in A$ platí $f(\{a\}) = 0$;

c) jsou-li množiny $X_n \subseteq A$, $n = 1, 2, \ldots$, po dvou disjunktní, pak

$$f\left(\bigcup_{n=1}^{\infty} X_n\right) = \sum_{n=1}^{\infty} f(X_n).$$

Číslo, které není měřitelné, se nazývá *neměřitelné*.

Dokažte následující tvrzení:

α) *$\aleph_0$ je neměřitelné.*

β) *Je-li $\aleph_\alpha$ neměřitelné, je každé číslo $m < \aleph_\alpha$ neměřitelné.*

γ) *Nejmenší měřitelné kardinální číslo je nedosažitelné, přičemž nejmenší nedosažitelné kardinální číslo je ještě neměřitelné.* (Viz [1], str. 318.)

Kapitola 4

Historický vývoj teorie množin

1 Vývoj pojmu nekonečno.

Dílo B. Bolzana

Co dobře začíná — špatně skončí.
Co špatně začíná — skončí ještě hůř.
PUDDERŮV ZÁKON

Teorie množin je dnes základem, na němž je vystavěna převážná část současné matematiky. Přes náročnost a vysokou abstraktnost této teorie jsou její základní pojmy natolik věrným odrazem reality, že jsou již zahrnuty i do učiva základní školy. Je proto do jisté míry překvapující, že se teorie množin jakožto samostatná matematická disciplína začala formovat až v 70. letech minulého století v díle vynikajícího německého matematika Georga Cantora. V této kapitole se budeme zabývat historií teorie množin a důsledky této teorie pro vývoj matematiky ve 20. století.

Vzhledem k tomu, že teorie množin vznikla především z potřeby vyrovnat se s problematikou **nekonečna**, připomeneme nejprve, jak se vyvíjely představy matematiků a filozofů v tomto směru.

Aktuální a potenciální nekonečno

Často podléháme klamnému dojmu, že lidské poznatky se rozvíjejí „přímočaře“: přidáváme pouze nové a nové poznatky k těm dřívějším, víme toho stále „více a více“. Své představy podsouváme našim předkům a mnohdy si vůbec neuvědomujeme, že leckteré naše „samozřejmosti“ ani zdaleka nemusely být „samozřejmé“ v minulosti.

Na základní škole dětem říkáme, že množina $\mathbb{N}$ všech přirozených čísel je nekonečná (a nikdo se nad tím nepozastaví), všichni samozřejmě víme, že bodů na úsečce je nekonečně mnoho (a navíc jsme zjistili, že je jich „více“ než přirozených čísel, protože je jich *nespočetně* mnoho, zatím co $\mathbb{N}$ je pouze *spočetná*). I malé děti chápou, že přímka nemá žádný konec a při pohledu na večerní oblohu přímo „cítíme“ nekonečno vesmíru, který nás obklopuje. Málokdo si přitom uvědomuje, že po dlouhá staletí, dokonce ještě v minulém století, bylo všechno jinak.

Vraťme se v našich úvahách do starého Řecka, kde se formovaly základy moderní vědy včetně matematiky. S pojmem „nekonečno“ samozřejmě starořečtí filosofové běžně pracovali. Byli si však dobře vědomi problémů, které jsou s tímto pojmem spojeny.[1] Postupně vykrystalizoval dvojí přístup k nekonečnu. Místo dlouhého teoretického popisu tyto přístupy ilustrujme na jednoduchém příkladu.

Samozřejmě, že již staří Řekové dobře věděli, že přirozených čísel

$$1, 2, 3, \ldots, n, \ldots$$

je nekonečně mnoho. Tuto skutečnost však můžeme popsat a chápat dvěma způsoby.

Budeme-li postupně psát přirozená čísla, **nikdy** je nevypíšeme všechna. Za každým číslem následuje další, jakoukoliv předem stanovenou mez dříve nebo později překročíme. Takto chápané nekonečno popisující **proces**, který nikdy neskončí, mez, které nikdy nedosáhneme, to je tzv. *potenciální nekonečno*.

My dnes však, pod vlivem vývoje, který trvá již několik desetiletí, chápeme nekonečnost systému přirozených čísel jinak: díváme se na množinu $\mathbb{N}$ jako kdybychom ji „viděli“ hotovou, stavíme se do pozice, kterou Řekové přenechali bohům a která nebyla určena lidskému zkoumání. Nekonečné množiny si představujeme jako završené a zkoumáme bez obav vlastnosti těchto systémů. Tomuto nekonečnu, chápanému v završené, definitivní formě, se říká *aktuální nekonečno*.

Z řady důvodů věcných i filozofických dospěli Řekové — jak jsme již naznačili — k tomu, že lidskému zkoumání je přístupné pouze nekonečno potenciální. Proto když Eukleidés ve 3. století př. Kr. hovoří o *přímce*, má na mysli úsečku, kterou může „neomezeně“ prodlužovat, nikdy ji však nemůže prodloužit „do nekonečna“, jak si to dnes představujeme my. Z téhož důvodu formuluje Eukleidés tvrzení o počtu prvočísel tak, že *jich je více než jakékoliv předem dané množství*, neboť věděl a uměl dokázat, že jich není jen konečně mnoho. Nemohl však říci, že jich je „nekonečně mnoho“, protože to by musel připustit aktuální nekonečno, tvářit se, že vidí množinu všech prvočísel *hotovou, dokončenou*.

A proto také, abychom nezůstali jen u příkladů z matematiky, byl vesmír v antickém Řecku **konečný**. Za nejvzdálenější sférou stálic nebylo nic a nikoho nenapadalo klást si otázku,

[1] Za mnohé uveďme Zénóna z Eleje, který proslulými *aporiemi*, z nichž nejznámější je *Achilleus a želva*, dokazoval nemožnost pohybu. Všechny aporie využívaly představy nekonečné dělitelnosti prostoru, respektive času.

kterou si my, navyklí již nekonečnu aktuálnímu, snad ani nedovedeme nepoložit: *co je* **za** *onou poslední sférou?* Krása jejich vesmíru spočívala v jeho **konečnosti**, v řádu, který odpovídal jejich představám o harmonii světa.

Vývoj pojmu nekonečno

Chápání nekonečna, které se vyvinulo v antice, se udrželo dlouhá staletí. Lidskému poznávání bylo dáno nekonečno potenciální a myšlenka na aktuální nekonečno se jevila jako nepatřičná a člověku nepřislušející. Až velký raně renesanční myslitel Mikuláš Kusánský si jako jeden z prvních troufá rozvíjet myšlenku, co by to znamenalo, **kdyby** byl vesmír nekonečný. Jeho myšlenky však byly příliš odvážné a ojedinělé.

Jen nesměle se v myšlenkách vědců rodily otázky, které nám dnes připadají samozřejmé, především pak ta, která v 70. letech 19. století koneckonců stála u zrodu teorie množin: *má vůbec smysl porovnávat nekonečné systémy podle velikosti?* Tuto otázku si například v roce 1638 položil jeden z géniů oné doby, Galileo Galilei. Ten si vypsal dvě řady čísel:
přirozená čísla

$$1, 2, 3, 4, 5, \ldots$$

a jejich druhé mocniny

$$1, 4, 6, 16, 25, \ldots$$

a uvědomil si, dnešní terminologií řečeno, že mezi těmito množinami **existuje bijekce!** To by však mělo znamenat, že uvedené systémy čísel jsou **stejně velké!** A to se, vcelku zákonitě, Galileimu jevilo jako naprostý nesmysl. Vždyť přece jeden ze základních Eukleidových logických axiómů, které byly nezpochybnitelným pilířem tehdejší matematiky, říká, že *celek je větší než část*. A tady se zdá, že by druhý systém, který je evidentní částí prvního, měl být stejně velký.

Jaký závěr z této „absurdní“ situace Galilei vyvodil? **Pro nekonečné systémy nemá otázka o jejich velikosti naprosto žádný smysl!**

Takový tedy byl stav úvah o nekonečnu zhruba v polovině 17. století. A záhy se měla celá situace ještě více zkomplikovat. Uvažovalo-li se zatím o (potenciálně) **nekonečně velkých** veličinách, ve druhé polovině 17. století se situace ještě více zdramatizovala.

Jak je všeobecně známo, vzniká v této době *diferenciální a integrální počet*. Přestože jeho tvůrci Gottfried Wilhelm Leibniz a Isaac Newton přistoupili k jeho výstavbě z odlišných pozic, byl infinitesimální počet u obou založen na pojmu **nekonečně malé** veličiny. Jakkoliv tento pojem nebyl řádně definován a pravidla pro počítání s nekonečně malými veličinami byla dána jen velmi vágně, ukázalo se záhy, že diferenciální a integrální počet je vskutku mocným nástrojem nejen v matematice, ale i v řadě aplikací, především pak ve fyzice. Nejasnosti v jeho základech se však postupně vyhrocovaly a posléze v 18. století vyústily ve stav, který dnes nazýváme *druhou krizí matematiky*.

Problémy matematické analýzy se postupně odstraňovaly až od počátku 19. století. Zásadní roli zde sehrál Augustin Louis Cauchy zavedením **limity** na počátku dvacátých let, významně však do této problematiky zasáhl svými pracemi z matematické analýzy i Bolzano.[2]

Dospěli jsme tak v tomto stručném přehledu do období, v němž Bolzano píše své dílo *Paradoxy nekonečna*, které nás v souvislosti s teorií množin mimořádně zajímá.

Zrekapitulujeme-li tedy stav v polovině 19. století, lze říci následující: vědecká komunita pracuje s potenciálním nekonečnem a odmítá nekonečno aktuální jako něco, co není přístupno lidskému zkoumání. V matematické analýze již sice existují nástroje k odstranění problémů s „nekonečně malými“ veličinami, přesto však v matematické, fyzikální a další literatuře přetrvávají nesprávné a nelogické postupy, které člověka s tak kritickým a analytickým myšlením, jaké měl Bolzano, musely zákonitě vyprovokovat k formulaci svého náhledu na problematiku nekonečna.

B. Bolzano a „Paradoxy nekonečna“

Paradoxy nekonečna, nejznámější Bolzanova kniha, vyšly v roce 1851, tři roky po jeho smrti. Bolzano ji psal poslední dva roky před smrtí, v letech 1847 – 1848, a tak ji lze v mnoha ohledech považovat za vyvrcholení a uzavření jeho díla.

Jakkoliv si Bolzano sám ze svých knih nejvíce cenil monumentální čtyřdílné učebnice logiky a metodologie vědy *Wissenschaftlehre* (v českém překladu *Vědosloví*), ovlivnily právě *Paradoxy nekonečna* další vývoj matematiky ze všech jeho děl nejvýrazněji. Podstatnou měrou k tomu samozřejmě přispěla i ta skutečnost, že rukopis nestihl osud mnoha jeho dalších děl, která zůstala ležet v nezpracované pozůstalosti dlouhá desetiletí. Bolzanův žák, František Příhonský, jenž po Bolzanově smrti rukopis obdržel se žádostí o přípravu do tisku, se tohoto úkolu vskutku obětavě a zodpovědně ujal a tak v roce 1851 mohly *Paradoxy* v Lipsku opravdu vyjít.[3]

Paradoxy nekonečna přitom nejsou ryze matematickou knihou. Jde spíše o dílo matematicko-filozofické, v němž je značná pozornost věnována i fyzice, lépe řečeno fyzikálnímu nazírání na svět, teologii apod. Bezesporu však je skutečností, jak v dalším ukážeme, že právě „matematické“ pasáže knihy patří k těm pozoruhodnějším.

Sledujeme-li vývoj hodnocení Bolzanova přínosu ke světové matematice, vypozorujeme záhy dva obvyklé extrémy: od přehlížení k nekritickému nadsazování a k podsouvání myšlenek a úmyslů, které Bolzano prokazatelně neměl. Jak v dalším uvedeme, hlavní Bolzanův přínos

[2] Poznamenejme, že tento proces zpřesňování matematické analýzy dovršil ve 2. polovině 19. století Karl Weierstrass zavedením tzv. „$\epsilon - \delta$ jazyka“. V rámci těchto snah byla v 70. letech minulého století řádně zavedena *reálná čísla* G. Cantorem a Richardem Dedekindem. V systému reálných čísel již samozřejmě nemohou existovat žádné „nekonečně malé“ veličiny.

[3] Jak známo, Bolzano psal své práce německy nebo latinsky. Originální název německy psaných *Paradoxů* je *Paradoxien des Unendlichen*. Česky vyšly *Paradoxy nekonečna* až v roce 1963 (!) v zasvěceném překladu Otakara Zicha, který knihu doprovodil podrobnými poznámkami a komentářem. Z tohoto překladu také v dalším textu citujeme.

lze spatřovat v těch myšlenkových proudech, které za zhruba čtvrt století vyvrcholily vznikem **teorie množin**. Zakladatel této teorie, Georg Cantor, *Paradoxy* dobře znal a vysoce je hodnotil.[4] V této souvislosti se často píše o Bolzanovi jako o spoluzakladateli teorie množin, což je poněkud nadsazené a někdy se dokonce objevují evidentní nesprávnosti. Tak například jeden z nejznámějších historiků matematiky, Dirk Struik, píše, že Bolzano dospěl k pojmu spočetné a nespočetné množiny, což je naprostá nepravda.

Pokusme se tedy objektivně zhodnotit faktický přínos *Paradoxů nekonečna*. Ty jsou ostatně natolik významné a v mnoha ohledech dodnes inspirativní, že ani v nejmenším nepotřebují nekritické a přehnané hodnocení k tomu, aby byly poprávu považovány za jedno z nejvýznamnějších děl matematické literatury minulého století.

Obsah Paradoxů nekonečna

Jak jsme již uvedli, nejsou *Paradoxy* ryze matematickou knihou, ale dílem, v němž se prolínají pasáže matematické, fyzikální, filozofické a teologické. Kdybychom se stručně snažili vystihnout základní myšlenky celého díla, byly by to asi dvě následující:

1. zdůvodnění, proč je v matematice **nutno** pracovat i s aktuálním nekonečnem;

2. analýza chyb, jichž se vědci dopouštějí při úvahách o nekonečnu.

První z uvedených myšlenek Bolzano zdůraznil již mottem celé knihy, za něž si zvolil následující Leibnizův citát: *Jsem natolik pro aktuální nekonečno, že namísto abych připustil, že se ho příroda děsí, jak se běžně říká, jsem přesvědčen, že je má v oblibě všude, aby lépe zdůraznila dokonalosti svého Tvůrce.*[5] Celá práce[6] je rozdělena do 70 paragrafů. I přečtení obsahu, v němž jsou jednotlivé paragrafy stručně charakterizovány, dá čtenáři alespoň hrubou orientaci o obsahu práce. Současně se však může stát zdrojem omylů a dezinterpretací podobných Struikovu omylu, o němž jsme se zmínili před chvílí. Například §19 má „název“ *Existují nekonečné množiny, které jsou větší nebo menší než jiné nekonečné množiny.* To by mohlo vskutku evokovat dojem, že Bolzano dospěl k něčemu, co připomíná pojem *kardinální číslo* a odtud je pak jen krůček k tomu podsouvat mu „objevení“ spočetných a nespočetných množin. Jak v dalším uvedeme, je podstata úplně jiná; Bolzano pouze v této pasáži dokumentuje, že například jedna úsečka (obsahující nekonečně mnoho bodů) může být částí jiné, větší úsečky apod. K pojmu „kardinální číslo“, jak rovněž uvidíme, Bolzano ani v náznaku nedospěl.

[4] V práci *Über unendliche lineare Punktmannigfaltigkeiten*, Math. Ann. **21**(1883) o nich píše jako o „skvělém a obsažném díle“.

[5] Z terminologického hlediska je přitom zajímavé, že Bolzano v celé knize sám **ani jednou** neužije pojmu „aktuální“, resp. „potenciální“ nekonečno. Z celého jeho textu je evidentní, že aktuální nekonečno považoval za tak samozřejmé, že nepotřebovalo žádný přívlastek. Naopak, potenciální nekonečno dle něho žádným faktickým nekonečnem není, což v různých obměnách mnohokrát opisuje.

[6] Bolzanův text, bez poznámkového aparátu překladatele, má v českém překladu 100 stran.

Všimněme si nyní konečně obsahu *Paradoxů* systematicky a podrobněji.

Prvních deset paragrafů tvoří stručný Bolzanův výklad toho, jak je nutno chápat pojem „nekonečný souhrn“; v naší dnešní terminologii je to nekonečná množina. Tato část dnešnímu čtenáři připadne zcela samozřejmá a argumentaci jistě přijme bez problémů, neboť je s aktuálním nekonečnem zvyklý zcela běžně pracovat. Následující pasáže knihy jsou polemikou a kritikou názorů některých filozofů a matematiků. Ocitujme některé pasáže z 11. a 12. paragrafu; v nich lze snadno vystopovat Bolzanův vztah k potenciálnímu nekonečnu. (Poznamenejme v této souvislosti, že například Cauchyho zmiňuje Bolzano ve své práci několikrát, vždy však v souvislostech poněkud nelichotivých. V pozdějších úvahách o matematické analýze, kde by odvolání se na Cauchyho bylo zcela na místě, se o něm zato nezmiňuje vůbec. Analogicky lze vystopovat i jeho „náklonnost“ k některým filosofům, například k Hegelovi.)

§11

> Tímto nekonečnem, tak dobře známým matematikům, nelze však ještě uspokojit některé filosofy, zvláště novější doby, jako **Hegela** a jeho přívržence, kteří je pohrdavě nazývají špatným nekonečnem a tvrdí, že znají ještě mnohem vyšší, pravé, **kvalitativní nekonečno**, které nacházejí zejména v bohu a vůbec jen v **absolutnu**. Jestliže si myslí, jako Hegel, Erdmann a jiní, matematické nekonečno pouze jako veličinu, která je proměnná a jejíž růst nemá žádnou hranici (což ovšem mnozí matematikové, jak brzo uvidíme, stanovili jako výměr svého pojmu), pak s nimi souhlasím, když kritizují tento pojem jako veličinu do nekonečna pouze **rostoucí**, nikdy však nekonečna **nedosahující.** . . .

§12

> Nevidím však také jinou možnost, než zamítnout jako nesprávné i jiné výměry nekonečna, jež byly podány samotnými matematiky v domnění, že představují jenom součásti tohoto jednoho a téhož pojmu.
>
> 1. Vskutku byli někteří matematikové přesvědčeni, jak jsem právě výše poznamenal, mezi nimi sám **Cauchy** (ve svém **Cours d’Analyse** a mnoha jiných spisech), autor článku **„Nekonečno“ v Klügelově** slovníku, že definují nekonečno, jestliže je popíší jako proměnnou veličinu, jejíž hodnota **neomezeně** roste a podle toho může být větší než **jakákoli sebe větší daná veličina.** Mezí tohoto neomezeného růstu je **nekonečně velká veličina**. Tak je tangenta pravého úhlu, myšlená jako spojitá veličina, neomezená, bez konce, **ve vlastním slova smyslu nekonečná**. Chybnost tohoto výměru vysvítá již z toho, že co nazývají matematikové **proměnnou veličinou**, není vlastně veličina, nýbrž pouhý pojem, pouhá **představa** veličiny, a to taková představa, která v sobě pojímá nejen jednu jedinou veličinu, nýbrž dokonce nekonečně mnoho veličin, které se navzájem liší

> ve své hodnotě, tj. ve své **velikosti**. To, co nazýváme nekonečným, nejsou ony **různé** hodnoty, které tu představuje výraz tangens φ, zvolený jako příklad, pro různé hodnoty φ, nýbrž pouze ona jediná hodnota, o níž si představují (ač v tomto případě neprávem), že jí onen výraz nabývá při hodnotě $\varphi = \pi/2$. Je v tom jistě také protimluv, mluví-li se o mezi neomezeného růstu a právě tak, mluví-li se při výměru nekonečně malého o mezi neomezeného ubývání. A prohlásí-li se ona první mez za nekonečnou veličinu: pak by se měla podle analogie tato druhá, tj. pouhá nula (nic) prohlásit za nekonečně malé: což je jistě nesprávné a ani **Cauchy** ani **Grunert** si to nedovolují říci.
>
> 2. Byl-li právě uvedený výměr příliš široký, je naproti tomu příliš úzký onen výměr, který přijímá Spinoza a mnoho jiných, jak filozofů, tak matematiků, a to že **nekonečné je pouze to, co není schopno žádného zvětšení**, nebo k čemu již nelze nic připojit (přičíst). Matematik si dovoluje připojit ke každé veličině, i k nekonečně velké, jiné veličiny, a to nejen konečné, nýbrž i jiné veličiny, které jsou samy nekonečné, ba dokonce znásobuje nekonečnou veličinu nekonečněkrát atd. A vedou-li ještě někteří spory o tom, zda je takový postup přípustný: který matematik, jen když nezavrhne jakékoli nekonečno, nebude musit uznat, že délka přímky, omezené jen v jednom směru a prostírající se v druhém směru do nekonečna, je nekonečně velká a že může být nicméně v onom prvním směru prodloužena? . . . .

V dalším si Bolzano všímá problematiky existence aktuálně nekonečných souhrnů, tj. nekonečných množin a vyvrací některé nejobvyklejší námitky proti jejich existenci. Otázky existence nekonečných množin se týká celý §13. Protože je argumentace v této části pro Bolzana v mnoha ohledech typická, ocitujeme jej celý.

Z obsáhlého §14 ocitujeme jen úvodní část, v níž Bolzano vyvrací některé námitky odpůrců aktuálního nekonečna. Přesně tytéž námitky se ovšem opakovaly o několik desetiletí později, kdy byly vznášeny proti Cantorově teorii.

§13

> Jestliže jsme se již shodli v tom, který pojem budeme vázat se slovem **nekonečno**, a jestliže jsme si také již jasně uvědomili části, z nichž tento pojem skládáme: pak je nejbližší otázka, má-li též **předmětnost**, tj. zda jsou také věci, na něž se dá aplikovat, zda existují množiny, které smíme nazývat nekonečnými ve vyloženém významu toho slova. A na toto si troufám rozhodně odpovědět kladně. Nepochybně existují množiny, které jsou nekonečné, již **v oblasti těch věcí, které si nečiní nárok na skutečnost, ba ani na možnost. Množina vět a pravd o sobě** je nekonečná, jak se dá velice snadno nahlédnout; neboť vezmeme-li jakoukoli pravdu, například větu, že vůbec existují pravdy, nebo ostatně jakoukoli jinou

větu, kterou označíme A; pak shledáme, že věta, kterou vyjadřujeme slovy **„A je pravdivé“** je odlišná od A sama; neboť tato věta má zřejmě zcela jiný subjekt než ona první. Jejím subjektem je totiž celá věta A sama. Avšak podle téhož zákona, podle něhož z věty A vyvozujeme větu od ní odlišnou, kterou nazvu B, dá se opět z B vyvodit třetí věta C, a tak stále bez konce. Souhrn všech těchto vět, kde každá následující je k nejblíže předcházející ve vztahu právě uvedeném, vezme totiž předcházející větu za svůj subjekt a vysloví o něm, že je pravdivou větou, tento souhrn — říkám — zahrnuje množinu částí (vět), která je větší, než jakákoli konečná množina. Neboť i bez mého upozornění si všimne čtenář podobnosti, kterou má řada těchto vět, sestrojená podle právě uvedeného vytvořujícího zákona, s **řadou číselnou**, o níž se uvažovalo v §8; podobnost spočívá v tom, že ke každému členu této druhé řady existuje odpovídající člen předchozí řady tak, že k jakémukoli sebe většímu jejich počtu existuje stejně velký počet různých vět, a že nad to můžeme ještě vždy tvořit nové věty, nebo, lépe řečeno, ža takové věty samy o sobě existují, ať již je tvoříme nebo ne. Z toho pak plyne, že souhrnu všech těchto vět přísluší množství, které převyšuje libovolné číslo, tj. nekonečné množství.

§14

Jakkoli jednoduchý a jasný je právě podaný důkaz: přece je značný počet učených a velmi bystrých mužů, kteří samu větu, o níž věřím, že jsem ji tu dokázal, prohlašují nejen za paradoxní, nýbrž dokonce za falešnou. Popírají, že **existuje vůbec nějaké nekonečno**. Nejen mezi věcmi, které jsou skutečné, ale ani mezi ostatními není podle jejich tvrzení ani jediná, a rovněž tak ani souhrn více věcí, u níž by se dala z nějakého hlediska předpokládat nekonečná množina částí. O důvodech, které uvádějí proti nekonečnu v říši skutečna, budeme uvažovat později, protože také teprve později podáme důvody pro existenci takového nekonečna. Zde tedy vyslechněme pouze důvody, jimiž má být prokázáno, že něco nekonečného není nikde, ani u těch věcí, které si činí nárok na skutečnost.

1. „Nekonečná množina“ říká se, „nemůže již proto existovat, protože nekonečná množina **nemůže být nikdy sjednocena v celek, nemůže být nikdy myšlením obsáhnuta**.“ — Toto tvrzení musím označit přímo za omyl, který byl vyvolán nesprávným názorem, že k tomu, abychom si mohli myslit celek, sestávající z předmětů $a, b, c, d, \ldots$ musili bychom si nejprve o každém z nich vytvořit představu, která představuje každý z těchto předmětů zvlášť (jednotlivé jejich představy). Tak tomu naprosto není: mohu si myslit množinu, souhrn, či chceme-li raději obyvatele Prahy nebo Pekinu jako **celek**, aniž bychom představovali každého z těchto obyvatel jednotlivě, tj. aniž bych měl představu, která se

> vztahuje výhradně jen k němu. Činím to skutečně právě nyní, mluvím-li o této množině obyvatel a vyslovím-li např. soud, že jejich počet je v Praze mezi čísly 100 000 a 120 000. Je totiž zcela snadné, mám-li představu A, která reprezentuje každý z předmětů a,b,c,d,. . . , ale již nic jiného, dospět k představě **souhrnu**, utvořeného všemi těmito předměty. K tomu není vskutku zapotřebí ničeho jiného, než spojit s představou A pojem, který je označen slovem souhrn, tak jak to naznačují slova: **souhrn všech A**. Touto jedinou poznámkou, jejíž správnost musí být každému zřejmá, jak jsem přesvědčen, padá celá obtíž, kterou hledají v pojmu množiny sestávající z nekonečně mnoha částí: pokud jen tu je rodový pojem, který zahrnuje každou z těchto částí, jinak však nic jiného, jak tomu je u pojmu: „**množina všech vět nebo pravd o sobě**“, kde není použito žádného jiného rodového pojmu než toho, který tu již máme, totiž: „věta nebo pravda o sobě“. — Nemohu však ponechat bez kritiky ještě **druhý** omyl, který se v uvedené námitce prozrazuje.
>
> Je to názor, že „ množina by nebyla, kdyby tu dříve nebyl někdo, kdo si ji myslí“. Kdo tvrdí toto, měl by nejen tvrdit, že neexistuje žádná **nekonečná** množina vět anebo pravd o sobě, aby tak byl důsledný, pokud je to vůbec při omylu možné, ale měl by tvrdit, že neexistují **vůbec žádné** věty a pravdy o sobě. Neboť jestliže si již jasně uvědomili pojem vět a pravd o sobě a nepochybujeme opravdu vůbec o jejich předmětnosti: můžeme jen ztěžka dospěti k tvrzením, že by množina nebyla bez někoho, kdo si ji myslí, avšak jistě u nich nesetrváme. Abych to každému jasně ukázal, dovolím si nadhodit otázku, zda se též na zemských pólech nevyskytují tělesa, tekutá i tuhá, vzduch, voda, kameny atd., zda tato tělesa na sebe navzájem nepůsobí podle určitých zákonů, např. tak, že rychlosti, které si navzájem sdělují při srážce, se mají k sobě v obráceném poměru jejich hmot apod., a zda se toto vše neděje i když tam není ani člověk, ani jiná myslící bytost, aby to pozoroval?. . .

Při čtení Bolzanova textu nás okamžitě napadá řada otázek. Jak Bolzano sám upozorňuje, nabízí se evidentní analogie jím popisované množiny vět s množinou všech přirozených čísel. Proč tedy vůbec onu konstrukci uvádí a nepopisuje přímo množinu přirozených čísel? Aniž bychom chtěli Bolzanovi podsouvat nepodložené domněnky, tkví zřejmě odpověď v odlišném chápání „existence“ čísel a pravd.[7]

Podstatnější námitka je následující: popsaná konstrukce vět přece popisuje *potenciální* nekonečno. Uvedená konstrukce přece nikdy nekončí, tak jako nekončí posloupnost přirozených čísel! Této námitky si Bolzano samozřejmě byl vědom, odpověď však nabídl již v §11. Tam totiž uvádí:

[7] Jak uvádí ve *Vědosloví*, alespoň jedna pravda nepochybně existuje: je to pravda o existenci Boží.

Říkám tedy: nazývám Boha nekonečným, poněvadž mu musíme přiznat síly více než jednoho druhu, které mají nekonečnou velikost. Tak mu musíme připsat poznávací schopnost, která je pravou vševědoucností, tedy obsáhne nekonečnou množinu pravd, protože je v sobě obsáhne vůbec všechny, atd.

Popsaná množina pravd je tedy podle Bolzana **aktuálně nekonečná**, protože **Bůh je všechny vidí**.

Konečně poslední námitka, o níž se chceme zmínit: ačkoliv Bolzano v úvodu paragrafu píše o „předmětnosti" nekonečna, je jeho příklad z oblasti, kterou sám nazývá „věcmi, které si nečiní nárok na skutečnost". O tom, že se nekonečno (a jak jsme se již zmínili, znamená to u něj vždy aktuální nekonečno) vyskytuje i v „oblasti samého skutečna", se Bolzano zmiňuje až mnohem později, v §25. Zde uvedené příklady však, po pravdě řečeno, nejsou příliš přesvědčivé. Kromě již očekávaného argumentu, že *existuje bůh, bytost která je více než v jednom ohledu nekonečná* . . . , je to jen argument založený na představě časového kontinua: *množina stavů, kterých každá bytost během sebekratší doby nabývá, musí být nekonečně velká (nebot' každá taková doba obsahuje nekonečně mnoho okamžiků)*.

Nyní se dostáváme k nejzajímavějším — alespoň pro matematiky — pasážím knihy. Uvedeme klíčové pasáže §§19-21, kde jsou prokazatelné úvahy, které předjímají vznik teorie množin. V §19 Bolzano nejprve zdůvodňuje, že i nekonečné množiny má smysl porovnávat podle velikosti, v dalších dvou paragrafech pak uvažuje o kritériu, které by nám to umožňovalo. Komentář k těmto úvahám uvedeme až po citaci.

§19

> Již u těch příkladů nekonečna, o kterých jsme dosud uvažovali, nám nemohlo uniknout, že není možno pokládat všechny nekonečné množiny **za sobě rovné z hlediska jejich množství;** ale že mnohá z nich je **větší** nebo **menší** než jiná, tj. obsahuje v sobě jinou množinu jako svůj díl (nebo naopak, je sama obsažena v jiné jako její pouhý díl). I to je tvrzení, které zní mnoha lidem **paradoxně**. Jistěže všichni, kteří vykládají nekonečno jako to, co není schopno žádného zvětšení, musí nejen uznat za paradoxní, ale přímo za **sporné**, že by jedno nekonečno bylo větší než jiné. Avšak poznali jsme již dříve, že tento názor spočívá na takovém pojmu nekonečna, který vůbec nesouhlasí s jazykovým užitím toho slova. Podle našeho výkladu, který odpovídá nejen jazykovému užití, nýbrž i účelům vědy, nemůže najít nikdo nic sporného, ba ani nápadného, na myšlence, že jedna nekonečná množina je větší než jiná. . . .

Domníváme se, že Bolzanova úvaha je zcela jednoznačně čitelná. Jsou-li dvě množiny ve vztahu inkluze, je samozřejmě jedna menší a druhá větší. (Což samozřejmě **není pravda** v cantorovské teorii množin. Už tento fakt, dle našeho názoru, evidentně znamená, že Bolzana

nelze považovat za spoluzakladatele Cantorovy teorie). Problém tedy podle Bolzana nastává, máme-li porovnat velikosti dvou množin, které ve vztahu inkluze nejsou. Ocitujme nejprve Bolzanovu úvahu.

§20

> Přejděme nyní k úvaze o nanejvýš pozoruhodné zvláštnosti, jež se může vyskytnout u vztahu dvou množin, **jsou-li obě nekonečné**, dokonce jež se vlastně vyskytuje vždy, avšak byla dosud přehlížena ke škodě pro poznání mnohých důležitých pravd metafyzických, jakož i fyzikálních a matematických, a která i nyní, vyřknu-li ji, bude pokládána za tak paradoxní, že by bylo velmi potřebné se při úvaze o ní trochu déle zdržet. Tvrdím totiž: dvě množiny, obě nekonečné, mohou být k sobě v takovém vztahu, že je **na jedné straně** možno spojit ve dvojici každou věc, náležející jedné z nich, s věcí, náležející druhé z nich, tak, aby vůbec žádná věc v obou množinách nezůstala bez spojení ve dvojici a také žádná aby se nevyskytovala ve dvou nebo více dvojicích; a přitom je **na druhé straně** možno, aby jedna z obou množin obsahovala druhou jako svůj pouhý díl, takže množství, která ony množiny představují, jsou k sobě **v nejrozmanitějších poměrech**, považujeme-li věci v nich za stejné, tj. za jednotky.. . .

Bolzano tedy uvádí fakt, jehož si povšiml již Galilei: **nekonečná množina může být ekvivalentní se svou vlastní podmnožinou**. Na rozdíl od Galileiho, který za této situace usoudil, že u nekonečných množin nemá smysl poměřovat jejich velikost, je Bolzano přesvědčen, že to nutné je. Domníváme se však, že v této chvíli se dopustil **osudového omylu**, který způsobil, že se nestal faktickým zakladatelem teorie množin. Jak z následujícího paragrafu uvidíme, usoudil, že existence bijekce mezi nekonečnými množinami nás ještě neopravňuje k tvrzení, že jsou stejně velké.[8] Jednoduše řečeno, Bolzano překročil mnohé dosavadní bariéry, evidentně však nepřesáhl horizont tvrzení, že *celek musí být větší než část.* Z následujícího textu je to zcela zřejmé.

§21

> Tedy jen z toho důvodu, že dvě množiny A a B jsou v takovém vzájemném vztahu, že ke každé části a, obsažené v A, můžeme též vyhledat podle určitého pravidla část b, obsaženou v B, tak aby všechny dvojice $(a+b)$, které vytvoříme, obsahovaly každý předmět z A nebo z B, a každý pouze jednou – jen z této okolnosti — jak vidíme — není ještě nijak dovoleno uzavírat, že by si **tyto množiny** z hlediska

[8] Jak víme, vyřešil tuto věc definitivně až o čtvrt století později Cantor, když dokázal, že mezi přirozenými a reálnými čísly **bijekce neexistuje**, takže lze existenci bijekce vzít za kritérium toho, zda jsou množiny **stejně velké**.

> množství svých částí byly **navzájem rovny** (tj. abstrahujeme-li od všech jejich rozdílů), **jsou-li nekonečné**; nýbrž mohou být přes tento svůj vztah, který je sám o sobě ovšem obapolně stejný, ve vztahu nerovnosti vzhledem ke svým množstvím, takže se může ukázat, že jedna z nich je celkem, jehož dílem je druhá. Na rovnost těchto množství se smí usoudit teprve tehdy, přistoupí-li k tomu ještě nějaký jiný důvod, jako například to, že obě množiny mají zcela stejná základní určení, například zcela stejný způsob vzniku.

Formulaci, že dvě množiny jsou stejně velké, když mají „zcela stejná základní určení“ sice Bolzano opakuje vícekrát, nikde však neprecizuje, co tím přesně myslí.

Okomentovali jsme tedy podrobně Bolzanovy úvahy, které byly předobrazem teorie množin. Přitom se domníváme, že právě v uvedených 21 prvních paragrafech jsou ukryty nejhodnotnější myšlenky celého díla. Přes veškeré (z dnešního hlediska viděné) nedostatky bylo Bolzanovou velkou zásluhou především fundované zdůvodnění nutnosti zkoumat aktuální nekonečno. O dalších pasážích *Paradoxů* se již zmíníme jen stručně.

Dalších cca 20 paragrafů se zabývá počítáním s „nekonečně malými“ a „nekonečně velkými“ veličinami v analýze a v geometrii. Stručně řečeno, Bolzano zde podává výklad toho, jak počítat s limitou (i když tohoto pojmu ani jednou neužije) a tím se vyhnout užívání nekonečně malých či velkých veličin. Zvláštní pozornost věnuje problémům spojeným s nulou, kterou nepovažuje za číslo, ale pouze za symbol, přičemž přesně specifikuje, jak lze tohoto symbolu užívat. Zhruba druhá polovina knihy je věnována úvahám o prostoru, čase, fyzikálních zákonech, o duchovních a hmotných substancích apod. Síla těchto pasáží je ve srovnání s matematickými partiemi podstatně menší. Některé Bolzanovy názory byly evidentně překonané již v době, kdy svou práci psal. Stručně řečeno, Bolzano zastává divnou směs tzv. mechanického materialismu kombinovaného s vírou v boží všemohoucnost. Ze stavu všech součástí vesmíru bychom mohli podle platných zákonů rekonstruovat stavy další, pokud ovšem *pomineme případ, kdy nastane přímý boží zásah, protože odchylka od tohoto zákona vyžaduje sílu, která by ve srovnání se spojitou silou musila být* **nekonečně velká** apod. Tělesa mohou podle Bolzana na sebe působit „bezprostředně na dálku“, a všechny tyto úvahy jsou prostoupeny dobovými úvahami o éteru a nedělitelných atomech. I v těchto partiích lze sice najít hodnotné myšlenky (například o „dimensi prostoru“, kterou Bolzano zavedl již ve svých dřívějších pracích), celkově je však vyznění této části knihy, byť je čtivá a poutavá, mnohem nižší.

Co říci závěrem? Bolzanova kniha je v mnoha ohledech pozoruhodná. Samozřejmě, že ve světle dalších objevů jsou některé pasáže nepřesné či zastaralé. V každém případě je to však dílo pozoruhodné a podává nám dobrý obrázek o pronikavosti Bolzanova ducha a o stavu vědeckého myšlení v polovině minulého století. O kterém současném textu to asi bude možno bez obav říci za půldruhé století?

2 Georg Cantor a jeho dílo

Historie je věda o tom,
co se nikdy nestane dvakrát.
VALERYHO ZÁKON

Viděli jsme, jak blízko byl Bolzano k odhalení a pochopení vlastností nekonečných množin. To, co se nám dnes ovšem jeví jako malý krůček v poznání, byl v tehdejší době — v polovině 19. století — velký myšlenkový posun, kvalitativní skok v matematickém a filozofickém myšlení. Učinit tento krok — to vyžadovalo hluboké matematické vzdělání, široký filozofický rozhled, bohatou tvůrčí fantazii a velkou osobní odvahu. Tím vším byl vrchovatě obdařen Georg Ferdinand Ludwig Philipp Cantor, jak se plným jménem jmenoval vynikající německý matematik, jenž je v celém světě zaslouženě uznáván za zakladatele teorie množin; teorie, která tak výrazně ovlivnila tvář soudobé matematiky, teorie, proti níž byly vedeny v matematických kruzích tak ostré boje a nevybíravé výpady jako proti málokteré jiné matematické disciplíně, které se však na přelomu 19. a 20. století dostalo prakticky všeobecného uznání a která se stala základnou téměř veškeré moderní matematiky. Zhroucení matematiky vystavěné na Cantorově teorii na počátku 20. století (budeme o něm podrobně hovořit v §3), které tak dramaticky poznamenalo vývoj matematiky ve 20. století, ani v nejmenším nesnižuje význam Cantorovy role v dějinách světové matematiky.

G. Cantor se narodil v r. 1845 v Petrohradě, kde jeho otec vedl až do r. 1856 obchodní firmu. Malý Georg od malička tíhnul k matematice a přes počáteční otcův odpor ji také (současně s fyzikou a filozofií) studoval v Curychu, Göttingen a především v Berlíně, kde r. 1867 promoval. Největší vliv ze všech učitelů na něj měl Karl Weierstrass, který také patřil k těm nemnoha matematikům, u nichž našel Cantor i v nejtěžších chvílích oporu. Od r. 1869 až do r. 1913 působil Cantor na univerzitě v Halle.

Od studentských let projevoval vynikající nadání; koncem 60. let napsal řadu prací z teorie čísel, algebry a teorie funkcí. Jeho nejplodnějším životním obdobím však byla léta 1873 – 1884, v nichž geniálním způsobem položil základy teorie množin a po obsahové stránce tuto teorii vybudoval prakticky do dnešní podoby.

Při studiu trigonometrických řad dokázal v r. 1873 nespočetnost množiny všech reálných čísel (v práci *Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen* – tj. *O jedné vlastnosti souhrnu všech reálných algebraických čísel*; tato práce byla publikována v r. 1874). Je to jeho první práce s množinovou tématikou. (Překlad této práce dále uvádíme.) V sérii dalších prací z uvedeného období zavedl pojem mohutnosti množiny a vybudoval teorii kardinálních a ordinálních čísel.

Proti teorii množin byly od počátku vznášeny četné výhrady. Hlavní námitky byly vznášeny proti tomu, jak se v ní pracuje s aktuálně nekonečnými množinami; řada matematiků nikdy nepochopila hloubku a dosah Cantorova učení. V čele tohoto proticantorovského tažení byl až

do své smrti bývalý Cantorův berlínský učitel Leopold Kronecker. Cantor měl četné problémy s uveřejňováním svých prací, byl napadán a jeho dílo bylo znevažováno. Skutečných přátel a zastánců měl jen nemnoho. Kromě Weierstrasse to byl především již zmiňovaný R. Dedekind, s nímž Cantora pojilo od r. 1872, kdy se víceméně náhodně ve Švýcarsku seznámili, dlouholeté přátelství. (Ze zachované korespondence mezi nimi lze dobře vysledovat, jak oboustranně plodné bylo toto přátelství prudkého bouřlivého „romantika“ Cantora a suchého střízlivého „klasika“ Dedekinda.)

Úporná práce, dílčí neúspěchy při řešení některých problémů, spojených především s „hypotézou kontinua“ a neustálé útoky jeho odpůrců však vykonaly své. V r. 1884 podléhá Cantor prudké depresi, musí být léčen na nervové klinice a vážně uvažuje o tom, že matematiky zcela zanechá. Od té doby se u něho střídají období tvůrčí práce s depresivními stavy. V r. 1897, tedy v době, kdy jeho teorie konečně dochází všeobecného uznání, publikuje Cantor svou poslední práci. V roce 1899 se ještě na krátký čas vrací k tvůrčí práci, aby se pak již definitivně odmlčel. V r. 1905 končí svou přednáškovou činnost, v r. 1913 odchází z univerzity a v r. 1918 v psychiatrické léčebně umírá.

Nebyl to lehký život, co Georg Cantor prožil. V mnoha směrech byl podobný osudu jiných géniů v historii lidské vědy a kultury. Jednou provždy však zůstane zapsán v dějinách lidského poznávání, neboť to byl on, kdo nám zpřístupnil krásný a tajuplný svět — svět nekonečných množin.

Ukázky z Cantorova díla

Nejprve uvedeme již zmiňovanou práci z r. 1874. Jak jsme již napsali, je to ve světové matematické literatuře první práce týkající se teorie množin (byť pojem „množina“ — německy „die Menge“ — se v ní vůbec nevyskytuje). (Cantor hovoří jen o „souhrnu“ čísel — tak překládáme výraz „Inbegriff“. Pojem „množina“ se vůbec poprvé vyskytuje až v jeho práci z r. 1879.) Stejně tak se v práci nevyskytují pojmy „spočetný“, respektive „nespočetný“. Přesto je tu však učiněn rozhodující krok — krok, který Bolzano, jak jsme viděli, možná tušil, ale neudělal; máme zde na mysli důkaz faktu, že existují dvě neekvivalentní nekonečné množiny. Tato skutečnost byla pro Cantora odrazovým můstkem k vybudování teorie kardinálních čísel.

O jedné vlastnosti souhrnu všech reálných algebraických čísel

Reálným algebraickým číslem obecně rozumíme reálnou veličinu ω, která vyhovuje neidentické rovnici tvaru

$$a_0\omega^n + a_1\omega^{n-1} + \cdots + a_n = 0 \qquad (1)$$

kde n, $a_0, a_1, \ldots, a_n$ jsou celá čísla. Můžeme zde přitom bez újmy na obecnosti předpokládat, že čísla n a a_0 jsou kladná, koeficienty $a_0, a_1, \ldots, a_n$ nemají společného dělitele a rovnost (1) je nerozložitelná. Za těchto předpokladů bude zaručeno, že podle známých základních aritmetických a algebraických pravidel je rovnost (1), jíž vyhovuje nějaké reálné algebraické číslo, plně určena. Obráceně, každé rovnici tvaru (1) přísluší nejvýše tolik reálných algebraických čísel ω, které jí vyhovují, kolik činí její stupeň n. Reálná algebraická čísla tvoří jako celek souhrn veličin, který označíme (ω). Jak je jednoduše vidět, má tento systém tu vlastnost, že v každém okolí jakéhokoliv myšleného čísla α leží nekonečně mnoho čísel z (ω). O to nápadnější proto na první pohled může být skutečnost, že souhrn (ω) může být jednoznačně přiřazen souhrnu (ν) všech celých kladných čísel tak, že každému algebraickému číslu ω přísluší jisté celé kladné číslo a naopak, každému celému číslu ν odpovídá plně určené reálné algebraické číslo ω, tak, že jinými slovy řečeno, souhrn (ω) si můžeme představit ve tvaru nekonečné zákonitě utvořené řady

$$\omega_1, \omega_2, \ldots, \omega_\nu, \ldots , \tag{2}$$

v níž se vyskytnou všechny prvky z (ω) a každý z nich přitom na určitém místě v (2), přičemž toto místo je dáno příslušným indexem. Jakmile nalezneme zákonitost, podle níž je toto přiřazení prováděno, je možno ji libovolně modifikovat. Bude tudíž postačovat, když v §1 uvedu to přiřazovací pravidlo, které, jak se domnívám, je nejjednodušší.

Této vlastnosti souhrnu všech reálných algebraických čísel využiji k tomu, abych pomocí §1 v §2 ukázal, že když utvoříme libovolnou řadu reálných čísel veličin tvaru (2), můžeme určit v každém zadaném intervalu $(\alpha \ldots \beta)$ číslo η, které nebude obsaženo v (2). Kombinací výsledků těchto dvou paragrafů podáme nový důkaz dřívějšího Liouvilleova tvrzení, že v každém zadaném intervalu $(\alpha \ldots \beta)$ leží nekonečně mnoho transcendentních, tj. nealgebraických čísel. Dále uvedeme v §2 Větu jako základ k zdůvodnění toho, proč souhrn reálných veličin, které tvoří kontinuum (jako reálná čísla, která jsou ≥ 0 a ≤ 1) nelze jednoznačně přiřadit souhrnu (ν). Tak najdeme zřetelný rozdíl mezi tak zvaným kontinuem a souhrnem utvořeným ze všech reálných algebraických čísel.

§1.

Vraťme se k rovnici (1), které vyhovuje algebraické číslo ω a která je za uvedených předpokladů plně určena. Zvětšeme číslo $n - 1$, kde n je stupeň čísla ω, o součet absolutních hodnot koeficientů uvedené rovnice a označme výsledek N;

N nazveme výškou čísla ω. Při použití obvyklého označení tedy platí

$$N = n - 1 + |a_0| + |a_1| + \cdots + |a_n|. \tag{3}$$

Výška N je podle toho pro každé reálné algebraické číslo ω jisté kladné celé číslo; obráceně, ke každé kladné celočíselné hodnotě N existuje jen konečně mnoho algebraických reálných čísel o výšce N; jejich počet označme $\varphi(N)$. Je například $\varphi(1) = 1$, $\varphi(2) = 2$, $\varphi(3) = 4$. Nyní čísla souhrnu (ω), tj. algebraická reálná čísla, postupně uspořádáme do řady tak, že nejprve vezmeme číslo ω_1 jako jediné číslo o výšce 1; poté vezmeme následující $\varphi(2) = 2$ algebraická reálná čísla o výšce 2 a označme je ω_2, ω_3. K těmto můžeme připojit $\varphi(3) = 4$ čísla o výšce $N = 3$ tak, aby jejich velikosti vzrůstaly. Obecně můžeme tímto způsobem očíslovat všechna čísla z (ω) až do určité výšky $N = N_1$, rozmístit je na určená místa a za ně připojit reálná algebraická čísla o výšce $N = N_1 + 1$ a sice tak, aby jejich velikosti vzrůstaly. Takto obdržíme souhrn (ω) všech reálných algebraických čísel ve tvaru

$$\omega_1, \omega_2, \ldots, \omega_\nu, \ldots$$

a s ohledem na dané uspořádání můžeme hovořit o ν-tém reálném algebraickém čísle, přičemž není opomenuto žádné z čísel souhrnu (ω).

§2.

Je-li dána jakýmkoliv způsobem utvořená nekonečná řada navzájem různých reálných veličin

$$\omega_1, \omega_2, \ldots, \omega_\nu, \ldots , \tag{4}$$

lze v každém zadaném intervalu $(\alpha \ldots \beta)$ určit číslo η (a tedy nekonečně mnoho takových čísel), které se nevyskytuje v řadě (4). Toto tvrzení nyní dokážeme. Mějme tedy libovolně zadaný interval $(\alpha \ldots \beta)$ takový, že $\alpha < \beta$. První dvě čísla naší řady (4), která leží uvnitř tohoto intervalu (z něhož vyloučíme hranici) můžeme označit α', β' tak, že $\alpha' < \beta'$. Stejně tak označme první dvě čísla z naší řady, která leží uvnitř $(\alpha' \ldots \beta')$ jako α'', β'' a to tak, že $a'' < \beta''$; podle téhož pravidla utvoříme následující interval $(\alpha'' \ldots \beta'')$ atd. Zde uvedená čísla $\alpha', \alpha'' \ldots$ jsou podle definice jistá čísla naší řady (4), jejichž velikosti se monotónně mění a totéž platí o číslech $\beta', \beta'' \ldots$; velikost čísel $a', \alpha'', \ldots$ neustále roste, velikost čísel $\beta', \beta'', \ldots$ klesá. Každý z intervalů $(\alpha \ldots \beta), (\alpha' \ldots \beta'), (\alpha'' \ldots \beta''), \ldots$ v sobě uzavírá všechny následující. — Jsou tedy nyní myslitelné dvě možnosti. Buďto je počet takto utvořených intervalů konečný; poslední z nich nechť je $(\alpha^{(\nu)} \ldots \beta^{(\nu)})$. Protože uvnitř tohoto intervalu může ležet nejvýše jedno číslo řady (4), můžeme

v tomto intervalu zvolit číslo η, které není ve (4) obsaženo. V tomto případě je věta dokázána.

Nebo je počet utvořených intervalů nekonečně velký. Pak ale mají čísla $\alpha, \alpha', \alpha'', \ldots$, vzhledem k tomu, že jejich velikosti neustále rostou aniž by rostly do nekonečna, jistou horní závoru α^∞. Totéž platí pro čísla $\beta, \beta', \beta'', \ldots$, jejichž velikosti klesají; jejich závoru označme β^∞. Je-li $\alpha^\infty = \beta^\infty$ (což je případ, který vždy nastane v případě souhrnu (ω) všech reálných algebraických čísel), lze se lehce přesvědčit, podíváme-li se nazpět na definici intervalu, že číslo $\eta = \alpha^\infty = \beta^\infty$ nemůže být v naší řadě obsaženo. (Kdyby totiž bylo číslo η v naší řadě obsaženo, měli bychom $\eta = \omega_p$, kde p je jistý index. To však není možné, protože ω_p neleží uvnitř intervalu $(\alpha^{(p)} \ldots \beta^{(p)})$, zatímco číslo η podle definice uvnitř tohoto intervalu leží.) Je-li však $\alpha^\infty < \beta^\infty$, pak žádné číslo η z vnitřku intervalu $(\alpha^\infty \ldots \beta^\infty)$ nebo též hranice tohoto intervalu, pokud jen odpovídá uvedeným požadavkům, není v řadě (4) obsaženo. Tvrzení dokázaná v tomto odstavci nám umožňují různá zobecnění, z nichž zvolíme následující: „Je-li $\omega_1, \omega_2, \ldots, \omega_n, \ldots$ konečná nebo nekonečná řada vzájemně lineárně nezávislých čísel (takže není splněna žádná rovnice tvaru $a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n = 0$ s celočíselnými koeficienty, které nejsou všechny nulové) a je-li dán souhrn (Ω) všech takových čísel Ω, která lze určit pomocí racionálních funkcí s celočíselnými koeficienty z daných čísel ω, pak v každém intervalu $(\alpha \ldots \beta)$ existuje nekonečně mnoho čísel, která nejsou v (Ω) obsažena.“ Skutečně, můžeme se podobně jako v §1 přesvědčit, že souhrn (Ω) lze seřadit do tvaru

$$\Omega_1, \Omega_2, \ldots, \Omega_\nu, \ldots ,$$

z čehož, vzhledem k §2, plyne správnost tvrzení.

★ ★ ★

Druhou Cantorovou prací, kterou zde v překladu uvedeme, je článek uveřejněný v r. 1890. V této krátké stati se poprvé objevuje známá důkazová metoda, dnes běžně nazývaná *Cantorova diagonální metoda*. Vyjádřeno v řeči kardinálních čísel je zde dokázáno, že $2^{\aleph_0} > \aleph_0$ a poté je ukázáno, že zcela analogicky lze pro *každé* kardinální číslo odvodit $2^m > m$.

Povšimněme si, že ani v této práci se nevyskytuje pojem „množina“, i když v této době již Cantor toto pojmenování v jiných pracích užíval.

O jedné elementární otázce z nauky o souhrnech

V práci nazvané: *O jedné vlastnosti souhrnu všech reálných algebraických čísel* (Journ. Math. Bd. **77**, S. 258) se poprvé nachází důkaz věty, že existují souhrny,

které nelze, byť jsou nekonečné, jednoznačně přiřadit souhrnu všech konečných celých čísel $1, 2, 3, \ldots, \nu, \ldots$ nebo, jak říkáme, které nemají mohutnost číselné řady $1, 2, 3, \ldots, \nu, \ldots$. Z toho, co jsme tam dokázali v §2, okamžitě plyne, že například systém všech reálných čísel ležících v libovolném intervalu $(\alpha \ldots \beta)$ nelze sestavit do řady tvaru

$$\omega_1, \omega_2, \ldots, \omega_\nu, \ldots .$$

Toto tvrzení však lze dokázat mnohem jednodušeji, nezávisle na vlastnostech iracionálních čísel.

Jsou-li totiž m a w dva navzájem rozdílné objekty, můžeme studovat souhrn M prvků tvaru

$$E = (x_1, x_2, \ldots, x_\nu, \ldots),$$

které závisí na nekonečně mnoha souřadnicích $x_1, x_2, \ldots, x_\nu, \ldots$, kde každá z těchto souřadnic je buďto m nebo w.

K prvkům M patří například tři následující:

$E^I = (m, m, m, m, \ldots)$,

$E^{II} = (w, w, w, w, \ldots)$,

$E^{III} = (m, w, m, w, \ldots)$.

Nyní tvrdím, že takový systém M nemá mohutnost řady $1, 2, \ldots, \nu, \ldots$.

Plyne to z následující věty:

Je-li $E_1, E_2, \ldots, E_\nu, \ldots$ jakákoliv jednoduchá nekonečná řada prvků systému M, pak existuje prvek E_0 z M, který není žádným z prvků E_ν.

K důkazu nechť je

$E_1 = (a_{1,1}, a_{1,2}, \ldots, a_{1,\nu}, \ldots)$,

$E_2 = (a_{2,1}, a_{2,2}, \ldots, a_{2,\nu}, \ldots)$,

. . . . . Tato $a_{\mu,\nu}$ jsou zde buďto m nebo w. Buď

$E_\mu = (a_{\mu,1}, a_{\mu,2}, \ldots, a_{\mu,\nu}, \ldots)$,

. . . . . .

nyní řada $b_1, b_2, , \ldots, b_\nu, \ldots$ definována tak, že b_ν bude rovněž rovno m nebo w a přitom různé od $a_{\nu,\nu}$.

Je-li tedy $a_{\nu,\nu} = m$, nechť je $b_\nu = w$ a je-li $a_{\nu,\nu} = w$, nechť $b_\nu = m$.

Povšimneme-li si nyní prvku

$$E_0 = (b_1, b_2, b_3, \ldots)$$

z M, vidíme okamžitě, že rovnost $E_0 = E_\mu$ nemůže být splněna pro žádné celé číslo μ. Kdyby totiž pro jisté μ a pro všechny hodnoty ν platilo

$$b_\nu = a_{\mu,\nu},$$

pak by zejména platilo

$$b_\mu = a_{\mu,\mu},$$

což je podle definice čísla b_ν vyloučeno.

Z této věty bezprostředně plyne, že souhrn všech prvků z M nelze seřadit do tvaru řady $E_1, E_2, \ldots, E_\nu, \ldots$; dostali bychom totiž spor, že E_0 by současně bylo i nebylo prvkem M.

Tento důkaz překvapuje nejen svou velkou jednoduchostí, ale zejména tím, že princip v něm uvedený lze bezprostředně použít k důkazu obecnějšího tvrzení, že totiž mohutnosti systémů nemají maximum, což je totéž jako tvrzení, že ke každému zadanému systému L existuje jiný systém M, který má větší mohutnost než L.

Buď například L lineární kontinuum, jako třeba souhrn všech reálných čísel, která jsou ≥ 0 a ≤ 1.

Pod M rozumějme souhrn všech jednoznačných funkcí $f(x)$, které nabývají hodnot 0 nebo 1, přičemž x proběhne všechny reálné hodnoty, které jsou ≥ 0 a ≤ 1.

To, že M nemá menší mohutnost než L, plyne z toho, že v M existují podmnožiny, které mají stejnou mohutnost jako L; například je to podmnožina utvořená z těch funkcí proměnné x, které mají v jednom jediném x_0 z x hodnotu 1 a ve všech ostatních x mají hodnotu 0.

M ale nemá ani stejnou mohutnost jako L. Kdybychom totiž souhrn M mohli jednoznačně popsat pomocí proměnné z, mohli bychom si M představit ve tvaru jednoznačné funkce obou proměnných x a z

$$\varphi(x, z),$$

a to tak, že zadáním z bychom mohli obdržet prvek $f(x) = \varphi(x, z)$ z M a také naopak, každý prvek $f(x)$ z M bychom získali jako $\varphi(x, z)$ jedinou volbou z. Tím však dostáváme spor. Myslíme-li si, že $g(x)$ je ta jednoznačná funkce x, která nabývá jen hodnot 0 a 1 a pro každou hodnotu x je různá od $\varphi(x, z)$, pak je na jedné straně $g(x)$ prvek M, na druhé straně však žádnou volbou $z = z_0$ nemůžeme tuto funkci dostat z $\varphi(x, z)$, neboť $\varphi(x_0, z_0)$ je různé od $g(z_0)$.

Není-li tedy mohutnost systému M ani menší ani rovna mohutnosti L, plyne odtud, že je větší než mohutnost L. (Viz Crelles Journal Bd. **84**, S. 242.)

V práci *Grundlagen einer allgemeinen Mannigfaltigkeitlehre* (Leipzig 1883) jsem dokázal pomocí zcela jiných metod, že mohutnosti nemají maximum. Dokonce je tam dokázáno, že souhrn všech mohutností, když ho uspořádáme podle velikostí, tvoří „dobře uspořádanou množinu“, takže ve skutečnosti

ke každé mohutnosti existuje větší a rovněž ke každé shora neohraničené množině mohutností existuje nějaká mohutnost ještě větší.

„Mohutnosti“ reprezentují jediné a zákonité zobecnění konečných „kardinálních čísel“; nejsou ničím jiným, než aktuálně nekonečně velkými kardinálními čísly a patří jim táž realita a určitost jako těm původním. Jen zákonitosti mezi nimi, nazývané „teorie čísel“, jsou zde částečně odlišné od zákonitostí ve světě „Konečna“.

Další objevy na tomto poli jsou úkolem budoucnosti.

★ ★ ★

Poslední ukázkou z Cantorova díla, kterou uvedeme, bude několik partií z obsáhlé práce *Beiträge zur Begründung der transfiniten Mengelehre*, tj. *Příspěvky k základům teorie transfinitních množin*, která je poslední Cantorovou publikovanou prací. (První část vyšla v časopise *Mathematische Annalen* v r. 1895, druhá část tamtéž v r. 1897. Celá práce má 76 stran.) Toto dílo je vynikajícím završením Cantorovy více než dvacetileté práce na výstavbě teorie množin.

V úvodu 1. paragrafu Cantor **poprvé vysvětluje**, co rozumí množinou. (Tato pasáž bývá často a nepřesně citována. Z textu je zřejmé, že ji Cantor zcela jistě **nepokládal** za *definici*, jak bývá často nesprávně uváděno. Pojem samotný na jedné straně podle Cantorových původních představ zjevně pro svou „samozřejmost“ žádnou definici nevyžadoval; na druhé straně v době publikace této práce již Cantor znal těžkosti, k nimž jeho intuitivní přístup vede.) Ve 2. paragrafu Cantor definuje nerovnost mezi kardinálními čísly.

Kromě těchto dvou paragrafů v následující ukázce uvedeme část §4, v němž je zavedeno umocňování kardinálních čísel, část §6, v němž je popsána specifická role čísla $\aleph_0$ a konečně část §15, v němž se hovoří o množině $Z(\aleph_0)$ ordinálních čísel. Čtenář jistě i bez zvláštního upozornění postřehne, že styl vyjadřování a důkazové metody této práce jsou již zcela moderní; §15 by mohl být bez větších úprav — stejně jako další části práce — zařazen i do moderní učebnice.

Rozdíl mezi první Cantorovou množinovou prací a touto poslední je jistě dostatečným svědectvím, jak obrovské dílo Cantor v uvedeném období vykonal.

Příspěvky k základům teorie transfinitních množin

§1.

MOHUTNOSTI ČILI KARDINÁLNÍ ČÍSLA

„Množinou“ rozumíme každý souhrn M určitých rozlišitelných objektů m našeho nazírání nebo našeho myšlení (nazývaných „prvky“ v M) shrnutých v jeden celek. Symbolicky to zapíšeme takto:

$$M = \{m\}. \tag{1}$$

Sjednocením více množin $M, N, P, \ldots,$ které nemají společné prvky, rozumíme množinu označenou

$$(M, N, P, \ldots). \tag{2}$$

Prvky této množiny jsou prvky z M, z N, z P atd., brány všechny společně.

„Část“ nebo „podmnožina“ množiny M je každá *jiná* množina M_1, jejíž prvky jsou současně prvky v M.

Je-li M_2 částí M_1 a M_1 částí M, pak je také M_2 částí M.

Každé množině M přísluší jistá „mohutnost“, kterou nazýváme také „kardinální číslo“.

„Mohutností“ nebo „kardinálním číslem“ množiny M rozumíme obecný pojem, který v našem myšlení přiřadíme každé množině M tak, že přitom abstrahujeme od vlastností jejích různých prvků m a od uspořádání při jejich zadávání!

Výsledek této dvojí abstrakce, kardinální číslo čili mohutnost množiny M, označujeme

$$\overline{\overline{M}}. \tag{3}$$

Takto z každého jednotlivého prvku m, nepřihlížíme-li k jeho vlastnostem, vznikne „jednotka“, takže kardinální číslo M samotné je určitá množina utvořená z těchto jednotek, jakožto rozumový odraz projekce dané množiny v naší mysli.

O dvou množinách M a N řekneme, že jsou ekvivalentní, což označíme

$$M \sim N \qquad \text{nebo} \qquad N \sim M, \tag{4}$$

jestliže lze nalézt takové jejich vzájemné přiřazení, že každému prvku z jedné odpovídá při tomto přiřazení jeden a jenom jeden prvek druhé.

Každé části M_1 v M odpovídá tedy jistá ekvivalentní část N_1 z N.

Je-li dáno takové přiřazení dvou ekvivalentních množin, pak lze toto přiřazení (až na případ, že obě množiny jsou jednoprvkové) libovolně modifikovat. Zejména lze zařídit, že danému prvku m_0 z M odpovídá jistý prvek n_0 z N. Jestliže si totiž prvky m_0 a n_0 neodpovídají při původním přiřazení, ale prvku m_0 z M odpovídá prvek n_1 z N a prvku n_0 z N odpovídá prvek m_1 z M, pak pozměníme zadání tak,

aby si vzájemně odpovídaly prvky m_0 a n_0 a rovněž tak m_1 a n_1; ostatní prvky pak zůstanou přiřazeny podle původního pravidla. Takto je úkol splněn.

Každá množina je ekvivalentní se sebou samotnou:

$$M \sim M. \tag{5}$$

Jsou-li dvě množiny ekvivalentní s třetí, pak jsou také vzájemně ekvivalentní:

$$\text{z } M \sim P \text{ a } N \sim P \text{ plyne } M \sim N. \tag{6}$$

Základní význam má nyní skutečnost, že *dvě množiny M a N jsou ekvivalentní tehdy a jen tehdy, když mají stejné kardinální číslo*:

$$\textit{ze vztahu } M \sim N \textit{ plyne } \overline{\overline{M}} = \overline{\overline{N}}, \tag{7}$$

a

$$\textit{ze vztahu } \overline{\overline{M}} = \overline{\overline{N}} \textit{ plyne} M \sim N. \tag{8}$$

Ekvivalence množin tedy tvoří nutné a neklamné kritérium toho, že jejich kardinální čísla jsou stejná.. . .

§2.

„VĚTŠÍ“ a „MENŠÍ“ MEZI MOHUTNOSTMI

Nechť pro dvě množiny M a N s kardinálními čísly $a = \overline{\overline{M}}$ a $b = \overline{\overline{N}}$ jsou splněny následující dvě podmínky:

1) M neobsahuje část ekvivalentní s N,

2) N obsahuje část N_1 takovou, že $N_1 \sim M$.

Pak je především patrno, že tyto podmínky zůstanou splněny, když množiny M a N nahradíme dvěma ekvivalentními M' a N'. Takto je však určen jistý vzájemný vztah mezi kardinálními čísly a, b.

Dále, ekvivalence množin M a N, jakož tedy i rovnost čísel a, b je vyloučena; kdyby platilo $M \sim N$, pak by vzhledem k tomu, že $N_1 \sim M$, také platilo $N_1 \sim N$ a tedy předpoklad $M \sim N$ by nás přivedl k tomu, že existuje část M_1 v M taková, že $M_1 \sim M$ a tedy také $M_1 \sim N$, což je spor s podmínkou 1).

Za třetí, tento vztah mezi čísly a, b je takový, že tentýž vztah mezi b, a není možný. Když tedy v 1) a 2) prohodíme role M a N, obdržíme dvě vzájemně kontradiktorické podmínky.

Vztah mezi a, b charakterizovaný podmínkami 1) a 2) vyjádříme slovy: a je menší než b nebo také b je větší než a; symbolicky

$$a < b \qquad nebo \qquad b > a. \tag{1}$$

Lehce lze dokázat, že

$$když\ a < b,\ b < c, \quad pak\ také\ a < c.$$

Právě tak okamžitě z definice plyne, že když P_1 je část množiny P, pak z $a < \overline{\overline{P_1}}$ plyne také $a < \overline{\overline{P}}$ a ze vztahu $\overline{\overline{P}} < b$ plyne $\overline{\overline{P}}_1 < b$.

Ukázali jsme, že ze tří vztahů

$$a = b, \quad a < b, \quad b < a$$

každý vylučuje zbývající dva.

Naproti tomu se v žádném případě nerozumí samo sebou, a také bychom to nyní nemohli dokázat, že pro každá dvě kardinální čísla a, b musí nutně nastat některá z uvedených možností.

Teprve později, až přehlédneme rostoucí posloupnost transfinitních kardinálních čísel a poznáme jejich vzájemné vztahy, budeme moci dokázat tvrzení: A. *„Jsou-li a,b libovolná dvě kardinální čísla, pak platí buďto $a = b$ nebo $a < b$ nebo $a > b$.“*

§4.

UMOCŇOVÁNÍ MOHUTNOSTÍ

„Pokrytím množiny N prvky množiny M“ nebo stručněji „pokrytím N prvky M“ rozumíme pravidlo, kterým je s každým prvkem n z N svázán jistý prvek z M, přičemž jeden a tentýž prvek z M může být použit i opakovaně. Takto je tedy prvek z M, který je svázán s n, jistou jednoznačnou funkcí n a můžeme ho proto označit $f(n)$. Tuto funkci nazveme „pokrývací funkcí prvků n“. Odpovídající pokrytí množiny N označíme $f(N)$.

Řekneme, že dvě pokrytí $f_1(N)$ a $f_2(N)$ jsou si rovna právě tehdy, když pro všechny prvky n z N platí rovnost

$$f_1(n) = f_2(n); \tag{1}$$

to znamená, že když existuje byť jen jediný prvek $n = n_0$, pro který uvedená rovnost není splněna, pak již považujeme pokrytí $f_1(N)$ a $f_2(N)$ za navzájem různá.

Kupříkladu můžeme, když m_0 je jistý prvek z M, zadat pro všechny n

$$f(n) = m_0.$$

Takto je pak určeno pokrytí N prvky množiny M.

Jiné pokrytí obdržíme, když pro dva různé prvky m_0 a m_1 z M a pro jistý prvek n_0 z N zadáme

$$f(n_0) = m_0, \qquad f(n) = m_1$$

pro všechna n různá od n_0.

Souhrn všech rozdílných pokrytí N množinou M tvoří jistou množinu s prvky $f(N)$. Nazveme ji „množinou všech pokrytí N prvky M“ a označíme ji $(N|M)$. Je tedy

$$mm(N|M) = \{f(N)\}. \tag{2}$$

Platí-li $M \sim M'$ a $N \sim N'$, pak lze lehce odvodit, že také

$$(N|M) \sim (N'|M'). \tag{3}$$

Kardinální číslo množiny $(N|M)$ tedy závisí jen na kardinálních číslech $\overline{\overline{M}} = a$ a $\overline{\overline{N}} = b$. Můžeme proto definovat mocninu a^b takto:

$$a^b = \overline{\overline{(N|M)}}. \tag{4}$$

§6.

NEJMENŠÍ KARDINÁLNÍ ČÍSLO ALEF NULA

Množiny s konečným kardinálním číslem nazýváme „konečnými množinami“; všechny ostatní množiny nazýváme „transfinitními množinami“ a jejich odpovídající kardinální čísla nazýváme „transfinitními kardinálními čísly“.

Souhrn všech konečných kardinálních čísel ν nám udává následující příklad transfinitní množiny; jí odpovídající kardinální číslo (§1) „alef nula“, symbolicky $\aleph_0$, definujeme vztahem

$$\aleph_0 = \overline{\overline{\{\nu\}}}. \tag{1}$$

To, že $\aleph_0$ je transfinitní číslo, tj. není rovno žádnému konečnému číslu μ, plyne z té jednoduché skutečnosti, že když přidáme k množině $\{\nu\}$ nějaký nový prvek e_0, je sjednocení $(\{\nu\}, e_0)$ ekvivalentní s původní množinou $\{\nu\}$. Existuje totiž mezi

nimi vzájemně jednoznačné přiřazení, při němž prvku e_0 odpovídá první prvek 1 druhé množiny, prvku ν první množiny pak odpovídá prvek $\nu + 1$. Podle §3 tak dostáváme

$$\aleph_0 + 1 = \aleph_0. \tag{2}$$

V §5 jsme však dokázali, že (pro konečná μ) je $\mu + 1$ různé od μ, takže $\aleph_0$ není rovno žádnému konečnému číslu μ.

Číslo $\aleph_0$ je větší než všechna konečná čísla μ:

$$\aleph_0 > \mu. \tag{3}$$

Toto plyne okamžitě z §3, neboť $\mu = \overline{\overline{\{1, 2, 3, \ldots, \mu\}}}$, žádná část množiny $\{1, 2, 3, \ldots, \mu\}$ není ekvivalentní s množinou $\{\nu\}$ a samotná množina $\{1, 2, 3, \ldots, \mu\}$ je částí $\{\nu\}$.

Na druhé straně je $\aleph_0$ nejmenší transfinitní kardinální číslo.

Je-li a jakékoliv transfinitní kardinální číslo různé od $\aleph_0$, pak

$$\aleph_0 < a. \tag{4}$$

Toto plyne z následujících vět:

A. *V každé transfinitní množině T existuje podmnožina s kardinálním číslem $\aleph_0$.*

D ů k a z: Odstraníme-li podle nějakého pravidla z T konečný počet prvků $t_1, t_2, \ldots, t_{\nu-1}$, zůstane zde pořád možnost odstranit i další prvek t_ν. Množina $\{t_\nu\}$, kde ν je libovolné konečné kardinální číslo, je podmnožinou v T s kardinálním číslem $\aleph_0$, protože $\{t_\nu\} \sim \{\nu\}$ (§1).

B. *Je-li S transfinitní množina s kardinálním číslem $\aleph_0$ a S_1 je transfinitní podmnožina v S, pak je rovněž $\overline{\overline{S_1}} = \aleph_0$.*

§15.

ČÍSLA DRUHÉ ČÍSELNÉ TŘÍDY $Z(\aleph_0)$

Druhá číselná třída $Z(\aleph_0)$ je souhrn $\{\alpha\}$ všech ordinálních typů dobře uspořádaných množin, jejichž kardinální číslo je $\aleph_0$ (§6).

A. Druhá číselná třída obsahuje nejmenší prvek $\omega = \mathrm{Lim}_\nu \nu$.

D ů k a z: Symbolem ω rozumíme typ dobře uspořádané množiny

$$F_0 = (f_1, f_2, \ldots, f_\nu, \ldots), \tag{1}$$

kde ν probíhá všechna konečná ordinální čísla a

$$f_\nu < f_{\nu+1}. \tag{2}$$

Je tedy (§7)

$$\omega = \overline{F_0} \tag{3}$$

a (§6)

$$\overline{\omega} = \aleph_0. \tag{4}$$

ω je tedy číslo druhé třídy a sice to nejmenší. Je-li γ jakékoliv ordinální číslo $< \omega$, musí být (§14) typem nějakého řezu v F_0. F_0 má však pouze řezy

$$A = (f_1, f_2, \ldots, f_\nu)$$

s *konečným* ordinálním číslem ν. Proto platí $\gamma = \nu$.

Neexistuje tedy *transfinitní* ordinální číslo, které by bylo menší než ω, takže ω je nejmenší takové. Podle toho, co jsme uvedli v §14 o $\mathrm{Lim}_\nu \alpha_\nu$ je zřejmě $\omega = \mathrm{Lim}_\nu \nu$.

B. *Je-li α libovolné číslo druhé třídy, pak za ním následuje jako nejbližší větší číslo téže číselné třídy číslo $\alpha + 1$.*

3 Antinomie teorie množin. Třetí krize matematiky

Nikdy není tak zle,
aby nemohlo být ještě hůř.
GATTUSOVO ROZŠÍŘENÍ MURPHYHO ZÁKONA

19. století bylo obdobím prudkého rozvoje přírodních i společenských věd. V řadách vědců řady oborů narůstá uspokojení nad dosaženými výsledky: zdá se jim, že přírodní vědy zmapovaly a popsaly vše podstatné v reálném světě. Zasloužilo by si hlubšího rozboru, čím to bylo způsobeno, že téměř současně — na přelomu 19. a 20. století — dochází v řadě z nich, včetně matematiky, k dramatickému zvratu.

Tak například známý americký fyzik Albert Abraham Michelson, jehož jistě nebudeme podezírat z malého přehledu a nedostatku odbornosti, v roce 1894 prohlašuje:

Důležité základní zákony a fakta ve fyzice již byly všechny objeveny a jsou dnes tak pevně prokázány, že možnost, že by vůbec kdy byly nahrazeny v důsledku nových objevů, je nesmírně vzdálená. . . Naše budoucí objevy je třeba hledat na šestém desetinném místě!

Dva roky poté, v r. 1896, objevuje Antoine Henri Becquerel přirozenou radioaktivitu, v r. 1905 publikuje Albert Einstein speciální teorii relativity (v r. 1916 pak obecnou), ve 20. letech se konstituuje kvantová mechanika atd.: co z fyzikálního obrazu světa z konce 19. století vlastně přetrvalo až do dneška?

Něco podobného se na přelomu století odehrálo i v matematice, s důsledky pro matematiku samotnou asi ještě závažnějšími.

Uváděli jsme již, jak podrážděné reakce vyvolaly první Cantorovy množinové práce. Postupně se však prokázalo, jak mocným a potřebným nástrojem se teorie množin pro matematiku stala. Ke konci 19. století dosáhla teorie množin téměř všeobecného uznání a stala se základnou, na níž byla budována prakticky celá matematika. Všeobecné mínění matematiků té doby vystihuje známý výrok čelného francouzského matematika a fyzika Henri Poincarého, jednoho z vůdčích duchů tehdejšího vědeckého světa, který na II. mezinárodním matematickém kongresu v Paříži v roce 1900 prohlašuje:

. . . nyní v matematice zůstávají jen celá čísla a konečné, respektive nekonečné systémy celých čísel . . . Matematika je plně aritmetizována. Dnes můžeme říci, že dosáhla absolutní přesnosti.

Je vskutku ironií osudu, že v době, kdy Poincaré tato slova pronášel, už bylo de facto jasné, že teorie oněch „nekonečných systémů celých čísel“, jakožto část teorie množin, má k oné absolutní přesnosti dále než daleko. Antinomie teorie množin, z nichž první již byla tehdy známa, vyvedly matematiky krutě z mylného zdání, že mají k dispozici spolehlivou základnu pro výstavbu svých teorií. A strastiplná cesta za překonáním těchto antinomií, cesta, na jejíž konec matematika dodnes nedorazila, nám ukázala, jak podstatně je nutno revidovat původní představy o možnosti spolehlivého vybudování základů matematiky. (O tom však budeme podrobněji hovořit v §4.) Z tohoto hlediska není označení ***3. krize matematiky*** pro období, které matematika od počátku 20. století prožívá, nijak přehnané.

(Připomeňme si, že *1. krize matematiky* cca v 5. stol. př. n.l. souvisela s objevem iracionálních čísel a se Zenónovými aporiemi o nemožnosti sestrojení konečných veličin z nekonečně mnoha částí. *2. krize matematiky*, jak jsme již uvedli, je spojována s nejasnostmi kolem počítání s nekonečně malými veličinami. Newton a Leibniz při výstavbě infinitesimálního počtu nedovedli tyto operace řádně zdůvodnit. Během doby bylo čím dál nejasnější jak je možné, že nezdůvodněné postupy s přesně nedefinovanými veličinami dávají převážně správné výsledky. Tato krize byla překonána díky práci Cauchyho, Weierstrasse a dalších v 19. století.)

V kapitole I jsme ukázali (viz větu 5.10), že když lze v nějaké teorii dokázat nějaké tvrzení a současně i jeho negaci, lze v této teorii dokázat *každé* tvrzení. Taková teorie je ovšem prakticky bezcenná. Přesně toto se ovšem stalo v Cantorově teorii množin, když se v ní objevily tzv. *antinomie*, někdy též nesprávně nazývané *paradoxy*.

První z těchto antinomií publikoval v r. 1897 italský matematik Cesare Burali-Forti v práci *Una questione sui numeri transfiniti*, Rendiconti Palermo **11**, 154 - 164). Cantor sám znal tuto

antinomii již v r. 1895; spočívá v tom, že *ordinální číslo dobře uspořádané množiny všech ordinálních čísel je větší než všechna ordinální čísla* (tzn., že existuje ordinální číslo větší než ono samo). (Srovnej s III. 6.2.)

Po objevení této antinomie bylo ještě možno chovat jistou naději, že ji bude možno nějak odstranit a situaci tedy bude možno zachránit. (Samotný Cantor až do konce života věřil, že jeho teorii bude možno nějak „opravit".) V prvním desetiletí 20. století se však těchto antinomií objevila celá řada; jednoznačně se tak prokázalo, že tato sporná tvrzení se neobjevují jen na „periférii" matematiky a netýkají se jen objektů, bez nichž se lze snadno obejít, ale právě naopak, ukázalo se, že obtíže tkví v podstatě věci a celá teorie množin musí být vybudována na zcela nových základech. Za 80 let, které od té doby uplynuly, ovšem nebylo nalezeno všeobecně přijaté řešení této situace — viz §4.

Nyní podáme stručný přehled nejznámějších antinomií.

Nejznámější je antinomie, kterou v r. 1902 objevil a v r. 1903 publikoval anglický matematik, filozof, logik, sociolog a veřejný činitel, lord Bertrand Russell. (Nezávisle na něm objevil tuto antinomii rovněž Ernst Zermelo. Russellova antinomie spočívá, jak jsme uvedli již v kapitole I, v tom, že když utvoříme „množinu S všech množin, které nejsou svým vlastním prvkem", vede ke sporu předpoklad $S \in S$ i předpoklad $S \notin S$.

Tato antinomie byla zpopularizována samotným Russellem a mnoha dalšími matematiky. Z celé řady těchto populárních variant uveďme alespoň následující:

Jistý vojín, povoláním holič, dostal od svého velitele příkaz, že musí holit všechny vojáky své čety, kteří se neholí sami a nesmí holit nikoho jiného. Tím se ovšem tento vojín ocitl v neřešitelné situaci, neboť *sám se má holit právě tehdy, když se sám nebude holit*.

V roce 1905 uveřejnil francouzský lékař a matematik — a v té době ředitel Oceánografického muzea v Monaku — Jules Richard *Richardova antinomie*antinomii, v níž vynikajícím způsobem využil (nebo zneužil?) Cantorovy diagonální metody. Nejsnáze lze tuto antinomii zformulovat takto: všech konečných posloupností českých slov (nazvěme tyto posloupnosti „větami") je spočetně mnoho. Některé z těchto vět jednoznačně definují nějaké reálné číslo, například „šest pětin", „nejmenší prvočíslo, které je větší než deset milionů" apod. Množina T všech těchto čísel je spočetná (neboť *všech* vět je pouze spočetně mnoho). Lze tedy množinu T uspořádat do posloupnosti. Nyní Cantorovou diagonální metodou sestrojíme číslo $r \notin T$. To podle definice množiny znamená, že *číslo r nelze definovat žádnou konečnou posloupností českých slov*. To je však zřejmý spor s tím, že *jsme takto číslo r právě definovali*.

Zjednodušením Richardovy antinomie je následující *antinomie Berryho*, kterou poprvé publikoval Russell v r. 1906: protože všech českých „vět" (ve výše uvedeném smyslu), které mají nejvýše 20 slov, je pouze konečně mnoho, existují nutně přirozená čísla, která takovou větou definovat nelze. Můžeme proto vyslovit následující definici:

Buď k nejmenší přirozené číslo, které nelze definovat českou větou o nejvýše dvaceti slovech.

Čtenář nechť si promyslí, co jsme právě udělali: větou o 14 slovech jsme definovali číslo,

které nelze definovat **žádnou** větou, která by měla dvacet nebo méně slov!

V literatuře (viz například [5]) lze najít ještě další antinomie. Uvedené ukázky však — doufejme — udávají dostatečný přehled o tom, jakého druhu byla ona tvrzení, která způsobila 3. krizi matematiky.

Pravděpodobně je však nyní nutné podrobněji vysvětlit, *proč* uvedené antinomie nejsou jen zajímavými logickými hříčkami bez hlubšího významu (jak se původně řadě matematiků zdálo a jak na ně ostatně i dnes může pohlížet ten, kdo k matematice přistupuje „pseudoinženýrsky“ jako ke snůšce výpočetních metod), ale závažnými problémy, které zbouraly pracně vybudovanou budovu moderní matematiky a způsobily v matematice dodnes nepřekonanou krizi.

Nešlo jen o to, že se objevila v teorii množin sporná tvrzení, znehodnocující tuto teorii. Horší bylo, že — jak jsme již uvedli — v uvedené době již byla teorie množin základnou převážné části matematiky. (Je zřejmé, že to znamenalo, že teorii množin je nutno buďto „opravit“ nebo najít jinou a „lepší“ základnu. Co by však mělo a mohlo být onou novou základnou? To si prakticky nikdo nedovedl představit. Vynikající německý matematik David Hilbert, o němž budeme ještě hovořit v §4, to v r. 1925 vyjádřil často citovanými slovy: *Nikdo nás nemůže vyhnat z ráje, který pro nás vybudoval Cantor*. (Opravám „cantorovského ráje“ se budeme věnovat v následujícím paragrafu.)

Nejzávažnější důsledky antinomií však spočívaly ještě v něčem jiném. Připomeňme si, jaké bylo východisko Cantorovy teorie. „Množina“ bylo jen synonymum slov souhrn, systém apod. Tento pojem je tak samozřejmý a názorný, že není nutno ho nijak definovat. (Podobně jako je v Eukleidově geometrii zřejmé, co je to bod nebo přímka. Ostatně pojem „množina“ je jistě intuitivně jednodušší než například pojem „přímka“.) O těchto souhrnech — množinách pak Cantor běžně užívanými matematickými a logickými metodami dokazuje tvrzení a odvozuje jejich vlastnosti. (Takto budované teorii se dnes říká „naivní“, respektive „intuitivní“ teorie množin.) Nebylo nejmenšího důvodu předpokládat, že teorie budovaná tímto způsobem by mohla být principiálně nesprávná; vždyť takto se matematika budovala od starověku. A přesto antinomie prokázaly, že matematiku takto bezelstně budovat nelze! Toto je nejzávažnější důsledek antinomií.

A jaký je tedy „správný“ způsob výstavby matematiky? Právě proto, že na odpovědi na tuto otázku se matematikové dodnes neshodli, hovoříme o důsledcích vzniklé situace jako o 3. krizi matematiky.

Tato krize pochopitelně neznamená, že by se matematika ve 20. století nevyvíjela; dobře víme, že je tomu právě naopak. Tato krize samozřejmě ani nemá bezprostřední negativní důsledky na ty matematické disciplíny — a těch je samozřejmě většina — které přímo nesouvisejí s výstavbou základů matematiky. Matematik, který by se však stavěl do pozice, že jeho práce se toto všechno nedotýká, by nápadně připomínal pštrosa, strkajícího hlavu do písku. Jeden z velkých matematiků 20. století, Hermann Weyl, jenž je právě autorem téze o nástupu 3. krize matematiky, tuto situaci charakterizoval v r. 1946 slovy:

Méně než kdykoliv dříve jsme přesvědčeni o prvotních základech logiky a matematiky. Jako všichni a všechno v dnešním světě prožíváme „krizi“. Ta trvá už téměř padesát let. Na první pohled nám nepřekáží v každodenní práci; mohu se však přiznat, že ve skutečnosti měla silný vliv na mou matematickou činnost: směrovala mé zájmy do oblasti, která se mě zdála relativně „bezpečnou“, a neustále ve mně podrývala nadšení a odhodlání nezbytné pro každou vědeckou práci.

4 Východiska z krize

Když se všechno daří,
něco se pokazí.
PRVNÍ CHISHOLMŮV ZÁKON

Jak jsme uvedli v §3, bylo po objevení antinomií teorie množin zřejmé, že dosavadní styl výstavby matematiky je neudržitelný. Přístup matematiků k řešení vzniklé situace byl samozřejmě odlišný podle jejich filozofického i profesionálního zaměření. Přesně definovat a ohraničit jednotlivé myšlenkové proudy je přitom nemožné. V hrubých rysech však lze říci, že základní přístup k řešení byl dvojí: *intuicionistický* a *formalistický*, přičemž mezi formalistické směry patří několik vyhraněných a velmi odlišných skupin.

Podle **intuicionistických** názorů byla matematika v posledních desetiletích budována nepřípustnými metodami. Některá logická pravidla, zřejmě platná pro konečné systémy, jako například *princip vyloučeného třetího* (*tertium non datur* — viz větu 3.15 (2)v kapitole I.), byla nedovoleným způsobem přenesena i na nekonečné systémy. Intuicionisté odmítají aktuální nekonečno, neuznávají existenční důkazy. Objekt, který nelze *zkonstruovat* pomocí jiných uznaných postupů, prostě neexistuje. Je evidentní, že tím před nimi vyvstaly obrovské potíže. Po formální i obsahové stránce byli nuceni prakticky nově budovat řadu matematických disciplín, neboť jen malá část klasické matematiky pro ně byla „přípustná“.

V poslední době sílí tendence dívat se na intuicionismus jako na historickou kuriozitu. Přínos intuicionistů k rozvoji matematiky však byl nemalý. A přinejmenším k zamyšlení by nás měla přimět skutečnost, že mezi ně patřila řada nejvěhlasnějších matematiků posledních generací. První intuicionistické ideje v novodobé matematice lze najít v 70. – 80. letech 19. století v díle Leopolda Kroneckera, o němž již z §2 víme, že stál v čele proticantorovského hnutí. Zrod moderního intuicionismu je však spojován se jménem holandského matematika Leutzena Egberta Jana Brouwera, který základní intuicionistické ideje zformuloval ve své disertační práci v r. 1907. Kromě již zmíněných H. Weyla a H. Poincarého lze k intuicionistům přiřadit například matematiky takového kalibru, jako byli Émile Borel, Henri Leon Lebesgue či Nikolaj Nikolajevič Luzin.

Základní **formalistické** přístupy k výstavbě teorie množin a základům matematiky jsou

dvojí: metoda *teorie typů* a *axiomatická výstavba*.

Zakladatelem teorie typů je již několikrát zmiňovaný B. Russell. Podle jeho mínění byly antinomie způsobeny tím, že pomocí všech prvků daného systému byl opět definován prvek daného systému. V teorii typů, kde jsou jednotlivé pojmy „hierarchicky“ rozvrstveny, nemůže být pomocí prvků jisté úrovně definován prvek téže úrovně. Tím je samozřejmě vyloučen vznik antinomií Russellova druhu. Z prací rozvíjejících teorii typů uveďme alespoň dvě nejvýznamnější a nejznámější. Je to především tzv. *New Foundations* amerického matematika Ormana Willarda van Quinea poprvé publikovaná v r. 1937 a dále tzv. *Systém* Σ jiného amerického matematika Hao Wanga, poprvé Wangem popsaný v roce 1954.

Teorie typů bývá často nesprávně zaměňována s jiným filozoficko-matematickým směrem, tzv. *logicismem*. Původ této záměny je jednoduchý — hlavním představitelem logicismu je zakladatel teorie typů Bertrand Russell. Zformulovat hlavní tézi logicismu není jednoduché; vyžadovalo by to zevrubnější rozbor vzájemného vztahu matematiky a matematické logiky. Nepřesně ji lze vyslovit asi následovně: *všechny speciální matematické pojmy lze definovat pomocí slovníku matematické logiky a k důkazům matematických tvrzení není třeba žádných axiómů kromě logických ani žádných odvozovacích pravidel kromě těch, která jsou akceptována logikou.*

Faktickým zakladatelem logicismu byl německý matematik Friedrich Ludwig Gottlob Frege. Jakou ideou byl Frege veden? Poslední čtvrtina 19. století byla obdobím značně úspěšné *aritmetizace matematiky*. (Svědectvím o této skutečnosti je například Poincarého výrok, který jsme citovali v úvodu 3. paragrafu nebo známý výrok Kroneckerův: *Celá čísla stvořil Bůh, vše ostatní je dílem lidí.*) Frege se pokoušel aritmetiku zredukovat na logiku. Jeho dílo zůstalo v době vzniku prakticky nepochopeno. Až Russell na tuto ideu navázal a pokoušel se totéž udělat s Cantorovou teorií množin. Právě při této práci přišel na onu klasickou antinomii nazvanou jeho jménem.

Základním dílem logicismu je třídílná monografie *Principia Mathematica*, kterou v letech 1910 – 1913 vydal Russell společně s anglickým matematikem, filozofem a logikem Alfredem Northem Whiteheadem. Logicismus měl sice značný vliv na rozvoj matematické logiky, mezi matematiky však logicistická redukce matematiky na odnož logiky nikdy nezaznamenala větší ohlas.

Většina matematiků za východisko z krize považovala **axiomatickou výstavbu matematiky**. Dnes je to nejběžnější a nejuznávanější způsob budování matematických teorií. Axiomatické metody již dokonce dávno překročily rámec matematiky samotné a jsou stále hojněji užívány i v jiných vědách, a to nejen přírodních. Proto se o nich zmíníme podrobněji.

Je samozřejmé, že při deduktivní výstavbě nějaké vědecké teorie, kdy složitější pojmy definujeme pomocí pojmů jednodušších a nová tvrzení odvozujeme z tvrzení již dokázaných, není principiálně možno definovat *všechny* pojmy a dokázat *všechna* tvrzení. Na jisté úrovni je nutno započít; jisté tzv. „primitivní“ pojmy je nutno zavést bez definice a jistá tvrzení —

tzv. axiómy — je nutno pokládat za pravdivé bez důkazu. Zásady takové deduktivní výstavby vědy zpracoval již Aristotelés. První — a geniální — takto zpracované matematické dílo jsou Eukleidovy *Základy*.

Nový impuls pro rozvoj axiomatické metody dala opět geometrie. Pokusy o důkaz 5. Eukleidova postulátu o rovnoběžkách, vedoucí — jak známo – až ke vzniku neeukleidovské geometrie, vyvolaly nový zájem o důslednou axiomatizaci geometrie. Tato práce byla završena dílem Davida Hilberta *Grundlagen der Geometrie* (1899), o němž se ještě později zmíníme. A 20. století je obdobím konjunktury axiomatického přístupu k matematice.

Je samozřejmé, že v průběhu doby axiomatické metody zaznamenaly značný vnitřní vývoj. Tento proces lze zhruba rozdělit do tří základních etap:

(a) tradiční axiomatika (Eukleidés);

(b) formální axiomatika (19. století);

(c) formalizovaná axiomatika (20. století).

V čem spočívají hlavní rozdíly mezi axiomatikami jednotlivých období?

Tradiční axiomatika byla popisována v běžném hovorovém jazyce. V tom ovšem bylo potenciálně skryto nebezpečí, že se v takto budované teorii objeví nepřesnosti, nejasnosti nebo dokonce zásadní obtíže; žádný hovorový jazyk není natolik přesný, aby se tomu dalo zabránit. Za druhé, při tradiční axiomatice nejsou přesně zformulována pravidla pro odvozování jedněch výroků z druhých. Při „intuitivně jasném“ odvozování je ovšem vyloučena jednoznačná kontrola správnosti úsudků. Jak prokázaly antinomie, byla především tato okolnost zdrojem těch největších problémů. A konečně, v klasické axiomatice byly axiómy tvrzení, která nebylo nutno dokazovat proto, že byla zcela „samozřejmá“. Teorie byla v tomto slova smyslu budována „sémanticky“.

V dalších dvou etapách vývoje axiomatických metod došlo ve všech uvedených bodech k výrazným změnám. Již ve 2. etapě, při budování formální axiomatiky, dochází mimo jiné k tomu, že:

(a) je dán přesný počet výchozích pojmů a tvrzení;

(b) jsou přesně stanovena odvozovací pravidla;

(c) systém axiómů se mění v souhrn pravidel implicitně určujících, jak je možno pracovat s výchozími pojmy;

(d) proces formální výstavby axiomatického systému je oddělován od jeho možných interpretací (tzv. modelů);

(e) zkoumá se *nezávislost*, *bezespornost* a *úplnost* systémů axiómů (jak o tom hovoříme dále) pomocí modelů daného systému.

Ve třetí, formalizované etapě, dochází navíc k důslednému oddělení jazyka, v němž je daná teorie budována (tzv. „objektový jazyk“) od jazyka užívaného k popisu objektového jazyka (tzv. „metajazyk“). (Řada antinomií právě vznikla záměnou těchto dvou jazyků.) Objektový jazyk je přitom „symbolizován“, tj. na začátku je zadána „abeceda“ (souhrn užívaných symbolů – znaků), jsou udána pravidla, jak tvořit, respektive poznávat správně utvořená „slova“ (nazývaná „formule“) a jsou dána pravidla odvozování jedněch formulí z dalších. Za axiómy jsou pak prohlášeny některé z formulí. Proces oddělení formální výstavby teorie od jejích modelů je takto zcela dovršen. (V uvedeném smyslu je například geometrie vyučovaná na školách pouze jedním z možných modelů axiomatické eukleidovské geometrie.

Podobně je tomu s teorií množin, vyučovanou dnes u nás již od 1. třídy. Již v 1. kapitole jsme ostatně uvedli, že ve školách se de facto učí model **ZF** teorie.)

Ještě než začneme hovořit o axiomatických teoriích množin, stručně k uvedeným požadavkům na volbu axiómů. Ta samozřejmě není předem jednoznačně determinována; volba axiómů je do značné míry věcí libovůle toho, kdo danou teorii vytváří. Jako přirozené se však jevilo požadovat, aby zvolená soustava axiómů byla vždy:

1. **nezávislá** (tzn., že žádný z axiómů nelze odvodit ze zbývajících; takové tvrzení by evidentně nebylo nutno považovat za axióm);

2. **úplná** (tzn., že axiómů je dostatečně mnoho k tomu, abychom mohli každé tvrzení této teorie buďto dokázat nebo vyvrátit — tj. dokázat jeho negaci);

3. **bezesporná** (chceme mít zaručeno, že z axiómů nelze odvodit současně nějaké tvrzení i jeho negaci; víme, že takové teorie je bezcenná).

Nyní je přirozená otázka, zda lze axiomatický systém s uvedenými vlastnostmi sestrojit. (Původně o tom ovšem nenapadlo nikoho pochybovat.)

Relativně nejméně problémů působí nezávislost. Její případné porušení je de facto jen „kosmetickou vadou“ dané teorie a její odstranění není obtížné. Není-li však teorie úplná, je to značně nepříjemné, neboť to značí, že v této teorii nutně existují tvrzení, která nelze ani dokázat, ani vyvrátit. (Zdálo by se ovšem, že tuto obtíž by mělo jít odstranit jednoduše přidáním dalších axiómů.) A není-li teorie bezesporná, je to pro ni naprostá katastrofa. Zatím však, co například pro eukleidovskou geometrii se podařilo úplnost a bezespornost prokázat ve výše uvedené Hilbertově monografii z r. 1899, dokázat úplnost a bezespornost budovaných axiomatických teorií množin se nikomu nepodařilo. To, že se podařilo objasnit, zda lze úplnou a bezespornou teorii množin (a další teorie) sestrojit, patří k největším úspěchům moderní matematiky. Skutečnost, že odpověď je *záporná*, byla jistě překvapující a nepříjemná. Značí totiž výrazné omezení možností axiomatických metod. Podrobněji však budeme o této problematice hovořit v §5.

První úspěšnou axiomatickou teorií množin byla teorie, kterou v letech 1904 - 1908 vybudoval již zmíněný německý matematik Ernst Zermelo. Základní Zermelova idea spočívala v tom,

že nelze předpokládat — jak to činil Cantor — že každý souhrn objektů tvoří množinu. Pomocí axiómů je nutno dosáhnout toho, aby množin bylo „dostatečně mnoho“, nikoliv však tolik, aby mohlo docházet k antinomiím. Zermelův systém axiómů později částečně modifikoval a dalšími axiómy doplnil izraelský matematik Abraham A. Fraenkel. *Zermelo-Fraenkelova* teorie množin (nadále ji budeme značit **ZF**) je dnes nejrozšířenější axiomatizovanou množinovou teorií.

Skutečnost, že v rámci **ZF** nelze pracovat se všemi systémy, například se „systémem všech množin“, „systémem všech grup“ a podobně, je však v mnoha ohledech nepříjemná. V roce 1925 však publikoval americký matematik maďarského původu John von Neumann práci, v níž se mu podařilo tuto obtíž obejít. Jeho ideu využil švýcarský matematik Isaak Paul Bernays, který v letech 1937 - 1954 vypracoval vlastní axiomatiku teorie množin (přesněji řečeno „teorie tříd“). Ta je základem tzv. *Gödel-Bernaysovy* teorie tříd (nadále ji značíme **GB**), která vznikla syntézou axiomatiky Bernaysovy a axiomatického systému Kurta Gödela, poprvé publikovaného v r. 1940. (O Gödelovi budeme podrobněji hovořit v §5.)

Zatímco v **ZF** jsou nedefinované pojmy „množina“ a $\in$, jsou to v **GB** pojmy „třída“ a $\in$. Některé axiómy **ZF** jsou současně i axiómy v **GB**. Proto lze řadu množinových pojmů na třídy převést. (Například „obvyklé“ množinové operace apod.) Třídy, které jsou prvkem nějaké jiné třídy, se v **GB** nazývají „množinami“. „Vlastní třídy“ jsou pak ty třídy, které množinami nejsou. Lze dokázat, že množiny ve smyslu **ZF** jsou i množinami ve smyslu **GB** (takže **GB** je vlastně „rozšířením“ **ZF**). Vlastní třídou je například „třída všech množin“. Na rozdíl od množin nemají vlastní třídy například žádné kardinální číslo. (Tuto problematiku jsme probírali v 1. kapitole.)

Podrobnější rozbor role jednotlivých axiómů a přehled dalších axiomatických systémů nebudeme uvádět. Obojí lze nalézt například v již citované knize [5], kde je uveden i obsáhlý přehled další literatury. Pouze o jednom axiómu se pro jeho výjimečné postavení zmíníme podrobněji. Jak čtenář jistě tuší, máme nyní na mysli *axióm výběru*. Tento axióm, jak známo, nám zajišťuje, že k libovolnému systému neprázdných množin existuje množina, která má s každou z těchto množin jednoprvkový průnik.

První — a negativní — zmínku o principu zformulovaném v tomto axiómu lze nalézt v r. 1890 u známého italského matematika Giuseppe Peana v práci *Démostration de l'integrabilité des équations differentielles ordinaires*, Math. Ann. **37**, 182-228. V roce 1902 se o tomto principu zmiňuje další italský matematik Beppo Levi. Intuitivně tohoto axiómu užíval i Cantor, aniž si ovšem uvědomoval, že užívá principu dosud v matematice, respektive v logice neužívaného.

V této souvislosti je zajímavá jedna okolnost. Již v §2 jsme uvedli, jak těžce na Cantora již v r. 1884 doléhaly neúspěchy spojené s hypotézou kontinua. Cantor byl vždy pevně přesvědčen, že každá mohutnost je některým alefem, nikdy se mu však nepodařilo tuto skutečnost dokázat; dnes, po vyřešení hypotézy kontinua, je nám ovšem jasné, proč tomu tak bylo. Jak však v jednom dopise píše Cantorův žák Felix Bernstein — který v r. 1897 jako první dokázal

známou větu o ekvivalenci dvou množin, po něm pojmenovanou (věta III. 2.1.) — pokoušel se někdy v r. 1901 společně s Cantorem sestrojit bijekci mezi kontinuem a množinou $Z(\aleph_0)$, která má mohutnost $\aleph_1$. Přitom však narazili na nepřekonatelné těžkosti, které právě Levi navrhoval odstranit pomocí uvedeného principu.

Axióm výběru poprvé explicitně zformuloval E. Zermelo v r. 1904 v práci *Beweis, dass jede Menge wohlgeordnet werden kann*, Math. Ann. **59**, 514-516, kde ho užil, jak to ostatně název práce uvádí, k důkazu tvrzení, že každou množinu lze dobře uspořádat. (Tomuto tvrzení se dnes běžně říká Zermelova věta, axióm výběru pak bývá často nazýván *Zermelovým axiómem*.) Řada matematiků vznášela proti axiómu výběru od počátku četné výhrady. (Samozřejmě, že vzhledem ke své nekonstruktivnosti byl zcela nepřijatelný především pro intuicionisty.)

Tyto výhrady se ještě zostřily poté, co Felix Hausdorff pomocí axiómu výběru dokázal tvrzení o paradoxním rozdělení koule; odvodil totiž, že její polovina je kongruentní s její třetinou. (Důkaz tohoto tvrzení je uveden v knize [8], která je první monografií věnovanou teorii množin. Tato kniha měla nesmírný vliv na řadu matematiků a na vývoj těch matematických disciplín, které jsou na teorii množin založené.)

Později dokázali další autoři, především polští matematici Stefan Banach a Alfred Tarski i jiné paradoxní důsledky axiómu výběru. Jak se však záhy prokázalo, zamítnutí tohoto axiómu by na druhé straně způsobilo neskonalé problémy, neboť řadu „běžných“ tvrzení v různých matematických teoriích nelze bez jeho užití prokázat. Poté, co A. Fraenkel v r. 1922 dokázal nezávislost axiómu výběru na ostatních axiómech v běžných teoriích množin a K. Gödel v r. 1938 odvodil jeho bezespornost, se situace víceméně ustálila ve stavu, který trvá dodnes. Axiómu výběru sice užíváme, ale jen tehdy, když je to nezbytné a jeho užití je většinou zdůrazněno.

Jak přívrženci axiomatické výstavby matematiky, tak matematici přiklánějící se k teorii typů, samozřejmě cítili nutnost *dokázat*, že jimi budované teorie jsou *bezesporné*. Klasické metody, použitelné ještě například pro důkaz bezespornosti eukleidovské, respektive neeukleidovské geometrie, však nebyly pro disciplíny operující s aktuálním nekonečnem použitelné. Bylo proto nutné vypracovat k těmto účelům metodu novou. Nejsystematičtěji se tímto úkolem zabýval již několikrát zmiňovaný David Hilbert, autor návrhu dnes všeobecně nazývaného **hilbertovský program**.

První nástin tohoto programu podal Hilbert již v r. 1904, aniž by se jím však dále zabýval. Až v roce 1917, kdy reagoval na neustálé výpady intuicionistů, se k této problematice vrátil a zabýval se jí pak prakticky do své smrti. Zvláště intenzívně se na tomto programu pracovalo v letech 1920 - 1930, kdy s Hilbertem spolupracovala celá řada mladých matematiků; kromě již zmíněných Bernayse a von Neumanna to byli především Wilhelm Ackermann a Jacques Herbrand.

Stručně popišme, jaká byla Hilbertova idea. Vycházel z toho, že je nutno dokázat, že užívané matematické důkazové metody jsou dostatečně silné k tomu, aby jimi bylo možno vybudovat

celou klasickou matematiku včetně teorie množin, vycházející přitom z vhodně zvolených axiómů, současně však nejsou natolik silné, aby jejich aplikací bylo možno dojít k antinomiím. (Jak vidět, Hilbert byl skálopevně přesvědčen o správnosti základů klasické matematiky.) Celý tento program měl být realizován ve dvou etapách.

V první etapě měla být matematika, především pak aritmetika, analýza a teorie množin, plně formalizována. Tato formalizace by spočívala v tom, že všechna pravdivá tvrzení, především samozřejmě axiómy, by byla převedena na posloupnosti symbolů zbavených jakéhokoliv obsahu. S těmito posloupnostmi by se pracovalo pomocí jistého počtu přesně definovaných odvozovacích pravidel. Takto — ryze syntakticky — by byla vybudována klasická matematika, přičemž by k této práci nebylo zapotřebí prakticky žádné „intuice“; povolené transformace posloupností by vzhledem k finitnosti všech procesů mohl teoreticky provádět i stroj.

Ve druhé etapě mělo být *dokázáno*, že výše uvedeným způsobem *nelze* nikdy dojít ke spornému tvrzení, například k formuli „1 = 2“. Použité metody přitom musí být natolik jednoduché, aby o jejich správnosti nebylo nejmenších pochyb. Základním požadavkem samozřejmě byla finitnost. (Tuto část, v níž měla být dokázána bezespornost matematiky, nazval Hilbert **metamatematikou**.)

Na uvedeném programu vykonal Hilbert se svými žáky obrovský kus práce. V době, kdy se již zdálo, že celý program by mohl být zdárně ukončen, však výsledky A. Tarského, Alonza Churche a především K. Gödela prokázaly, že hilbertovský program je nerealizovatelný. Jak uvidíme v dalším paragrafu, plyne z Gödelových výsledků nerealizovatelnost 1. i 2. etapy.
Hilbert, který byl ještě po objevení antinomií v Cantorově teorii množin tak pevně přesvědčen o správnosti základů matematiky, že prohlásil: *Předpoklad existence objektivních rozporů ve vnějším světě je klasickým případem nesmyslu*, nesl velmi těžce toto zhroucení svých idejí. Nedlouho před svou smrtí prohlásil: *Kde máme hledat naději a jistotu, když dokonce matematické myšlení selhalo*.

Dnes si sice nemyslíme, že selhalo matematické myšlení, avšak vyrovnat se s Gödelovými výsledky znamenalo podstatně revidovat představy o možnostech formální výstavby matematiky — a nejen matematiky.

5 Gödelovy výsledky

Zákonitě musí jednou nastat
ta nejhorší možná situace.
DRUHÝ SODDŮV ZÁKON

Kurt Gödel, jeden z největších matematiků a logiků moderní éry, se narodil v r. 1906 v Brně, kde absolvoval střední školu. Studoval na univerzitě ve Vídni, kde promoval v r. 1930. V r. 1940 emigroval do USA a až do své smrti v r. 1978 působil v Princetonu (což bylo mimo jiné působiště

A. Einsteina). Dostalo se mu řady poct a uznání; jmenujme za všechny alespoň Einsteinovu cenu za rok 1951, což je nejvyšší americké ocenění vědecké práce. Svými výsledky ovlivnil tvář moderní matematiky jako málokdo jiný.

V poslední době se stalo jistou módou citovat Gödelovy výsledky, zejména proslulou **větu o neúplnosti** z r. 1931 ([9]) i mimo matematiku (většinou samozřejmě nepřesně nebo zcela překrouceně). Vzhledem k mimořádné závažnosti této věty se o ní zmíníme podrobněji. (Mohli bychom samozřejmě uvést původní Gödelovu práci, ale čtenář bez hlubší logické přípravy by pravděpodobně měl s jejím studiem nepřekonatelné potíže. V dalším se proto pokusíme alespoň popsat ideu důkazu, mimochodem geniální a elegantní.)

Předpokládejme, že zkoumáme nějakou axiomatickou teorii $\mathcal{T}$ zahrnující aritmetiku (tj. axiómy aritmetiky jsou tvrzeními v $\mathcal{T}$). Víme, že takovou teorií je například teorie množin.

Jak dobře víme z kapitoly I, výstavba takové formalizované teorie začíná zadáním *abecedy*. Označme abecedu teorie symbolem A. Vzhledem k tomu, že A je konečná nebo spočetná množina (což jistě můžeme bez újmy na obecnosti předpokládat), existuje jistě prosté zobrazení množiny A do množiny $\mathbb{N}$ všech přirozených čísel. Definujme speciálně toto zobrazení tak, že pro každé $\alpha \in A$ je $g(\alpha)$ prvočíslo eventuálně číslo 1.

Nechť je například toto zobrazení definováno takto:

α:	$\vee$	$\wedge$	$\Rightarrow$	$\Leftrightarrow$	$\neg$	(	)	$\forall$	$\exists$	=	$\in$	X	Y	Z	...
$g(\alpha)$:	1	2	3	5	7	11	13	17	19	23	29	31	37	41	...

Víme, že „slovo“ nad danou abecedou je konečná posloupnost prvků množiny A. Protože je A nejvýše spočetná množina (a samozřejmě neprázdná), je množina S všech slov nad A spočetná. Existuje tedy prosté zobrazení h $S \to \mathbb{N}$. Sestrojení této injekce nazýváme „gödelizací“ dané množiny slov.

Abychom ze znalosti čísla $h(\varphi)$ — tzv. „malého Gödelova čísla“ slova φ — mohli snadno zjistit slovo φ, zadáme zobrazení h takto:

$$h(\alpha_1\alpha_2 \ldots \alpha_n) = 2^{g(\alpha_1)}3^{g(\alpha_2)} \ldots p_n^{g(\alpha_n),} \qquad \text{kde } p_n \text{ je } n\text{-té prvočíslo.}$$

Tak například malé Gödelovo číslo slova $X \in Y$ je $2^{31}3^{29}5^{37}$; obráceně, protože $9000 = 2^3 3^2 5^3$, je 9000 malé Gödelovo číslo slova $\Rightarrow \wedge \Rightarrow$.

Označíme-li G množinu všech malých Gödelových čísel, je zřejmě G vlastní podmnožinou v $\mathbb{N}$. I když je většina těchto čísel nesmírně veliká, lze pro každé přirozené číslo rozhodnout, zda platí $x \in G$ nebo $x \notin G$. Pro dané přirozené číslo x je tedy „$x \in G$“ aritmetické tvrzení.

Víme však, že v teorii $\mathcal{T}$ se nepracuje se všemi slovy, ale jen s tzv. „formulemi“, což jsou slova utvořená podle zadaných pravidel. Například $X \in Y$ je formule v teorii množin, $\Rightarrow \wedge \Rightarrow$ samozřejmě formule není. Označíme-li F množinu všech formulí, je F vlastní podmnožina množiny S.

Množina všech konečných posloupností formulí je spočetná, protože F je nejvýše spočetná. Některé z těchto posloupností — vytvořené podle přesně stanovených pravidel — se nazývají „důkazy“. Označme D množinu všech důkazů.

Je-li $\varphi_1, \varphi_2, \ldots, \varphi_n$ důkaz, říkáme, že je to důkaz formule φ_n a o formuli φ_n říkáme, že je *dokazatelná*. (Dokazatelné formule jsou tedy poslední formule v důkazech.)

Je zřejmé, že dokazatelná formule může mít i více důkazů (i když nalezení alespoň některého z nich může být nesmírně obtížné.) Je-li φ libovolná formule, je však zřejmě pravdivé **právě jedno** z následujících dvou tvrzení: „φ je dokazatelná“, respektive „φ není dokazatelná“. (Samozřejmě přitom nemusíme vědět, **které** z těchto tvrzení je pravdivé.)

Je-li $\varphi_1, \varphi_2, \ldots, \varphi_n$ důkaz, nazveme jeho „velkým Gödelovým číslem“ číslo

$$2^{h(\varphi_1)}3^{h(\varphi_2)}\ldots p_n^{h(\varphi_n)}.$$

Označme H množinu všech velkých Gödelových čísel. Podobně jako u množiny G je zřejmé, že H je vlastní podmnožina v $\mathbb{N}$ a tvrzení „$x \in H$“ je pro dané přirozené číslo x aritmetické tvrzení.

Je-li $y \in H$ velké Gödelovo číslo důkazu formule φ, jejíž malé Gödelovo číslo $g(\varphi)$ je číslo $x \in G$, řekneme, že „y má konec x“. Je zřejmé, že

$$\text{„}y \text{ má konec } x\text{“}$$

je aritmetické tvrzení a tudíž ho lze zapsat nějakou formulí v teorii $\mathcal{T}$. Přitom si uvědomme, že pro dané číslo $x \in G$ je tvrzení „$\exists y \in H$ y má konec x“ pravdivé právě tehdy, když je formule s malým Gödelovým číslem x dokazatelná.

Procesem popsané „gödelizace“ dané teorie $\mathcal{T}$ jsme tedy dosáhli toho, že tvrzení o dokazatelnosti formule φ v teorii $\mathcal{T}$ jsme převedli na pravdivost, respektive nepravdivost aritmetického tvrzení „$\exists y \in H$ y má konec $h(\varphi)$“.

Buď nyní $x \in G$ libovolné. Víme, že je buďto pravdivé tvrzení „Formule s malým Gödelovým číslem x je dokazatelná“ nebo tvrzení „Formule s malým Gödelovým číslem x není dokazatelná“.

Je-li například

$$h(\varphi) = 2^{11}3^{31}5^{29}7^{37}11^{13}13^{3}17^{11}19^{37}23^{29}29^{31}31^{13},$$

je φ formule

$$(X \in Y) \Rightarrow (Y \in X)\,;$$

protože tato formule evidentně nemůže být v „rozumné“ teorii množin dokazatelná, je aritmetické tvrzení „$\exists y \in H$ y má konec $h(\varphi)$“ v tomto případě nepravdivé.

K. Gödel nyní dokázal následující pozoruhodnou skutečnost: existuje číslo $k \in G$, které má následující vlastnost. Utvoříme-li formuli φ odpovídající tvrzení „Formule s malým Gödelovým číslem k není dokazatelná“, tj. formuli popisující aritmetické tvrzení

$$\text{„}\neg(\exists y \in H \; y \text{ má konec } k)\text{“}\ ,$$

pak platí $h(\varphi) = k$ (tj. malé Gödelovo číslo takto zkonstruované formule je právě ono číslo k).

Nyní dokážeme, že v teorii $\mathcal{T}$, pokud je bezesporná — a takové teorie samozřejmě chceme budovat — není dokazatelná ani formule φ ani její negace $\neg\varphi$.

(1) Připusťme, že formule φ je dokazatelná. To však znamená, že formuli ψ, jejíž malé Gödelovo číslo je k, nelze dokázat. Touto formulí je však právě formule φ. Obdrželi jsme tedy spor.

(2) Připusťme, že lze dokázat formuli $\neg\varphi$. To však znamená, že lze dokázat skutečnost, že formule s malým Gödelovým číslem k, což je právě φ, je dokazatelná. Opět jsme tedy obdrželi spor.

Je-li tedy $\mathcal{T}$ bezesporná, musí být formule φ v $\mathcal{T}$ „nerozhodnutelná“; nelze dokázat ani φ ani $\neg\varphi$.

Odvodili jsme takto právě *Gödelovu větu o neúplnosti:*

Je-li dána libovolná bezesporná teorie obsahující aritmetiku, pak v této teorii existuje nerozhodnutelné tvrzení.

Na dovršení podivnosti tohoto výsledku si navíc uvědomme, že výše zkonstruovaná nerozhodnutelná formule φ je zjevně **pravdivá**! Uvedli jsme totiž před chvílí, že každé tvrzení o dokazatelnosti nějaké formule v $\mathcal{T}$ je nutně pravdivé nebo nepravdivé. Protože předpoklad, že φ je nepravdivá formule vede okamžitě ke sporu, je φ — i když je nerozhodnutelná — nutně pravdivá.

Jaké jsou důsledky věty o neúplnosti? Protože v každé „dostatečně bohaté“ teorii při jakékoliv volbě axiómů, pokud je jen tato volba bezesporná, existují nutně nerozhodnutelná tvrzení (a situaci nelze spravit přidáním dalších axiómů!), je neuskutečnitelná již 1. etapa hilbertovského programu. Z žádného systému axiómů, pokud je bezesporný, nelze uvažovanými metodami odvodit „celou“ matematiku. (Prvním konkrétním příkladem v teorii množin nerozhodnutelného tvrzení se stala hypotéza kontinua; jak jsme uvedli již v poznámce III.6.23, její nerozhodnutelnost v **ZF** dokázal v r. 1963 Paul Cohen, nezávisle na něm dokázal totéž v **GB** v r. 1964 Petr Vopěnka.)

Z Gödelových výsledků však plyne nerealizovatelnost i 2. etapy hilbertovského programu. Z věty o neúplnosti lze totiž snadno odvodit, že *v teorii s výše uvedenými vlastnostmi nikdy není možno dokázat formuli tvrdící bezespornost této teorie*.

Co odtud plyne pro axiomatické teorie množin (nebo pro axiomatizaci samotné aritmetiky)?

Tyto teorie byly budovány proto, že antinomie prokázaly neudržitelnost cantorovského „intuitivního“ přístupu. Jsou tedy axiomatické teorie bezesporné? Můžeme si být jisti, že v nich nejsou na nějaké jiné úrovni také nějaké antinomie? V to můžeme jen doufat. Jak odvodil K. Gödel, dokázat to nemůžeme. Můžeme odvodit jen relativní tvrzení typu „Je-li **GB** bezesporná, je i **ZF** bezesporná“ a podobně. Je však **GB** bezesporná? Otázka se vrací jako bumerang; v rámci **GB** to nelze dokázat. Jen v rámci nějaké jiné, „bohatší“ teorie by bylo možno eventuelně dokázat, . . . atd.

Že to není příliš optimistické? Alespoň si uvědomíme, že reálný svět je nesrovnatelně složitější, než svět i těch nejlépe vymyšlených formulí. (I když nám jejich vymýšlení — a učení — přináší tolik starostí i potěšení.)

DODATEK

Relace mezi množinami

Symbolem $[x, y]$ značíme *uspořádanou dvojici* prvků x, y. Platí tedy

$$[x, y] = [u, v] \iff x = u \wedge y = v.$$

Kartézským součinem množin A, B nazýváme množinu

$$A \times B := \{[x, y];\ x \in A,\ y \in B\}.$$

Je zřejmé, že operace $\times$ není komutativní. Nerozlišujeme-li však součiny $(A \times B) \times C$ a $A \times (B \times C)$, můžeme operaci $\times$ považovat za asociativní. Zejména je tak zřejmé, co rozumíme množinou $A^{n+1} := A^n \times A$ pro každé přirozené n. $(A^1 = A)$.

Relací mezi množinami A, B (v tomto pořadí) rozumíme každou podmnožinu ϱ součinu $A \times B$.

Je-li ϱ relace mezi množinami A, B, nazýváme jejím *definičním oborem* množinu

$$\mathrm{Dom}\varrho := \{x \in A;\ \exists y \in B \text{ tak, že } [x, y] \in \varrho\}.$$

Oborem hodnot této relace ϱ rozumíme množinu

$$\Im\varrho := \{y \in B;\ \exists x \in A \text{ tak, že } [x, y] \in \varrho\}.$$

Je-li $\varrho \subseteq A \times B$ relace, pak relace ϱ^{-1} k ní *inverzní* je relace mezi B, A definovaná takto:

$$\varrho^{-1} := \{[x, y];\ [y, x] \in \varrho\}.$$

Je-li $\varrho \subseteq A \times B$ a $\sigma \subseteq B \times C$, pak jejich *složením* rozumíme relaci $\sigma \circ \varrho \subseteq A \times C$ definovanou takto:

$$\sigma \circ \varrho := \{[x, z]; x \in A, z \in C,\ \exists y \in B \text{ tak, že } [x, y] \in \varrho, [y, z] \in \sigma\}.$$

Buď $\varrho \subseteq A \times B$. Říkáme, že ϱ je *zobrazení z A do B*, jestliže ke každému prvku $x \in A$ existuje nejvýše jeden prvek $z \in B$ takový, že $[x, y] \in \varrho$. Místo $[x, y] \in \varrho$ pak obvykle píšeme $y = \varrho(x)$.

Je-li ϱ zobrazení z A do B a platí $\mathrm{Dom}\varrho = A$, říkáme, že ϱ je *zobrazení A do B*. Tuto skutečnost symbolicky označíme $\varrho\colon A \to B$.

Zobrazení $f\colon A \to B$ se nazývá *surjektivní* (též *surjekce* nebo zobrazení *na*), jestliže $\Im f = B$.

Zobrazení $f\colon A \to B$ se nazývá *injektivní* (též *injekce* nebo *prosté* zobrazení), jestliže $x, y \in A, x \neq y \Rightarrow f(x) \neq f(y)$.

Zobrazení, které je současně injekcí i surjekcí, se nazývá *bijekce*.

Je-li $f\colon A \to B$ zobrazení, je relace f^{-1} zobrazení z B do A zřejmě právě tehdy, když je f injektivní.

Symbolem id_A rozumíme *identické zobrazení* na množině A (tj. zobrazení A do A definované tak, že $\mathrm{id}_A(x) = x$ pro každý prvek $x \in A$).

Jsou-li A, B množiny, pak A^B značí množinu všech zobrazení B do A.

Buď $f\colon A \to B$, $C \subseteq A$. *Restrikcí* $f|C$ zobrazení f na množinu C rozumíme zobrazení $g\colon C \to B$ definované takto: $g(x) = f(x)$ pro každý prvek $x \in C$.

Relace na množině

Relací na množině A rozumíme každou podmnožinu ϱ množiny A^2. Označíme-li $\mathcal{P}(x)$ množinu všech podmnožin množiny X, je množina $\Re(A)$ všech relací na A rovna množině $\mathcal{P}(A^2)$.

Diagonální relací na A rozumíme relaci $\triangle_A := \{[x, x];\ x \in A\}$.

Je-li ϱ relace na A, píšeme místo $[x, y] \in \varrho$ obvykle $x\varrho y$ a místo $[x, y] \notin \varrho$ píšeme $x\overline{\varrho}y$.

Některé často se vyskytující vlastnosti relací mají speciální pojmenování. Zejména řekneme, že relace ϱ na A je:

(a) *reflexivní*, jestliže pro každý prvek $x \in A$ platí $x\varrho x$;

(b) *areflexivní*, jestliže pro každý prvek $x \in A$ platí $x\overline{\varrho}x$;

(c) *symetrická*, jestliže $x, y \in A$, $x\varrho y \Rightarrow y\varrho x$;

(d) *asymetrická*, jestliže $x, y \in A$, $x\varrho y \Rightarrow y\overline{\varrho}x$;

(e) *antisymetrická*, jestliže $x, y \in A$, $x\varrho y \wedge y\varrho x \Rightarrow x = y$;

(f) *tranzitivní*, jestliže $x, y, z \in A$, $x\varrho y \wedge y\varrho z \Rightarrow x\varrho z$;

(g) *úplná*, jestliže pro každé $x, y \in A$ platí $x\varrho y$ nebo $y\varrho x$ nebo $x = y$.

Poněvadž relace na A jsou množiny, má smysl hovořit o průniku relací, sjednocení relací, rozdílu relací a podobně.

Je například zřejmé, že když ϱ, σ jsou tranzitivní relace na A, pak $\varrho \cap \sigma$ je rovněž tranzitivní relace na A, avšak $\varrho \cup \sigma$ je relace na A, která nemusí být tranzitivní.

Uspořádané množiny

Uspořádáním na množině A nazýváme každou relaci na A, která je současně reflexivní, antisymetrická i tranzitivní.

Je-li A množina, ϱ uspořádání na A, nazývá se dvojice (A, ϱ) *uspořádaná množina*. Nemůže-li však dojít k nedorozumění, hovoříme často o uspořádané množině A (a nikoliv (A, ϱ)).

Je-li uspořádání ϱ úplné, tj. pro každé dva prvky $x, y \in A$ platí $x\varrho y$ nebo $y\varrho x$, nazývá se (A, ϱ) *řetězec*.

Relaci uspořádání nejčastěji značíme symbolem $\leq$.

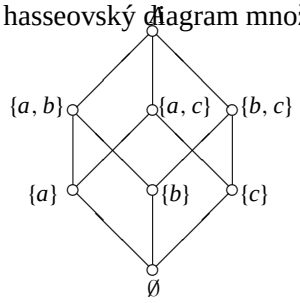
Prvky x, y v uspořádané množině $(A, \leq)$ se nazývají *srovnatelné*, platí-li $x \leq y$ nebo $y \leq x$. V opačném případě se nazývají *nesrovnatelné*. Je-li $x \leq y$ avšak $x \neq y$, píšeme $x < y$. Jestliže platí $x < y$ a neexistuje z tak, že $x < z < y$, říkáme, že prvek y *pokrývá* prvek x (nebo prvek x *je pokryt* prvkem y).

Uspořádaná množina se nazývá *protiřetězec*, když jsou každé dva její různé prvky nesrovnatelné. (Uspořádáním na této množině je pak zřejmě diagonální relace.) V řetězci jsou naopak každé dva prvky srovnatelné.

Je-li $\mathcal{A}$ nějaký systém množin, pak je zřejmě inkluze $\subseteq$ uspořádáním na $\mathcal{A}$. Máme-li nějaký systém množin uspořádat, pak to právě nejčastěji uděláme inkluzí. Pro libovolnou množinu A jsou tedy $(\mathcal{P}(A), \subseteq)$ i $(\mathfrak{R}(A), \subseteq)$ uspořádané množiny.

Konečné uspořádané množiny obvykle znázorňujeme tzv. *hasseovským diagramem*. Prvky uspořádané množiny A při tom znázorníme jako body v rovině, větší prvky umístíme „výše“ než menší prvky a dva různé prvky spojíme úsečkou právě tehdy, když jeden pokrývá druhý.

Na následujícím obrázku je hasseovský diagram množiny $(\mathcal{P}(A), \subseteq)$, kde $A = \{a, b, c\}$.



Je-li $(A, \leq)$ uspořádaná množina, značí $\breve{A}$ množinu A s *duálním* uspořádáním, tj. množinu $(A, \geq)$. Místo $\breve{A}$ se často píše též A^*.

Buďte A, B uspořádané množiny. Zobrazení $f\colon A \to B$ se nazývá *izotonní*, jestliže pro každé dva prvky $x, y \in A$ platí: $x \leq y \Rightarrow f(x) \leq f(y)$. Zobrazení $f\colon A \to B$ se nazývá *izomorfismus*, když:

(i) f je bijekce,

(ii) f je izotonní,

(iii) f^{-1} je izotonní.

Uspořádané množiny A, B se nazývají *izomorfní* (což značíme $A \cong B$), jestliže existuje alespoň jeden izomorfismus $f\colon A \to B$.

Buď A uspořádaná množina, $\emptyset \neq B \subseteq A$. Prvek $a \in A$ se nazývá *horní závora* množiny B, když pro každý prvek $x \in B$ platí $x \leq a$. B se nazývá *shora ohraničená* (v A), jestliže v A existuje alespoň jedna horní závora množiny B. Analogicky se definuje *dolní závora* a *zdola ohraničená* množina. Řekneme, že B je v A *ohraničená*, je-li v A ohraničená shora i zdola.

Buď A uspořádaná množina. Prvek $a \in A$ se nazývá *největší* prvek množiny A, když pro každý prvek $x \in A$ platí $x \leq a$. Prvek $a \in A$ se nazývá *maximální* prvek množiny A, jestliže v A neexistuje prvek $x > a$. Analogicky je definován *nejmenší* a *minimální* prvek uspořádané množiny.

Je zřejmé, že největší prvek v A je maximálním prvkem a nejmenší prvek minimálním prvkem. Největší (respektive nejmenší) prvek v A — pokud existuje — je určen jednoznačně, zatím co maximálních (respektive minimálních) prvků může v A existovat víc.

Buď A uspořádaná množina, $\emptyset \neq B \subseteq A$. Nejmenší horní závora množiny B v A (pokud existuje) se nazývá *suprémum* množiny B v A; značíme ji $\sup_A B$. Z výše uvedeného plyne, že suprémum množiny — pokud existuje — je určeno jednoznačně.

Duálně je definováno *infimum* množiny B v A ($\inf_A B$).

Uspořádaná množina A se nazývá *svaz*, existuje-li pro každé dva prvky $x, y \in A$ jejich suprémum i infimum v A. A se nazývá *úplný svaz*, má-li každá $\emptyset \neq B \subseteq A$ v A suprémum i infimum.

Je zřejmé, že pro každou množinu A je $(\mathcal{P}(A), \subseteq)$ úplný svaz. (Protože $\Re(A) = \mathcal{P}(A^2)$, plyne odtud, že systém všech relací na libovolné množině tvoří vzhledem k množinové inkluzi úplný svaz.)

Ekvivalence a rozklady

Relace ϱ na množině A se nazývá *ekvivalence*, je-li reflexivní, symetrická a tranzitivní. Symbolem $\mathcal{E}(A)$ označme množinu všech ekvivalencí na množině A.

Snadno lze dokázat, že $(\mathcal{E}(A), \subseteq)$ je úplný svaz s nejmenším prvkem $\emptyset$ a největším prvkem A^2. Infimum neprázdné množiny relací je přitom jejich průnik, suprémum však obecně není jejich sjednocení (vzhledem k tomu, že sjednocení nezachovává tranzitivitu).

Buď $A \neq \emptyset$ množina. Systém $\overline{A}$ po dvou disjunktních neprázdných podmnožin množiny A se nazývá *rozklad* na A, když $\bigcup_{X \in \overline{A}} X = A$.

Prvky rozkladu $\overline{A}$ nazýváme *třídy rozkladu* $\overline{A}$. Každý prvek tak podle definice leží právě v jedné třídě daného rozkladu $\overline{A}$.

Označme $\mathcal{K}(A)$ množinu všech rozkladů na množině A. Definujme na $\mathcal{K}(A)$ relaci $\leq$ takto:

Pro $\overline{A}, \overline{B} \in \mathcal{K}(A)$ je $\overline{A} \leq \overline{B}$ právě tehdy, když ke každé třídě $X \in \overline{A}$ existuje třída $Y \in \overline{B}$, tak, že $X \subseteq Y$.

Pak je $\leq$ uspořádání na $\mathcal{K}(A)$.

Je-li $\overline{A} \leq \overline{B}$, říkáme, že $\overline{A}$ je *zjemnění* rozkladu B a $\overline{B}$ je *zákryt* rozkladu A.

Buď $A \neq \emptyset$ libovolná množina. Pak ke každé ekvivalenci ϱ na A existuje právě jeden rozklad $\overline{A}$ na A a ke každému rozkladu $\overline{A}$ na A existuje právě jedna ekvivalence ϱ na A tak, že pro každé prvky $x, y \in A$ platí

$$x \varrho y \text{ právě tehdy když } x, y \text{ patří do téže třídy rozkladu } \overline{A}.$$

Ve výše uvedeném smyslu každá ekvivalence $\varrho \in \mathcal{E}(A)$ určuje právě jeden rozklad na A. Tento rozklad nazýváme *faktormnožinou* množiny A podle ϱ; značíme jej A/ϱ.

Zobrazení $F\colon \mathcal{E}(A) \to \mathcal{K}(A)$ definované vztahem $F(\varrho) = A/\varrho$ je nejen bijekce, ale dokonce izomorfismus $(\mathcal{E}(A), \subseteq)$ na $(\mathcal{K}(A), \leq)$. Platí tedy

$$(\mathcal{E}(A), \subseteq) \cong (\mathcal{K}(A), \leq).$$

Zejména odtud plyne, že $(\mathcal{K}(A), \leq)$ je úplný svaz.

LITERATURA

[1] KURATOWSKI K., MOSTOWSKI A.: *Set Theory,* Amsterdam, 1967.

[2] TARSKI A.: *Introduction to Logic and to the Methodology of Deductive Sciences,* New York, 1965, český překlad: *Úvod do logiky a metodologie deduktivních věd,*Praha 1966.

[3] BLAŽEK J., KUSSOVÁ B.: *Množiny a přirozená čísla,* Praha, 1977.

[4] WANG HAO, MCNAUGHTON R.: *Les systémes axiomatiques de la théorie des ensembles,* Paris, 1953.

[5] FRAENKEL A. A.,Y. BAR-HILLEL: *Foundations of Set Theory,* Amsterdam, 1958.

[6] KLEENE, S. C., *Introduction to Metamathematics,* New York–Toronto, 1952.

[7] KUROŠ, A. G.: *Lekciji po obščej algebre,* Moskva, 1962.

[8] HAUSDORFF F.: *Grundzüge der Mengenlehre,* Leipzig, 1914.

[9] GÖDEL K.: *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I,* Monatsch. Math. Ph., **38** (1931), 173–198.

REJSTŘÍK