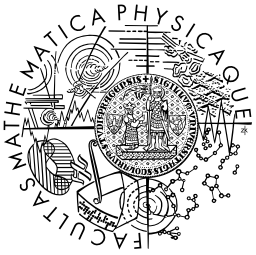


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

**BAKALÁŘSKÁ PRÁCE**

David Weber

# Stručný úvod do teorie množin pro středoškoláky

Katedra didaktiky matematiky

Vedoucí bakalářské práce: RNDr. Martin Rmoutil, Ph.D.

Studijní program: Matematika se zaměřením na vzdělávání
Studijní obor: Matematika se zaměřením na vzdělávání se sdruženým studiem informatika se zaměřením na vzdělávání

Praha 2022

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne .....  .....

Podpis autora

(TODO: Doplnit poděkování.)

Název práce: Stručný úvod do teorie množin pro středoškoláky

Autor: David Weber

Katedra: Katedra didaktiky matematiky

Vedoucí bakalářské práce: RNDr. Martin Rmoutil, Ph.D., Katedra didaktiky matematiky

Abstrakt: (TODO: Doplnit abstrakt.)

Klíčová slova: teorie množin kardinál ordinál přirozené číslo nekonečno Georg Cantor Bernard Bolzano

Title: A Brief Introduction to Set Theory for High Schools

Author: David Weber

Department: Department of Mathematics Education

Supervisor: RNDr. Martin Rmoutil, Ph.D., Department of Mathematics Education

Abstract: (TODO: Doplnit abstrakt (EN).)

Keywords: set theory cardinal number ordinal number natural number infinity Georg Cantor Bernard Bolzano

# Obsah

# Kapitola 1

# Historický úvod k teorii množin

Čtenář se s pojmem *množina* již jistě setkal. Často se o množině hovoří jako o „celku“, „souboru“ nebo „souhrnu“ obsahujícím jisté prvky. Na střední škole jsme si s tímto chápáním uvedeného pojmu nejspíše vystačili, když jsme se např. učili o Vennových diagramech. To nám poskytovalo poměrně názorný způsob, jak si představit množiny a vztahy mezi nimi. Většinou jsme se dotazovali např. na velikost množiny či zda jí nějaký zvolený prvek náleží či nikoliv. Pojem „náležení“ jsme stejně jako množinu též nejspíše nikterak formálně nedefinovali, přesto ale intuitivně tušíme, co to znamená, když se řekne, že „prvek náleží množině“. Jak byste ale formálně definovali množinu? Nebo co teprve „býti prvkem množiny“?

Zkusme ještě otázku jiného charakteru. Jak by čtenář odpověděl na otázku, jestli je více čísel v intervalu (0,1) nebo všech přirozených čísel? A jak by svou odpověď zdůvodnil? Odpověď **stejně**, neboť jich je nekonečně mnoho zní velmi intuitivně, ale jak se později dozvíme, odpověď na tuto otázku je daleko složitější, než se může zdát.

Důvod proč se najednou místo množin zabýváme *nekonečnem*, je ten, že ve skutečnosti tento termín je hlavní příčinou vzniku teorie množin (nikoliv definice pojmu „množina“, jak by se mohlo zdát). V následujících sekcích se proto podíváme na to, jak se na pojem nekonečna nahlíželo v historii a jaké problémy způsobovalo.

## 1.1 Potenciální versus aktuální nekonečno

Co je vlastně nekonečno? Čtenáři toho může připadat jako absurdní dotaz, ale tento zdánlivě jasný pojem způsoboval ve své době potíže.

Fakt, že přirozených čísel je nekonečně mnoho byl znám již ve starověku.

$$1,2,3,\ldots$$

I žáci na základních školách jsou si této skutečnosti vědomi a pravděpodobně se nad tím nikdo z nich nepozastaví. Jak ale toto můžeme chápat? Existují dva základní způsoby.
Pokud začneme postupně vypisovat všechna přirozená čísla, jistě je nikdy nevypíšeme všechna, protože bez ohledu na to, jakou si zvolíme mez, vždy ji nakonec

přesáhneme. Takovémuto nekonečnému **procesu** pak říkáme *potenciální nekonečno*.

Druhou možností ale je, že se na množinu přirozených čísel budeme dívat již jako na „hotovou“. To znamená, že nebudeme řešit, jak všechna přirozená čísla vypíšeme, ale budeme na tuto množinu nahlížet již jako na **celek**, tedy nekonečno budeme chápat v uzavřené formě. V takovém případě mluvíme o tzv. *aktuálním nekonečnu*.

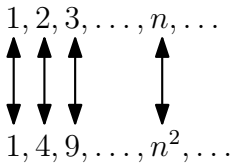
Starým Řekům se však jak z důvodů matematických, tak filozofických, zdálo, že lidskému myšlení je přístupné pouze nekonečno **potenciální**. O tom se lze přesvědčit už ze samotných *Eukleidových axiómů*. K axiomatice čtenář bude mít možnost blíže nahlédnout v kapitole (TODO: doplnit odkaz na kapitolu.) v sekci (TODO: doplnit odkaz na sekci.). Eukleidés právě z důvodu nemyslitelnosti aktuálního nekonečna mluvil o *přímce* jako o úsečce, kterou může libovolně prodlužovat, nikoliv, že je „nekonečná“ nebo „nekonečně dlouhá“, jak říkáme dnes.

### 1.1.1 Galileova úvaha o velikosti

S problémem nekonečna se však pojily i další problémy. Při zrodu samotné teorie množin v 70. letech 19. století se totiž nabízela otázka, zdali *má vůbec smysl porovnávat nekonečné množiny*. Nad tím se pozastavil už jeden z géniů 16. a 17. století Galileo Galilei (1564–1642). Ten si vypsal dvě posloupnosti čísel:

$$1,\ 2,\ 3, \ldots,\ n, \ldots \quad \text{a} \quad 1,\ 4,\ 9, \ldots,\ n^2, \ldots,$$

tzn. přirozená čísla a jejich druhé mocniny. Avšak při pohledu na tyto dvě posloupnosti si Galileo uvědomil, že každý prvek množiny přirozených čísel lze „spárovat“ s jeho druhou mocninou (v dnešní terminologii bychom řekli, že existuje *bijekce*; na tu se blíže podíváme v kapitole (TODO: doplnit odkaz na kapitolu s bijekcí.)).




To by však znamenalo, že přirozených čísel a jejich druhých mocnin je **stejně mnoho**! Avšak jeden z Eukleidových logických axiomů říká, že *celek je větší část*. Proto se tehdy Galileovi zdál tento závěr jako naprostý nesmysl a tak usoudil, že porovnávat nekonečné množiny podle velikosti zkrátka nemá žádný smysl. Jinak řečeno, tvrdil, že **aktuální nekonečno** je sporné a tedy nemůže existovat. [1]

### 1.1.2 Grandiho řada

Dalším typickým problémem týkajícího se nekonečna je tzv. *Grandiho řada*. Čtenář se nejspíše již s řadami setkal na střední škole, specificky s řadou aritmetickou a geometrickou. Řadou v matematice rozumíme zápis

$$a_1 + a_2 + a_3 + \cdots + a_n,$$

kde pro všechna přirozená $i$ je $a_i$ člen nějaké posloupnosti. U řad nás celkem pochopitelně zajímal jejich součet. To nebyl většinou problém, neboť jsme se převážně zajímali o řady konečné (a speciálně pro aritmetickou a geometrickou posloupnost jsme měli i elegantní vzorce), ale uvážíme-li řady nekonečné, mohou nastat potíže.

Co se vůbec rozumí pod pojmem „součet nekonečné řady“? Jako příklad si vezměme řadu

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\cdots,$$

tedy sčítáme členy posloupnosti $\{1/2^n\}_{n=1}^{\infty}$. Podívejme se, jak se situace bude vyvíjet, když budeme členy postupně přičítat:

$$\begin{aligned}\frac{1}{2}&=0{,}5\\ \frac{1}{2}+\frac{1}{4}&=0{,}75\\ \frac{1}{2}+\frac{1}{4}+\frac{1}{8}&=0{,}875\\ \frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}&=0{,}9375.\end{aligned}$$

Těmto součtům se říká tzv. *částečné součty*. Po součtu prvních dvaceti členů bude výsledek následující:

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\cdots+\frac{1}{2^{20}}=0{,}999999046.$$

Jak je vidět, částečné součty se postupně „blíží“ nejspíše číslu 1. Dávalo by tedy smysl prohlásit číslo 1 za výsledek této nekonečné řady, tj.

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\cdots=1.$$

Tímto způsobem obecně vnímáme součet nekonečné řady: **hodnota, ke které se blíží částečné součty**. (Formální definici součtu nekonečné řady si zde odpustíme.)

Problému s nekonečnými řadami si všiml italský matematik Gildo Grandi (1671–1742). Uvažme následující rovnost:

$$0=0+0+0+\cdots.$$

To nejspíše nevypadá nikterak zajímavě. Přeci jen nekonečným sčítáním nul celkem přirozeně nemohu dostat jiný výsledek než opět nulu. Nulu si však můžeme vyjádřit jako $1-1$. Aplikací na rovnost výše dostaneme

$$0=(1-1)+(1-1)+(1-1)+\cdots. \tag{1.1}$$

Podle asociativního zákona pro sčítání můžeme změnit uzávorkování. Změníme jej proto takto

$$0=1+(-1+1)+(-1+1)+(-1+1)+\cdots$$

a nakonec z každé závorky vytkneme znaménko „−“

$$0 = 1 - (1 - 1) - (1 - 1) - (1 - 1) - \cdots .$$

Tedy dostáváme, že

$$\begin{aligned} 0 &= (1 - 1) + (1 - 1) + (1 - 1) + \cdots \\ &= 1 + (-1 + 1) + (-1 + 1) + (-1 + 1) + \cdots \\ &= 1 - (1 - 1) - (1 - 1) - (1 - 1) - \cdots \\ &= 1 - 0 - 0 - 0 - \cdots = 1. \end{aligned}$$

Aplikací jednoduchých aritmetických pravidel jsme dospěli k závěru, že $0 = 1$. To je samozřejmě nesmysl, ale kde je tedy chyba? (Zde poprosím čtenáře, aby se zkusil zamyslet.)
*Grandiho řadou* nazýváme zápis

$$1 - 1 + 1 - 1 + 1 - 1 + \cdots ,$$

kterou jsme obdrželi u rovnosti (1.1) (až na uzávorkování). Není těžké si všimnout, že postupným sčítáním jednotlivých členů se budou částečné součty opakovat

$$\begin{aligned} 1 &= 1, \\ 0 &= 1 - 1, \\ 1 &= 1 - 1 + 1, \\ 0 &= 1 - 1 + 1 - 1, \\ &\vdots \end{aligned}$$

Zkusme k této řadě přistoupit ještě jedním způsobem. Uvažujme, že řada má součet, který si označíme $S$. Pak

$$S = 1 - 1 + 1 - 1 + \cdots .$$

Opět využitím asociativního zákona a vytknutím znaménka „−“ si upravíme řadu na pravé straně takto:

$$S = 1 - (1 - 1 + 1 - 1 + \cdots ).$$

Čtenář si však již možná všiml, že výraz v závorce na pravé straně je opět námi vyšetřovaná řada se součtem $S$, tedy z toho vyplývá

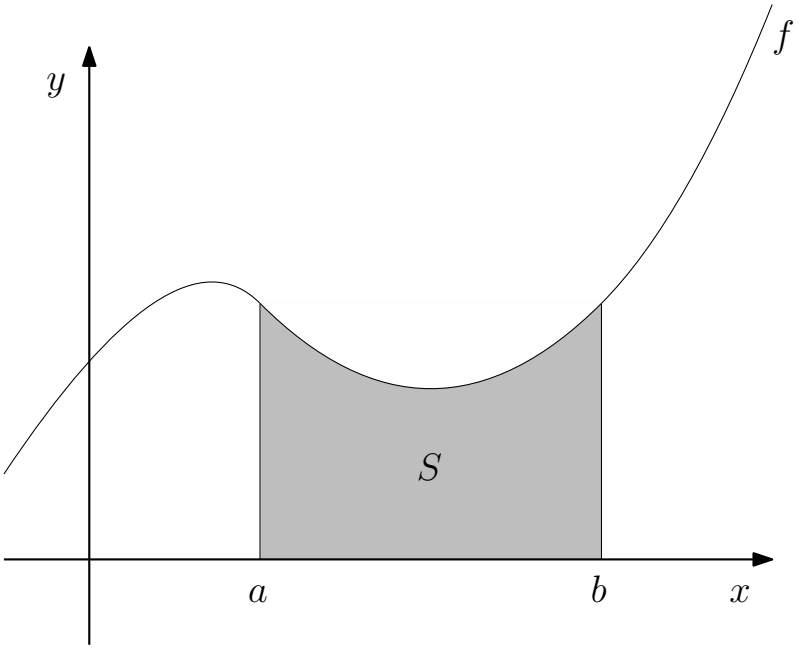
$$\begin{aligned} S &= 1 - S \\ S &= \frac{1}{2}. \end{aligned}$$

Toto je však také zarážející výsledek, neboť jak jsme se sami přesvědčili, tak částečné součty pouze oscilují mezi 0 a 1.

Všimněme si, že rovnosti uvedené výše jsme obdrželi pouhou aplikací základních početních pravidel; přesto jsou však sporné. Tyto výsledky později vedly k novým poznatkům v aritmetice, a to sice faktu, že asociativita a komutativita definitivně platí pouze u konečných součtů.

### 1.1.3 Nekonečno v matematické analýze

Velká část matematické analýzy je založená na úvahách s *nekonečně malými veličinami*; často se mluví o tzv. *infinitezimálním počtu*. Čtenář se s těmito pojmy již možná setkal, ačkoliv nemusí mít nutně představu o jeho přesném významu. Asi nejznámějším příkladem je integrální počet, specificky výpočet „plochy pod křivkou“.




Obrázek 1.1: Příklad určitého integrálu funkce $f$ na uzavřeném intervalu $\langle a,b\rangle$.

Obrázek 1.1 a obrázky jemu podobné se často uvádí ve spojitosti s tzv. *určitým integrálem*. Zde bychom mohli psát

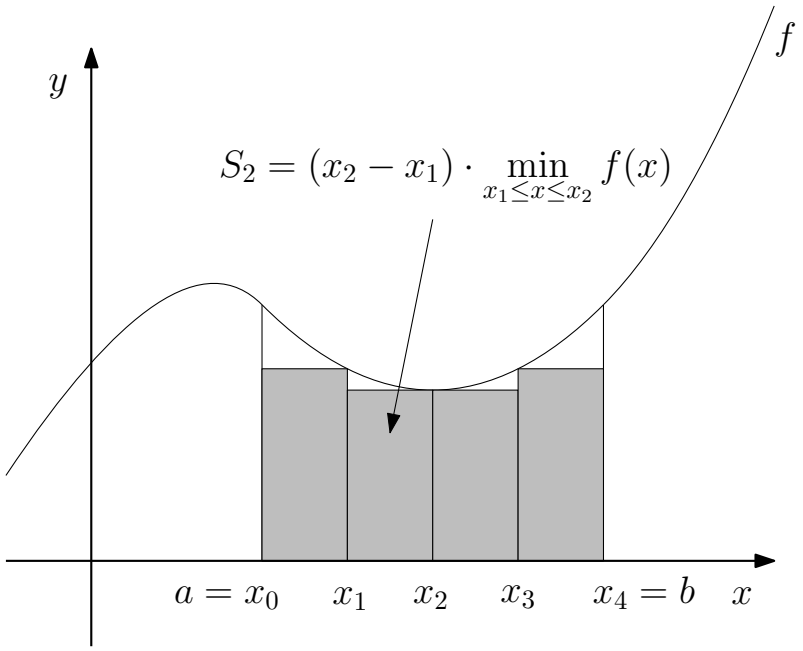
$$S = \int_a^b f(x)\ \mathrm{d}x.$$

Pro upřesnění, pokud platí, že funkce $f$ je na intervalu $\langle a,b\rangle$ kladná, pak integrál $\int_a^b f(x)\ \mathrm{d}x$ je obsah plochy pod grafem funkce $f$ na intervalu $\langle a,b\rangle$. Výpočet obsahu takové složitě vypadající plochy, jako na obrázku 1.1, se může zdát bez znalosti integrálního počtu takřka nemožným úkolem. Pokusme se ale na danou problematiku podívat právě optikou infinitezimálního počtu. (Znalý čtenář snad promine, že se zatím zdržím formalismů a pouze jednoduše naznačím myšlenku.)

Pro začátek zkusíme plochu pouze aproximovat. K tomu využijeme tvar, jehož obsah jsme schopni triviálně vypočítat – obdélníka. Pro začátek zkusíme plochu aproximovat pomocí 4 obdélníků (viz obrázek 1.2). Všechny 4 obdélníky jsme zvolili tak, aby měly stejnou šířku a jejich výška odpovídala minimální hodnotě v daném dílčím intervalu. Obecně obsah $i$-tého obdélníku $S_i$ bychom zapsali jako

$$S_i = (x_i - x_{i-1}) \cdot \min_{x_{i-1} \le x \le x_i} f(x),$$

kde $\min_{x_{i-1}\le x\le x_i} f(x)$ je minimální hodnota funkce $f$ na intervalu $\langle x_{i-1},x_i\rangle$ (předpokládáme pro jednoduchost, že $f$ je spojitá, takže nabývá svého minima na kaž-




Obrázek 1.2: Aproximace plochy pod grafem funkce $f$ na intervalu $\langle a,b\rangle$ pomocí 4 obdélníků.

dém z daných intervalů). Rozdíl $x_i - x_{i-1}$ odpovídá šířce obdélníku a $\min_{x_{i-1} \le x \le x_i} f(x)$ jeho výšce.

Pokud bychom si však interval $\langle a,b\rangle$ rozdělili ještě „jemněji“, není těžké vidět, že se náš odhad zpřesní (viz obrázek 1.3). Volbou stále „jemnějšího“ dělení intervalu $\langle a,b\rangle$ se náš odhad bude zpřesňovat. Budeme-li mít tedy plochu aproximovanou $n$ obdélníky, pak[1]

$$S \approx (x_1 - x_0) \cdot \min_{x_0 \le x \le x_1} f(x) + \cdots + (x_n - x_{n-1}) \cdot \min_{x_{n-1} \le x \le x_n} f(x). \tag{1.2}$$

Pro rostoucí $n$, tedy počet dílčích intervalů $\langle x_{i-1},x_i\rangle$, se bude rozdíl $x_i - x_{i-1}$ blížit nule (obdélníky se budou „zužovat“). V konečném důsledku bude rozdíl $x_i - x_{i-1}$ „nekonečně malý“ a součet uvedený výše u aproximace v obrázku 1.2 přejde v integrál

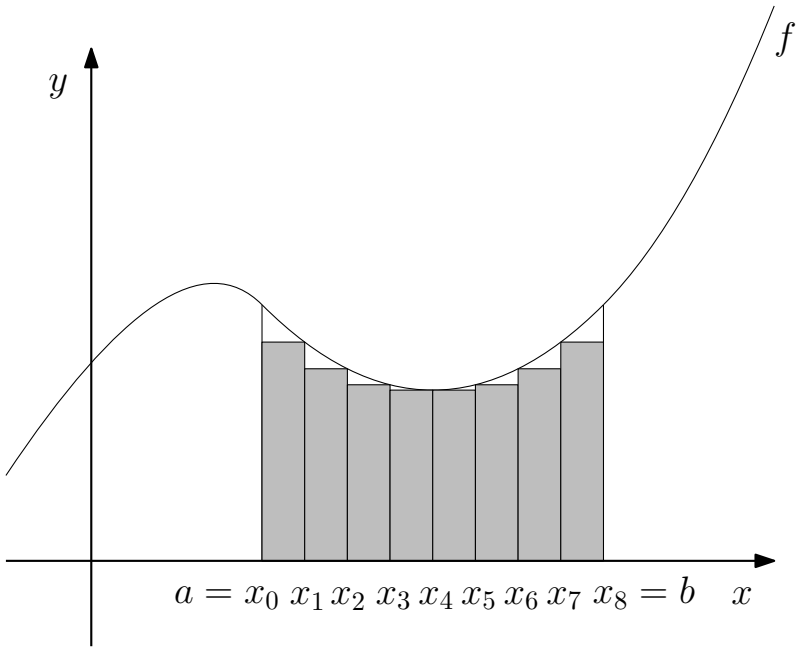
$$S = \int_a^b f(x)\ \mathrm{d}x,$$

kde rozdíl $x_i - x_{i-1}$ přešel v diferenciál $\mathrm{d}x$ a minimum $\min_{x_{n-1} \le x \le x_n} f(x)$ přešlo přímo ve funkční hodnotu $f(x)$.

V matematice značíme součty pomocí řeckého symbolu $\sum$ (velké písmeno *sigma*). Proto se čtenář může často setkat v jiných textech se zápisem

$$S \approx \sum_{i=1}^{n} (x_i - x_{i-1}) \cdot \min_{x_{i-1} \le x \le x_i} f(x).$$

[1]Symbolem $\approx$ značíme přibližnou rovnost (ve starších textech lze najít i symbol $\doteq$).




Obrázek 1.3: Aproximace plochy pod grafem funkce $f$ na intervalu $\langle a,b\rangle$ pomocí 8 obdélníků.

Prohodíme-li činitele v součinu, pak už je o něco jednodušeji vidět přechod v integrál, který jsme popsali výše

$$\sum_{i=0}^{n} \overbrace{\min_{x_{i-1}\le x\le x_i} f(x)}^{\to f(x)} \cdot \underbrace{(x_i - x_{i-1})}_{\to \mathrm{d}x} \longrightarrow \int_a^b f(x)\ \mathrm{d}x.$$

Toto je velmi zjednodušené vysvětlení určitého integrálu, avšak hlavní myšlenkou bylo právě ono potenciálně „nekonečné dělení“, které bylo jedním z příkladů využití **nekonečně malých veličin**. (Zde konkrétně roli nekonečně malé veličiny zastávala postupně zmenšující se šířka obdélníků kvůli „zjemňování“ dělení.)

Na podobných úvahách jsou založeny různé další pojmy v matematické analýze, jako např. *limita* nebo i *derivace*. Je však nutno si uvědomit, že co je nám známo dnes, nebylo zcela známo matematikům v 17. století. V této době se začal *integrální* a *diferenciální* počet pořádně rozvíjet. Jejich tvůrci Gottfried Wilhelm Leibniz (1646–1716) a Isaac Newton (1642–1726/27) základy své tehdejší úvahy o infinitezimálním počtu postavili právě na nekonečně malých veličinách. Problémem tehdy však bylo, že tento pojem nebyl pořádně definován a pravidla pro počítání s (aktuálně) nekonečně malými veličinami byla definována pouze velmi vágně. I přesto se však integrální a diferenciální počet ukázal být opravdu mocným nástrojem (hlavně ve fyzice). Postupně se ale začaly nejasnosti v jejich samotných základech vyhrocovat, což nakonec vyústilo v období, které dnes nazýváme *druhou krizí matematiky*[2].

Problémy v matematické analýze se začaly odstraňovat až na počátku 19. století, kdy významnou roli sehrál ve dvacátých letech Augustin Louis Cau-

[2]První krize matematiky nastala v dobách antického Řecka a souvisela s objevem iracionálních čísel (TODO: případně doplnit do přílohy.).

chy zavedením limity. Její formální definici však podal později Karl Theodor Wilhelm Weierstrass, která pracovala opět s potenciálním nekonečnem. [1]

## 1.2 Počátky teorie množin a současnost

V matematice se přibližně až do poloviny 19. století uvažovalo pouze **potenciální nekonečno**. Myšlenka pohlížet na množiny jako na nekonečné byla silně odmítána, neboť na nekonečno **aktuální** se v té době pohlíželo jako na koncept nedostupný lidskému myšlení. Ačkoliv v matematické analýze již existovaly metody k odstranění problémů s „nekonečně malými“ veličinami, přesto se v matematické literatuře nacházely spousty postupů s nekonečnem, které často vedly k nesprávným výsledkům.

### 1.2.1 Bernard Bolzano

Problémů s nekonečnem a s jeho vnímáním si všiml i český matematik, filozof a kněz Bernard Placidus Johann Nepomuk Bolzano[3] (1781–1848). Byl jedním z matematiků, kteří prosazovali existenci aktuálního nekonečna, o čemž později píše i ve svém díle *Paradoxy nekonečna*[4] (v německém originále *Paradoxien des Unendlichen*). Bolzanovo dílo však není až tak úplně dílem ryze matematickým, jako spíše matematicko-filozofickým. Kromě nekonečna je zde věnována pozornost i fyzice a jejímu náhledu na svět.

Ve svém díle se Bolzano snaží (mimo jiné) ukázat, proč je zapotřebí pracovat v matematice s aktuálním nekonečnem a také se zaměřuje na některé chyby, kterých se vědci dopouštějí při úvahách o nekonečnu. Je nutné však dodat, že ačkoliv svými úvahami byl Bolzano blízko úvahám, s nimiž dneska v teorii množin pracujeme, přesto se v některých záležitostech došel k jiným výsledkům. Např. dospěl k závěru, že pokud je jedna množina obsažena v druhé (tzn. je její podmnožinou), pak musí jedna mít menší mohutnost než druhá nebo pokud existuje „párování“ mezi prvky dvou množin (viz podsekce 1.1.1 o Galileově úvaze o velikosti), neznamená to nutně, že mají stejnou mohutnost (blíže nahlédneme v sekci (TODO: doplnit odkaz na sekci.)). To však nic nemění na faktu, že Paradoxy nekonečna jsou pozoruhodným dílem, které nám dává skvělý vhled do vědeckého myšlení v Bolzanově době. Pozornost si zaslouží parafráze myšlenky, pomocí které se Bolzano pokusil existenci aktuálního nekonečna zdůvodnit.

#### Množina pravd o sobě

Představme si, že máme nějaký libovolný **pravdivý** výrok, který si označíme $A$. O tomto výroku můžeme určitě vyslovit výrok: „A je pravdivé“, který si označíme $B$. Jsou tyto výroky stejné? Z čistě matematického pohledu jsou si tato tvrzení ekvivalentní, co do jejich pravdivostní hodnoty, neboť i kdyby neplatilo

[3] Ačkoliv byl B. Bolzano čech, publikoval své práce v němčině a latině.

[4] Dílo vyšlo až 3 roky po Bolzanově smrti, tj. v roce 1851, kdy se jeho publikace ujal Bolzanův žák František Příhonský. Českého překladu se však dílo dočkalo až roku 1963 od Otakara Zicha (viz seznam použité literatury).

$A$, pak jistě neplatí ani $B$. Avšak zněním si stejná již tato tvrzení nejsou. Ať už si za výrok $A$ dosadíme jakékoliv tvrzení, je třeba si uvědomit, že subjektem $B$ je samotný výrok $A$ (což pro výrok $A$ samotný již neplatí). Pokud zkonstruujeme další výrok $C$ stejným způsobem, jeho znění bude „Je pravdivé, že je pravdivé $A$“, což je opět odlišný výrok od $B$. Takto můžeme pokračovat libovolně dlouho. Množina těchto výroků by svou velikostí jistě musela převyšovat jakékoliv přirozené číslo, tedy je *nekonečné velikosti*.

Bolzano zde však uznává, že tento myšlenkový konstrukt je svou povahou stále záležitostí nekonečna potenciálního. Reagoval tak na námitky tehdejší matematické společnosti, že je nesmysl se bavit o nekonečných množinách, neboť taková množina **nemůže být nikdy sjednocena v celek a být celá obsáhnuta naším myšlením**. Zkusme se na chvilku vrátit ke konečným množinám. Uvážíme-li množinu všech obyvatel Prahy, málokdo z nás nejspíše zná každého z nich. Přesto však hovoříme o každém z nich, když řekneme např. „všichni obyvatelé Prahy“. Tedy ani tato (konečná) množina nemůže být celá obsáhnuta naší myšlením. Tuto myšlenku se Bolzano snažil aplikovat i na množiny nekonečné. Uvážíme-li množinu přirozených čísel, také jistě neznáme všechna **přirozená čísla**, ale i přesto nám nedělá problém hovořit o nich jako o celku.

Teologicky zdůvodňoval Bolzano existenci aktuálního nekonečna ve své knize tak, že je-li Bůh považován za **vševědoucího**, tedy zná všechny pravdy, pak jistě vidí i ty, které jsme zkonstruovali v prvním odstavci. Množina pravd o sobě je tak podle Bolzana nekonečná, neboť **Bůh je všechny zná**.[2]

### 1.2.2 Georg Cantor

Bolzano byl vskutku velmi blízko k odhalení a pochopení vlastností nekonečných množin, avšak v jeho práci bylo vidět, že stále nebyl schopen se plně dostat za hranici myšlenky, že „celek je větší než část“. To se podařilo až Georgu Cantorovi[5] (1845–1918), kterému se podařilo učinit při úvahách s nekonečnými množinami velký myšlenkový posun. Cantor je dodnes považován a zaslouženě uznáván za zakladatele teorie množin, která výrazně ovlivnila soudobou matematiku. Svou prací navázal na Bolzanovy Paradoxy nekonečna, neboť též zastával názor existence aktuálního nekonečna. Konkrétně se dostal k otázce, zdali je mohutnější množina přirozených čísel nebo reálných. (Všimněte si, že oproti otázce v úvodu této kapitoly zde již používáme termín *mohutnost*. Blíže nahlédneme v kapitole (TODO: doplnit odkaz na kapitolu.) v sekci (TODO: doplnit odkaz na sekci.)) Cantor došel k překvapivému závěru, a to sice, že **množina reálných čísel je mohutnější než množina přirozených čísel**. Tyto výsledky Cantora dovedly postupně k definici pojmu mohutnosti množiny a také vybudování teorie tzv. *kardinálních* a *ordinálních* čísel.

Cantor tehdy považoval za množinu libovolný souhrn objektů, kdy o každém prvku lze (v principu) rozhodnout, zdali dané množině náleží, či nikoliv. Tedy při výstavbě své teorie vnímal Cantor pojem množiny velmi intuitivně. Dnes tuto teorii označujeme jako *naivní teorii množin*. Důvod tohoto názvu je v objevených paradoxech.

[5] Celým jménem se jmenoval Georg Ferdinand Ludwig Philipp Cantor.

Cantorova teorie byla ve své době mnohými neuznávána a velmi znevažována, což mu velmi ztížilo činnost publikování. Práce byla hodně kritizována za to, jak Cantor zachází s aktuálně nekonečnými množinami. Problém s Cantorovou teorií však nastal tehdy, když se zjistilo, jak silné dopady má ono intuitivní chápání pojmu množina.

### Russellův paradox

V roce 1902 přemýšlel Bertrand Arthur William Russell (1872–1970) o samotném Cantorově zavedení pojmu množina. Cantor považoval za množinu jakýkoliv souhrn objektů, kde o každém prvku je možné (alespoň v principu) rozhodnout, zdali je či není jejím prvkem. S tímto chápáním množiny jsme většinou pracovali na střední škole, neboť nám nejspíše znělo poměrně rozumně, ale Russell si v tomto pojetí množiny všiml problému.

Uvažujme, že je dána množina $S$, která obsahuje všechny množiny takové, že nejsou samy sobě prvkem.

Jak si takovou množinu vůbec představit? Co to znamená, že je množina sama sobě prvkem? Zkusme se nejdříve podívat na několik příkladů.

- Uvažujme množinu všech obyvatel Prahy. Je taková množina sama obyvatelem Prahy? Nejspíše není, taková množina tedy **není prvkem sebe sama**.
- Mějme množinu všech možných ideí. Je taková množina sama ideou? Ale jistě, že je. Taková množina tedy naopak **je sama sobě prvkem**.
- Je množina všech států sama sobě prvkem? (Tj. je sama státem?) **Ne**, není.
- Množina všech objektů popsatelných méně než deseti slovy **je sama sobě prvkem**. (Popsali jsme ji pomocí osmi slov.)

Takové množiny jsou tedy skutečně představitelné a má smysl se jimi zabývat. Russell tedy uvážil právě takovou množinu, která obsahuje množiny, jenž samy sebe neobsahují.

Symbolicky bychom množinu $S$ zapsali (značení viz podsekce (TODO: doplnit odkaz.))

$$S = \{X \mid X \notin X\}\,.$$

Množina $S$ je dobře definovaná v Cantorově pojetí (jedná se o souhrn objektů). Pokud bychom si vzali např. množiny

$$A = \{X,Y,Z,A\} \quad \text{a} \quad B = \{X,Y,W\}\,,$$

kde $X$,$Y$,$Z$,$W$ jsou libovolně zvolené prvky, pak podle definice $S$ platí, že $A \notin S$ a $B \in S$. Podle takto zvolené definice $S$, patří do ní sama množina $S$?

Postupujme podle dané logiky. Pokud množina $S$ neobsahuje sebe sama, pak by ale podle své definice sama sebe obsahovat měla. A naopak pokud množina sama sebe obsahuje, pak je to spor s její definicí a sama sebe by obsahovat neměla. Tím jsme však v obou případech došli ke sporu, neboť z tohoto plyne závěr,

že množina $S$ je sama sobě prvkem právě tehdy, když není sama sobě prvkem. Symbolicky (viz sekce o logice 2.1)

$$S \in S \Leftrightarrow S \notin S.$$

Tento paradox se uvádí v mnoha analogiích. Asi nejtypičtější a nejčastěji uváděný je tzv. *paradox holiče*.

„Holič holí všechny lidi, kteří se neholí sami. Podle uvedeného pravidla, holí holič sám sebe?“

I zde bychom došli ke sporu stejným způsobem. Pokud by se holič holil, pak by se podle pravidla holit neměl a pokud by se neholil, pak by se naopak holit měl. Zkuste si sami rozmyslet souvislost s originálním zněním Russellova paradoxu.

V teorii množin se postupně začalo objevovat více paradoxů[6] a nesrovnalostí. Překvapivě některé z nich byly objeveny již před samotným Russellovým paradoxem. Za jedny z nejdůležitějších lze považovat ještě

- *Burali-Fortiův paradox* - objeven roku 1897 Cesarem Burali-Fortim (1861–1931),
- *Cantorův paradox* - objeven roku 1899.

K vysvětlení těchto paradoxů však zatím nemáme vyvinutý dostatečný matematický aparát, nicméně ještě se k nim později vrátíme pro doplnění (TODO: dopsat např. do přílohy.).

### 1.2.3 Teorie množin v současnosti

Cantorova tehdejší naivní teorie množin začala být nakonec ke konci 19. století uznávána. Začalo se ukazovat, že teorie množin je skutečně mocným nástrojem k vybudování samotných základů matematiky. Chvíli se zdálo, že matematici mají dostupný skutečně pevný základ pro výstavbu dalších teorií. Avšak postupné objevování antinomií v teorii množin je vyvedlo z jejich omylu a bylo jasné, že pro spolehlivé vybudování základů bude třeba daleko více práce. Toto období proto nazýváme *3. krizí matematiky*.

Jak se ukázalo, dosavadní způsob budování matematiky byl neudržitelný, a tak se matematici snažili přijít s řešením. Ta se však svou povahou velmi lišila podle matematického a filozofického uvažování každého z nich. Hrubě bychom mohli tehdy rozlišit dva hlavní myšlenkové proudy: *intuicionismus* a *formalismus*.

Intuicionismus byl svým přístupem velmi omezený, neboť v jeho duchu bylo možné pracovat pouze s omezenou částí matematiky, která byla „přípustná“. Aktuální nekonečno s existenčními důkazy[7] jsou odmítány. Uznávány jsou pouze objekty, které lze přímo zkonstruovat (tzv. *konstruktivní důkazy*). Proto byl tehdy např. kritizován Cantorův důkaz existence tzv. *transcendentních čísel*[8] (blíže v

[6] Též *antinomie*, tj. sporné tvrzení vyvozené z korektně vyvozených závěrů.

[7] *Existenční důkazy* jsou takové důkazy, které prokáží existenci nějakého objektu, ale není možno z nich obdržet žádný příklad daného objektu.

[8] Tak nazýváme čísla, která nejsou kořeny žádné algebraické rovnice s racionálními koeficienty (např. Ludolfovo číslo $\pi$ nebo Eulerovo číslo $e$).

kapitole (TODO: doplnit odkaz na kapitolu.) v sekci (TODO: doplnit odkaz na sekci.)). Zajímavostí a kontroverzí jeho důkazu byl fakt, že při tehdejším dokázání jejich existence neuvedl příklad ani jednoho nich.

Formalismus naopak dále pracoval s aktuálními znalostmi. Matematici se snažili vybudovat matematiku na množinách tak, jak zamýšlel Cantor, avšak jedním z cílů byla eliminace dosavadně známých antinomií. Objevují se dva rozdílné přístupy, přičemž prvním z nich byla tzv. *teorie typů*[9] a *axiomatická výstavba*.

Protože axiomatická výstavba pro nás jako koncept bude dále podstatným stavebním kamenem, zaměříme se právě na ni. Axiomatická výstavba je dnes asi nejrozšířenějším způsobem budování různých teorií. Ať už budujeme jakoukoliv teorii, v principu není možné definovat všechny pojmy a dokázat všechna možná tvrzení. Dříve nebo později bychom došli k závěru, že abychom mohli dojít k různým tvrzením, je třeba zavést nějaké „primitivní pojmy“, na nichž budeme stavět další definice, a tzv. *axiómy* neboli tvrzení, která implicitně považujeme za pravdivá a nedokazujeme jejich platnost. Ve skutečnosti však axiomatika nebyla nikterak novou záležitostí; byla známa již od starověku.

Jedním z nejstarších děl jsou v tomto ohledu Eukleidovy *Základy*. Eukleidés se pokusil tehdejší rovinou geometrii (dnes nazývanou *eukleidovskou geometrií*) vybudovat na celkem pěti základních postulátech. Čtenář si nejspíše všiml, že jsme použili termín postulát (též „předpoklad“ či „prvotný úkol“), nikoliv axióm, avšak není mezi nimi významný rozdíl. Většinou se tyto termíny uvádí vzhledem k historickému kontextu. Uveďme si zde pro představu několik Eukleidových základních pojmů (citováno z českého překladu Základů z roku 1907 od Františka Servíta [3]):

- Bod jest, co nemá dílu.
- Čára pak délka bez šířky.
- Plocha jest, co jen délku a šířku má.
- Hranicemi plochy jsou čáry.
- Tupý jest úhel pravého větší.

*Eukleidovy postuláty*:

(i) Budiž úkolem od kteréhokoliv bodu ke kterémukoliv bodu vésti přímku.

(ii) A přímku omezenou nepřetržitě rovně prodloužiti.

(iii) A z jakéhokoli středu a jakýmkoli poloměrem narýsovati kruh.

(iv) A že všecky pravé úhly sobě rovny jsou.

(v) A když přímka protínajíc dvě přímky tvoří na téže (přilehlé) straně úhly menších dvou pravých, ty dvě přímky prodlouženy jsouce do nekonečna že se sbíhají na straně, kde jsou úhly menších dvou pravých.

[9] O té se zmiňuje Russell v knize *Principia Mathematica*, na které se s ním podílel anglický matematik Alfred North Whitehead. Kniha vyšla v letech 1910–1913.

Toto je první historicky známé dílo, kde byla teorie takto deduktivně budována. Dnešním axiomatickým systémům je však celkem pochopitelně vzdálená, neboť tehdy byly základní pojmy a axiomy, resp. postuláty, psány běžnou řečí a odvozování tvrzení na jejich základě probíhalo intuitivně. Dnešní axiomatika je v těchto směrech formálnější, protože se využívá formálního jazyka a též jsou dána přesná odvozovací pravidla. Co však matematiky tehdy zajímalo na axiomaticky budovaných systémech byla jejich:

- *nezávislost* (tzn. zdali žádný z axiómů nelze odvodit ze zbylých axiómů; takové tvrzení pak již není axióm, nýbrž věta);
- *úplnost* (tzn. zdali je dána taková soustava axiómů, abychom každé tvrzení mohli dokázat, nebo dokázat jeho negaci);
- *bezespornost* (tzn. zdali není možné z daných axiómů odvodit tvrzení a současně jeho negaci).

Čtenáře možná napadne, že pokud jde o nezávislost, jedná se v podstatě jen o „vadu na krásе“, neboť pokud nějaký axióm lze v teorii odvodit z ostatních, pak jej stačí odstranit. Není-li systém úplný, je to již poměrně nepříjemné, neboť by to znamenalo, že v teorii existují tvrzení, která nelze dokázat, ani vyvrátit. Nejhorší je však pochopitelně, pokud je teorie sporná.

První úspěšnou teorii množin axiomaticky vybudoval v letech 1904–1908 německý matematik Ernst Friedrich Ferdinand Zermelo (1871–1953), které se v tomto textu budeme dále věnovat. Základní Zermelovou myšlenkou při budování jeho teorie bylo, že ne každý souhrn objektů je možné považovat za množinu (blíže si jednotlivé axiómy vysvětlíme v kapitole (TODO: doplnit odkaz na kapitolu.)). Pojem **množina** a **býti prvkem** jsou zde považovány za primitivní (nedefinované) pojmy, s nimiž se dále pracuje. Zermelovu teorii později upravil izraelský matematik Adolf Abraham ha-Levi Fraenkel (1891–1965), čímž vznikla tzv. *Zermelova-Fraenkelova teorie množin*. Dodnes se jedná o nejrozšířenější variantu.

Později vyšla i tzv. *Gödelova-Bernaysova teorie množin*, jíž dal základ švýcarský matematik Issak Paul Bernays (1888–1977) v letech 1937–1954 a rakouský matematik Kurt Friedrich Gödel (1906–1978) v reakci na omezení, která se objevovala v Zermelově-Fraenkelově teorii množin.

Bohužel se nikdy nikomu nepodařilo dokázat, zdali jsou budované axiomatické teorie bezesporné a úplné (což se pro srovnání podařilo např. u varianty zmíněné eukleidovské geometrie). Jak ukázal Kurt Gödel (viz tzv. *Gödelovy věty o neúplnosti*), tak ve skutečnosti takovou teorii není ani možné sestrojit, neboť v libovolném „dostatečně bohatém“ axiomatickém systému teorie množin budou vždy existovat tvrzení, která nelze dokázat a ani nelze dokázat jejich negaci, což tehdy odhalilo výraznou omezenost axiomatických metod.

# Kapitola 2

# Logika

(TODO: Změnit úvodní popis.)

V této kapitole zavedeme některá základní značení a pojmy v oblasti logiky. Je dosti možné, že některé záležitosti již čtenář dobře zná nebo o nich slyšel a to především v úvodní části. I přesto však považuji zmínku za nezbytnou, neboť na těchto pojmech budeme dále stavět. Posléze se dostaneme k zajímavější části a to sice kvantifikátorům, které budeme dále využívat, neboť nám umožní zápisy některých složitějších výroků.

## 2.1 Výroková logika

Tato část je čtenáři pravděpodobně již z části známa ze střední školy. Řadu vět (matematických i nematematických) lze matematicky chápat jako *výrok*, tj. tvrzení, o kterém lze jednoznačně prohlásit, zdali je či není pravdivé. Výrokům přiřazujeme tzv. *pravdivostní hodnotu*, která je buď 1 pro *pravdivý* výrok nebo 0 pro *nepravdivý* výrok.

Za výroky lze považovat např. tvrzení:

- „Prší.“,
- „Prší a svítí slunce.“,
- „Nebude-li pršet, nezmoknem.“,
- „Když bude pršet, zmokneme.“,

a mnohé jiné (u každého z nich jsme schopni jednoznačně určit jeho pravdivostní hodnotu). K formálnímu zápisu tvrzení v matematice vyžíváme tzv. *logické spojky* a *kvantifikátory*.

### 2.1.1 Logické spojky

Mezi logické spojky řadíme *negaci* $\neg$, *konjunkci* $\wedge$, *disjunkci* $\vee$, *implikaci* $\Rightarrow$ a *ekvivalenci* $\Leftrightarrow$. Připomeňme si stručně jejich významy.

**Úmluva 2.1.1** (Abeceda pro výrokové proměnné)**.** Pro označení *výroků* nebo též *výrokových proměnných* budeme používat velká písmena latinské abecedy $A$,$B$,...,$X$,$Y$,$Z$, případně opatřenými indexy.

Uvažujme libovolné výroky $A$ a $B$.

- Negace $\neg A$ má opačnou pravdivostní hodnotu než $A$.
- Konjunkce $A \wedge B$ je pravdivá, pokud je pravdivý výrok $A$ **a současně** je pravdivý výrok $B$. Tedy má-li $A$ nebo $B$ pravdivostní hodnotu 0, pak i $A \wedge B$ má pravdivostní hodnotu 0. Čteme *„A a (zároveň) B“*.
- Disjunkce $A \vee B$ je pravdivá, pokud alespoň jeden z výroků $A$ a $B$ je pravdivý. Výrok $A \vee B$ je tedy nepravdivý pouze když jsou současně nepravdivé výroky $A$ i $B$. Čteme *„A nebo B“*
- U implikace se často mluví o výroku $A$ jako o *předpokladu* a o $B$ jako o *závěru*. Výrok $A \Rightarrow B$ pak říká, že pokud platí výrok $A$, **pak nutně platí** i výrok $B$. Čteme *„jestliže A, pak B“*, *„z A vyplývá B“* či *„A implikuje B“*. Zde se hodí upozornit na to, že mezi předpokladem a závěrem nemusí být nutně souvislost.
- Ekvivalence $A \Leftrightarrow B$ je pravdivá, pokud jsou výroky $A$ a $B$ **současně pravdivé** nebo **současně nepravdivé**. Čteme *„A právě tehdy, když B“*.

Výroky uvedené výše obsahující dané logické spojky lze přehledně zapsat do tabulky pravdivostních hodnot (viz tabulka 2.1).

| $A$ | $B$ | $\neg A$ | $A \wedge B$ | $A \vee B$ | $A \Rightarrow B$ | $A \Leftrightarrow B$ |
|---|---|---|---|---|---|---|
| 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 |

Tabulka 2.1: Tabulka pravdivostních hodnot pro základní logické spojky

Vraťme se nyní ještě ke zmíněné implikaci. Ve skutečnosti tato logická spojka je pravděpodobně tou nejsložitější na pochopení ze všech čtyř zmíněných, neboť při neobezřetnosti je často (a to i v běžné mluvě) zaměňována za ekvivalenci. Uvažme tvrzení „Jestliže nebudeš jíst, nedostaneš zmrzlinu.“. Synáček by v takovou chvíli očekával, že když naopak oběd sní, tak zmrzlinu dostane, avšak ze striktně matematického hlediska mu ji tatínek i tak dát nemusí a přesto by nelhal. Je důležité si uvědomit, že v případě nesplnění předpokladu nám implikace o závěru nic neříká.

### 2.1.2 Výrokové formule

Pokud se ohlédneme za výroky, které jsme zatím uvažovali, vždy se jednalo o výroky *složené*. Vezmeme-li např. výrok „Číslo 2 je sudé nebo liché.“, tak jej lze rozdělit na dva „jednodušší“ výroky, tj. „Číslo 2 je sudé.“ a „Číslo 2 je liché.“,

přičemž dané výroky jsou spojeny disjunkcí $\vee$. Tyto výroky však již žádné logické spojky neobsahuje a tedy je nelze dále „rozložit“. S tímto souvisí terminologie zavedená v definici 2.1.3.

**Úmluva 2.1.2** (Abeceda pro výrokové formule)**.** Pro označení výrokových formulí budeme používat malá písmena řecké abecedy, tj. $\alpha$,$\beta$,$\gamma$,..., případně opatřenými indexy.

**Definice 2.1.3** (Výroková a atomická formule)**.**

(i) Každá výroková proměnná je *výroková formule* (tzv. *atomická formule*).

(ii) Jsou-li $\varphi$ a $\psi$ výrokové formule, pak $\neg(\varphi)$, $(\varphi) \wedge (\psi)$, $(\varphi) \vee (\psi)$, $(\varphi) \Rightarrow (\psi)$ a $(\varphi) \Leftrightarrow (\psi)$ jsou také výrokové formule.

(iii) Výraz, který nelze získat pomocí pravidel (i) a (ii) není výrokovou formulí.

(Převzato z [1], str. 14 a [4], str. 30).

**Poznámka 2.1.4.** Občas budeme v této sekci zkráceně psát pouze *formule*. Nicméně vždy tím bude míněna výroková formule ve smyslu definice 2.1.3.

**Úmluva 2.1.5** („Rovnost“ výrokových formulí)**.** Uvažujme, že máme libovolné výrokové formule $\varphi$ a $\psi$. Pokud $\varphi$ a $\psi$ vyjadřují stejnou výrokovou formuli, pak budeme psát $\varphi \sim \psi$.

Řekneme-li, že výrokové formule „jsou stejné“, pak se formule shodují ve svém zápisu. Máme-li např. výrokové formule

$$\begin{aligned}
&\varphi_1 \sim (A) \wedge \Big((B) \vee (C)\Big),\\
&\varphi_2 \sim \Big((A) \wedge (B)\Big) \vee \Big((A) \wedge (C)\Big) \text{ a}\\
&\varphi_3 \sim \Big((A) \wedge (B)\Big) \vee \Big((A) \wedge (C)\Big),
\end{aligned}$$

pak můžeme psát, že $\varphi_2 \sim \varphi_3$, ale nikoliv $\varphi_1 \sim \varphi_2$, byť $\varphi_1$ a $\varphi_2$ mají shodnou tabulku pravdivostních hodnot.

Definice výrokové formule 2.1.3 nám v podstatě říká, jakým způsobem můžeme sestrojit potenciálně všechny možné formule. Mějme výrokové proměnné $A$, $B$ a $C$. Ty jsou podle (i) v definici 2.1.3 výrokovými formulemi. Podle (ii) jsou pak formulemi i výrazy

$$(A) \wedge (B)\ ,\ (A) \vee (C) \text{ a } \neg(B). \tag{2.1}$$

Nyní můžeme opakovaně použít (ii) k sestrojení dalších složitějších formulí. Tedy užitím formulí (2.1) můžeme dále postupně sestrojit např. výrazy

$$\Big((A) \wedge (B)\Big) \Rightarrow \Big((A) \vee (C)\Big) \quad \text{a} \quad \Big((A) \wedge \Big(\neg(B)\Big)\Big) \Leftrightarrow \Big(\neg\Big((A) \vee (B)\Big)\Big),$$

které jsou opět podle (ii) výrokovými formulemi. Opětovným užitím (ii) pak je dále výrokovou formulí např.

$$\Big(\Big((A) \wedge (B)\Big) \Rightarrow \Big((A) \vee (C)\Big)\Big) \Rightarrow \Big(\Big((A) \wedge \Big(\neg(B)\Big)\Big) \Leftrightarrow \Big(\neg\Big((A) \vee (B)\Big)\Big)\Big).$$

Takto můžeme postupovat dál a opakovanou aplikací pravidla (ii) vytvořit ještě složitější výrokové formule.

Naopak pokud bychom uvážili nějaký výraz, můžeme obdobně zjistit, jestli se jedná o výrokovou formuli či nikoliv.

**Příklad 2.1.6.** Mějme výraz

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

Ověřte, zda $\varphi$ je výroková formule.

*Řešení.* Aby $\varphi$ byla formule, musí být

$$\varphi_1 \sim (A) \wedge (C) \quad \text{a} \quad \varphi_2 \sim \Big((A) \vee (B)\Big) \Rightarrow \neg(C)$$

též formulemi. Výraz $\varphi_1$ zřejmě je formulí, neboť $A$ a $C$ jsou atomické formule. Ovšem u $\varphi_2$ lze již vidět, že výraz nesplňuje definici výrokové formule, neboť u $\neg(C)$ chybí vnější závorky. Z bodu (iii) definice 2.1.3 tedy plyne, že výraz $\varphi$ **není výrokovou formulí**, neboť jej nelze získat pomocí pravidel (i) a (ii).

□

Čtenáře možná již napadlo, že formule, které jsme sestrojili z definice 2.1.3, jsou zapsány poměrně komplikovaně, především co do nadměrného používání závorek. Např. výraz

$$A \wedge \neg C, \tag{2.2}$$

není podle 2.1.3 výrokovou formulí. I přesto je však nejspíše zřejmé, že tímto zápisem vyjadřujeme výrok „Platí $A$ a zároveň neplatí $C$.“. Nebo vrátíme-li se k příkladu 2.1.6, i při vypuštění uzávorkování u výrazu $\varphi_2$ by dávalo smysl interpretovat výraz

$$A \vee B \Rightarrow \neg C$$

jako výrok „Jestliže platí $A$ a zároveň $B$, pak neplatí $C$.“. Pro zjednodušení zápisu dalších výrokových formulí se proto budeme držet následující úmluvy 2.1.7.

**Úmluva 2.1.7** (Pořadí logických operací)**.**

(1) Negace $\neg$ má přednost před všemi ostatními logickými spojkami.

(2) Konjunkce a disjunkce $\wedge$,$\vee$ jsou rovnocenné a mají přednost před implikací a ekvivalencí $\Rightarrow$ , $\Leftrightarrow$, které jsou sobě rovnocenné.

**Příklad 2.1.8.** Zjednodušení některých formulí při aplikaci zavedeného pořadí logických operací v úmluvě 2.1.7.

(i) $(A) \wedge (B) \quad \rightsquigarrow \quad A \wedge B,$

(ii) $\neg(\neg A) \quad \rightsquigarrow \quad \neg\neg A,$

(iii) $\neg\Big((A) \vee (B)\Big) \quad \rightsquigarrow \quad \neg(A \vee B),$

(iv) $\Big(\big((A) \wedge (B)\big) \vee \big(\neg(C)\big)\Big) \Rightarrow \big(\neg(A)\big) \wedge \big(\neg(C)\big)$
$\rightsquigarrow \quad (A \wedge B) \vee \neg C \Rightarrow \neg A \wedge \neg C.$

Nyní se vraťme k původní definici výrokové formule 2.1.3, kterou jsme zavedli. S ní souvisí čtenářovi pravděpodobně známý postup pro vyhodnocování logických formulí, a to sice *tabulková metoda*. Její myšlenkou bylo rozdělit danou výrokovou formuli postupně na dílčí formule a takto postupovat u i daných dílčích formulí. Tímto způsobem nakonec dojdeme až k samotným atomickým formulím, kde zkoumáme všechny možné kombinace jejich pravdivostních hodnot (resp. kombinace pravdivostních hodnot jejich výrokových proměnných).

Před ukázkou na příkladech si ještě zavedeme jedno značení, které budeme potřebovat.

**Definice 2.1.9** (Logická ekvivalence výrokových formulí)**.** Mějme výrokové formule $\varphi$ a $\psi$. Řekneme, že $\varphi$ a $\psi$ jsou *logicky ekvivalentní*, což zapisujeme jako $\varphi \equiv \psi$, pokud je formule $\varphi \Leftrightarrow \psi$ pro všechny pravdivostní hodnoty výrokových proměnných obsažených ve $\varphi$ a $\psi$ pravdivá.

Pokud tedy budeme mít např. formule

$$\varphi_1 \sim \neg(A \wedge B),$$
$$\varphi_2 \sim \neg A \vee \neg B,$$

pak můžeme psát $\varphi \equiv \psi$, neboť jak se lze přesvědčit, formule $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ je vždy pravdivá.

Nabízí se otázka: jaký je rozdíl mezi $\equiv$ a $\Leftrightarrow$? Formálně vzato bychom mohli mezi formule jednoduše vkládat ekvivalenci, avšak pak se nám tato logická spojka mohla plést s ekvivalencemi, které jsou součástí $\varphi$ a $\psi$.

**Příklad 2.1.10.** Mějme formuli

$$\varphi \sim A \wedge \neg B \Leftrightarrow A \vee B.$$

Pro jaké pravdivostní hodnoty výroků $A$ a $B$ je formule $\varphi$ pravdivá?

*Řešení.* Postupujme způsobem popsaným výše, tj. rozdělme nejdříve danou formuli na dílčí formule. V tomto případě dílčími formulemi $\varphi$ jsou

$$\varphi_1 \sim A \wedge \neg B \quad \text{a} \quad \varphi_2 \sim A \vee B,$$

které jsou spojeny ekvivalencí $\Leftrightarrow$, tj.

$$\varphi \sim \varphi_1 \Leftrightarrow \varphi_2.$$

Formule $\varphi_1$ obsahuje atomický výrok $A$ a formuli $\neg B$ spojené konjunkcí $\wedge$. Označme tedy ještě

$$\varphi_3 \sim \neg B$$

$\varphi_3$ již obsahuje pouze atomický výrok $B$ v negaci $\neg$.

Podívejme se nyní na dílčí formuli $\varphi_2$. Ta obsahuje atomické výroky $A$ a $B$ spojené disjunkcí $\vee$. Zapišme nyní vše zmíněné po řadě do tabulky pravdivostních hodnot (viz tabulka 2.2).

| $A$ | $B$ | $\varphi_3 \sim \neg B$ | $\varphi_1 \sim A \wedge \neg B$ | $\varphi_2 \sim A \vee B$ | $\varphi \sim A \wedge \neg B \Leftrightarrow A \vee B$ |
|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 1 |

Tabulka 2.2: Tabulka pravdivostních hodnot pro $\varphi_1$, $\varphi_2$, $\varphi_3$ a $\varphi$

Z tabulky 2.2 můžeme již vidět, že formule $\varphi$ je pravdivá pro $A \equiv 1$ a $B \equiv 0$, nebo pro $A \equiv 0$ a $B \equiv 0$.

□

Tento středoškolský postup je zcela jistě vždy funkční. Avšak ne vždy je moudré jej ihned aplikovat. Zkusme se podívat ještě na jeden příklad výrokové formule.

**Příklad 2.1.11.** Mějme logickou formuli

$$\psi \sim (A \wedge \neg A \Rightarrow B) \vee \Big((A \Leftrightarrow B) \wedge (C \vee \neg C)\Big).$$

Pro jaké pravdivostní hodnoty výroků $A$,$B$,$C$ je formule $\psi$ pravdivá?

*Řešení.* V tuto chvíli bychom aplikací metody použité v příkladu 2.1.10 museli vyšetřit pravdivostní hodnotu formule $\psi$ pro celkem $2^3 = 8$ různých kombinací pravdivostních hodnot $A$,$B$,$C$. Jistě bychom takto též došli k řešení, nicméně práci si můžeme značně ulehčit. (Prosím čtenáře, aby se zde pozorněji zaměřil na formuli $\psi$ v zadání.)

Ve skutečnosti jsou některé dílčí formule zjednodušitelné. Zaměřme se pro začátek na formuli

$$A \wedge \neg A.$$

Může tato formule být někdy pravdivá? Jistě, že nemůže. Libovolný výrok buď **platí a nebo platí jeho negace**, což nikdy nemůže nastat současně. Taková formule má pak vždy pravdivostní hodnotu 0 bez ohledu na pravdivostní hodnotu $A$. Tedy

$$A \wedge \neg A \equiv 0.$$

Z výše uvedeného také ovšem plyne, že formule

$$C \vee \neg C \equiv 1,$$

neboť opět platí buď $C$, nebo jeho negace $\neg C$.

Vyšetřovanou formuli $\psi$ tedy můžeme zjednodušit

$$\begin{aligned} \psi \sim \Big(\overbrace{(A \wedge \neg A)}^{\equiv 0} \Rightarrow B\Big) \vee \Big((A \Leftrightarrow B) \wedge \overbrace{(C \vee \neg C)}^{\equiv 1}\Big) \equiv \\ \equiv (0 \Rightarrow B) \vee \Big((A \Leftrightarrow B) \wedge 1\Big). \end{aligned}$$

Tento krok nám však umožňuje provést další úpravy. Podívejme se blíže na formuli

$$(A \Leftrightarrow B) \wedge 1.$$

Výsledek této konjunkce vždy bude záviset na pouze na pravdivostní hodnotě $A \Leftrightarrow B$, tzn. konjunkce je zde nadbytečná a můžeme psát

$$(A \Leftrightarrow B) \wedge 1 \equiv A \Leftrightarrow B.$$

Čeho si lze dále všimnout je, že výrok

$$0 \Rightarrow B$$

je také vždy pravdivý (viz tabulka 2.1). Celkově se tedy výroková formule $\psi$ zjednoduší takto

$$\begin{aligned} \psi \sim (\overbrace{0 \Rightarrow B}^{\equiv 1}) \vee \Big( \overbrace{(A \Leftrightarrow B) \wedge 1}^{\equiv A \Leftrightarrow B} \Big) \equiv \\ \equiv 1 \vee (A \Leftrightarrow B). \end{aligned}$$

Disjunkce je však pravdivá právě tehdy, když je alespoň jeden z výroků pravdivý, což zde platí. Z tohoto dostáváme výsledek, že

$$\psi \equiv 1.$$

Tedy bez ohledu na to, jaké pravdivostní hodnoty budou mít výroky $A$,$B$,$C$, bude formule $\psi$ vždy pravdivá. Pokud bychom přeci jen přistoupili na použití tabulkové metody, které jsme se zpočátku vyhnuli, můžeme se skutečně přesvědčit, že náš závěr je správný (viz tabulky 2.3 a 2.4).

| $A$ | $B$ | $C$ | $\neg A$ | $\neg C$ | $A \wedge \neg A$ | $C \vee \neg C$ | $A \Leftrightarrow B$ | $(A \wedge \neg A) \Rightarrow B$ |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |

Tabulka 2.3: Tabulka pravdivostních hodnot podformulí formule $\psi$ (1. část).

| $A$ | $B$ | $C$ | $(A \Leftrightarrow B) \wedge (C \vee \neg C)$ | $\psi$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 |

Tabulka 2.4: Tabulka pravdivostních hodnot podformulí formule $\psi$ (2. část).

□

Tento typ formulí je poměrně významný a proto pro ně zavádíme speciální pojmenování v definici 2.1.12.

**Definice 2.1.12** (Tautologie)**.** Výrokovou formuli $\varphi$ nazveme *tautologií*, pokud $\varphi \equiv 1$.

Některé tautologie jsme využili již pri řešení příkladu 2.1.11. Uveďme si zde ještě několik dalších významných příkladů.

**Věta 2.1.13** (Významné tautologie)**.** *Následující výrokové formule jsou tautologie:*

*(i)* $\neg(A \Leftrightarrow \neg A)$

*(ii)* $A \vee \neg A$ ◁ *zákon vyloučeného třetího*

*(iii)* $A \Leftrightarrow A$ ◁ *zákon identity*

*(iv)* $\neg\neg A \Leftrightarrow A$ ◁ *zákon dvojí negace*

*(v)* $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ ◁ *de Morganovo pravidlo*

*(vi)* $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$ ◁ *de Morganovo pravidlo*

*(vii)* $\Big(A \wedge (A \Rightarrow B)\Big) \Rightarrow B)$ ◁ *pravidlo Modus ponens*[1]

*(viii)* $\Big((A \Rightarrow B) \wedge \neg B\Big) \Rightarrow \neg A$ ◁ *pravidlo Modus tollens*[2]

*(ix)* $(A \Rightarrow \neg A) \Rightarrow \neg A$ ◁ *reductio ad absurdum*

*(x)* $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$

*(xi)* $(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$

*(xii)* $(A \Rightarrow B) \Leftrightarrow B \vee \neg A$

*(xiii)* $(A \Rightarrow B) \wedge (B \Rightarrow C) \Leftrightarrow (A \Rightarrow C)$

*(xiv)* $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$

*(xv)* $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$

Čtenář si pravdivosti těchto výroků může ověřit prostým sestavením tabulek pravdivostních hodnot daných logických formulí. Tautologie (vii), (x) a (xi) se hodně využívají při dokazování tvrzení (blíže nahlédneme v sekci A.1).

[1] Česky *pravidlo vynětí*.
[2] Česky *popírání důsledku*.

## 2.2 Kvantifikátory a predikátový počet

Logické spojky nám jistě poskytují nástroj pro vyjádření celé řady různých výroků. Vyjádřit např. výrok „Anička má zelené vlasy ($Z$) a modré oči ($M$).“ tak pro nás není problém. Symbolicky bychom mohli napsat např.

$$Z(\text{Anička}) \wedge M(\text{Anička}).$$

Co kdybychom toto chtěli prohlásit místo o jednom člověku např. o všech obyvatelích Prahy? Užitím čistě logických spojek, jak jsme prováděli doposud, bychom museli napsat např.

$$(Z(\text{Anička})\wedge M(\text{Anička}))\wedge(Z(\text{Eva})\wedge M(\text{Eva}))\wedge(Z(\text{Tomáš})\wedge M(\text{Tomáš}))\wedge\cdots\wedge(Z(\text{Jiří})\wedge M(\text{Jiří})$$

To je sice správné, ale poměrně těžkopádné vyjádření tak jednoduchého výroku. Jistě bychom neřekli „Anička má zelené vlasy a modré oči a zároveň Eva má zelené vlasy a modré oči a zároveň . . . “. Čtenář nejspíše tuší, že existuje jednodušší způsob vyjádření takového výroku, resp. výrokové formule. K tomu v logice slouží právě takzvané *kvantifikátory*.

V praxi bychom zkrátka řekli: „Všichni obyvatelé Prahy mají zelené vlasy a modré oči.“ (takové tvrzení je jistě výrok). Tímto způsobem formulujeme podobné výroky i v logice. Zkrátka prohlásíme, že pro každého obyvatele Prahy $x$ platí

$$M(x) \wedge Z(x).$$

K formálnímu zápisu podobných tvrzení využíváme tzv. *univerzální kvantifikátor* (též *obecným*), který zapisujeme pomocí $\forall$.

Nyní se ještě zamysleme, co nám toto říká z pohledu logiky. Tvrzení je takové, že je-li $x$ obyvatelem Prahy, pak má zelené vlasy a modré oči. V řeči logických spojek toto není nic jiného, než implikace. Označíme-li výrok „$x$ je obyvatelem Prahy.“ jako $P(x)$, pak bychom mohli napsat

$$\forall x\Big(P(x) \Rightarrow Z(x) \wedge M(x)\Big), \tag{2.3}$$

nebo podle (xii) ve větě 2.1.13 o tautologiích

$$\forall x\Big(Z(x) \vee M(x) \vee \neg P(x)\Big).$$

Takový výrok bychom četli: „**pro všechna** $x$ **platí**, že pokud platí $P(x)$, pak platí $Z(x)$ a zároveň $M(x)$“. Ve výrazu (2.3) můžeme uvažovat libovolná $x$ (nemusí se ani jednat o lidi), avšak pouze u $x$, která splňují předpoklad $P(x)$ tvrdíme, že splňují i závěr $Z(x) \wedge M(x)$. Proto jsme ve výrazu nepoužili konjunkci, tj.

$$\forall x\Big(P(x) \wedge Z(x) \wedge M(x)\Big),$$

neboť bychom vzali např. obyvatele Brna, pak by byl již výrok nepravdivý (kvůli $P(x)$).

Druhým typem kvantifikátoru je tzv. *existenční kvantifikátor*. Uvažme, že bychom chtěli naopak říci, že ze všech obyvatel Prahy má alespoň jeden zelené

vlasy a modré oči. S využitím čistě logických spojek by pak znamenalo, že jedna z dílčích formulí je pravdivá

$$(Z(\text{Anička}) \wedge M(\text{Anička})) \vee (Z(\text{Eva}) \wedge M(\text{Eva})) \vee (Z(\text{Tomáš}) \wedge M(\text{Tomáš})) \vee \cdots \vee (Z(\text{Jiří}) \wedge M(\text{Jiří})$$

I zde však máme kratší alternativu, a to s využitím symbolu $\exists$ pro existenční kvantifikátor. Opět se však nejdřív podívejme na naše tvrzení. To říká, že existuje $x$ takové, že $x$ je obyvatelem Prahy a zároveň má zelené vlasy a modré oči. Zde si tedy naopak vystačíme pouze s konjunkcí:

$$\exists x \Big( P(x) \wedge Z(x) \wedge M(x) \Big). \tag{2.4}$$

Přirozeně se zde nabízí otázka, proč jen nenahradit univerzální kvantifikátor ve výrazu (2.3) za existenční. Pokud bychom napsali

$$\exists x \Big( P(x) \Rightarrow Z(x) \wedge M(x) \Big), \tag{2.5}$$

pak by tvrzení již neplatilo pouze na obyvatele Prahy (v případě nesplněného předpokladu je implikace pravdivá), ale třeba pro obyvatele Brna by toto tvrzení také byla pravda. Pokud by však v Praze neexistoval občan se zelenými vlasy a modrýma očima, pak by výraz (2.4) by nepravdivý, ale výraz (2.5) by pravdivý již byl.

### 2.2.1 Primitivní predikáty

Vzpomeneme-li si na definici výrokových formulí (viz 2.1.3), tak zde jsme formule tvořili opakovanou aplikací jistých pravidel, přičemž „nejtriviálnější“ výrokovou formulí (tj. atomickou formulí) pro nás byly **výrokové proměnné**. Těm jsme přiřazovali pravdivostní hodnotu 0 (nepravda) nebo 1 (pravda). V tomto se však nachází jisté omezení. U předešlého příkladu jsme, kromě jiných, uvažovali výrok „$x$ je obyvatelem Prahy.“, který jsme značili výrokovou proměnnou $P(x)$. Tím jsme přiřadili $P(x)$ jistý význam.

Zkusme takto zapsat matematické tvrzení „Pokud je $x$ větší než $y$ a zároveň $y$ je větší než $z$, pak $x$ je větší než $z$“. Výrok „$x$ je větší než $y$“ označme $A$, „$y$ je větší než $z$“ označme $B$ a „$x$ je větší než $z$“ označme $C$. Pak původní výrok bychom symbolicky zapsali jako

$$A \wedge B \Rightarrow C.$$

Nebylo by však jednodušší a smysluplnější zapsat takový výrok zkrátka jako $x > y \wedge y > z \Rightarrow x > z$ ? Takový zápis by odporoval definici výrokové formule, přesto jeho význam je zřejmý. Navíc bychom si tak ušetřili ono přiřazování významu jednotlivým výrokovým proměnným, jako tomu bylo doposud, neboť bychom měli možnost jejich syntaktického popisu. To nám je umožněno v *predikátovém počtu*.

Ve výrokové logice zastávaly výrokové proměnné roli těch „nejednodušších“ formulí, které již nevznikaly z formulí jiných. V predikátovém počtu tuto roli zastávají tzv. *primitivní predikáty* (nebo jen zkráceně *predikáty*). Ty obsahuje každá matematická teorie. V aritmetice jsou to právě např. $x < y$ , $x + y < z$,

apod., v teorii množin považujeme za primitivní predikát $x \in X$ (ostatně celou teorii množin lze vybudovat pouze za použití tohoto predikátu). Po dosazení konkrétních hodnot dané proměnné již obdržíme nějaký atomární výrok v dané teorii.

Výroky složené z primitivních predikátů již nenazýváme výrokové formule, ale *predikátové formule*. I ty lze definovat obdobně jako formule výrokové pomocí jistých pravidel, avšak pro pochopení konceptu si vystačíme s tímto vystačíme.

**Úmluva 2.2.1.** V dalším textu této sekce budeme slovo formule užívat ve významu predikátové formule.

**Příklad 2.2.2.** Ukázky některých predikátových formulí:

- $x > y$ ◁ *Primitivní predikát (aritmetika) je predikátovou formulí*
- $\forall x(x = 0 \vee x < 0 \vee x > 0)$
- $\forall x\Big(2 \mid x \Rightarrow \exists k(x = 2k)\Big)$[3]
- $\exists k\Big(k \in \mathbb{N} \wedge \exists x(x = 2k + 1)\Big)$

### 2.2.2 Jiné zápisy formulí s kvantifikátory

Formule s obecným kvantifikátorem $\forall$ jsme zatím uvažovali ve tvaru

$$\forall x(\varphi \Rightarrow \psi),$$

kde $\varphi$ a $\psi$ jsou nějaké predikátové formule obsahující proměnnou $x$. (Formálně vzato, formule $\varphi$ a $\psi$ nemusí v tomto zápisu obsahovat proměnnou $x$, nicméně pak je kvantifikátor redundantní.) Existuje však o něco úspornější (a častěji používaný) zápis. Např. formuli

$$\forall n(n \in \mathbb{N} \Rightarrow n > 0)$$

můžeme též zapsat jako

$$\forall n \in \mathbb{N} : n > 0.$$

Čteme jako „pro všechna přirozená čísla $n$ platí, že $n$ je větší než nula“. Obecněji formuli ve tvaru $\forall x(\varphi \Rightarrow \psi)$ lze psát jako $\forall \varphi : \psi$ . Stejně tak můžeme zapisovat i formule s existenčním kvantifikátorem, tj. $\exists \varphi : \psi$ místo $\exists x(\varphi \wedge \psi)$ .

Často se nám může stát, že se kvantifikátory ve formuli kumulují. Zápisy prováděné dosavadním způsobem by se mohly značně zkomplikovat. Jako příklad uvažme formuli

$$\forall x\Big(x \in \mathbb{N} \Rightarrow \exists k(k > n)\Big).$$

Podle zmíněného již víme, že tento zápis můžeme zjednodušit na

$$\forall x \in \mathbb{N} : \exists k : k > n.$$

[3] Zápis $a \mid b$ znamená $a$ dělí (beze zbytku) $b$

V takovém případě můžeme dvojtečku mezi obecným a existenčním kvantifikátorem vynechat a ponechat ji pouze před závěrem, nebo nahradit dvojtečku mezi kvantifikátory čárkou, tj. můžeme psát

$$\forall x \in \mathbb{N}\, \exists k : k > n \quad \text{nebo} \quad \forall x \in \mathbb{N}, \exists k : k > n.$$

Čteme: „Pro všechna přirozená čísla $n$ existuje $k$ takové, že $k$ je větší než $n$“. Speciálně, může se stát, že dvě nebo více proměnných jsou součástí stejného predikátu u stejného typu kvantifikátoru. Kupříkladu formuli

$$\forall n\Big(n \in \mathbb{N} \Rightarrow \forall k(k \in \mathbb{N} \Rightarrow n^k \geq n)\Big)$$

můžeme zjednodušit jako

$$\forall n \in \mathbb{N}, \forall k \in \mathbb{N} : n^k \geq n.$$

Proměnné $n$ a $k$ však uvažujeme ze stejné množiny a jsou součástí stejného typu kvantifikátoru (obecného). V takových případech můžeme zápis sloučit a psát

$$\forall n,k \in \mathbb{N} : n^k \geq n.$$

Je třeba však upozornit na fakt, že pořadí kvantifikátorů může mít vliv na význam daného výroku (a tudíž i jeho pravdivostní hodnotu). Např. formule

$$\forall n \in \mathbb{N}, \exists k \in \mathbb{N} : k > n \quad \text{a} \quad \exists k \in \mathbb{N}, \forall n \in \mathbb{N} : k > n.$$

neříkají totéž (zkuste si je přečíst). První říká, že **pro každé** $n$ **existuje nějaké** $k$ **takové, že** $k$ **je větší než** $n$, kdežto druhá formule má význam takový, že **existuje** $k$ **takové, že pro všechna** $n$ **je** $k$ **větší než** $n$. Jinými slovy říkáme, že existuje jedno **univerzální** číslo $k$ tak, že je splněna daná podmínka. První formule je tak pravdivá, ale druhá již není.

Tento způsob zápisu však neplatí pouze pro kvantifikátory. Mějme např. formuli

$$\forall x,y \in \mathbb{R} : x \neq y \Rightarrow x < y \vee x > y.$$

Zde též není nutné explicitně psát implikaci. Když se nám to hodí, můžeme předpoklad také uvést před dvojtečkou.

$$\forall x,y \in \mathbb{R}, x \neq y : x < y \vee x > y$$

### 2.2.3 Negace formulí s kvantifikátory

V sekci o výrokové logice 2.1 jsme si zmínili některé důležité tautologie. Specificky, de Morganova pravidla (i) a (ii) zmíněné ve větě 2.1.13.

$$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B,$$
$$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B.$$

Tyto tautologie nám dávaly způsob, jak negovat složené výroky obsahující konjunkci nebo disjunkci. Jak ovšem negovat formule s kvantifikátory?

Zkusme se na problematiku podívat opět skrze příklad o obyvatelích Prahy. Měli jsme tvrzení, že každý obyvatel Prahy má zelené vlasy a modré oči, což jsme zapisovali

$$\forall x : P(x) \Rightarrow Z(x) \wedge M(x).$$

Pro začátek si vezměme jednodušší variantu bez konjunkce:

$$\forall x : P(x) \Rightarrow M(x).$$

Tedy uvažovaný výrok je „Každý obyvatel Prahy má zelené vlasy.“. Jak by zněla negace takového výroku? Zamysleme se nad tím, v jakém případě by výrok neplatil. Pokud by v Praze byl obyvatel, který nemá modré oči, pak naše tvrzení neplatí. Zdá se tedy, že by mohlo platit

$$\neg(\forall x : P(x) \Rightarrow M(x)) \Leftrightarrow \exists x : P(x) \wedge \neg M(x).$$

Tj. tvrdíme, že existuje $x$ takové, že $x$ je obyvatelem Prahy a $x$ nemá modré oči. Jak se tedy změnila naše formule? Obecný kvantifikátor se změnil na existenční a znegovali jsme formuli $P(x) \Rightarrow M(x)$ (viz tautologie (xii) ve větě 2.1.13). Skutečně, toto je negace původního výroku.

Podobně tomu bude i pro náš původní výrok s konjunkcí:

$$\neg(\forall x : P(x) \Rightarrow Z(x) \wedge M(x)) \Leftrightarrow \exists x : \neg(P(x) \Rightarrow Z(x) \wedge M(x)).$$

Tj. existuje $x$ takové, že $x$ je obyvatelem Prahy a platí, že nemá zelené vlasy nebo nemá modré oči. Opět užitím tautologie (xii) a následně de Morganova pravidla pro negaci konjunkce (i) ve větě 2.1.13 můžeme formuli upravit na

$$\exists x : P(x) \wedge (\neg Z(x) \vee \neg M(x)).$$

Funguje i opačná úvaha. Pokud naše tvrzení je, že existuje obyvatel Prahy se zelenými vlasy a modrými oči, pak negace naopak říká, že všichni obyvatelé Prahy nemají zelené vlasy nebo nemají modré oči. Tzn.

$$\neg(\exists x : P(x) \wedge Z(x) \wedge M(x)) \Leftrightarrow \forall x : P(x) \Rightarrow \neg Z(x) \vee \neg M(x).$$

Obecně řečeno, formule s kvantifikátory se negují tak, že kvantifikátory si prohodí roli, tj. obecný kvantifikátor se změní na existenční a naopak, a znegujeme dílčí formuli $\varphi$, tzn.

$$\begin{array}{lcll} \forall x : \varphi & \rightsquigarrow & \exists x : \neg\varphi & \text{a} \\ \exists x : \varphi & \rightsquigarrow & \forall x : \neg\varphi & \end{array}$$

Kvantifikátory se mohou pochopitelně ve formulích různě kumulovat. V takovou chvíli postupujeme pořád stejně. Např. negace formule

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : y > x.$$

bude

$$\exists x \in \mathbb{R}, \forall y \in \mathbb{R} : y \leq x.$$

(TODO: doplnit cvičení.)

# Kapitola 3

# Axiomy teorie množin

Jak jsme si již zmínili v historickém úvodu tohoto textu, teorie množin se po objevu různých paradoxů (viz Russellův paradox a jiné v 1.2.2) v Cantorově zavedení začala později budovat axiomaticky. K tomu jsme měli možnost nahlédnout v sekci 1.2.3. Jednou z variant axiomatické teorie množin je tzv. **Zermelova-Fraenkelova teorie množin**, která je literatuře pravděpodobně tou nejrozšířenější; označujeme ji zkratkou *ZF*[1]. Proto se právě jí budeme v této sekci věnovat. V dalších odstavcích se postupně zaměříme na jednotlivé axiomy ZF a ukážeme si, jak z nich vyplývají definice dalších pojmů (i některých nám již známých).

Nutno dodat, že ZF má více variant a tak v různých textech se může „soubor" axiomů, s nimiž se pracuje, jemně lišit. Odlišné přístupy v této axiomatické teorii lze krásně vidět např. v knihách [4] a [5]. Lze však ukázat, že tyto varianty jsou si ekvivalentní. (Zmíníme se ještě později.)

Pro začátek si zde přehledně vypišme všechny axiomy ZF, s nimiž budeme pracovat, a v dalších sekcích si je detailněji popíšeme.

**Axiomy Zermelovy-Fraenkelovy teorie množin**:

(ZF1) *Axiom extenzionality.*

$$\forall x\, \forall y \left( x = y \Leftrightarrow \forall z \, (z \in x \Leftrightarrow z \in y) \right)$$

(ZF2) *Axiom existence.*

$$\exists x : x = x$$

(ZF3) *Axiom dvojice.*

$$\forall a\, \forall b\, \exists y\, \forall x \, (x \in y \Leftrightarrow x = a \vee x = b)$$

(ZF4) *Schéma axiomů vydělení.*

$$\forall a\, \exists y\, \forall x \, (x \in y \Leftrightarrow x \in a \wedge \varphi(x)),$$

kde $\varphi(x)$ je formule neobsahující proměnnou $y$.

(ZF5) *Axiom potence.*

$$\forall a\, \exists y\, \forall x \left( x \in y \Leftrightarrow x \subseteq a \right)$$

[1] Obdobně Gödelova-Bernaysova teorie množin je označována *GB*.

(ZF6) *Axiom sumy.*

$$\forall a\, \exists z\, \forall x \left( x \in z \Leftrightarrow \exists y \, (x \in y \wedge y \in a) \right)$$

(ZF7) *Axiom nekonečna.*

$$\exists y \, (\emptyset \in y \wedge \forall x \, (x \in y \Rightarrow x \cup \{x\} \in y)$$

(ZF8) *Schéma axiomů nahrazení.*

$$\forall u\, \forall v\, \forall v' \, (\varphi(u,v) \wedge \varphi(u,v') \Rightarrow v = v') \Rightarrow$$
$$\Rightarrow \forall a\, \exists z\, \forall x \left( x \in z \Leftrightarrow \exists y \, (y \in a \wedge \varphi(y,x)) \right),$$

kde formule $\varphi(u,v)$ neobsahuje proměnné $v'$ a $z$.

(ZF9) *Axiom fundovanosti.*

$$\forall a \left( a \neq \emptyset \Rightarrow \exists x : \left( x \in a \wedge x \cap a = \emptyset \right) \right)$$

Mohlo by se zdát zarážející, že ve formulaci axiomů (ZF5), (ZF7) a (ZF9) jsme využili symboly $\emptyset$ a $\subseteq$, které jsme zatím formálně nedefinovali. Učinili jsme tak z didaktického hlediska, aby byly dané axiomy jasnější. Nicméně čtenář si bude moci později rozmyslet, že tyto symboly lze definovat pomocí predikátu $x \in y$ jako zbytek axiomů.

Je dobré zmínit, že ve skutečnosti nám na seznamu výše jeden axiom chybí – *axiom výběru*. Ten byl skutečně součástí původní Zermelovy axiomatiky z roku 1908 a v teorii množin měl dosti netriviální důsledky[2]. Dnes jej však nepočítáme základní axiomy teorie množin. Pokud se tedy mluví o **Zermelově-Fraenkelově teorii množin**, pracujeme se soustavou axiomů popsaných výše (tu značíme právě ZF). Naopak v případě varianty s axiomem výběru označujme *ZFC*[3].

## 3.1 Axiomy 1 až 3

Než začneme s dalším vysvětlováním, je nutné mít na paměti, že **množiny** jsou pro nás základními objekty, tzn. prvky množin mohou být opět pouze množiny a žádné jiné nepřipouštíme. V dalších částech toho textu uvidíme, že si s tím skutečně vystačíme.

### 3.1.1 Axiom existence

$$\exists x : x = x$$

Formulace axiomu (ZF2) se může jevit na první pohled zvláštní, ale jednoduše nám zaručuje, že nějaká **množina existuje**. Tento axiom se též někdy nahrazuje *axiomem prázdné množiny*. Později si však ukážeme, že axiom existence a axiom prázdné množiny jsou spolu ekvivalentní (tedy z platnosti jednoho plyne druhý a naopak).

[2] Asi nejznámějším příkladem je tzv. *Banachův-Tarského paradox*. Jeho formální vysvětlení je však zcela na rámec tohoto textu.

[3] Písmeno C vychází z anglického názvu axiomu výběru – *Axiom of choice*

### 3.1.2 Axiom extenzionality

$$\forall x\, \forall y \left( x = y \Leftrightarrow \forall z \, (z \in x \Leftrightarrow z \in y) \right)$$

(ZF1) dává do souvislosti predikáty rovnosti a náležení: množiny jsou si rovny, když obsahují stejné prvky. Z tohoto axiomu vyplývá, že opakované výskyty prvku v množině jsou pro nás irelevantní, tj. např.

$$\{a,b,c,c\} = \{a,b,c\} \text{ apod.}$$

### 3.1.3 Axiom dvojice

$$\forall a\, \forall b\, \exists y\, \forall x \, (x \in y \Leftrightarrow x = a \wedge x = b)$$

Existence množiny garantovaná axiomem existence (ZF2) nám bohužel nezaručuje existenci žádné konkrétní množiny. Axiom dvojice nám zaručuje, že pokud máme dvě (ne nutně různé) množiny $x$ a $y$, pak i $\{x,y\}$ je množina (resp. že existuje množina obsahující prvky $a$ a $b$). Např. když máme množiny

$$\{a,b\} \text{ a } \{c\} \text{ pak existuje množina } \{\{a,b\}, \{c\}\}.$$

Není těžké se přesvědčit, že taková množina je vždy unikátní. V následujícím tvrzení si představíme variantu existenčního kvantifikátoru se symbolem „!“, tj. $\exists!$. Jeho význam je „**existuje právě jeden/jedno**“.

**Lemma 3.1.1.** *Pro každou množin $a$ a pro každou množinu $b$ existuje jediná množina $y$, jejíž prvky jsou právě $a$ a $b$. Symbolicky*

$$\forall a\, \forall b\, \exists! y\, \forall x \, (x \in y \Leftrightarrow x = a \wedge x = b).$$

*Důkaz.* K důkazu lze přistoupit např. sporem. Pro spor nechť jsou dány dvě různé množiny $y$ a $y'$, pro které platí

$$\forall x \, (x \in y \Leftrightarrow x = a \vee x = b) \qquad \text{a} \qquad \forall x \, (x \in y' \Leftrightarrow x = a \vee x = b).$$

Pak tedy platí

$$\forall x \, (x \in y \Leftrightarrow x \in y')$$

a z axiomu extenzionality (ZF1) vyplývá $y = y'$, což je spor s předpokladem, že $y$ a $y'$ jsou různé množiny.

□

Množiny $a$,$b$ nemusí být však nutně různé. Pokud budeme mít množinu $x$, pak z axiomu dvojice existuje množina $\{x,x\}$. Ta je však podle axiomu extenzionality rovna množině $\{x\}$, která podle výše dokázaného je jediná (stačí uvážit $a = x$ a $b = x$).

**Definice 3.1.2** (Neuspořádaná dvojice)**.** Nechť $x$ a $y$ jsou množiny. Pak množinu $\{x,y\}$ nazýváme *(neuspořádanou) dvojicí.*

Tato definice nejspíše není moc zajímavá, neboť zavedený termín je již v názvu axiomu. Avšak ono přídavné jméno „**neuspořádaná**“ nás může přivádět k otázce, jak reprezentovat *uspořádanou dvojici*. Čtenáři je tento termín nejspíše již známý v jiných podobách; typicky např. **vektory** využívané v analytické geometrii. Ty jsme typicky značili $(x,y)$. Nejdůležitější vlastností tohoto objektu pro nás byl fakt, že $(x,y) \neq (y,x)$ a tedy záleželo na pořadí prvků. Jak toto vyjádřit pomocí množin? Je nejspíše jasné, že reprezentace pomocí množiny $\{x,y\}$ již nebude dostačující, protože podle axiomu extenzionality (ZF1) je $\{x,y\} = \{y,x\}$ (proto název *neuspořádaná dvojice*). Naše požadavky pro objekt uspořádané dvojice tedy jsou:

1. pro každou množinu $x$ a pro každou množinu $y$ existuje jediná uspořádaná dvojice $(x,y)$,
2. uspořádané dvojice $(x,y)$ a $(a,b)$ se rovnají právě tehdy, když $x = a$ a $y = b$.

Již víme, že neuspořádané dvojice nám v tomto směru nepostačí. Potřebovali bychom umět nějak rozlišit, která souřadnice je „první“ a která „druhá“. Tento problém poměrně elegantně řeší definice, se kterou přišel polský matematik a logik Kazimierz Kuratowski (1896–1980).

**Definice 3.1.3** (Uspořádaná dvojice)**.** Nechť $x$ a $y$ jsou množiny. Pak definujeme *uspořádanou dvojici* $(x,y)$ jako

$$\{\{x\}, \{x,y\}\}.$$

Po chvilce zamyšlení nad touto definicí si můžeme uvědomit, že název „uspořádaná dvojice“ je zcela oprávněný. Množina $\{x\}$ nám v podstatě říká, která z množin $x,y$ je na „prvním místě“. Přesvědčme se, že takto definovaná uspořádaná dvojice má skutečně požadované vlastnosti.

Začneme jednodušším požadavkem a to sice, aby pro libovolné množiny $x,y$ existovala právě jedna uspořádaná dvojice $(x,y)$.

**Lemma 3.1.4.** *Jsou-li $x,y$ libovolné množiny, pak existuje právě jediná uspořádaná dvojice $(x,y)$.*

*Důkaz.* V důkazu tohoto tvrzení se můžeme přímo odvolat na fakt, který jsme dokázali dříve v lemmatu 3.1.1. Podle něj pro libovolné množiny $x,y$ existuje právě jediná neuspořádaná dvojice $\{x,y\}$. K důkazu můžeme opět přistoupit sporem.

Pro spor nechť existují dvě různé uspořádané dvojice $t$ a $t'$. Z výše uvedené definice 3.1.3 musí platit

$$\forall x' \, (x' \in t \Leftrightarrow x' = \{x\} \vee x' = \{x,y\}) \quad \text{a} \quad \forall x' \, (x' \in t' \Leftrightarrow x' = \{x\} \vee x' = \{x,y\}).$$

Podle lemmatu 3.1.1 existují právě jedny neuspořádané dvojice $\{x,y\}$ a $\{x\}$[4]. Z toho dostáváme, že $t$ a $t'$ mají stejné prvky a podle axiomu extenzionality (ZF1) platí $t = t'$, což je spor s předpokladem, že $t$ a $t'$ jsou různé množiny.

□

[4]Množina obsahující pouze jeden prvek je také neuspořádanou dvojicí. Podle axiomu extenzionality je rovna množině $\{x,x\}$.

**Lemma 3.1.5.** *Pro libovolné množiny $x$,$y$ platí:*

$$(a,b) = (x,y) \Rightarrow a = x \wedge b = y.$$

Před uvedením důkazu si ještě zavedeme úmluvu pro zjednodušení zápisu.

**Úmluva 3.1.6.** Zápisem $x_1 = x_2 = \cdots = x_n$ budeme rozumět formuli tvaru $x_1 = x_2 \wedge x_2 = x_3 \wedge \cdots \wedge x_{n-1} = x_n$.

*Důkaz.* Tvrzení dokážeme opakovanou aplikací axiomu extenzionality (ZF1). Mějme uspořádané dvojice $(a,b)$ a $(x,y)$ takové, že $(a,b) = (x,y)$, tj. podle definice 3.1.3

$$\{\{a\},\{a,b\}\} = \{\{x\},\{x,y\}\}.$$

Podle (ZF1) musí mít množin na pravé a levé straně stejné prvky. Rozdělme si tento důkaz na dva případy.

(a) $\{a\} = \{x\}$. Pak opět podle (ZF1) platí $a = x$. Rozlišme dále případy, když $a = b$ a když $a \neq b$.

- $a = b$. Pak

  $$\{\{a\},\{a,b\}\} = \{\{a\},\{a,a\}\} \overset{(ZF1)}{=} \{\{a\},\{a\}\} \overset{(ZF1)}{=} \{\{a\}\}.$$

  Musí tedy platit $\{\{a\}\} = \{\{x\},\{x,y\}\}$. Opět z (ZF1) vyplývá $\{x,y\} = \{a\}$, tj. $x = a$ a $y = a$. Celkově dostáváme $a = b = x = y$ a tedy i $a = x$ a $b = y$, jak jsme chtěli.
- $a \neq b$. V takovém případě nemůže platit, že $\{a,b\} = \{a\}$ (zkuste si rozmyslet podle (ZF1)), tj. nutně musí $\{a,b\} = \{x,y\}$. Protože však $a = x$, pak $b = y$.

  Celkově tak v obou případech dostáváme, že pokud $\{a\} = \{x\}$, pak $x = a$ a $y = b$.

(b) $\{a\} = \{x,y\}$. Podle (ZF1) pak platí $x = a$ a $y = a$, tedy $x = y$. Stejným postupem tak dostáváme

$$\{\{x\},\{x,y\}\} = \{\{x\},\{x,x\}\} \overset{(ZF1)}{=} \{\{x\},\{x\}\} \overset{(ZF1)}{=} \{\{x\}\}.$$

Tedy $\{\{a\},\{a,b\}\} = \{\{x\}\}$. Protože prvky množiny na levé straně musí být prvky množiny na pravé straně, pak $\{a\} = \{a,b\} = \{x\}$. Z toho opět dostáváme, že $a = b = x = y$, tj. $a = x$ a $b = y$.

V obou dílčích případech jsme dostali, že $a = x$ a $b = y$, což jsme chtěli dokázat. □

## 3.2 Axiomy 4 až 6

První trojice axiomů se zdá být dobrým základem, avšak stále je stále hodně typů množin, jejichž existence z nich neplyne. Trochu „podvodným“ způsobem jeden takový typ použili (a pokud čtenář odpustí, budeme i nadále používat pro lepší názornost) v diskuzi axiomu extenzionality, konkrétně množinu $\{a,b,c\}$. Při zamyšlení zjistíme, že čistě z axiomů (ZF1), (ZF2) a (ZF3) nelze takovou množinu „sestrojit“. Pomocí axiomu dvojice plyne pro množiny $a,b,c$ existence množin

$$\{a,b\} \text{ a tudíž i } \{\{a,b\},c\},$$

což jak víme, není to samé co $\{a,b,c\}$. Její existenci a existenci mnoha dalších množin nám zaručí (společně se (ZF1), (ZF2) a (ZF3)) axiomy (ZF4), (ZF5) a (ZF6).

### 3.2.1 Schéma axiomů vydělení

$$\forall a\, \exists y\, \forall x\, (x \in y \Leftrightarrow x \in a \wedge \varphi(x)), \tag{3.1}$$

kde $\varphi(x)$ je formule neobsahující proměnnou $y$.
Často potřebujeme z určité množiny prvků vybrat množinu prvků takových, že všechny sdílejí jistou vlastnost. Např.

- všechna sudá čísla z množiny $\mathbb{Z}$,
- všechna nezáporná čísla z množiny $\mathbb{R}$,
- všechna prvočísla z množiny $\mathbb{N}$, apod.

Schéma axiomů vydělení[5] nám obecně říká, že pro každou množinu $a$ existuje množina $y$ taková, že každý její prvek $x$ je zároveň prvek $a$ splňuje určitou formuli $\varphi(x)$ (ta reprezentuje danou vlastnost). Podle axiomu extenzionality (ZF1) je množina v (3.1) jednoznačně určena. Čtenář je nejspíše zvyklý množiny, jejichž prvky sdílejí určitou vlastnost, zapisovat např. jako

$$\{x \in \mathbb{R} \mid x \geq 0\}.$$

Obecněji množinu z (3.1) zapisujeme výrazem

$$\{x \mid x \in a \wedge \varphi(x)\} \text{ nebo též } \{x \in a \mid \varphi(x)\}.$$

Pokud se nyní vrátíme k množinám, se kterými jsme doteď pracovali, můžeme pro množiny $a$ a $b$ definovat množinu

$$\{x \in a \mid x \notin b\},$$

kde formule $\varphi(x)$ je $x \notin b$. Toto schéma axiomů má následující důsledek.

[5] Slovo „schéma“ přidáváme z důvodu, že pro každou volbu formule $\varphi$ dostáváme jeden konkrétní axiom teorie – axiom vydělení. Tedy schéma axiomů vydělení představuje nekonečně mnoho různých axiomů, které vzniknou tím, že $\varphi$ proběhne všechny možné formule s proměnnou $x$.

**Důsledek 3.2.1.** *Existuje množina, která nemá žádné prvky.*

*Důkaz.* Důkaz je jednoduchý. Máme-li libovolnou množinu $a$, pak podle schématu axiomů vydělení lze sestrojit množinu, která nemá žádné prvky. Toho docílíme volbou formule $\varphi(x)$ jako $x \neq x$, tzn.

$$\{x \in a \mid x \neq x\}$$

je také množina.

□

Takovou množinu pak nazýváme *prázdná množina* a typicky ji označujeme znakem $\emptyset$ nebo též někdy prázdnými složenými závorkami $\{\}$. Toto tvrzení se v jiných variantách ZF považuje za axiom a nahrazuje axiom existence. Všimněte si, že důkaz výše (a prakticky důkazy všech zatím zformulovaných tvrzení) závisely (mimo jiné) právě na axiomu existence. Jinak bychom množinu $a$ vůbec nemohli uvažovat. Naopak pokud bychom přijali existenci prázdné množiny jako axiom, pak to automaticky implikuje existenci množiny obecně, kterou nám zaručuje axiom existence.

Pomocí schématu axiomů vydělení můžeme definovat některé základní operace s množinami.

**Definice 3.2.2** (Průnik a rozdíl množin)**.** Nechť jsou dány libovolné množiny $a$ a $b$, pak

(i) *průnikem* množin $a$ a $b$ rozumíme množinu $a \cap b$, kterou definujeme

$$a \cap b = \{x \mid x \in a \wedge x \in b\}.$$

(ii) *rozdílem* množin $a$ a $b$ rozumíme množinu $a \setminus b$, kterou definujeme

$$a \setminus b = \{x \mid x \in a \wedge x \notin b\}.$$

**Příklad 3.2.3.** Ukázky průniku a rozdílu množin:

(i) $\{a,b,c\} \cap \{a,c,d\} = \{a,c\}$,

(ii) $\{a,b,c\} \cap \emptyset = \emptyset$,

(iii) $\{x,y,z\} \setminus \{y\} = \{x,z\}$,

(iv) $\{y,z\} \setminus \emptyset = \emptyset$.

**Poznámka 3.2.4.** Speciálně, pokud pro množiny $a$,$b$ platí, že $a \cap b = \emptyset$ (tzn. $a$ a $b$ nemají žádný společný prvek), pak říkáme, že jsou *disjunktní*.

Proč rovnou nedefinovat i *sjednocení* množin? Protože schéma axiomů vydělení (ZF4) garantuje existenci pouze takové množiny $y$, že všechny její prvky náleží množině $a$. To však při sjednocení množin neplatí, neboť některé prvky množiny $b$ nemusí být prvky množiny $a$. S touto vlastností všech množin, jejichž existenci máme díky schématu axiomů vydělení se pojí ještě jeden termín.

**Definice 3.2.5** (Podmnožina a vlastní podmnožina)**.** Nechť $a$ je libovolná množina. Pak $b$ nazveme *podmnožinou* množiny $a$, pokud

$$\forall x\,(x \in b \Rightarrow x \in a).$$

Pokud navíc platí, že $a \neq b$, pak $b$ nazýváme *vlastní podmnožinou.*

**Příklad 3.2.6.** Ukázky vztahů množin mezi sebou:

(i) $x_1 = \{a,b\}$ , $x_2 = \{a,b,c\}$, pak platí $x_1 \subset x_2$ a tj. i $x_1 \subseteq x_2$, ale nikoliv $x_2 \subseteq x_1$ ;

(ii) $y_1 = \{a,b,c\}$ , $y_2 = \{a,b,c\}$, pak platí $y_1 \subseteq y_2$ a i $y_2 \subseteq y_1$, ale nikoliv $y_1 \subset y_2$ nebo $y_2 \subset y_1$ ;

(iii) $z_1 = \emptyset$, $z_2 = \{k\}$, pak platí $z_1 \subset z_2$ a tudíž i $z_1 \subseteq z_2$.

Poslední ze zmíněných příkladů je celkem pozoruhodný, neboť s ním souvisí následující lemma.

**Lemma 3.2.7.** *Platí:*

*(i)* $\forall x : \emptyset \subseteq x$,

*(ii)* $\forall x : x \subseteq \emptyset \Leftrightarrow x = \emptyset$.

Zde se dostáváme k poměrně zajímavé části logiky. Pokud bychom si rozepsali definici podmnožiny (viz 3.2.5), formule by vypadala takto:

$$\forall x\,(x \in \emptyset \Rightarrow x \in a) \text{ nebo ekvivalentně } \forall x \in \emptyset :\Rightarrow x \in a. \tag{3.2}$$

Problém je však, že prázdná množina žádné prvky nemá. Jak tedy rozhodnout o pravdivosti (3.2)? Ve skutečnosti,jakékoliv tvrzení obsahující obecný kvantifikátor, kde množina, z níž $x$ uvažujeme, je prázdná, implicitně považujeme za pravdivé. Tzn. výrok

$$\forall x \in \emptyset : \varphi,$$

kde $\varphi$ je libovolná formule, považujeme vždy za pravdivý[6].

*Důkaz. (i).* Z výše uvedeného je tato část tvrzení implicitně pravdivá.
*(ii).* ($\Rightarrow$). Pokud pro libovolné $x$ platí $x \subseteq \emptyset$, pak z definice

$$\forall y\,(y \in x \Rightarrow y \in \emptyset)$$

je vidět, že tvrzení platí pouze pro $x = \emptyset$ (pro neprázdnou množinu $x$ by libovolný její prvek nikdy neležel v $\emptyset$).

($\Leftarrow$). Plyne přímo z (i). Prázdná množina je podmnožinou každé množiny, tedy i sebe sama.

□

[6]Analogicky výroky s existenčním kvantifikátorem, kde $x$ uvažujeme z prázdné množiny, pokládáme vždy za nepravdivé.

### 3.2.2 Axiom potence

$$\forall a\, \exists y\, \forall x \left( x \in y \Leftrightarrow x \subseteq a \right)$$

Pro každou množinu $a$ existuje množina $y$ taková, že obsahuje **právě** všechny její podmnožiny. Z axiomu extenzionality navíc opět platí, že taková množina je vždy jediná. Na základě tohoto axiomu můžeme definovat:

**Definice 3.2.8** (Potenční množina)**.** Nechť $a$ je libovolná množina. Pak *potenční množinu* (též *potenci*) $\mathcal{P}(a)$[7] množiny $a$ definujeme

$$\mathcal{P}(a) = \{x \mid x \subseteq a\}.$$

**Příklad 3.2.9.** Příklady potenčních množin:

(i) $\mathcal{P}(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$,

(ii) $\mathcal{P}(\{x,y,z\}) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x,y\}, \{x,z\}, \{y,z\}, \{x,y,z\}\}$,

(iii) $\mathcal{P}(\emptyset) = \{\emptyset\}$ (potence má jeden prvek).

### 3.2.3 Axiom sumy

$$\forall a\, \exists z\, \forall x \left( x \in z \Leftrightarrow \exists y\, (x \in y \wedge y \in a) \right)$$

Ke každé množině $a$ existuje (podle axiomu extenzionality jediná) množina $y$ obsahující **právě** takové prvky, které jsou prvkem některého z prvků (tj. množin) množiny $a$. Obdobně jako potenční množinu můžeme i tento typ množiny definovat.

**Definice 3.2.10** (Suma množiny)**.** Nechť $a$ je libovolná množina. *Sumou množiny* $a$ rozumíme množinu $\bigcup a$ definovanou

$$\bigcup a = \{x \mid \exists y\, (x \in y \wedge y \in a)\}.$$

**Příklad 3.2.11.** Ukázky sum množin:

(i) $\bigcup \{\{a,b\}, \{c\}\} = \{a,b,c\}$,

(ii) $\bigcup \{\{x\}\} = \{x\}$.

Jak lze vidět vidět z příkladu (i), který jsme si ukázali v úvodu této sekce, axiom sumy nám dovoluje opět pracovat s větším spektrem množin, kde můžeme uvažovat množiny libovolné (konečné) velikosti. Trochu precizněji, společně s axiomem dvojice (ZF3) a axiomem extenzionality (ZF1) víme, že pro množiny $a$ a $b$ existuje jediná dvojice $\{a,b\}$ a pro množinu $c$ existuje dvojice $\{c,c\} \overset{(\mathrm{ZF1})}{=} \{c\}$. Opět podle axiomu dvojice pak je i množinou

$$\{\{a,b\}, \{c\}\}$$

[7] V jiných textech se lze též setkat se značením $2^a$.

a nakonec podle axiomu sumy (ZF6) je množina i

$$\{a,b,c\}\,.$$

Díky axiomu sumy můžeme repertoár základních množinových operací rozšířit o sjednocení.

**Definice 3.2.12** (Sjednocení množin)**.** Nechť $a$,$b$ jsou libovolné množiny. *Sjednocením množin* $a$ a $b$ rozumíme množinu $a \cup b$ definovanou

$$a \cup b = \{x \mid x \in a \vee x \in b\}\,.$$

Zde si můžeme všimnout souvislosti se sumou množiny, neboť sjednocení množin $a$,$b$ lze zapsat i takto:

$$a \cup b = \bigcup \{a,b\}\,.$$

(Zkuste si rozmyslet z definice.) Z toho je také vidět, že definice sjednocení množin je zcela oprávněná, neboť je v souladu s axiomem sumy.

**Příklad 3.2.13.** Ukázky sjednocení:

(i) $\{a,b,c\} \cup \{c,d\} = \{a,b,c,d\}$,

(ii) $\{x,y\} \cup \emptyset = \{x,y\}$

Nyní se ještě chvíli budeme držet zavedených operací **sjednocení, průniku a rozdílu**. Máme-li množiny $X_1, \ldots, X_n$, pak jejich sjednocení můžeme zapsat jako

$$\bigcup_{i=1}^{n} X_i = X_1 \cup X_2 \cup \cdots \cup X_n$$

a průnik jako

$$\bigcap_{i=1}^{n} X_i = X_1 \cap X_2 \cap \cdots \cap X_n.$$

Ačkoliv jsme si společně ukázali, že sjednocení $\bigcup_{i=1}^{n}$ lze ekvivalentně zapsat pomocí sumy $\bigcup$, přesto se nejedná o stejné operace a je důležité vnímat rozdíl v jejich značení.

Celkově o sjednocení, průniku a rozdílu dvou množin můžeme dokázat řadu tvrzení. Pro operace sjednocení a průniku platí jak *komutativní*, tak i *asociativní zákon*:

$$\begin{aligned} X \cup Y &= Y \cup X, \\ X \cap Y &= Y \cap X, \\ (X \cup Y) \cup Z &= X \cup (Y \cup Z), \\ (X \cap Y) \cap Z &= X \cap (Y \cap Z). \end{aligned}$$

Navíc sjednocení a průnik jsou vzájemně vůči sobě *distributivní*:

$$\begin{aligned} X \cup (Y \cap Z) &= (X \cup Y) \cap (X \cup Z), \\ X \cap (Y \cup Z) &= (X \cap Y) \cup (X \cap Z). \end{aligned}$$

Tento poznatek můžeme zobecnit užitím velkých operátorů $\bigcup$, $\bigcap$ jako

$$A \cup \left( \bigcap_{i=1}^{n} X_i \right) = \bigcap_{i=1}^{n} (A \cup X_i),$$
$$A \cap \left( \bigcup_{i=1}^{n} X_i \right) = \bigcup_{i=1}^{n} (A \cap X_i).$$

Ještě jedny známé vztahy pro množiny jsou tzv. *de Morganovy vzorce*, které si zde zformulujeme jako větu.

**Věta 3.2.14** (de Morganovy vzorce)**.** *Nechť $A$,$X_1, \ldots, X_n$ jsou libovolné množiny. Pak platí*

*(i)* $A \setminus \left( \bigcup_{i=1}^{n} X_i \right) = \bigcap_{i=1}^{n} (A \setminus X_i),$

*(ii)* $A \setminus \left( \bigcap_{i=1}^{n} X_i \right) = \bigcup_{i=1}^{n} (A \setminus X_i).$

*Důkaz.* Nejdříve se zamysleme, co vlastně říkají dané rovnosti. Vyjadřují, že množiny a pravé a levé straně jsou si rovny. Z axiomu extenzionality (ZF1) víme, že to platí právě tehdy, když mají dané množiny stejné prvky.

Ukážeme pouze platnost (i), avšak důkaz (ii) je zcela analogický. Budiž dán libovolný prvek $x \in A \setminus (\bigcup_{i=1}^{n} X_i)$. Ukážeme, že $x \in \bigcap_{i=1}^{n} (A \setminus X_i)$. Z definice rozdílu množin (viz 3.2.2) tedy musí platit

$$x \in A \setminus \left( \bigcup_{i=1}^{n} X_i \right) \Leftrightarrow x \in A \wedge x \notin \bigcup_{i=1}^{n} X_i.$$

Protože však $x$ nenáleží sjednocení množin $X_1, \ldots, X_n$, pak nenáleží (podle definice 3.2.12) žádné z nich:

$$x \in \bigcup_{i=1}^{n} X_i \Leftrightarrow \forall i \in \{1, \ldots, n\} : x \notin X_i.$$

Tedy víme, že platí:

$$x \in A \wedge \forall i \in \{1, \ldots, n\} : x \notin X_i.$$

Pokud prvek $x$ náleží množině $A$ a zároveň nenáleží žádné z množin $X_1, \ldots, X_n$, pak nenáleží ani množině $A \setminus X_i$ pro libovolné $i$, kde $1 \leq i \leq n$. Tj.

$$x \in A \wedge (\forall i \in \{1, \ldots, n\} : x \notin X_i) \Leftrightarrow \forall i \in \{1, \ldots, n\} : x \in A \setminus X_i.$$

Z tohoto faktu již lze vidět, že $x$ nutně leží v průniku těchto množin, tzn.

$$x \in \bigcap_{i=1}^{n} (A \setminus X_i),$$

což jsme chtěli dokázat.

□

## 3.3 Axiom nekonečna

Už jsme zde ukázkově zmínili nám asi jedny z nejznámějších množin jako jsou přirozená čísla $\mathbb{N}$ nebo reálná čísla $\mathbb{R}$. Ačkoliv je šestice již zmíněných axiomů poměrně silná a umožňuje nám pracovat velkou škálou množin, přesto by bylo stále ambiciózní tvrdit např. o přirozených, racionálních či reálných číslech jako o množinách. Axiom dvojice nebo axiomy sumy nám zatím dávají možnost mluvit pouze o konečných množinách, byť libovolně velkých. Mohli bychom ještě udat jako důvod, že množiny jsou pro nás jediným přípustným objektem (jak jsme zmiňovali na začátku kapitoly) a prvky množin musí být opět množiny. Jak ale později uvidíme (viz (TODO: doplnit odkaz.)), číselné obory jsou také množinami v ZF. Podívejme se na axiom nekonečna (ZF7).

$$\exists y\,(\emptyset \in y \wedge \forall x\,(x \in y \Rightarrow x \cup \{x\} \in y)$$

Existuje množina $y$, kde pro každý její prvek $x$ platí, že je prvkem i $x \cup \{x\}$. Zkráceně tento axiom postuluje existenci **aktuálně** nekonečné množiny.

Zde opět narážíme na problematiku, kterou jsme diskutovali v historické části, a to sice **potenciální** vs **aktuální** nekonečno. Axiomy dvojice a sumy nám zaručovaly existenci **potenciálně** nekonečných množin, zatímco axiom nekonečna nám zaručuje existenci **aktuálně** nekonečné množiny (bez udání způsobu, jak takovou sestavit z již existujících množin).

## 3.4 Relace

Axiom nekonečna opět posiluje „souhrn“ množin, se kterými můžeme pracovat, avšak stále nemůžeme hovořit o všech. K pochopení **schématu axiomu nahrazení**, budeme potřebovat zavést nový termín, s nímž budeme nejen v tomto kontextu dále pracovat.

Množiny nám dávají možnost definovat řadu rozličných matematických pojmů. Jedním z nich je tzv. *relace*. Jak čtenář později zjistí, tento termín nám ve skutečnosti není tak vzdálený a setkáváme se s ním v matematice neustále. Před jeho zavedením však budeme potřebovat ještě jiné pojmy.

### 3.4.1 Kartézský součin

**Definice 3.4.1** (Kartézský součin množin)**.** Nechť $a$,$b$ jsou libovolné množiny. Pak *kartézský součin* $a$ a $b$ značíme $a \times b$ a definujeme jej jako

$$A \times B = \{(x,y) \mid x \in A \wedge y \in B\}\,.$$

Slovně řečeno, kartézský součin $A \times B$ je množina všech uspořádaných dvojic $(x,y)$, kde $x \in A$ a $y \in B$. Takový objekt je podle axiomu dvojice (ZF3) a axiomu sumy (ZF6) množinou v ZF.

**Příklad 3.4.2.** Mějme množiny $A = \{x,y,z\}$ a $B = \{1,2,3,4\}$. Vypočítejte kartézský součin $A \times B$.

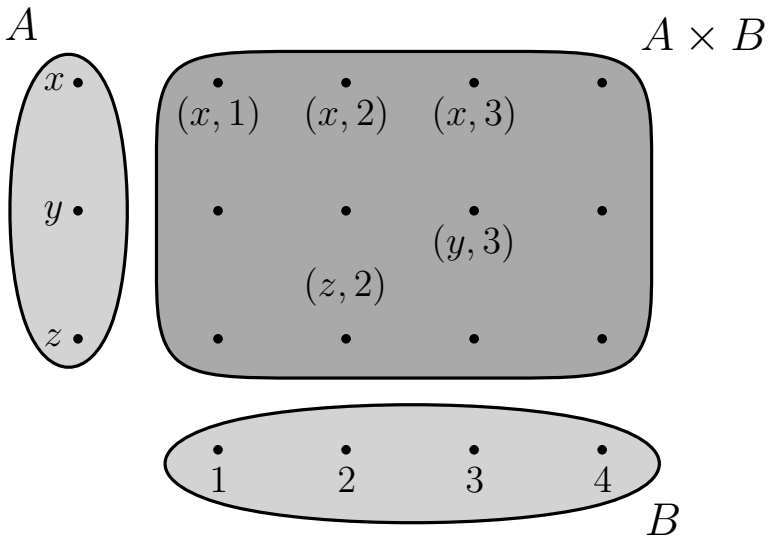
*Řešení.* Stačí postupovat podle definice, tj.

$A \times B = \{(x,1),(x,2),(x,3),(x,4),(y,1),(y,2),(y,3),(y,4),(z,1),(z,2),(z,3),(z,4)\}$. ▌

Kartézský součin množin $A, B$ lze interpretovat i graficky (viz obrázek 3.1).

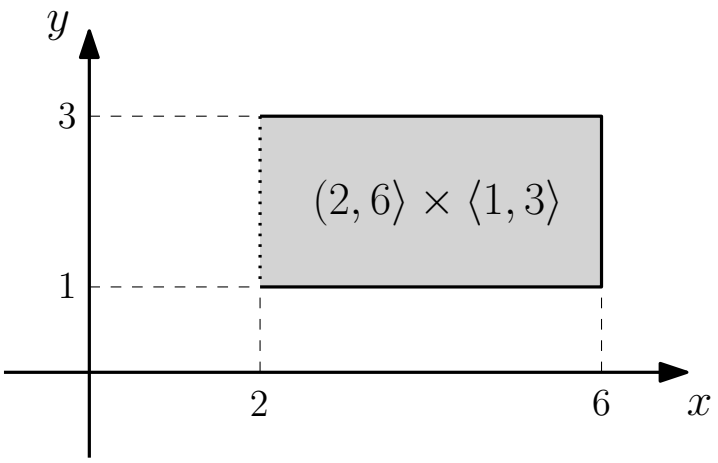
□

Pokud budeme však pracovat např. s intervaly reálných čísel, pak již nemůžeme




Obrázek 3.1: Grafické znázornění kartézského součinu z příkladu 3.4.2.

takto kartézský součin znázornit, ale můžeme reprezentovat uspořádané dvojice jako body v rovině. Např. pro $A = (2,6\rangle$ a $B = \langle 1,3\rangle$ je grafické znázornění na obrázku 3.2. Podobně jako v případě součinu čísel, i zde můžeme kartézské




Obrázek 3.2: Grafické znázornění kartézského součinu intervalů $(2,6\rangle$ a $\langle 1,3\rangle$.

součiny stejných množin značit pomocí horního indexu (tzv. *kartézské mocniny*), např. $A \times A = A^2$, $A \times A \times A = A^3$, atd. Obecně lze definovat

$$A^1 = A, A^n = A^{n-1} \times A.$$

Neplatí zde však asociativní ani komutativní zákon:

$$(A \times B) \times C \neq A \times (B \times C),$$
$$A \times B \neq C \times A,$$

protože jak jsme si již dříve uvedli, tak obecně $(x,y) \neq (y,x)$. (Zkuste si rozmyslet.)

**Příklad 3.4.3.** Nechť je dána množina $X = \{a,b\}$. Vypočítejte $x^3$.

*Řešení.* Kartézský součin $A^3$ můžeme vypočítat jako $x^2 \times x$.

$$X^2 = \{(a,a),(a,b),(b,a),(b,b)\}$$

Nyní stačí dopočítat $x^2 \times x = x^3 = \{(a,a),(a,b),(b,a),(b,b)\} \times \{a,b\}$, čímž obdržíme

$$\begin{aligned} X^3 =& \{(a,(a,a)),(a,(a,b)),(a,(b,a)),(a,(b,b)),(b,(a,a)),(b,(a,b)),(b,(b,a)),\\ & (b,(b,b))\}. \end{aligned}$$

Ovšem jak jsme již zmiňovali, tak $(x',(y',z')) = (x',y',z')$, tedy množina $X^3$ jednoduše obsahuje všechny uspořádané trojice prvků z $x$.

$$X^3 = \{(a,a,a),(a,a,b),(a,b,a),(a,b,b),(b,a,a),(b,a,b),(b,b,a),(b,b,b)\}.$$

□

### 3.4.2 Zavedení relace

Relace (jak název napovídá) odpovídá jistému „vztahu“. Z reálného života takové příklady známe, např. vztah „matka – dcera“, „stát – hlavní město státu“, apod. Jsou-li např. Jitka a Lenka spolu ve vztahu „matka – dcera“, pak bychom mohli jednoduše psát

$$(\text{Jitka}, \text{Lenka}).$$

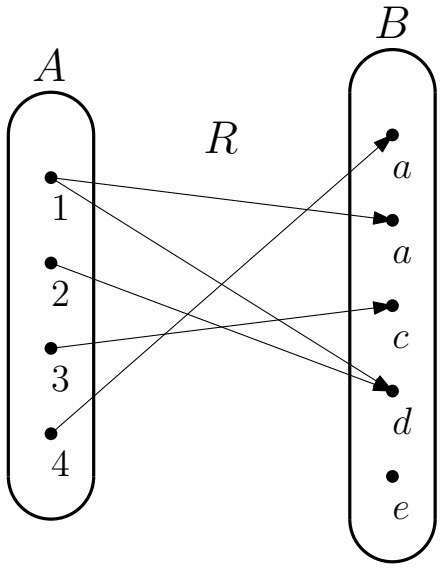
To však v řeči matematiky není nic jiného, než uspořádaná dvojice prvků. K tomu se nám bude hodit již zavedený kartézský součin.

**Definice 3.4.4** (Relace)**.** Nechť $X$,$Y$ jsou libovolné množiny. Pak *relací mezi $X$ a $X$* nazýváme libovolnou podmnožinu $R$ kartézského součinu $X \times Y$, tj. $R \subseteq X \times Y$. Speciálně, pokud $X = Y$, pak mluvíme o *relaci na množině $X$*, tzn. $R \subseteq X^2$.

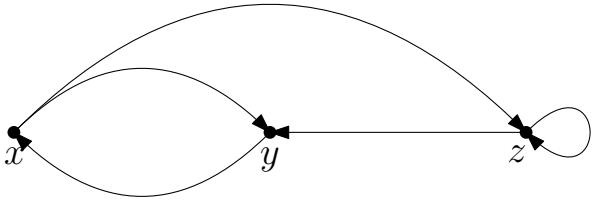
Pokud $(x,y) \in R$, pak říkáme, že *prvky $x$ a $y$ jsou v relaci $R$*, což ekvivalentně zapisujeme jako $xRy$. Jak už jsme si zmínili, tak relace již známe a i v tomto textu jsme je mnohokrát použili. Např. relace rovnosti „$=$“ na $\mathbb{N}$ by obsahovala prvky $(1,1),(2,2),(3,3),\ldots$. Pochopitelně bychom mohli psát „$(2,2) \in =$“, ale to neděláme; místo toho zkrátka píšeme „$2 = 2$“. Podobně např. relace „$\leq$“ na množině $\mathbb{R}$, „$>$“, „$\geq$“, aj.

**Úmluva 3.4.5.** Pro značení relací budeme používat velká písmena latinské abecedy $A$,$B$,$C$,…,$X$,$Y$,$Z$.

Relace můžeme znázornit více způsoby v závislosti na jejich typu. Např. máme-li relaci $R = \{(1,b),(1,d),(2,d),(3,c),(4,a)\}$ mezi množinami $A = \{1,2,3,4\}$ a $B = \{1,2,3,4,5\}$, pak ji můžeme znázornit způsobem uvedeným na obrázku 3.5. Avšak pokud máme relaci $S$ **na množině** $C = \{x,y,z\}$, kupříkladu $S = \{(x,z),(x,y),(y,x),(z,y),(z,z)\}$, pak volíme spíše znázornění na obrázku 3.5. Jako poslední si ještě zmíníme tzv. *skládání relací*.




Obrázek 3.3: Grafické znázornění relace $R$ mezi množinami $A$ a $B$.




Obrázek 3.4: Grafické znázornění relace $S$ na množině $C$.

**Definice 3.4.6** (Složení relací)**.** Nechť $X$,$Y$,$Z$ jsou libovolné množiny, $R \subseteq X \times Y$ a $S \subseteq Y \times Z$. Relaci $T \subseteq X \times Z$ definujeme následovně:

$$xTz \Leftrightarrow \exists y \in Y : xRy \wedge ySz.$$

Složení relací $R$ a $S$ značíme $S \circ R$, tzn. $T = S \circ R$.

**Příklad 3.4.7.** Mějme množiny $A = \{a,b,c\}$, $B = \{x,y,z\}$ a $C = \{i,j,k,l\}$. Na nich definujme relace

$$R = \{(a,z),(a,y),(c,x)\} \subseteq A \times B \quad \text{a} \quad S = \{(x,k),(y,i),(y,j),(z,j)\} \subseteq B \times C.$$

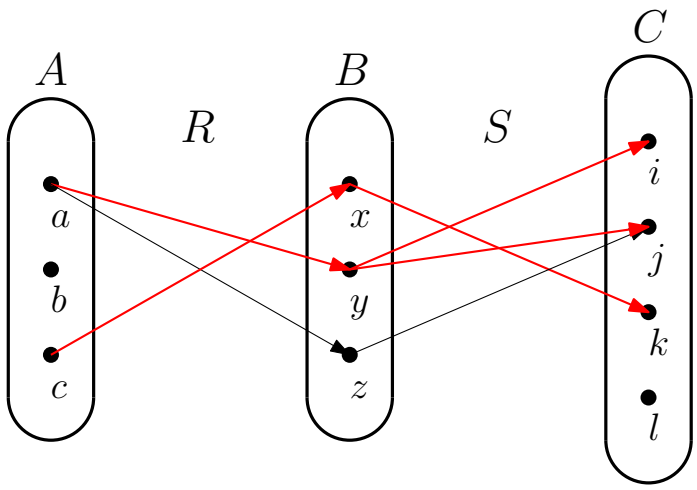
Určete $T = S \circ R$.

*Řešení.* Postupujme podle definice 3.4.6 výše. Pro každou z dvojic v $R$ se podíváme, zda existuje nějaká dvojice v $s$ taková, že platí: $t_1 R t_2$ a $t_2 S t_3$, kde $t_1 \in a$ $t_2 \in b$ a $t_3 \in C$.

$$\begin{aligned} &aRj \wedge zSj \Rightarrow aTj, \\ &aRy \wedge ySi \Rightarrow aTi, \\ &aRy \wedge ySj \Rightarrow aTj \text{ (duplikátní)}, \\ &cRx \wedge xSk \Rightarrow cTk. \end{aligned}$$

Tedy $T = \{(a,i),(a,j),(c,k)\}$.

□




Obrázek 3.5: Grafické znázornění relace složení relací $R$ a $S$ z příkladu 3.4.7.

Podívejme se ještě na jeden příklad:

**Příklad 3.4.8.** Mějme relace $R = \{(x,x),(x,y),(y,z)\}$ a $S = \{(x,z),(z,y)\}$. Určete $T = S \circ R$ a $T' = R \circ S$.

*Řešení.* Začneme s $T = S \circ R$.

$$xRx \wedge xSz \Rightarrow xTz$$
$$yRz \wedge zSy \Rightarrow yTy$$

Tzn. $T = \{(x,z),(y,y)\}$. Nyní analogicky pro $T\prime$.

$$zSy \wedge yRz \Rightarrow zTz$$

Tím získáváme $T' = \{(z,z)\}$.

□

Z příkladu 3.4.8 lze vidět, že skládání relací není komutativní a tedy záleží na pořadí.
(Sekce inspirována [6], str. 34–39.)

(TODO: Doplnit cvičení.)

## 3.5 Zobrazení

Jedním z nejdůležitějších typů relací je tzv. *zobrazení*. Zde se zároveň dostáváme trochu zpět k tématu, kterým se čtenář na střední škole jistě zabýval, akorát se o něm nemluvilo v souvislosti s relacemi, a to sice k *funkcím*. Termíny jako definiční obor, obor hodnot, aj. nejspíše tak pro nás nebudou velkou neznámou, ale přesto nezanedbáme jejich formální zavedení.

### 3.5.1 Zavedení a související pojmy

**Definice 3.5.1** (Zobrazení)**.** *Zobrazením z množiny $X$ do množiny $Y$* nazýváme relaci $f \subseteq X \times Y$, když platí

$$\forall x \in X, \exists! y \in Y : xfy.$$

U relací jsme si zaváděli úmluvu, kde jsme si pro jejich značení rezervovali velká písmena latinské abecedy. U zobrazení je tomu trochu jinak.

**Úmluva 3.5.2.** Zobrazení budeme značit malými písmeny latinské abecedy $a$,$b$,$c$,$\ldots$,$x$,$y$,$z$, nebo případně malými písmeny řecké abecedy $\alpha$,$\beta$,$\gamma$,$\ldots$,$\chi$,$\psi$,$\omega$.

Že $f$ je zobrazení z $X$ do $Y$ zapisujeme jako

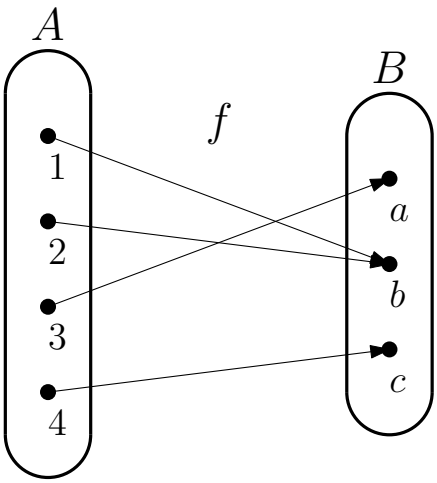
$$f : X \to Y,$$

a to, že zobrazení $f$ přiřazuje prvku $x$ prvek $y$ vyjádříme zápisem

$$f : x \mapsto y.$$

Tato definice by nám měla být povědomá, neboť takto jsme si nejspíše na střední škole definovali funkci. Jaký je tedy rozdíl mezi **funkcí** a **zobrazením**? Ve skutečnosti toto není v matematice jednotné. V určitých odvětvích se tyto termíny považují za synonyma a jinde se zase naopak funkcí nazývá speciální typ zobrazení, kdy množina $Y$ je číselná, tj. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, ... (tedy funkce je zobrazení, avšak ne naopak). My tyto pojmy budeme v dalším textu rozlišovat, aby byl výklad jasnější.

Např. zobrazení $f : \{1,2,3,4\} \to \{a,b,c\}$, kde $f = \{(1,b), (2,b), (3,a), (4,c)\}$ je znázorněno na obrázku 3.6. U zobrazení $f : X \to Y$, kde $f : x \mapsto y$, se




Obrázek 3.6: Grafické znázornění zobrazení $f = \{(1,b), (2,b), (3,a), (4,c)\}$.

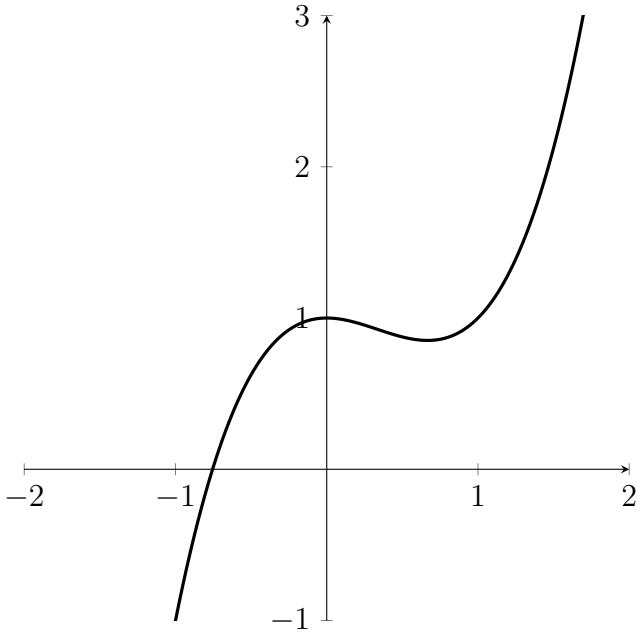
- $x$ nazývá *vzor* prvku $y$ a
- $y$ se nazývá *obraz* prvku $x$ nebo také *hodnota zobrazení $f$ v bodě $x$*.

Množiny $X$ a $Y$ pak po řadě nazýváme *množina vzorů* a *množina obrazů*. U funkcí je zvykem tyto množiny nazývat *definiční obor* a *obor hodnot*.

Též se zavádí *obraz množiny*, tj. je-li $A \subseteq X$, pak

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

V případě funkce, co by podmnožiny kartézského součinu, byl čtenář nejspíše zvyklý je zadávat pomocí tzv. *funkčního předpisu*, např. $f : \mathbb{R} \to \mathbb{R}$, přičemž $f(x) = x^3 - x^2 + 1$. Tu jsme znázorňovali pomocí *grafu* (viz 3.7). Tento způsob proto budeme používat i u zobrazení (tedy nejen u funkcí).




Obrázek 3.7: Graf funkce $f : \mathbb{R} \to \mathbb{R}$, kde $f(x) = x^3 - x^2 + 1$.

### 3.5.2 Druhy a vlastnosti zobrazení

Skládání zobrazení je zcela stejné, jako v případě relací (ostatně zobrazení je relace). Avšak pro ujasnění si jej zformulujme jako samostatnou definici.

**Definice 3.5.3** (Skládání zobrazení)**.** Nechť $f : X \to Y$ a $g : Y \to Z$ jsou zobrazení. *Složením zobrazení $f$ a $g$* nazveme zobrazení $h : X \to Z$, pro které platí

$$\forall x \in X : h(x) = g(f(x)).$$

Složení zobrazení $g$ a $f$ se značí (stejně jako u relací) $g \circ f$, tzn. $h = g \circ f$.

Podle právě zformulované definice 3.5.3 tedy platí:

$$\forall x \in X : \Big(g \circ f\Big)(x) = g(f(x)).$$

**Definice 3.5.4** (Důležité druhy zobrazení)**.** Nechť je dáno zobrazení $f : X \to Y$. Pak $f$ je

(i) *prosté* (též *injektivní* či *injekce*), jestliže $\forall x,y \in X, x \neq y : f(x) \neq f(y)$.

(ii) *na* (též *surjektivní*[8] či *surjekce*), jestliže $\forall y \in Y, \exists x \in X : f(x) = y$.

(iii) *vzájemně jednoznačné* (též *bijektivní* či *bijekce*), když $f$ je prosté a na.

**Příklad 3.5.5.** Ukázky některých zobrazení a jejich klasifikace podle 3.5.4. ($A$ je libovolná množina.)

(i) Zobrazení $f_1 : \mathbb{Z} \to \mathbb{Z}$, kde $f_1(n) = -n$, je *bijekce*.

[8] Z francouzštiny, čteme „syrjektivní“/„syrjekce“.

(ii) Zobrazení $f_2 : \mathbb{Z} \to \mathbb{N}$, kde $f_2(n) = |n| + 1$, je *na*, avšak není *prosté* a tedy ani *bijekce*.

(iii) Zobrazení $f_3 : \mathbb{R} \to \mathbb{R}_0^+$, kde $f_3(x) = x^2$, je *na*, ale není *prosté*.

(iv) Zobrazení $f_4 : \mathbb{R} \to \mathbb{R}_0^+$, kde $f_4(x) = x^2 + 1$, není *prosté*, ani *na*.

(v) Zobrazení $f_5 : \mathbb{R} \to \mathbb{R}^+$, kde $f_5(x) = e^x$, je *bijekce*.

(vi) Zobrazení $f_6 : A^2 \to A^2$, kde $f_6\Big((x,y)\Big) = (y,x)$, je *bijekce*.

(vii) Zobrazení $f_7 : A \to A$, kde $f_7(x) = x$, je *bijekce*.

(viii) Zobrazení $f_8 : A \to \mathcal{P}(A)$, kde $A$ je libovolná množina a $f_8(a) = \{X \in \mathcal{P}(A) \mid a \in X\}$, je *bijekce*.

Psát v matematice $f\Big((x_1,x_2,\ldots,x_n)\Big)$ je nezvyklé (jak jsme provedli v (vi)). Nejspíše by dávalo větší smysl v takovém případě nepsat vnořené závorky. Proto si zaveďme následující úmluvu.

**Úmluva 3.5.6.** Zápis $f\Big((x_1,x_2,\ldots,x_n)\Big)$ budeme nahrazovat symbolem $f(x_1,x_2,\ldots,x_n)$ stejného významu (tj. obraz uspořádané $n$-tice).

Poslední bod (vii) je dosti významným příkladem zobrazení, které si zaslouží vlastní definici (viz 3.5.7).

**Definice 3.5.7** (Identita)**.** Nechť $f : X \to X$ je zobrazení takové, že $f(x) = x$. Pak $f$ nazýváme *identitou* nebo též *identické zobrazení*a značíme jej $1_X$.

(Inspirováno [7], str. 10.)
U zobrazení a jejich skládání můžeme pozorovat jisté závislosti. Jejich důkazy jsou triviální a plynou přímo z definice, ale přesto si je zde uvedeme.

**Lemma 3.5.8** (Vlastnosti skládání zobrazení)**.** *Nechť $f : X \to Y$ a $g : Y \to Z$ jsou zobrazení. Pak*

*(i) jsou-li $f$,$g$ prostá zobrazení, je i $g \circ f$ prosté zobrazení.*

*(ii) jsou-li $f$,$g$ zobrazení na, je i $g \circ f$ zobrazení na.*

*(iii) jsou-li $f$,$g$ bijekce, je i $g \circ f$ bijekce.*

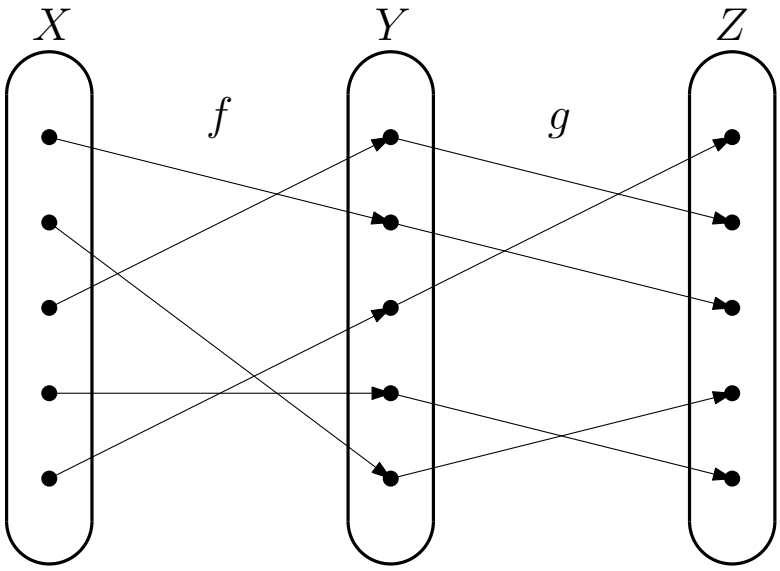
*Důkaz. (i).* Budiž dány prvky $x,y \in X$ takové, že $x \neq y$. Protože $f$ je prosté, pak $f(x) \neq f(y)$. Protože prvky $f(x),f(y) \in Y$ jsou různé a $g$ je prosté, pak $g(f(x)) \neq g(f(y))$.

*(ii).* Zde budeme postupovat opačně. Mějme prvek $z \in Z$. Z předpokladu, že $g$ je na, plyne, že existuje $y \in Y$ takové, že $g(y) = z$. Analogicky pro $y$ musí existovat $x \in X$ takové, že $f(x) = y$, neboť $f$ je na. Tzn. $g(f(x)) = z$.

*(iii).* Přímý důsledek *(i)* a *(ii)*.

□

Princip bodu (iii) je znázorněn na obrázku 3.8.




Obrázek 3.8: Příklad složení bijekcí $f$ a $g$.

(Sekce inspirována [6], str. 39–43.)

(TODO: Doplnit cvičení..)

## 3.6 Schéma axiomů nahrazení

$$\forall u\,\forall v\,\forall v'\,(\varphi(u,v) \wedge \varphi(u,v') \Rightarrow v = v') \Rightarrow$$
$$\Rightarrow \forall a\,\exists z\,\forall x\,\Big(x \in z \Leftrightarrow \exists y\,(y \in a \wedge \varphi(y,x))\Big),$$

kde formule $\varphi(u,v)$ neobsahuje proměnné $v'$ a $z$.

Tento axiom je pravděpodobně nejsložitější, co do jeho zápisu. Zaměřme se nyní pouze na předpoklad

$$\forall u\,\forall v\,\forall v'\,(\varphi(u,v) \wedge \varphi(u,v') \Rightarrow v = v').$$

Ten udává, jakou vlastnost musí splňovat formule $\varphi(u,v)$. Tvrzení je takové, že pokud existují množiny $v,v'$ takové, že platí $\varphi(u,v)$ i $\varphi(u,v')$, pak množiny $v$ a $v'$ musí být stejné. Resp. předpoklad požaduje, aby pro každé $u$ platila formule $\varphi(u,v)$ pro nejvýše jeden prvek $v$. Ekvivalentně bychom toto mohli napsat jako

$$\forall u\,\exists! v : \varphi(u,v).$$

Toto by nám již mělo být povědomé. Podobně jsme definovali zobrazení v definici 3.5.1. V tomto případě můžeme tak $\varphi$ chápat jako formuli udávající, zda obrazem prvku $u$ je prvek $v$.

Druhá část

$$\forall a\,\exists z\,\forall x\,\Big(x \in z \Leftrightarrow \exists y\,(y \in a \wedge \varphi(y,x))\Big)$$

nám zaručuje, že všechny prvky $v$, kterým odpovídá (v rámci formule $\varphi(u,v)$) nějaký prvek $u \in a$, tvoří množinu $z$. Stručně řečeno, **obrazem libovolné množiny při definovatelném zobrazení je opět množina**.

Tento axiom nebyl součástí původních Zermelových axiomů. Posléze se však ukázalo, že existují množiny, jejichž existence není zbývajícími axiomy implikovaná. Např.

$$m = \{x, \mathcal{P}(x), \mathcal{P}(\mathcal{P}(x)), \mathcal{P}(\mathcal{P}(\mathcal{P}(x))), \dots\},$$

kde $x \neq \emptyset$. Z axiomu nekonečna zaručující existenci nekonečné množiny $z$ víme, že pokud $x$ je prvkem $z$, pak i $x \cup \{x\}$ je prvkem $z$. Není těžké si rozmyslet, že toto pro $m$ není splněno. Nicméně při vhodné volbě formule $\varphi$ lze definovat zobrazení prvků nějaké aktuálně nekonečné množiny postulované axiomem nekonečna na množiny $x, \mathcal{P}(x), \mathcal{P}(\mathcal{P}(x)), \dots$ a podle axiomu nahrazení tak tyto obrazy

$$\{x, \mathcal{P}(x), \mathcal{P}(\mathcal{P}(x)), \mathcal{P}(\mathcal{P}(\mathcal{P}(x))), \dots\}$$

tvoří opět množinu.

## 3.7 Axiom fundovanosti

$$\forall a \left( a \neq \emptyset \Rightarrow \exists x : \left( x \in a \wedge x \cap a = \emptyset \right) \right)$$

Tento axiom slouží svým způsobem jako omezení množin, které lze uvažovat. Tvrzení je takové, že každá neprázdná množina musí obsahovat alespoň jeden prvek, který je s ní *disjunktní* (tj. má s ní prázdný průnik). Tím zamezujeme existenci některých typů množin, jako třeba množiny obsahující samy sebe, tj. $a \in a$. Jmenovitě např.

$$a = \{a\}, \; b = \{b, \emptyset\} \text{ a jiné.}$$

Lze se snadno přesvědčit, že při existenci takových množin by axiom fundovanosti byl porušen. Pokud bychom připustili např. existenci množiny $x'$, pro kterou by platilo, že $x' \in x'$, pak podle axiomu dvojice (ZF3) je též množinou i $u = \{x'\}$. Podle axiomu fundovanosti musí $u$ obsahovat prvek $x$, takový, že $x \cap x' = \emptyset$. Protože však pouze $x'$ je prvkem $u$, pak musí nutně platit (protože $x' \neq \emptyset$), že $x' \cap u = \emptyset$. To ale neplatí!

$$x' \cap \{x'\} = x',$$

neboť $x' \in x'$. Tzn. $u$ tedy **nesplňuje** axiom fundovanosti a není tak množinou v ZF.

Dalšími důsledky axiomu fundovanosti je vyloučení cyklů v relaci „býti prvkem“, tj. např.

$$x_1 \in x_2 \in x_3 \in x_1.$$

Trochu obecněji lze nahlédnout, že nikdy tak nemůže nastat situace, kdy bychom našli nekonečný řetězec „do sebe zanořených“ množin

$$\dots \in x_n \in \dots \in x_2 \in x_1 \in x_0.$$

(TODO: Doplnit případně důkaz.)

Axiom fundovanosti tedy slouží jako obecná charakteristika všech myslitelných množin v ZF. Oproti všem ostatním je tedy trochu jiného charakteru, neboť

doposud zmíněné axiomy byly spíše „konstrukční“. Jejich postupnou aplikací jsme byli schopni sestrojit z menších množin množiny větší. Lze ukázat, že axiom fundovanosti je ekvivalentní s tvrzením, že všechny množiny v ZF lze generovat z prázdné množiny opakovanou aplikací axiomu potence a sumy.

# Kapitola 4

# Budování číselných množin

Ne nadarmo se někdy metaforicky teorii množin říká *svět matematiky*. Množiny jsou skutečně silným nástrojem pro budování různých matematických objektů. Již jsme si vysvětlovali, že zobrazení mezi množinami $A$ a $B$ není nic jiného, než množina uspořádaných dvojic, což podle Kuratowského definice uspořádané dvojice 3.1.3 není opět nic jiného než množina. Tedy i funkce tak, jak je známe ze střední, lze bez problému vnímat jako „pouhé“ množiny, splňující určité vlastnosti.

Jak ale reprezentovat pomocí množin čísla? Takto se jedná o dosti složitou otázku, neboť číselných oborů máme hned několik: přirozená čísla, racionální čísla, iracionální čísla, reálná čísla a jiné další. Je tomu tak až s podivem, že takto pro nás elementární záležitost by mohla mít množinovou definici. V této kapitole se podíváme na to, jak můžeme v tomto ohledu zavést *přirozená čísla* $\mathbb{N}$ a *racionální čísla* $\mathbb{Q}$, které jsou pro ostatní číselné obory základním stavebním kamenem. Pokud jde o budování např. reálných čísel $\mathbb{R}$, velmi pěkně je toto popsáno v knize [5] (str. 8–17), z níž je ostatně v dalších odstavcích čerpáno.

## 4.1 Peanovy axiomy

Jedním ze způsobů, jak popsat přirozená čísla, je zavedením určitých axiomů pro ně. Tímto se zabýval matematik, logik a filozof Giuseppe Peano (1858–1932), který zavedl soustavu axiomů, dnes nazývanou *Peanovy axiomy*, která vystihuje jejich vlastnosti. Později uvidíme, tak tyto vlastnosti splňují **právě** přirozená čísla s nulou $\mathbb{N}_0$[1].

**Peanovy axiomy pro přirozená čísla**:
$X$ je množina obsahující (speciální) prvek $0_X \in X$ a $s : X \to X$ zobrazení takové, že platí:

(P1) zobrazení $s$ je prosté, tj. $\forall x,y \in X\, x \neq y : s(x) \neq s(y)$,

(P2) $\forall x \in X : s(x) \neq 0_X$ a

[1] Ve skutečnosti takových množin existuje více. Lze však ukázat, že pro všechny existuje bijekce na $\mathbb{N}_0$, která zachovává všechny vztahy mezi jejich odpovídajícími prvky (přesněji tzv. *izomorfismus*). Všechny množiny splňující Peanovy axiomy mají tak „shodnou strukturu“. Důkaz tohoto faktu zde však vynecháme.

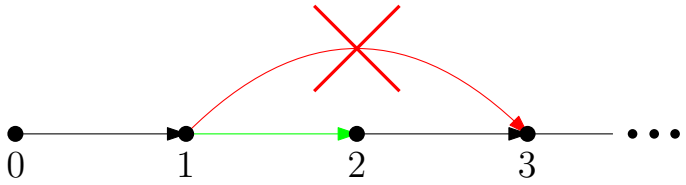
(P3) $\forall A \subseteq X \left(0_X \in X \wedge (x \in A \Rightarrow s(x) \in A) \Rightarrow A = X\right)$.

Idea zobrazení $s$ v kontextu Peanových axiomů je taková, že každému $x$ je přiřazen jeho *následník*[2] $s(x)$.

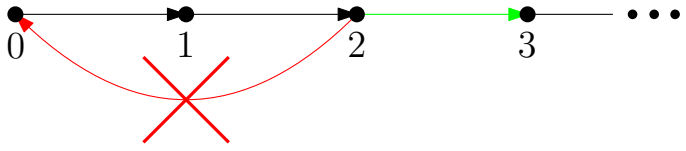
- První axiom (P1) tak říká, že pokud máme dva různé prvky $x$,$y$, pak nikdy nemohou mít stejného následníka.
- Druhý axiom (P2) se týká speciálně prvku $0_X$ a zaručuje, že $0_X$ není následníkem žádného prvku.
- Třetí axiom (P3) postuluje, že pokud libovolná podmnožina $A$ obsahuje prvek $0_X$ a pro každé její $x$ obsahuje i jeho následníka $s(x)$, pak nutně $A$ je nutně rovna celé množině $X$. Tento axiom se též nazývá *princip matematické indukce* a často jej využíváme v důkazech (viz podsekce A.1.4 v příloze).

Z kontextu lze vidět, že prvek $0_X$ zde zastává roli čísla nula. Skutečně, pokud bychom si označili postulovanou množinu $X$ jako $\mathbb{N}_0$ a její prvky 1,2,3,..., tj. $\mathbb{N}_0 = \{0,1,2,\dots\}$, kde $0_X$ interpretujeme právě symbolem 0 a funkci $s$ definovali $s(n) = n + 1$, pak lze vidět, že $\mathbb{N}_0$ splňuje axiomy (P1), (P2) a (P3).

Nutnost prvních dvou axiomů si můžeme poměrně lehce představit. První požadavek na prostost zobrazení $s$ je celkem přirozený. Např. číslo 7 je následníkem čísla pouze čísla 6. Nikdy tak nemůže vzniknout situace jako na obrázku 4.1. Podobně prvek 0 není následníkem žádného prvku (viz obrázek 4.2).




Obrázek 4.1: Každý prvek je následníkem právě jednoho prvku.




Obrázek 4.2: Žádný prvek není následníkem 0.

[2]Tento termín si formálně definujeme v sekci (TODO: doplnit odkaz.) pomocí množin.

# Seznam použité literatury


[1] E. Fuchs. *Teorie množin pro učitele*. Masarykova univerzita, Brno, 2003. ISBN 80-210-2201-9.

[2] B. Bolzano. *Paradoxy nekonečna*. Československá akademie věd, Praha, 1963.

[3] Eukleidés. *Základy*. Jednota českých mathematiků a fysiků, Praha, 1907.

[4] B. Balcar a P. Štěpánek. *Teorie množin*. Academia, Praha, 1986. ISBN 80-200-0470-X.

[5] Derek C. Goldrei. *Classic Set Theory: For Guided Independent Study*. Chapman & Hall Mathematics. CRC Press, 2017. ISBN 9781351460613.

[6] J. Matoušek a J. Nešetřil. *Kapitoly z diskrétní matematiky*. 4., upr. a dopl. vyd. Karolinum, Praha, 2009. ISBN 978-80-246-1740-4.

[7] J. Bečvář. *Lineární algebra*. Vydání páté. Matfyzpress, Praha, 2019. ISBN 978-80-7378-378-5.

[8] Gary Chartrand, Albert D. Polimeni, and Ping Zhang. *Mathematical proofs: A transition to Advanced Mathematics*. Pearson Education, 2014. ISBN 9780321797094.

[9] Univerzita Karlova. Katedra didaktiky matematiky, Matematicko-fyzikální fakulta. Matematická logika. *[online]*, Citováno 24. března 2022. Dostupné z: `https://www2.karlin.mff.cuni.cz/~portal/logika/?page=prim`.

# Seznam obrázků

# Seznam tabulek

# Seznam použitých zkratek

# Příloha A

# Přílohy

## A.1 Důkazy

V matematice se lze setkat s celou řadou různých tvrzení. Od primitivních, jejichž platnost je zřejmá až po složitější, nad jejich platností je třeba se více zamyslet. Čtenář se nejspíše zatím spíše setkával s matematikou, která zahrnovala užívání jistých postupů. Např. zjednodušování algebraických výrazů, řešení soustav rovnic, ověřování trigonometrických identit, aj. Avšak hodně postupů v matematice je založeno na již známých výsledcích, o nichž bylo dokázáno, že jsou pravdivé. Pokud ovšem máme dokázat určité tvrzení, je třeba, aby bylo naše zdůvodnění jednoznačné a logicky správné. V této sekci se proto podíváme na důkazové techniky používané v matematice, které budeme dále v textu využívat.

Matematická tvrzení jsou často různě klasifikována v závislosti na jejich povaze. Základními typy jsou tyto.

- *Axióm.* Tvrzení, které implicitně považujeme za pravdivé a nedokazujeme jej. S axiomatikou jsme se již částečně seznámili v historické předmluvě (viz 1.2.3).
- *Věta.* Matematické tvrzení, jehož pravdivost můžeme ověřit důkazem.
- *Lemma.* Pomocné tvrzení, které běžně využíváme pro důkaz jiného (typicky složitějšího) tvrzení.
- *Důsledek.* Tvrzení, které je přímým důsledkem jiného tvrzení.

Čistě formálně však mezi **větou**, **lemmatem** a **důsledkem** není žádný rozdíl.

### A.1.1 Důkaz přímý

Jedná se o asi nejjednodušší typ důkazu. Často jsou matematická tvrzení formulována jako implikace, tzn. „Jestliže platí $A$, pak platí $B$.“. Konkrétně, např. „Je-li $x < 0$, pak $x^2 > 0$.“.

Myšlenka důkazu je taková, že začínáme od předpokladu $A$, z něhož dále odvozujeme dílčí tvrzení tak dlouho, až dojdeme k požadovanému závěru $B$. Symbolicky, pokud si označíme dílčí tvrzení v důkazu $X_1, X_2, \ldots, X_n$, pak vlastně

dokazujeme výrokovou formuli

$$(A \Rightarrow X_1) \wedge (X_1 \Rightarrow X_2) \wedge \cdots \wedge (X_{n-1} \Rightarrow X_n) \wedge (X_n \Rightarrow B). \tag{A.1}$$

V tomto procesu dokazování se využívá tautologie (xiii) z věty 2.1.13

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \Leftrightarrow (A \Rightarrow C).$$

Z tohoto faktu vyplývá, že pokud je každá z dílčích implikací pravdivá, pak je nutně pravdivá i implikace $A \Rightarrow B$, kterou jsme chtěli dokázat[1]. Podívejme se na příklad podobný příklad z úvodu.

**Tvrzení A.1.1.** *Nechť $x \in \mathbb{R}$. Je-li $x < 0$, pak $x^2 + 1 > 0$.*

*Důkaz.* Předpokladem našeho tvrzení je $x \in \mathbb{R} \wedge x < 0$. Víme, že pro každé reálné číslo $x$ platí, že $x^2 \geq 0$. Tj. určitě platí implikace

$$x < 0 \Rightarrow x^2 > 0.$$

Dále víme, že triviálně platí $1 > 0$, tedy také jistě platí

$$x^2 + 1 > x^2.$$

Protože však $x^2 > 0$, pak také $x^2 + 1 > 0$, což jsme chtěli dokázat.

□

Posloupnost dokázaných implikací bychom mohli podle (A.1) zapsat nyní jako

$$(x \in \mathbb{R} \wedge x < 0 \Rightarrow x^2 > 0) \wedge (x^2 > 0 \Rightarrow x^2 + 1 > x^2) \wedge (x^2 + 1 > x^2 \Rightarrow x^2 + 1 > 0),$$

a tedy jsme dokázali i implikaci v původním tvrzení $x < 0 \Rightarrow x^2 + 1 > 0$.

V praxi důkazy takto samozřejmě nerozepisujeme a řadu věcí považujeme za samozřejmé, např. právě $1 > 0$, $x^2 + 1 > x^2$, apod. Takový důkaz bychom bez většího rozepisování mohli napsat klidně na jeden řádek.

$$x < 0 \Rightarrow 0 < x^2 < x^2 + 1 \Rightarrow x^2 + 1 > 0.$$

Všimněte si zároveň, že jsme zde použili jistou generalizaci. Předvedený důkaz totiž není závislý na volbě $x$ a náš argument je tak univerzální. Tedy platí

$$\forall x < 0 : x^2 + 1 > 0.$$

Obecně tvrzení formulovaná stylem „je-li $x \in X$, pak ...“ jsou míněna jako

$$\forall x \in X : \ldots$$

**Tvrzení A.1.2.** *Nechť $n \in \mathbb{N}$ je liché. Pak $3n + 7$ je sudé číslo.*

*Důkaz.* Začneme u předpokladu, že $n \in \mathbb{N}$ je liché číslo. To znamená, že

$$\exists k \in \mathbb{N} : n = 2k + 1.$$

Po dosazení obdržíme

$$3(2k + 1) + 7 = 6k + 3 + 7 = 6k + 10 = 2(3k + 5).$$

Protože $3k + 5$ je přirozené číslo, pak $3n + 7$ je dělitelné dvěma a je tedy sudé, což jsme chtěli dokázat.

□

[1] Výrokové proměnné lze v konkrétním případě nahradit příslušnými predikáty.

**Tvrzení A.1.3** (AG nerovnost)**.** *Pro* $a,b \in \mathbb{R}_0^+$ *platí*

$$\sqrt{ab} \leq \frac{a+b}{2}.$$

*Důkaz.* Při důkazu tohoto tvrzení vyjdeme z jednoduchého pozorování:

$$(\sqrt{a} + \sqrt{b})^2 \geq 0.$$

Nyní stačí výraz upravit a dostaneme požadovanou nerovnost.

$$(\sqrt{a} + \sqrt{b})^2 = a + 2\sqrt{ab} + b \geq 0 \Rightarrow \sqrt{ab} \leq \frac{a+b}{2}.$$

□

**Tvrzení A.1.4.** *Pro* $\forall x,y \in \mathbb{R}$ *platí*

$$x < y \Rightarrow x < \frac{x+y}{2} < y.$$

*Důkaz.* Zde je třeba si všimnout „dvojité“ nerovnosti v dokazovaném tvrzení. To nám již napovídá, že ve skutečnosti musíme dokázat 2 dílčí tvrzení, konkrétně

$$x < \frac{x+y}{2} \quad \text{a} \quad \frac{x+y}{2} < y.$$

Při důkazu obou částí vyjdeme opět z předpokladu. Tedy mějme libovolná čísla $x,y \in \mathbb{R}$ taková, že $x < y$. Pak jistě platí

$$x + x < x + y \Rightarrow 2x < x + y \Rightarrow x < \frac{x+y}{2}.$$

Tím jsme dokázali první nerovnost. Platnost druhé dokážeme analogicky:

$$x + y < y + y \Rightarrow x + y < 2y \Rightarrow \frac{x+y}{2} < y.$$

□

(Převzato z [8], str. 79 a [9], sekce *důkaz přímý.*)
Ne všechna tvrzení jsou v matematice nutně formulována jako implikace. Často se lze setkat s tvrzeními formulovanými jako ekvivalence, tj. $A \Leftrightarrow B$. Důkazy takových výroků jsou již trochu delší, neboť už nestačí pouze ukázat $A \Rightarrow B$. Vzpomeňme si však na tautologii, která nám dávala do souvislosti ekvivalenci s implikací (viz (xi) ve větě 2.1.13):

$$(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A).$$

Z toho je již vidět, jak u takových tvrzení při důkazu postupovat. Zkrátka dokážeme zvlášť $A \Rightarrow B$ a $A \Leftarrow B$.

**Tvrzení A.1.5.** *Nechť* $x,y \in \mathbb{Z}$*. Pak* $3 \mid xy$ *právě tehdy, když* $3 \mid x$ *nebo* $3 \mid y$*.*

*Důkaz.* *(⇒)*. Začneme s předpokladem, že $3 \mid xy$. Víme, že pokud je číslo dělitelné třemi, pak jej lze zapsat jako $3k$, kde $k \in \mathbb{Z}$. Uvažujme následující případy:

- $3 \mid x \wedge 3 \mid y$. Tehdy tvrzení jistě platí.
- $3 \nmid x$. Ukážeme, že pak nutně musí platit $3 \mid y$. Pokud $x$ není dělitelné třemi, pak jej lze zapsat buď jako $3k+1$, nebo $3k+2$, kde $k \in \mathbb{Z}$.

  $$xy = (3k+1)y \quad \text{nebo} \quad xy = (3k+2)y$$

  Protože čísla $3k+1$ a $3k+2$ nejsou dělitelná třemi, pak je vidět, že musí platit $3 \mid y$.
- $3 \nmid y$. Zde je postup analogický.

Tím máme dokázanou implikaci $3 \mid xy \Rightarrow 3 \mid x \vee 3 \mid y$.
*(⇐)*. Nyní předpokládáme, že platí $3 \mid x \vee 3 \mid y$; chceme ukázat, že $3 \mid xy$ Bez újmy na obecnosti[2], nechť je $x$ dělitelné třemi. Pak existuje $x = 3k$, kde $k \in \mathbb{Z}$. Po dosazení dostaneme

$$xy = (3k)y = 3(ky) \Rightarrow 3 \mid xy.$$

Tedy dokázali jsme obě implikace a tím i původní tvrzení.

□

### A.1.2 Důkaz nepřímý

Řada tvrzení v matematice však není až tak jednoduchá na dokázání přímo. Důkazy, které jsme si ukazovali, vždy začínaly od předpokladu a postupně jsme došli k požadovanému závěru. Lze ale postupovat i jinak. Opět se odkážeme na dříve zmíněné tautologie věty 2.1.13, konkrétně na (x):

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A). \tag{A.2}$$

Implikace je ve skutečnosti ekvivalentní s tvrzením, že pokud neplatí závěr, pak neplatí ani předpoklad. Na této skutečnosti je založen *důkaz nepřímý* (též *důkaz obměnou*). Podívejme se na příklady užití.

**Tvrzení A.1.6.** *Nechť $x \in \mathbb{Z}$ a $3 \nmid (x^2-1)$. Pak $3 \mid x$.*

V tomto případě máme dvě možnosti. Buď začneme s předpokladem $3 \nmid (x^2-1)$ a dokážeme, že $3 \mid x$ (tedy dokážeme tvrzení přímo), nebo naopak budeme předpokládat, že $3 \nmid x$ a dokážeme negaci původního předpokladu. Ačkoliv by se jistě našla možnost, jak tvrzení dokázat přímo, přesto se nejspíše zdá jednodušší začít s předpokladem, že $x$ není dělitelné třemi.

*Důkaz.* Nechť $3 \nmid x$. Ukážeme, že platí $3 \mid (x^2-1)$. Podle předpokladu lze $x$ zapsat jako $3k+1$ nebo $3k+2$, kde $k \in \mathbb{Z}$. Bez újmy na obecnosti pišme $x = 3k+1$. Pak

$$x^2-1 = (3k+1)^2-1 = 9k^2+6k+1-1 = 9k^2+6k = 3(3k^2+2k) \Rightarrow 3 \mid (x^2-1).$$

[2]Termín *bez újmy na obecnosti* (někdy zkráceně *BÚNO*) se v matematických textech používá v situacích, kdy může nastat více možností, avšak říkáme, že jejich důkazy jsou analogické.

Tedy dokázali jsme, že

$$3 \nmid x \Rightarrow 3 \mid (x^2 - 1),$$

což je však podle A.2 ekvivalentní s

$$3 \nmid (x^2 - 1) \Rightarrow 3 \mid x$$

a původní tvrzení je tak dokázané.

□

**Tvrzení A.1.7.** *Nechť jsou dány množiny $A$ a $B$. Pak*

$$A \cup B = A \Leftrightarrow B \subseteq A.$$

*Důkaz. ($\Rightarrow$).* Tuto implikaci dokážeme obměnou. Nechť jsou dány množiny $A$ a $B$ takové, že $B$ není podmnožinou $A$. Pak

$$\exists x \in B : x \notin A.$$

Prvek $x$ se se tedy objeví i ve sjednocení $A \cup B$, tj.

$$x \in A \cup B.$$

Ale protože $x \notin A$, pak $A \cup B \neq A$.
*($\Leftarrow$).* Opačnou implikaci lze již dokázat přímo a využijeme zde poměrně hezkého triku, který se při dokazování podobných tvrzení využívá. Tvrdíme-li, že dvě množiny se rovnají, pak ovšem i platí, že jsou vzájemně podmnožinami té druhé. Symbolicky

$$X = Y \Leftrightarrow (X \subseteq Y) \wedge (Y \subseteq X).$$

V našem případě budeme chtít ukázat, že platí

$$(A \subseteq A \cup B) \wedge (A \cup B \subseteq A).$$

Platnost inkluze $A \subseteq A \cup B$ je vidět okamžitě (vyplývá z definice sjednocení), neboť pro libovolný prvek $x$ platí:

$$x \in A \Rightarrow x \in A \cup B$$

a tedy skutečně $A \subseteq A \cup B$.

Zbývá ukázat, že $A \cup B \subseteq A$. Vezměme libovolný prvek $x \in A \cup B$; ukážeme že $x \in A$. Nyní mohou nastat dvě možnosti:

- $x \in A$. Pak máme triviálně požadovaný výsledek.
- $x \in B$. Z předpokladu víme, že $B \subseteq A$, z čehož opět plyne $x \in A$.

Dokázali jsme tedy obě inkluze, tj. $A \subseteq A \cup B$ a $A \cup B \subseteq A$ a tedy platí

$$A \cup B = A.$$

□

(Převzato z [8], str. 111.)

### A.1.3 Důkaz sporem

Už jsme si představili dvě základní důkazové techniky. Nyní k nim přidáme metodu třetí – *důkaz sporem*.

Uvažme, že máme tvrzení ve tvaru implikace $A \Rightarrow B$, které chceme dokázat. Podle (ix) ve větě 2.1.13 víme, že vždy platí

$$(P \Rightarrow \neg P) \Rightarrow \neg P. \tag{A.3}$$

Tato tautologie říká, že pokud z výroku $P$ lze odvodit jeho negaci $\neg P$, pak výrok $P$ neplatí.

Myšlenka důkazu sporem je tedy taková, že **budeme předpokládat platnost negace dokazovaného tvrzení $\neg(A \Rightarrow B)$ a dojdeme k závěru, který je v rozporu předpokladem**. Z toho pak podle (A.3) plyne, že znegované tvrzení neplatí a podle *zákona vyloučeného třetího* (viz (ii) ve větě 2.1.13) musí platit tvrzení opačné (což je původní tvrzení).

Ještě si vzpomeňme na tautologii

$$(A \Rightarrow B) \Leftrightarrow B \vee \neg A.$$

Pomocí ní můžeme psát

$$\neg(A \Rightarrow B) \equiv \neg(B \vee \neg A) \equiv A \wedge \neg B.$$

To ostatně dává i smysl. Implikace je nepravdivá pouze, když platí její předpoklad, ale neplatí její závěr.

**Tvrzení A.1.8.** *Nechť jsou dána $a$,$b \in \mathbb{Z}$, kde $a$ je sudé a $b$ je liché. Pak $4 \nmid (a^2 + 2b^2)$.*

*Důkaz.* Nejprve znegujeme dokazované tvrzení, tj.

$$\neg\Big((2 \mid a \wedge 2 \nmid b) \Rightarrow 4 \nmid (a^2 + 2b^2)\Big) \Leftrightarrow (2 \mid a \wedge 2 \nmid b) \wedge 4 \mid (a^2 + 2b^2).$$

Pro spor tedy předpokládejme, že je-li $a$ sudé a $b$ liché, pak výraz $a^2 + 2b^2$ je dělitelný čtyřmi. Tedy existují čísla $k$,$l \in \mathbb{Z}$ taková, že $a = 2k$ a $b = 2l - 1$. Tedy

$$a^2 + 2b^2 = (2k)^2 + 2(2l-1)^2 = 4k^2 + 8l^2 - 8l + 2 = 4(k^2 + 2l^2 - 2l) + 2.$$

Výraz $4(k^2+2l^2-2l)$ je jistě dělitelný 4. Avšak protože platí $4 \mid a^2+2b^2$, pak musí také platit $4 \mid 2$. To očividně však neplatí. To znamená, že znegované tvrzení je nepravdivé a platí tvrzení původní, což jsme chtěli dokázat.

□

(Převzato z [8], str. 126) V případě důkazu sporem je asi nejznámější (a též i nejstarší dochovaný) důkaz, že číslo $\sqrt{2}$ je iracionální.

**Tvrzení A.1.9.** *Číslo $\sqrt{2}$ je iracionální.*

*Důkaz.* Než začneme s důkazem, trochu si rozmysleme dokazované tvrzení. Jak bude vypadat jeho negace? Opačným tvrzením je, že *číslo $\sqrt{2}$ je racionální*. Z definice racionálního čísla to však znamená

$$\exists p,q \in \mathbb{Z} : \sqrt{2} = \frac{p}{q}.$$

O každém zlomku však víme, že jej lze zapsat v základním tvaru, tj. můžeme zároveň předpokládat, že $p$ a $q$ jsou nesoudělná. S tímto budeme dále pracovat. Pišme

$$\begin{aligned}\sqrt{2} &= \frac{p}{q}\\ 2 &= \frac{p^2}{q^2}\\ 2q^2 &= p^2.\end{aligned}$$

Z posledního řádku lze vidět, že $p^2$ lze zapsat jako dvojnásobek nějakého jiného čísla. Tedy $p^2$ je určitě sudé. Co nám to říká o samotném $p$? Že $p$ je také sudé. (O tom není těžké se přesvědčit. Stačí si spočítat $(2k)^2$ a analogicky pro lichá čísla $(2l-1)^2$.) Tzn. že existuje $r \in \mathbb{Z}$ takové, že $p = 2r$. Nyní dosadíme:

$$\begin{aligned}2q^2 &= (2r)^2\\ 2q^2 &= 4r^2\\ q^2 &= 2r^2.\end{aligned}$$

Tedy $q^2$ je také nutně sudé a tedy i $q$ je sudé. Dohromady tedy $p$ a $q$ jsou obě sudá. To je však spor, neboť jsme předpokládali, že $p$ a $q$ jsou nesoudělná. Tzn. nemůže neexistovat zlomek $p/q$, který by byl roven $\sqrt{2}$ a byl v základním tvaru.

□

**Tvrzení A.1.10.** *Prvočísel je nekonečně mnoho.*

*Důkaz.* Pro spor naopak uvažujme, že prvočísel je konečně mnoho; označme si je $p_1, p_2, \ldots, p_n$. Definujeme číslo $m$ následovně:

$$m = p_1 p_2 \cdots p_n.$$

Nyní k číslu $m$ přičteme 1

$$m + 1 = p_1 p_2 \cdots p_n + 1.$$

Na závěr celou rovnost vydělíme kterýmkoliv z čísel $p_1, p_2, \ldots, p_n$; bez újmy na obecnosti zvolme $p_1$:

$$\frac{m+1}{p_1} = \frac{p_1 p_2 \cdots p_n + 1}{p_1} = p_2 \cdots p_n + \frac{1}{p_1}.$$

Číslo $p_2 \cdots p_n$ je jistě přirozené, avšak $1/p_1$ již přirozené není (nejmenší prvočíslo je 2). Je vidět, že nově vzniklé přirozené číslo $m + 1$ není dělitelné žádným z prvočísel $p_1, p_2, \ldots, p_n$. To však znamená, že $m+1$ je buď samo prvočíslo, nebo je dělitelné prvočíslem, které není součástí posloupnosti $p_1, p_2, \ldots, p_n$. V obou případech však dostáváme spor, neboť jsme předpokládali, že posloupnost $p_1, p_2, \ldots, p_n$ obsahuje všechna prvočísla.

□

### A.1.4 Důkaz matematickou indukcí

K této důkazové technice si na úvod ukažme příklad. Čtenáři je jistě znám vzorec pro součet prvních $n$ členů geometrické posloupnosti. Jistě tak pro nás neměl být problém určit součet

$$\sum_{k=0}^{n} 2^k.$$

Představme si na chvíli, že bychom neznali daný vzorec. Zkusme si vypočítat prvních několik hodnot:

$$\begin{aligned} 2^0 &= 1, \\ 2^0 + 2^1 &= 3, \\ 2^0 + 2^1 + 2^2 &= 7, \\ 2^0 + 2^1 + 2^2 + 2^3 &= 15. \end{aligned}$$

Zdá se, že vzorec pro obecné $n$ by mohl být $2^{n+1} - 1$. Ale i kdybychom to ověřili pro jakékoliv množství hodnot $n$, stále to nebude není důkaz. Jak na to? K podobným tvrzením se využívá tzv. *matematická indukce* (někdy zkráceně jen *indukce*). Ukažme si na tomto příkladu způsob použití (formální princip si vysvětlíme později).

Naším cílem je tedy dokázat, že $\forall n \in \mathbb{N}_0$ platí

$$\sum_{k=0}^{n} 2^k = 2^{n+1} - 1.$$

(i) Nejdříve ověříme platnost vzorce pro nejmenší možné $n$, tj. pro $n = 0$:

$$\sum_{k=0}^{0} 2^k = 2^0 = 1 \quad \text{a} \quad 2^{0+1} - 1 = 2 - 1 = 1.$$

Pro $n = 0$ vzorec platí.

(ii) Nyní předpokládejme, že tvrzení platí pro určité $n = n_0 \in \mathbb{N}$. Ukážeme, že pak tvrzení nutně musí platit i pro $n = n_0 + 1$. Pišme

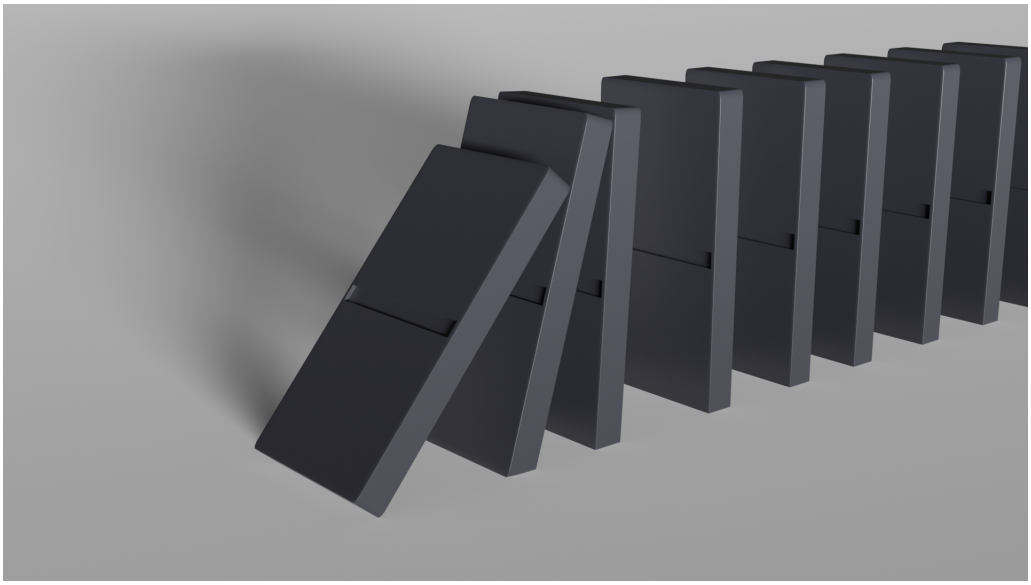
$$\sum_{k=0}^{n_0+1} 2^k = \sum_{k=0}^{n_0} 2^k + 2^{n_0+1}.$$

Podle předpokladu vzorec platí pro $n_0$, tedy za $\sum_{k=0}^{n_0} 2^k$ můžeme dosadit $2^{n_0+1} - 1$. Tedy

$$\sum_{k=0}^{n_0} 2^k + 2^{n_0+1} = 2^{n_0+1} - 1 + 2^{n_0+1} = 2 \cdot 2^{n_0+1} - 1 = 2^{n_0+2} - 1.$$

To je ale přesně vzorec pro $n = n_0 + 1$.

Tím jsme dokázali dané tvrzení. Jak? Podle (i) vzorec platí pro $n = 0$. Podle (ii) pak platí, že když tvrzení platí pro $n = 0$, pak platí i pro $n = 1$ (pro $n_0 = 0$). Pro $n = 1$ pak opět podle (ii) platí, že tvrzení platí i pro $n = 2$. Opět podle (ii) víme, že když tvrzení platí pro $n = 2$, pak platí i pro $n = 3$ a tak dále.



Obrázek A.1: Důkaz indukcí lze přirovnat k efektu padajícího domina.

Z tohoto principu plyne, že tvrzení tedy platí pro všechna $n \in \mathbb{N}$ (viz obrázek A.1). Krok (ii) se nazývá *indukční krok* a předpoklad, že dokazované tvrzení platí pro nějaké $n = n_0$ se nazývá *indukční předpoklad*. Někdy se v důkazech indukcí pro upřesnění specifikuje, podle jaké proměnné dané tvrzení dokazujeme. V tomto případě bychom řekli *„indukcí podle $n$“*. (Inspirováno [6], str. 32.)
Tento postup vychází z tzv. *principu matematické indukce*, který lze zformulovat jako větu.

**Věta A.1.11** (Princip matematické indukce)**.** *Nechť pro každé $n \in \mathbb{N}$ je $\varphi_n$ libovolný výrok. Pokud platí*

*(i)* $\varphi_1$ *a*

*(ii)* $\forall k \in \mathbb{N} : \varphi_k \Rightarrow \varphi_{k+1}$,

*pak platí* $\forall n \in \mathbb{N} : \varphi_n$.

(Převzato z [8], str. 144.)
Tuto větu v různých textech lze najít i v jiných formulacích. Důkaz této věty však vyžaduje složitější znalosti a uvedeme si jej proto až později (viz (TODO: doplnit odkaz.)). Uveďme si ještě jeden příklad.

**Úmluva A.1.12.** Při aplikaci indukčního předpokladu se někdy píše zkratka *I. P.*, čehož se budeme držet v dalším textu.

**Tvrzení A.1.13.** *Pro každé přirozené $n \geq 5$ platí $2^n > n^2$.*

*Důkaz.* Tvrzení dokážeme indukcí podle $n$.

- Pro nejmenší hodnotu $n = 5$ dostáváme $2^5 = 32 > 5^2 = 25$, což jistě platí.

- Nyní dokážeme indukční krok. Předpokládejme, že tvrzení platí pro libovolné $n_0 \geq 5$; ukážeme platnost pro $n_0 + 1$:

$$2^{n_0+1} = 2^{n_0} \cdot 2 \overset{\text{I. P.}}{>} n_0^2 \cdot 2.$$

  Pro dokázání tvrzení nyní stačí ukázat, že $2n_0^2 > (n_0 + 1)^2$.

$$\begin{aligned} 2n_0^2 &= n_0^2 + n_0^2 > n_0^2 + 5n_0 = n_0^2 + 2n_0 + 3n_0 = n_0^2 + 2n_0 + 15 \\ &> n_0^2 + 2n_0 + 1 = (n_0 + 1)^2. \end{aligned}$$

  Celkově tedy dostáváme $2^{n_0+1} > (n_0 + 1)^2$.

Podle principu matematické indukce platí $\forall n \geq 5 : 2^n > n^2$, což jsme chtěli dokázat.

□

(Převzato z [8], str. 153.)

**Tvrzení A.1.14.** *Nechť $X$ je libovolná $n$-prvková množina. Pak $|\mathcal{P}(X)| = 2^n$.*

*Důkaz.* Postupujme indukcí podle mohutnosti $n$ množiny $X$. Pro $n = 0$ obsahuje potenční množina množiny $X$ pouze prázdnou množinu, tj. $|\mathcal{P}(\emptyset)| = 2^0 = 1$.

Předpokládejme, že tvrzení platí pro množinu o $n_0$ prvcích. Pro důkaz indukčního kroku mějme množinu $X$ o $n_0 + 1$. Vezměme libovolný prvek $x \in X$. Prvky potenční množiny $\mathcal{P}(X)$ si rozdělíme do množin $T$ a $T'$ takto:

- $T = \{Q \in \mathcal{P}(X) \mid x \in Q\}$ a
- $T' = \{Q \in \mathcal{P}(X) \mid x \notin Q\}$.

Tedy v $T$ se nachází všechny podmnožiny množiny $X$ obsahující prvek $x$ a v $T'$ všechny podmnožiny, které jej neobsahují. Z definice lze vidět, že $T$ a $T'$ jsou disjunktní, tj. $T \cap T' = \emptyset$ a tedy $X = T \cup T'$. Jaké jsou mohutnosti $T$ a $T'$? Množina $T'$ obsahuje všechny podmnožiny množiny $X \setminus \{x\}$ a tedy podle indukčního předpokladu má $2^{n_0}$ podmnožin, tj. $|\mathcal{P}(X \setminus \{x\})| = 2^{n_0}$.

Jak vypadají množiny obsažené v $T$? Uvažme libovolnou podmnožinu $A'$ množiny $X$, která neobsahuje prvek $x$. Taková množina musí být (z definice) prvkem množiny $T'$. Pokud nyní položíme množinu $A = A' \cup \{x\}$, získáme tak množinu obsahující prvek $x$ a tudíž $A \in T$. Naopak pokud bychom měli množinu $B$ obsahující prvek $x$, tj. $B \in A$, pak definováním $B' = B \setminus \{x\}$ získáme množinu z $T'$. To však znamená, že každé množině $A' \in T'$ odpovídá právě jedna množina $A \in T$.

Z toho plyne, že počet množin v $T$ je stejný[3] jako v $T'$, tj. $|T| = |T'|$, což podle již aplikovaného indukčního předpokladu znamená, že $|T| = 2^{n_0}$. Protože však množiny $T$ a $T'$ jsou disjunktní, pak celkový počet prvků je $2^{n_0} + 2^{n_0} = 2^{n_0+1}$, což jsme chtěli dokázat.

□

[3] Formálně vzato jsme sestrojili *bijekci* mezi množinami $T$ a $T'$, kde obrazem množiny $A \in T$ je $A \setminus \{x\} \in T'$. Termín je zaveden v sekci 3.5.