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

Zde bych rád poděkoval RNDr. Martinu Rmoutilovi, Ph.D. za jeho vstřícný přístup, cenné rady a množství času, které mi věnoval v době psaní této bakalářské práce. Dále patří velké poděkování Michaele Dvořákové za pomoc při korekci gramatiky a pravopisu a Martinu Kopeckému za poskytnutí grafické ilustrace domina v příloze. Též chci poděkovat své rodině za trpělivost a pomoc při psaní této práce.

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: Práce poskytuje vysvětlení základních konceptů z oblasti teorie množin se zaměřením především na studenty středních škol se zájmem o matematiku. Práce je členěna do celkem šesti kapitol. První kapitola poskytuje historický kontext, kde je vysvětlen vývoj pojmu „nekonečno“ a důvody pro vznik axiomatické teorie množin. Druhá kapitola připomíná základní pojmy z výrokové logiky a zjednodušeně představuje koncept predikátového počtu. Pozornost je hlavně věnována práci s kvantifikátory. Třetí kapitola se zabývá axiomy Zermelovy-Fraenkolovy teorie množin a základními poznatky z nich vyplývajících. Kapitola čtvrtá je samostatně věnována zavedení relací a souvisejícím termínům, především pak zobrazením a jejich vlastnostem. V páté kapitole je ukázán způsob zavedení přirozených čísel pomocí množin. Úvodem je stručně prezentován způsob zavedení pomocí Peanových axiomů. Dále jsou rozšířeny znalosti o relacích, je definována relace uspořádání společně s uspořádanou množinou a jsou dokázány některé základní vlastnosti přirozených čísel při popsaném zavedení. Poslední kapitola se věnuje problematice porovnávání nekonečných množin. Je zde vysvětlena myšlenka Hilbertova hotelu, porovnávání pomocí zobrazení a především je prezentováno užití Cantorovy diagonální metody. V závěru jsou zavedeny termíny spočetné a nespočetné množiny a je společně s důkazem zformulována Cantorova věta. Výklad je doprovázen ukázkovými příklady a též grafickými ilustracemi pro snadnější pochopení. Doplňující informace a složitější koncepty v obsažených tématech jsou rozvedeny v přílohách práce.

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: This thesis gives an explanation of the basic concepts of set theory, focusing primarily on high school students interested in mathematics. The text of the thesis is divided into six chapters. The first chapter provides a historical context, mainly explaining the development of the term „infinity“ and the reasons for the establishment of axiomatic set theory. The second chapter reminds the reader of propositional logic and gives a simplified explanation of predicate calculus. Main focus of this chapter is on the explanation of working with logical quantifiers. The third chapter deals with the Zermelo-Fraenkel set theory axioms and some basic properties about sets they imply. Chapter Four separately introduces relations and related terminology, especially mappings and their properties. The penultimate chapter shows how to establish natural numbers using sets. In its introductory part, it is concisely presented a method of such establishment by means of Peano axioms. Further on, the knowledge concerning relations are extended along with the definition of ordering and ordered sets, and some basic properties of natural numbers in context of the described establishment are proved. The last chapter is devoted to the problem of comparing infinite sets. The idea of Hilbert hotel, comparison of sets using mappings, and especially the use of Cantor's diagonal argument are explained. Finally, the terms countable and uncountable sets are introduced and Cantor's theorem is formulated together with its proof. The text is accompanied by examples and also graphical illustrations for easier understanding. Additional information and more complex concepts in the topics covered are developed in the appendices of the thesis.

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

Obsah

Seznam obrázků

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 učili např. 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 následující otázku: je více všech 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 se ve skutečnosti jedná o hlavní příčinu 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 způsoboval.

1.1 Potenciální versus aktuální nekonečno

Co je vlastně nekonečno? Čtenáři toto 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 můžeme na tuto skutečnost pohlížet? 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 se nebudeme zabývat tím, 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**. ([2], str. 104.) O tom se lze přesvědčit už ze samotných *Eukleidových axiomů*. K axiomatice čtenář bude mít možnost blíže nahlédnout v podsekci 1.2.4 a později je jí též věnována kapitola 3. Eukleidés právě z důvodu nemyslitelnosti aktuálního nekonečna mluvil o *přímce* jako o úsečce, kterou může libovolně prodlužovat, netvrdil, 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 sekci 4.3).

$$\begin{array}{ccccccc} 1, & 2, & 3, & \ldots, & n, & \ldots \\ \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \\ 1, & 4, & 9, & \ldots, & n^2, & \ldots \end{array}$$

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. Tvrdil tak, že **aktuální nekonečno** je sporné, a tedy nemůže existovat. ([2], str. 103-105.)

1.1.2 Grandiho řada

Dalším typickým problémem týkajícím 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 (stejné) 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 řadu 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:

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots + \frac{1}{2^{20}} = 0{,}9999990463256836.$$

Jak je vidět, částečné součty se postupně „blíží“ nejspíše číslu 1. Dávalo by tedy smysl prohlásit číslo 1 za součet 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 „−“ upravíme řadu na pravé straně takto:

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

Výraz v závorce na pravé straně je opět námi vyšetřovaná řada se součtem S, tedy z toho vyplývá

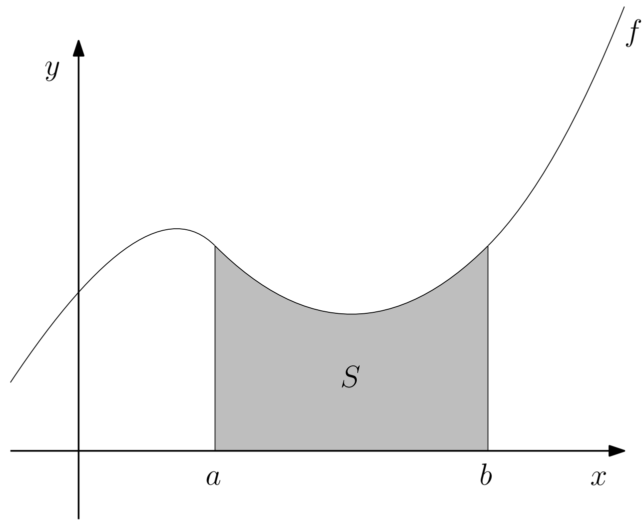
$$\begin{aligned} S &= 1 - S \\ S &= \frac{1}{2}. \end{aligned}$$

Toto je však také zarážející výsledek, neboť, jak jsme se sami přesvědčili, 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 mluvu o jzv. *infinitezimálním počtu.* Čtenář se s těmito pojmy již možná setkal, ačkoliv nemusí mít nutně představu o jejich přesném významu. Asi nejznámějším příkladem je integrální počet, specificky výpočet „obsahu plochy pod křivkou“.



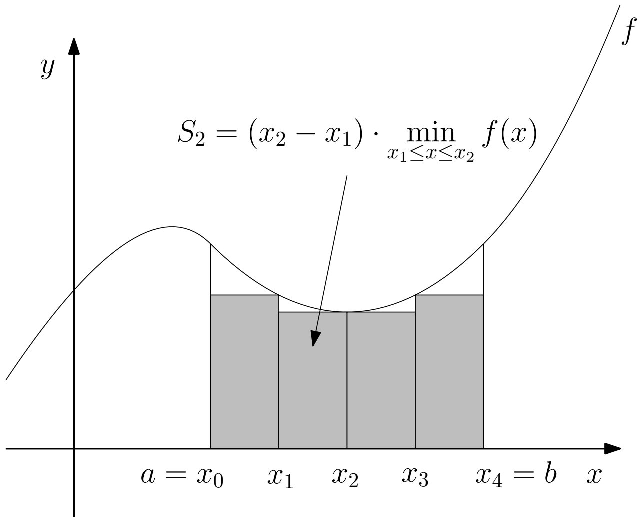
Obrázek 1.1: Příklad určitého integrálu funkce f na uzavřeném intervalu $\langle a,b \rangle$.

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 je ta 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 – obdélník. Pro začátek zkusíme plochu aproximovat pomocí čtyř obdélníků (viz obrázek 1.2).



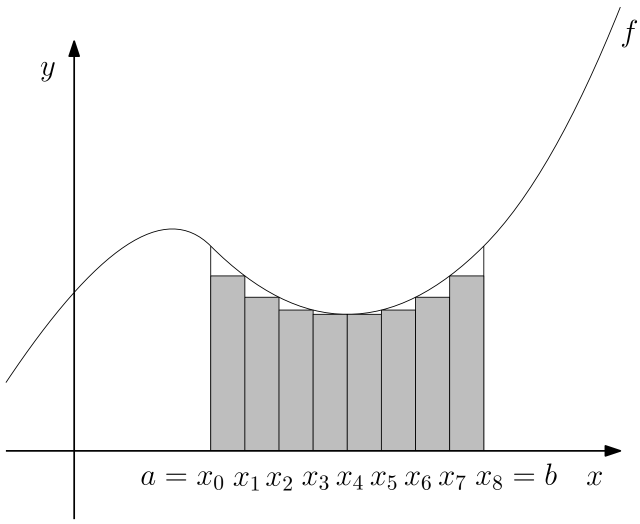
Obrázek 1.2: Aproximace plochy pod grafem funkce f na intervalu $\langle a,b\rangle$ pomocí 4 obdélníků.

Všechny čtyři 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[1] funkce f na intervalu $\langle x_{i-1}, x_i\rangle$. Rozdíl $x_i - x_{i-1}$ odpovídá šířce obdélníku a jeho výšce hodnota $\min_{x_{i-1} \le x \le x_i} f(x)$.

Pokud bychom si však interval $\langle a,b\rangle$ rozdělili ještě „jemněji“, není těžké vidět, že odhad by se zpřesnil (viz obrázek 1.3).



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

[1] Předpokládáme pro jednoduchost, že f je spojitá, takže nabývá svého minima na každém z daných intervalů.

Volbou stále „jemnějšího“ dělení intervalu $\langle a,b \rangle$ se náš odhad bude zpřesňovat. Budeme-li mít tedy plochu aproximovanou n obdélníky, pak[2]

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

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 $\min\limits_{x_{n-1} \leq x \leq x_n} f(x)$ 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

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

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

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

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 šířka obdélníků, která se kvůli „zjemňování“ dělení postupně zmenšovala.)

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 matematik Gottfried Wilhelm Leibniz (1646-1716) a fyzik 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*[3].

Problémy v matematické analýze se začaly odstraňovat až na počátku 19. století, kdy významnou roli sehrál ve dvacátých letech Augustin Louis Cauchy zavedením limity. Její formální definici však podal později Karl Weierstrass. Ta pracovala opět s potenciálním nekonečnem. ([2], str. 105-106.)

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

[3]První krize matematiky nastala v dobách antického Řecka a souvisela s objevem iracionálních čísel.

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 Bolzano[4] (1781-1848). Byl jedním z matematiků, kteří prosazovali existenci aktuálního nekonečna, o čemž později píše i ve svém díle *Paradoxy nekonečna*[5] (v německém originále *Paradoxien des Unendlichen*). Bolzanovo dílo však není 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 myslitelé dopouštějí při úvahách o nekonečnu. Je nutné však dodat, že ačkoliv svými úvahami byl Bolzano blízko úvahám, s nimiž dnes v teorii množin pracujeme, přesto 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 1.1.1 o Galileově úvaze), neznamená to nutně, že mají stejnou mohutnost (blíže nahlédneme v kapitole 6). 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 A, pak jistě neplatí ani B. Avšak zněním 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

[4]Ačkoliv byl B. Bolzano Čech, publikoval své práce v němčině a latině.

[5]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).

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 naším 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**.[3]

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 německému matematikovi Georgu Cantorovi (1845-1918), který učinil 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. 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, kde 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.

Cantorova teorie byla ve své době mnohými neuznávána a velmi znevažována, což mu velmi ztížilo publikační činnost. 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 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? Jistě není, taková množina tedy **není prvkem sebe sama**.
- Mějme množinu všech možných ideí. Je taková množina sama ideou? Ano, 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, jež samy sebe neobsahují.

Symbolicky bychom množinu S zapsali

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

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 definované množiny S, je tato množina sama sobě prvkem?

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.

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 paradoxů 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]. Zajímavostí a kontroverzí jeho důkazu byl fakt, že při něm 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 paradoxů. Objevují se dva rozdílné přístupy, přičemž prvním z nich byla tzv. *teorie typů*[9] a druhým *axiomatická výstavba.*

---

[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 π nebo Eulerovo číslo e).

[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.

1.2.3 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. *axiomy* 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 rovinnou 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 axiom, 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 [4]):

- *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:

(E1) *Budiž úkolem od kteréhokoliv bodu ke kterémukoliv bodu vésti přímku.*

(E2) *A přímku omezenou nepřetržitě rovně prodloužiti.*

(E3) *A z jakéhokoli středu a jakýmkoli poloměrem narýsovati kruh.*

(E4) *A že všecky pravé úhly sobě rovny jsou.*

(E5) *A když přímka protínajíc dvě přímky tvoří na téže straně (přilehlé) úhly menší dvou pravých, ty dvě přímky prodlouženy jsouce do nekonečna že se sbíhají na té straně, kde jsou úhly menších dvou pravých.*

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 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 axiomů nelze odvodit ze zbylých axiomů);
- *úplnost* (tzn. zdali je dána taková soustava axiomů, abychom každý výrok mohli dokázat, nebo vyvrátit (tj. dokázat jeho negaci));
- *bezespornost* (tzn. zdali není možné z daných axiomů odvodit výrok a současně jeho negaci).

Čtenáře možná napadne, že pokud jde o nezávislost, jedná se v podstatě jen o „vadu na kráse“, neboť pokud nějaký axiom 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.

1.2.4 Teorie množin v současnosti

První úspěšnou teorii množin axiomaticky vybudoval v letech 1904–1908 německý matematik Ernst Zermelo (1871-1953), které se budeme v tomto textu dále věnovat. Základní Zermelovou myšlenkou při budování jeho teorie bylo, že ne každý souhrn objektů je možné považovat za množinu (blíže si jednotlivé axiomy vysvětlíme v kapitole 3). Pojmy **množina** a **býti prvkem** jsou zde považovány za primitivní (nedefinované) pojmy, s nimiž se dále pracuje. Zermelovu teorii později upravil izraelský matematik Adolf Abraham Fraenkel (1891-1965), čímž vznikla tzv. *Zermelova-Fraenkelova teorie množin*. Dodnes se jedná o nejrozšířenější variantu.

Později byla vytvořena 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 zjistit, že 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 výrazné a neodstranitelné omezení metod.

Kapitola 2

Logika

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. I přesto však považuji zmínku o nich za nezbytnou, neboť na těchto pojmech budeme dále stavět. Posléze se dostaneme k kvantifikátorům, které budeme dále využívat, neboť nám umožní zápisy některých složitějších výroků, a též v základním rozsahu vysvětlíme predikátový počet.

2.1 Výroková logika

Tato část je čtenáři pravděpodobně již zčásti 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* (tj. proměnných, které mohou nabývat pravdivostních hodnot 0, nebo 1) budeme používat velká písmena latinské abecedy A,B, ...,Y,Z, případně opatřená 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 pokud 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 k 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".

Úmluva 2.1.2 (Abeceda pro výrokové formule)**.** Pro označení výrokových formulí budeme používat malá písmena řecké abecedy, tj. α,β,$\gamma, \ldots$, případně opatřená indexy.

Pro výroky zavádíme následující terminologii.

- *Výrokovou formulí* nebo též *logickou formulí* nazveme výrok obsahující libovolný počet výrokových proměnných a logických spojek.
- Speciálně, pokud výrok neobsahuje žádnou logickou spojku, nazýváme jej nazýváme *atomickým*, resp. *atomickou formulí*.

Tento popis však nelze považovat za definici, neboť je zde pochopitelně řada nepřesností. Např. $A\neg$ nebo $AB \Rightarrow \wedge C$ určitě nejsou korektní výrokové formule. Podrobnější informace k tomuto se čtenář může dočíst v příloze B.

Poznámka 2.1.3. Občas budeme v této sekci zkráceně psát pouze *formule*. Později se zmíníme i o tzv. *predikátových formulích*, nicméně z kontextu vždy bude zřejmé, v jakém smyslu daný termín používáme.

Úmluva 2.1.4 („Rovnost“ výrokových formulí)**.** Uvažujme, že máme libovolné výrokové formule φ a ψ. Pokud φ a ψ jsou stejné výrokové formule, 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

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

pak můžeme psát, že $\varphi_2 \sim \varphi_3$, ale nikoliv $\varphi_1 \sim \varphi_2$, byť φ_1 a φ_2 mají shodnou tabulku pravdivostních hodnot.

Z příkladu výše lze však vidět poměrně nadměrné používání závorek. Ačkoliv bychom tak jednoznačně určili pořadí jednotlivých logických operací, existuje o něco příjemnější přístup. Pro zjednodušení zápisu dalších výrokových formulí se proto budeme držet následující úmluvy 2.1.5.

Úmluva 2.1.5 (Pořadí logických operací)**.** Budeme dodržovat následující 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 2.1.6. Zjednodušení některých formulí při aplikaci zavedeného pořadí logických operací v úmluvě 2.1.5.

(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 si připomeňme asi nejznámější postup pro vyhodnocování logických formulí, a to sice *tabulkovou metodu*. Její myšlenkou bylo rozdělit danou výrokovou formuli postupně na dílčí formule a takto postupovat i u daných dílčích formulí. Tímto způsobem nakonec dojdeme 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 2.1.7 (Logická ekvivalence výrokových formulí)**.** Mějme výrokové formule φ a ψ. Řekneme, že φ a ψ jsou *logicky ekvivalentní*, což zapisujeme jako $\varphi \equiv \psi$, pokud je formule $\varphi \Leftrightarrow \psi$ pro všechny pravdivostní hodnoty výrokových proměnných obsažených ve φ a ψ 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.

Jaký je rozdíl mezi $\equiv$ a $\Leftrightarrow$? Formálně vzato bychom mohli mezi formule jednoduše vkládat ekvivalenci, avšak pak by se nám tato logická spojka mohla plést s ekvivalencemi, které jsou součástí φ a ψ.

Příklad 2.1.8. Mějme formuli

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

Pro jaké pravdivostní hodnoty výroků A a B je formule φ pravdivá?

Řešení. Postupujme způsobem popsaným výše, tj. rozdělme nejdříve danou formuli na dílčí formule. V tomto případě dílčími formulemi φ 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 φ_1 obsahuje atomický výrok A a formuli $\neg B$ spojené konjunkcí $\wedge$. Označme tedy ještě

$$\varphi_3 \sim \neg B$$

φ_3 již obsahuje pouze atomický výrok B v negaci $\neg$.

Podívejme se nyní na dílčí formuli φ_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 φ_1, φ_2, φ_3 a φ

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

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 2.1.9. 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 ψ pravdivá?

Řešení. V tuto chvíli bychom aplikací metody použití v příkladu 2.1.8 museli vyšetřit pravdivostní hodnotu formule ψ 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 ψ 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 ψ 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 ψ zjednoduší takto

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

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 ψ 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 ψ (1. část).

Tento typ formulí je poměrně významný, a proto pro ně zavádíme speciální pojmenování v definici 2.1.10.

Definice 2.1.10 (Tautologie)**.** Výrokovou formuli φ nazveme *tautologií*, pokud $\varphi \equiv 1$. To znamená, že formule φ je pravdivá pro všechny pravdivostní hodnoty výrokových proměnných.

Některé tautologie jsme využili již pri řešení příkladu 2.1.9. Uveďme si zde ještě několik dalších významných příkladů.

A	B	C	$(A \Leftrightarrow B) \wedge (C \vee \neg C)$	ψ
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 ψ (2. část).

Věta 2.1.11 (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*[3]

(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 (viz příloha A).

[1] Česky *pravidlo vynětí*
[2] Česky *popírání důsledku*
[3] Česky *důkaz sporem*

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 konjunkci více než 2 milionů výroků, např.

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

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 prohlášení 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 *obecný*), pro který používáme symbol „$\forall$".

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

$$\forall x\Big(P(x) \Rightarrow Z(x) \wedge M(x)\Big), \tag{2.1}$$

nebo podle (xii) ve větě 2.1.11 o tautologiích

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

Takový výrok bychom četli: „**pro všechna** x **platí**, že pokud platí $P(x)$, pak platí $Z(x)$ a zároveň $M(x)$". Ve výrazu (2.1) 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 kdybychom 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. To znamená, že jedna z dílčích formulí musí být pravdivá:

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

I zde však máme kratší alternativu 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:

$$\exists x \Big(P(x) \wedge Z(x) \wedge M(x) \Big). \tag{2.2}$$

Přirozeně se zde nabízí otázka, proč jen nenahradit univerzální kvantifikátor ve výrazu (2.1) za existenční. Pokud bychom napsali

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

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 výrok (2.2) byl nepravdivý, ale výrok (2.3) by pravdivý byl.

2.2.1 Primitivní predikáty

Vzpomeneme-li si na předešlou sekci 2.1 věnovanou výrokové logice, tak „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.

Opusťme příklad s obyvateli Prahy a zkusme takto zapsat např. 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 je zřejmý jeho význam. 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 „nejjednodušších“ 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[4] predikátu). Po dosazení konkrétních hodnot dané proměnné již obdržíme nějaký atomický (nedělitelný) výrok v dané teorii.

[4]Lze použít i jiné proměnné.

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 s tímto vystačíme.

Příklad 2.2.1. Ukázky některých predikátových formulí:

- $x > y$,
- $\forall x(x = 0 \vee x < 0 \vee x > 0)$,
- $\forall x\big(2 \mid x \Rightarrow \exists k(x = 2k)\big)$[5],
- $\exists k\big(k \in \mathbb{N} \wedge \exists x(x = 2k + 1)\big)$.

2.2.2 Jiné zápisy formulí s kvantifikátory

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

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

kde φ a ψ jsou nějaké predikátové formule obsahující[6] proměnnou x. 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“.

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

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

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“. Může se stát, že dvě nebo více proměnných jsou součástí stejného predikátu u stejného typu kvantifikátoru. Kupříkladu formuli

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

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

[6] Formálně vzato, formule φ a ψ nemusí v tomto zápisu obsahovat proměnnou x, nicméně pak je kvantifikátor redundantní.

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 však třeba 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 tak je 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) zmíněná ve větě 2.1.11.

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

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, přičemž písmenem P označme **množinu** obyvatel Prahy (tedy každý obyvatel x z množiny P automaticky splňuje výrok $P(x)$):

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

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 je v Praze obyvatel, který nemá modré oči, pak naše tvrzení neplatí. Zdá se tedy, že by mohlo platit

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

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 výrok $M(x)$. Skutečně, toto je negace původního výroku.

Podobně tomu bude i pro náš původní výrok s konjunkcí a výroky $P(x)$ a $M(x)$:

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

Tj. existuje x takové, že x je obyvatelem Prahy a platí, že nemá zelené vlasy nebo nemá modré oči. Užitím tautologie (xii) a následně De Morganova pravidla pro negaci konjunkce (i) ve větě 2.1.11 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 modrýma očima, 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 znegujeme dílčí formuli φ, 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

$$\exists x \in \mathbb{R}, \forall y \in \mathbb{R} : \neg(y > x)$$

neboli

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

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. Na to jsme měli možnost nahlédnout v sekci 1.2.4. Jednou z variant axiomatické teorie množin je tzv. **Zermelova-Fraenkelova teorie množin**, která je v 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 v různých textech se může systém axiomů, s nimiž se pracuje, jemně lišit. Odlišné přístupy v této axiomatické teorii lze krásně vidět např. v knihách [5] a [6].

Než začneme s dalším vysvětlováním, je nutné mít na paměti, že množiny jsou pro nás **jedinými** základními objekty, tzn. prvky množin mohou být opět pouze množiny a nic jiného nepřipouštíme. Tedy různé matematické objekty, zejména čísla, vybudujeme pouze pomocí množin. Jak později uvidíme, skutečně si s tím vystačíme.

Pro začátek si zde přehledně vypišme všechny axiomy ZF, s nimiž budeme pracovat, a v dalších sekcích si některé detailněji popíšeme. **Schéma axiomů nahrazení** a **axiom fundovanosti** zde nebudeme probírat, nicméně čtenář si jejich podrobnější vysvětlení může přečíst v příloze C.

Úmluva 3.0.1. Množiny budeme v dalším textu podle potřeby značit velkými i malými písmeny latinské abecedy, tj. $a,b,c,\dots,x,y,z,A,B,C,\dots,X,Y,Z$.

Axiomy Zermelovy-Fraenkelovy teorie množin:

(ZF1) *Axiom existence.*

$$\exists x\,(x = x)$$

(ZF2) *Axiom extenzionality.*

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

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

(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.*

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

(ZF6) *Axiom sumy.*

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

(ZF7) *Axiom nekonečna.*

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

(ZF8) *Schéma axiomů nahrazení.*

$$\begin{aligned} &\forall u\,\forall v\,\forall v'\,(\varphi(u,v) \wedge \varphi(u,v') \Rightarrow v = v') \Rightarrow \\ &\Rightarrow \forall a\,\exists z\,\forall x\,\Big(x \in z \Leftrightarrow \exists y\,(y \in a\ \wedge \varphi(y,x))\Big), \end{aligned}$$

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

(ZF9) *Axiom fundovanosti.*

$$\forall a\,\Big(a \neq \emptyset \Rightarrow \exists x\,(x \in a\ \wedge x \cap a = \emptyset)\Big)$$

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 $x \in y$ podobně jako zbytek axiomů.

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

[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 *axiom of choice*

3.1 Axiomy 1 až 3

3.1.1 Axiom existence

$$\exists x\,(x = x)$$

Formulace axiomu (ZF1) 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 vzájemně nahraditelné (z platnosti jednoho plyne platnost druhého a naopak).

Množiny zde budeme standardně značit pomocí složených závorek $\{,\}$, mezi něž píšeme jednotlivé prvky, které množina obsahuje. Např.

$$\{a,b,c\}\,,\ \{x\} \quad \text{atp.}$$

Později si uvedeme ještě jiné způsoby zápisu.

3.1.2 Axiom extenzionality

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

(ZF2) 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

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

Existence množiny garantovaná axiomem existence (ZF1) nám bohužel nezaručuje existenci žádné **konkrétní** množiny. Pouze zaručuje, že množina, z níž uvažujeme množiny v ostatních axiomech je neprázdná. Axiom dvojice nám zaručuje, že pokud máme dvě (ne nutně různé) množiny a a b, pak i $\{a,b\}$ je množina (resp. existuje množina obsahující prvky a a b). Dále, když máme např. množiny

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

Není těžké se přesvědčit z axiomu extenzionality (ZF2), 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 množinu 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. Nechť jsou dány dvě různé množiny y a y', pro které platí

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

Z toho plyne

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

a z axiomu extenzionality (ZF2) vyplývá $y = y'$. □

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 (Dvojice)**.** Nechť x a y jsou libovolné 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 známý v jiných podobách; typicky např. **vektory** využívané v analytické geometrii. Ty se běžně značí (x,y). Důležitou vlastností tohoto objektu byl pro nás 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 (ZF2) 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 $\{x,y\}$.

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 jedinečné neuspořádané dvojice $\{x,y\}$ a $\{x\}$[4]. Z toho dostáváme, že t a t' mají stejné prvky a podle axiomu extenzionality (ZF2) platí $t = t'$. □

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.

Důkaz. Tvrzení dokážeme opakovanou aplikací axiomu (ZF2). 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 (ZF2) musí mít množin na pravé a levé straně stejné prvky. Rozdělme si tento důkaz na dva případy.

(a) $\{a\} = \{x\}$. Pak opět podle (ZF2) platí $a = x$. Rozlišme dále případy, když $a = b$ a když $a \neq b$.

- $a = b$. Pak
$$\{\{a\}, \{a,b\}\} = \{\{a\}, \{a,a\}\} \stackrel{\text{(ZF2)}}{=} \{\{a\}, \{a\}\} \stackrel{\text{(ZF2)}}{=} \{\{a\}\}.$$
Musí tedy platit $\{\{a\}\} = \{\{x\}, \{x,y\}\}$. Opět z (ZF2) vyplývá $\{x,y\} = \{a\}$, tj. $x = a$ a $y = a$. Celkově dostáváme $a = b = x = y$ a tedy $a = x$ a $b = y$, jak jsme chtěli.
- $a \neq b$. V takovém případě nemůže platit, že $\{a,b\} = \{a\}$ (zkuste si rozmyslet podle (ZF2)), 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 (ZF2) pak platí $x = a$ a $y = a$, tedy $x = y$. Stejným postupem tak dostáváme
$$\{\{x\}, \{x,y\}\} = \{\{x\}, \{x,x\}\} \stackrel{\text{(ZF2)}}{=} \{\{x\}, \{x\}\} \stackrel{\text{(ZF2)}}{=} \{\{x\}\}.$$
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. □

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

3.2 Axiomy 4 až 6

První trojice axiomů se zdá být dobrým základem, avšak stále je zde hodně typů množin, jejichž existence z nich neplyne. Trochu „podvodným“ způsobem jsme 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 totiž zjistíme, že čistě z axiomů (ZF2), (ZF1) 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 jako $\{a,b,c\}$. 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 s jistou vlastností. 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, který je zároveň prvek a, splňuje určitou formuli $\varphi(x)$ (ta reprezentuje danou vlastnost). Podle axiomu extenzionality (ZF2) je množina v (3.1) jednoznačně určena. Čtenář je nejspíše zvyklý množiny všech objektů s jistou vlastností zapisovat např. jako

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

Obecněji množinu z (3.1) zapíšeme výrazem

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

Toto schéma axiomů má následující důsledek.

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

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, zvolíme-li za $\varphi(x)$ formuli $x \neq x$. Z axiomu extenzionality je vidět, že takovou vlastnost nesplňuje žádná množina, neboť každá množina má stejné prvky jako ona sama. Podle schématu axiomů vydělení je

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

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.

Nyní můžeme definovat některé základní operace s množinami a pomocí schématu axiomů vydělení jsme schopni dokázat existenci výsledné množiny.

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

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*. Píšeme $b \subseteq a$, resp. $b \subset a$[6].

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 plyne z následujícího lemmatu.

Lemma 3.2.7. *Platí:*

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

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

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

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

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

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

kde φ je libovolná formule, je vždy pravdivý[7]. Pokud není čtenáři jasné, že α platí, pak snad bude jasnější se přesvědčit, že opačné tvrzení $\neg\alpha$ neplatí, tj.

$$\exists x \in \emptyset : \neg\varphi$$

(tzn. nutně platí α).

(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] V jiných textech se symbolem „$\subset$" rozumí podmnožina. Toto značení nebývá zcela jednotné.

[7] Analogicky výroky s existenčním kvantifikátorem, kde x uvažujeme z prázdné množiny, jsou vždy nepravdivé.

3.2.2 Axiom potence

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

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*) $\mathcal{P}(a)$[8] 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 podle (ii)).

3.2.3 Axiom sumy

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

Ke každé množině a existuje (podle axiomu extenzionality jediná) množina y obsahující **právě** takové prvky (připomeňme, že v ZF jsou prvky zase množiny), které jsou prvkem některého z prvků (tj. množin) množiny a. To znamená, existuje množina obsahující prvky množin v ní obsažených. 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), 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 (ZF2), víme, že pro množiny a a b existuje jediná dvojice $\{a,b\}$ a pro množinu c existuje dvojice $\{c,c\} \overset{\text{(ZF2)}}{=} \{c\}$. Opět podle axiomu dvojice pak je i množinou

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

[8] 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**. Celkově o sjednocení, průniku a rozdílu dvou množin lze ukázat řadu vlastností. 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*:

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

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.

Poznatek o distributivitě sjednocení a průniku můžeme zobecnit užitím velkých operátorů $\bigcup$, $\bigcap$ jako

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

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 s velkou škálou množin, přesto by bylo stále ambiciózní hovořit např. o přirozených, racionálních či reálných číslech jako o množinách v kontextu ZF. Axiom dvojice nebo axiomy sumy nám zatím dávají možnost mluvit pouze o konečných množinách, byť libovolně velkých. Jako důvod bychom mohli ještě udat, 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 kapitola 5), 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 $x \cup \{x\}$. Specificky, množina $\emptyset$ náleží y, tzn. i $\emptyset \cup \{\emptyset\}$ je prvkem y, a protože $\emptyset \cup \{\emptyset\} \in y$, pak i $(\emptyset \cup \{\emptyset\} \in y) \cup \{\emptyset \cup \{\emptyset\} \in y\} \in y$. Tento výčet prvků zjevně pokračuje do nekonečna. 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 libovolně velkých množin, které jsme mohli libovolně „zvětšovat“ (tj. potenciální nekonečno), zatímco axiom nekonečna nám zaručuje existenci **aktuálně** nekonečné množiny (bez udání způsobu, jak takovou množinu „sestavit“ z již existujících množin).

Kapitola 4

Relace

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.

4.1 Kartézský součin

Definice 4.1.1 (Kartézský součin množin)**.** Nechť A,B jsou libovolné množiny. Pak *kartézský součin* množin A a B značíme $A \times B$ a definujeme jej jako

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

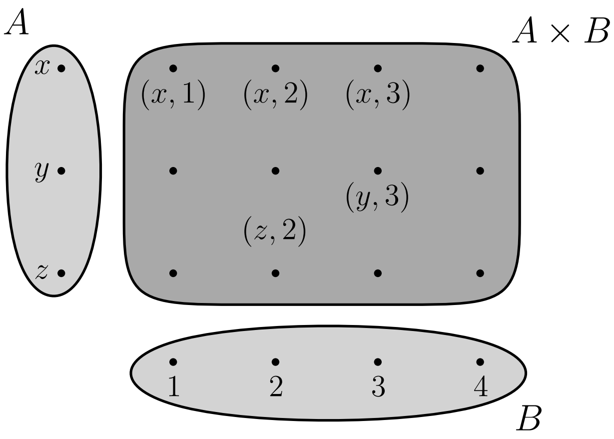
Slovně řečeno, kartézský součin $A \times B$ je množina všech uspořádaných dvojic (x,y), kde $x \in A$ a $y \in B$. Takový objekt je podle axiomu dvojice (ZF3) a axiomu sumy (ZF6) množinou v ZF.

Příklad 4.1.2. Mějme množiny $A = \{x,y,z\}$ a $B = \{1,2,3,4\}$. Vypočítejte kartézský součin $A \times B$.

Řešení. Stačí postupovat podle definice, tj.

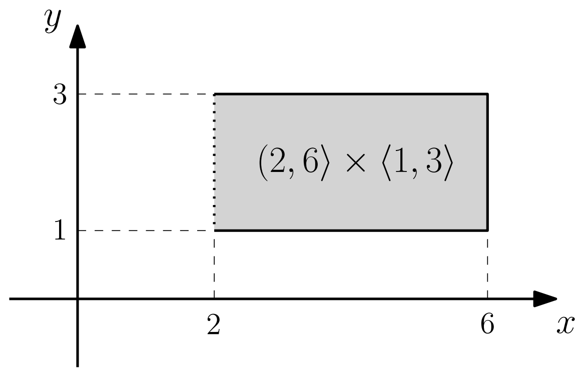
$$\begin{aligned} A \times B = &\{(x,1),(x,2),(x,3),(x,4),(y,1),(y,2),(y,3),\\ &(y,4),(z,1),(z,2),(z,3),(z,4)\}. \end{aligned}$$

Kartézský součin množin A, B lze interpretovat i graficky (viz obrázek 4.1). $\square$



Obrázek 4.1: Grafické znázornění kartézského součinu z příkladu 4.1.2 (Převato a upraveno z **??**, str. 36).

Pokud budeme však pracovat např. s intervaly reálných čísel, pak již nemůžeme takto kartézský součin znázornit, ale můžeme reprezentovat uspořádané dvojice jako body v rovině. Např. pro intervaly v $\mathbb{R}$ $A = (2, 6\rangle$ a $B = \langle 1{,}3\rangle$ je grafické znázornění na obrázku 4.2.



Obrázek 4.2: Grafické znázornění kartézského součinu intervalů $(2, 6\rangle$ a $\langle 1{,}3\rangle$.

Podobně jako v případě součinu čísel, i zde můžeme kartézské 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 komutativní zákon:

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

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

Podle definice uspořádané dvojice 3.1.3, kterou jsme si uvedli v minulé kapitole 3 v sekci 3.1, by mělo platit

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

protože $((a,b),c) \neq (a,(b,c))$. Avšak dávalo by smysl např. chápat prvky $\mathbb{R}^3$ jako spořádané trojice podobně (trojice souřadnic x,y,z), jako tomu je u $\mathbb{R}^2$. Tyto objekty tedy ztotožníme úmluvou.

Úmluva 4.1.3. Uspořádané dvojice $((a,b),c)$ a $(a,(b,c))$ ztotožňujeme se symbolem (a,b,c) (tj. uspořádanou trojicí). Obecně uspořádané dvojice

$$((x_1,x_2,\ldots,x_{n-1}),x_n) \quad \text{a} \quad (x_1,(x_2,x_3,\ldots,x_n))$$

ztotožňujeme se symbolem $(x_1,x_2,\ldots,x_n)$ (tj. uspořádanou n-ticí). Tzn. můžeme psát

$$((x_1,x_2,\ldots,x_{n-1}),x_n) = (x_1,(x_2,x_3,\ldots,x_n)) = (x_1,x_2,\ldots,x_n).$$

Dle této úmluvy tak platí

$$(A \times B) \times C = A \times (B \times C)$$

(zkuste si rozmyslet).

Příklad 4.1.4. Nechť je dána množina $X = \{a,b\}$. Vypočítejte X^3.

Řešení. Kartézský součin X^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

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

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

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

□

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

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

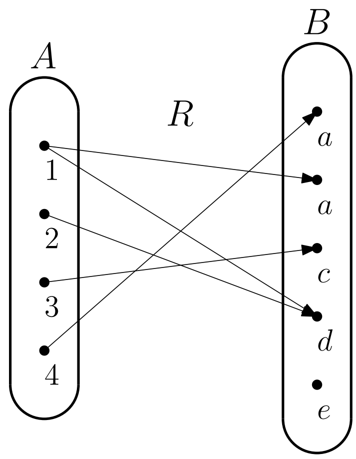
To však v řeči matematiky není nic jiného, než uspořádaná dvojice prvků. K tomu se nám bude hodit již zavedený kartézský součin.

Definice 4.2.1 (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.

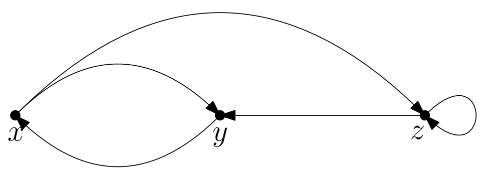
Úmluva 4.2.2. Pro značení relací budeme používat velká písmena latinské abecedy $A,B,C,\ldots,X,Y,Z$.

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 4.5.



Obrázek 4.3: Grafické znázornění relace R mezi množinami A a B.

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 4.4.



Obrázek 4.4: Grafické znázornění relace S na množině C.

Jako poslední si ještě zmíníme tzv. *skládání relací.*

Definice 4.2.3 (Složení relací)**.** Nechť X,Y,Z jsou libovolné množiny, $R \subseteq X \times Y$ a $S \subseteq Y \times Z$. Relace $T \subseteq X \times Z$ je složení relací R a S, pokud

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

Složení relací R a S značíme $S \circ R$, tzn. $T = S \circ R$. (Všimněte si pořadí zápisu!)

Příklad 4.2.4. Mějme množiny $A = \{a,b,c\}$, $B = \{x,y,z\}$ a $C = \{i,j,k,l\}$. Na nich definujme relace

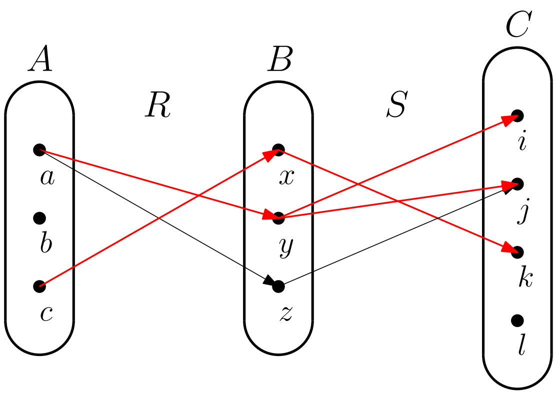
$$R = \{(a,z),(a,y),(c,x)\} \subseteq A \times B \quad \text{a} \quad S = \{(x,k),(y,i),(y,j),(z,j)\} \subseteq B \times C.$$

Určete $T = S \circ R$.

Řešení. Postupujme podle definice 4.2.3 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 $t_3 \in C$.

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

Tedy $T = \{(a,i),(a,j),(c,k)\}$. □



Obrázek 4.5: Grafické znázornění relace složení relací R a S z příkladu 4.2.4.

Podívejme se ještě na jeden příklad:

Příklad 4.2.5. 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 $T = S \circ R$.

$$\begin{aligned} xRx \wedge xSz &\Rightarrow xTz \\ yRz \wedge zSy &\Rightarrow yTy \end{aligned}$$

Tzn. $T = \{(x,z),(y,y)\}$. Nyní analogicky pro T'.

$$zSy \wedge yRz \Rightarrow zTz$$

Tím získáváme $T' = \{(z,z)\}$. □

Z příkladu 4.2.5 lze vidět, že skládání relací není komutativní a tedy záleží na pořadí.
(Sekce inspirována knihou [7], str. 34-39.)

4.3 Zobrazení

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

4.3.1 Zavedení a související pojmy

Definice 4.3.1 (Zobrazení)**.** *Zobrazením 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 4.3.2. Zobrazení budeme obvykle 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 X do Y zapisujeme jako

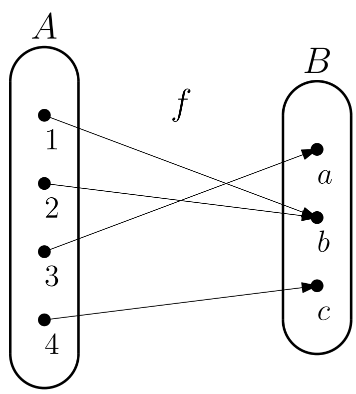
$$f : X \to Y$$

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

$$f : x \mapsto y.$$

Čtenářovi je nejspíše známější vyjádření této skutečnosti pomocí zápisu $f(x)$ (jako u funkcí), tj. prvku $x \in X$ je přiřazen prvek $f(x)$ $(= y)$ z množiny Y. Jaký je tedy rozdíl mezi **funkcí** a **zobrazením**? Ve skutečnosti toto nene v matematice jednotné. V určitých odvětvích se tyto termíny považují za synonyma a jinde se zase 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 4.6.



Obrázek 4.6: Grafické znázornění zobrazení $f = \{(1,b),(2,b),(3,a),(4,c)\}$.

U zobrazení $f : X \to Y$, kde $f : x \mapsto y$, se

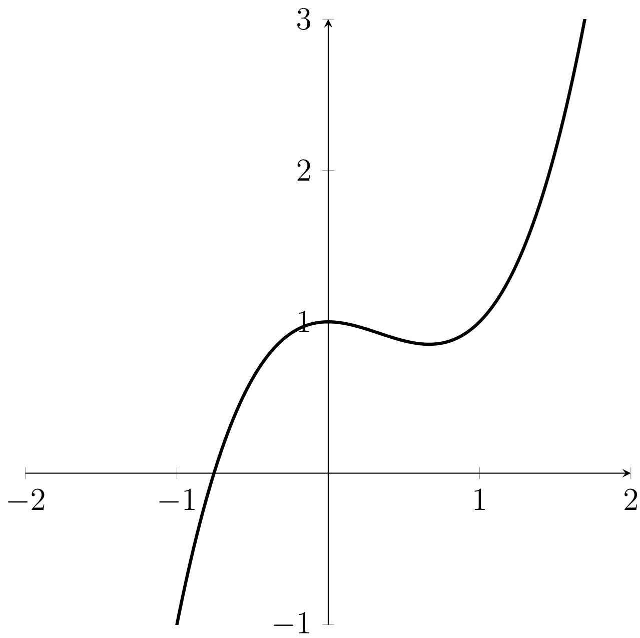
- x nazývá *vzor* prvku y a
- y se nazývá *obraz* prvku x nebo také *hodnota zobrazení f v bodě x.*

Množinu X nazýváme *množina vzorů.* U funkcí je zvykem tuto množinu nazývat *definiční obor.*

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

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

Obraz $f(A)$ libovolné množiny $A \subseteq X$ je vždy podmnožinou Y. Speciálně, obraz $f(X)$ množiny X se u funkcí nazývá *obor hodnot.* 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 $f(x) = x^3 - x^2 + 1$. Takto zadanou funkci jsme znázorňovali pomocí *grafu* (viz 4.7).



Obrázek 4.7: Graf funkce $f : \mathbb{R} \to \mathbb{R}$, kde $f(x) = x^3 - x^2 + 1$.

Tento způsob proto budeme používat i u zobrazení (tedy nejen u funkcí).

4.3.2 Druhy zobrazení

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

Definice 4.3.3 (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 tedy platí:

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

Definice 4.3.4 (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*[1] (též *surjektivní*[2] 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 4.3.5. Ukázky některých zobrazení a jejich klasifikace podle 4.3.4.

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

(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 $f_3 : \mathbb{R} \to \langle 0,\infty)$, kde $f_3(x) = x^2$, je *na*, ale není *prosté.*

(iv) Zobrazení $f_4 : \mathbb{R} \to \langle 0,\infty)$, kde $f_4(x) = x^2 + 1$, není *prosté* ani *na.*

(v) Zobrazení $f_5 : \mathbb{R} \to (0,\infty)$, 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* (pro libovolnou množinu A).

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

(Inspirováno [8], str. 10.)

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 4.3.6. Zápis $f\Big((x_1,x_2,\ldots,x_n)\Big)$ budeme jednoduše 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 4.3.7).

Definice 4.3.7 (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.

U zobrazení a jejich skládání můžeme pozorovat jisté závislosti. Jejich důkazy jsou triviální a plynou přímo z definice, ale přesto si je zde uvedeme.

[1]Obšírněji f je zobrazení X *na* Y (nikoliv *do* Y), pokud platí uvedený výrok.

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

Tvrzení 4.3.8 (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.

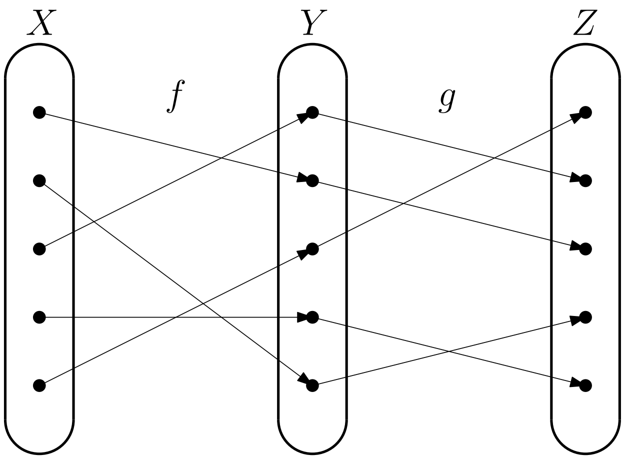
(iii) jsou-li f,g bijekce, je i $g \circ f$ bijekce.

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

(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 4.8.



Obrázek 4.8: Příklad složení bijekcí f a g.

(Sekce inspirována [7], str. 39-43.)

Kapitola 5

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 školy, lze bez problému vnímat jako „pouhé“ množiny, splňující určité požadavky.

Jak ale reprezentovat pomocí množin čísla? Takto se jedná o dosti složitou otázku, neboť číselných oborů máme hned několik: přirozená čísla, racionální čísla, reálná čísla a jiné další. Je 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* $\mathbb{N}$, která jsou pro ostatní číselné obory základním stavebním kamenem (jejich konstrukce je prováděna právě na základě přirozených čísel $\mathbb{N}$). Pokud jde o budování např. racionálních čísel $\mathbb{Q}$ či reálných čísel $\mathbb{R}$, velmi pěkně je toto popsáno v knize [6] (str. 8-32), z níž je ostatně v dalších odstavcích čerpáno.

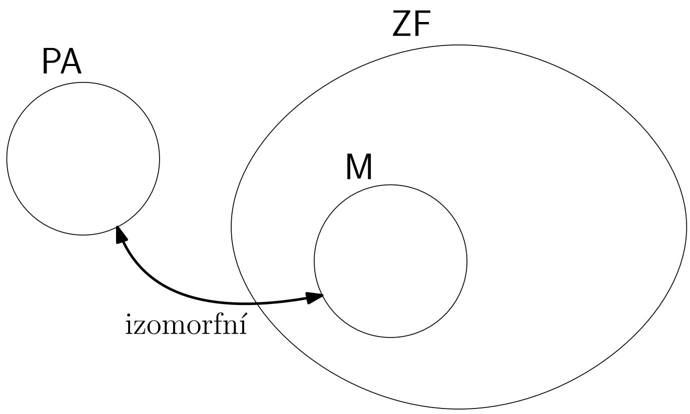
5.1 Peanovy axiomy

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

Zde si dovolím čtenáře upozornit, že v dalším výkladu této sekce se budeme pohybovat (chvíli) mimo teorii množin. Peanovy axiomy jsou ve skutečnosti základem pro samostatnou teorii, tzv. Peanovu aritmetiku (PA). Později si ukážeme, jak vybudovat přirozená čísla v rámci ZF a uvidíme, že Peanovy axiomy jsou i v jejím rámci splněny (i když zde již technicky nepůjde o axiomy, nýbrž o věty).

[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.

Trochu obecněji lze ukázat, že axiomatizovaná Peanova aritmetika existuje v jisté izomorfní formě právě i v ZF (viz znázornění na obrázku 5.1).



Obrázek 5.1: Model M v rámci ZF, který je izomorfní s PA.

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

(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

(P3) pro každou formuli $\varphi(x)$ platí $\Big(\varphi(0_X) \wedge \forall x \in X : \varphi(x) \Rightarrow \varphi(s(x))\Big) \Rightarrow \forall x \in X : \varphi(x)$.

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 pro libovolnou formuli $\varphi(x)$ platí $\varphi(0_X)$ a pro každé její x z platnosti $\varphi(x)$ plyne i platnost $\varphi(s(x))$ (tedy je-li formule φ splněna pro x, pak je splněna i pro jeho následníka $s(x)$), pak nutně formule φ platí pro všechna $x \in X$. Tento axiom[3] se též nazývá *princip matematické indukce* a často jej využíváme v důkazech (viz podsekce A.4 v příloze A).

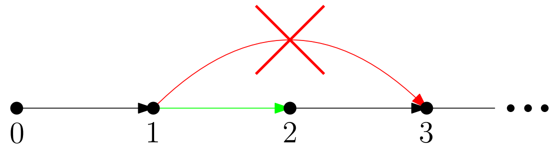
Z kontextu lze vidět, že prvek 0_X zde zastává roli čísla nula. Skutečně, pokud bychom si označili postulovanou množinu X jako $\mathbb{N}_0$ a její prvky $1,2,3,\ldots$, tj.

[2]Tento termín si formálně definujeme v sekci 5.2 pomocí množin.

[3]Přesněji bychom měli psát *schéma axiomů*, neboť každou formuli φ představuje tvrzení samostatný axiom. Tedy axiomů je (stejně jako v případě schématu axiomů vydělení) nekonečně mnoho.

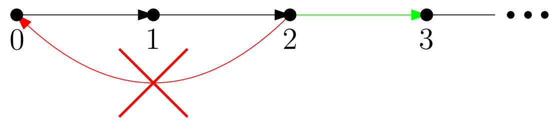
$\mathbb{N}_0 = \{0,1,2,\dots\}$, kde 0_X interpretujeme právě jako číslo 0 a funkci s definovali $s(n) = n + 1$, pak lze vidět, že $\mathbb{N}_0$ splňuje axiomy (P1), (P2) a (P3).

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 5.2.



Obrázek 5.2: Každý prvek je následníkem právě jednoho prvku.

Podobně prvek 0 není následníkem žádného prvku (viz obrázek 5.3).



Obrázek 5.3: Žádný prvek není následníkem 0.

Není těžké si též uvědomit, že přirozená čísla bez nuly $\mathbb{N}$ též splňují (P1), (P2) a (P3), stačí za prvek 0_X vzít číslo 1.

5.2 Přirozená čísla

Peanovy axiomy nám dávají poměrně jasnou představu, co od přirozených čísel požadovat. Naším cílem tak pochopitelně bude, aby naše definice přirozeného čísla v ZF zachovala všechny základní vlastnosti, které přirozená čísla mají splňovat. Zároveň by naše definice neměla být takto samoúčelná, ale měla by být dále použitelná při definici základních aritmetických operacích na přirozených číslech a také definování relací mezi nimi, tj. např. $\leq$, $\geq$, aj.

Čtenář nejspíše nebude nic namítat, pokud řekneme, že „nejjednodušší“ množinou pro nás je **prázdná množina**. Z toho by nás tak mohlo přirozeně napadnout definovat prvek (číslo) 0 jako $\emptyset$. Jak pak ale definovat následníka čísla x? Zde přichází poměrně chytrá definice, která zde zastoupí zmíněnou funkci s (viz sekce 5.1).

Definice 5.2.1 (Následník)**.** Nechť x je libovolná množina. Pak *následníkem* x rozumíme množinu

$$x^+ = x \cup \{x\}\,.$$

Zápis x^+ je v tomto případě zkratkou pro $s(x)$. Z této definice tedy máme např.:

$$
\begin{aligned}
\emptyset &= \emptyset, \\
\emptyset^{+} &= \emptyset \cup \{\emptyset\} = \{\emptyset\}\,, \\
\emptyset^{++} &= (\emptyset^{+})^{+} = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}\,, \\
\emptyset^{+++} &= (\emptyset^{++})^{+} = \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}\,, \{\emptyset, \{\emptyset\}\}\}\,, \\
&\vdots
\end{aligned}
$$

(Převzato z [6], str. 38.)

Na začátku jsme si řekli, že nejpřirozenější se pro nás zdá definovat číslo 0 právě jako $\emptyset$. Společně s definicí následníka libovolné množiny se zdá nyní velmi lákavé definovat množinu $\mathbb{N}_0$ jako

$$\left\{0{,}0^{+}{,}0^{++}{,}0^{+++}, \dots\right\}.$$

Pochopitelně zapisovat obecný prvek n množiny $\mathbb{N}_0$ jako

$$0^{\overbrace{+\,+\,+\cdots+}^{n\text{-krát}}}$$

je dosti nepraktické. Lepší pro nás bude, když si každého z nich nějak označíme:

$$
\begin{aligned}
&1 = 0^{+} = 0 \cup \{0\} = \{0\}\,, \\
&2 = (0^{+})^{+} = 1^{+} = 0 \cup \{1\} = \{0{,}1\}\,, \\
&3 = (0^{++})^{+} = 2^{+} = \{0{,}1\} \cup \{2\} = \{0{,}1{,}2\}\,, \\
&4 = (0^{+++})^{+} = 3^{+} = \{0{,}1{,}2\} \cup \{3\} = \{0{,}1{,}2{,}3\}\,, \\
&\ \vdots
\end{aligned}
$$

Zde se ukazuje jedna technická výhoda této definice, a to sice, že každý prvek x obsahuje všechny své předchůdce. Formálně bychom takový termín mohli definovat následovně:

Definice 5.2.2 (Předchůdce)**.** Nechť $n \in \mathbb{N}_0$. Pak *předchůdcem* prvku n nazveme každý prvek $m \in n$.

Čtenář si již nyní může zkusit rozmyslet, jakou relaci mezi přirozenými čísly můžeme takto poměrně snadno definovat. Předtím se však ještě trochu detailněji podíváme na **relace**, kterým jsme se věnovali v kapitole 4 v sekci 4.2.

5.3 Relace podrobněji

U relací ještě chvíli zůstaneme, neboť ty budou pro nás v dalším textu nejpodstatnější. Mezi nimi lze najít mnoho zvláštních typů, které jsou svojí strukturou velmi význačné. Pokud se čtenář do této chvíle stihl ztratit v záplavě nových pojmů a znalostí, doporučuji se vrátit k sekcím 4.2 o relacích a 4.3 o zobrazeních.

5.3.1 Druhy relací

Zatím jsme si uvedli pouze jeden zvláštní typ relace, který nám (nejspíše) byl již trochu povědomý, a to sice zobrazení. Lze se však setkat i s relacemi, které jsou svojí povahou zcela odlišné. V této sekci si zavedeme dva takové typy. Nejdříve se však podíváme na čtyři nejdůležitější druhy relací.

Ačkoliv jsme si zaváděli relaci obecně mezi dvěma množinami X a Y, v dalším textu se omezíme již pouze na relace na množině.

Definice 5.3.1 (Důležité vlastnosti relací)**.** Nechť R je relace na množině X. Pak R je

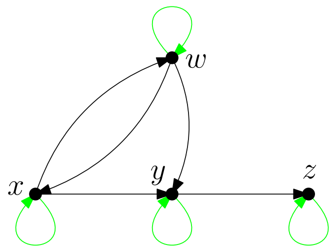
(i) *reflexivní*, jestliže $\forall x \in X : xRx$.

(ii) *symetrická*, jestliže $\forall x,y \in X : xRy \Rightarrow yRx$.

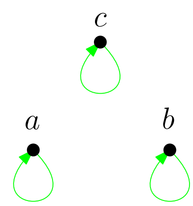
(iii) *tranzitivní*, jestliže $\forall x,y,z \in X : xRy \land yRz \Rightarrow xRz$.

(iv) *antisymetrická*, jestliže $\forall x,y \in X : xRy \land yRx \Rightarrow x = y$.

Reflexivní relace je jednoduše taková relace, kdy jsou všechny prvky v relaci samy se sebou (viz 5.4).



(a) Příklad reflexivní relace na čtyřech prvcích.

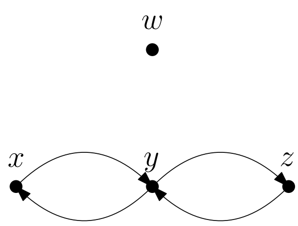


(b) Příklad minimální reflexivní relace na třech prvcích.

Obrázek 5.4: Příklady reflexivních relací.

Speciálně obrázek 5.4b je příkladem nejmenší možné reflexivní relace. Z definice 4.3.7 můžeme vidět, že se jedná o *identitu*.

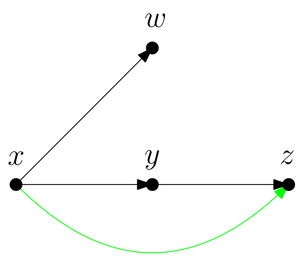
Podobně si můžeme znázornit i symetrii na obrázku 5.5.



Obrázek 5.5: Symetrická relace na čtyřech prvcích.

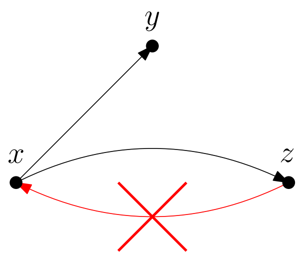
Z obrázku 5.5 můžeme vidět, že mezi dvojicí prvků, které jsou v relaci, vedou šipky oběma směry.

U tranzitivity musí platit, že pokud máme šipku mezi x a y a zároveň mezi y a z, pak musí být i šipka mezi x a z (viz 5.6).



Obrázek 5.6: Tranzitivní relace na čtyřech prvních.

Antisymetrie je pravděpodobně nejtěžší z těchto vlastností, co se týče definice. Zatímco u symetrie platí, že relace musí být „vzájemná“, u antisymetrie naopak říkáme, že pokud jsou prvky ve „vzájemné“ relaci, pak se jedná o tentýž prvek. Z toho si však můžeme uvědomit, že u antisymetrické relace nemůže nastat, že by mezi dvěma různými prvky vedly šipky oběma směry, jak lze vidět na obrázku 5.7.



Obrázek 5.7: Antisymetrická relace na třech prvcích.

Nyní si zadefinujeme další důležitý pojem v definici 5.3.2.

Definice 5.3.2 (Inverzní relace)**.** Nechť R je relace na množině X. *Inverzní relací* k relaci R nazýváme relaci

$$R^{-1} = \{(y,x) \mid xRy\} .$$

Proč právě inverzní? Mějme libovolnou relaci $R \subseteq X \times Y$ a k ní inverzní relaci R^{-1} (ta je naopak podmnožinou „obráceného“ kartézského součinu $Y \times X$). Zkusme relace R a R^{-1} složit (pro připomenutí viz definice 4.2.3).

$$R \circ R^{-1} = \left\{(x,z) \,\middle|\, \exists y \in Y : xRy \wedge yR^{-1}z\right\}$$

Ovšem víme, že když xRy, pak $yR^{-1}x$, což znamená, že $x(R \circ R^{-1})x$. Tedy složením získáme identitu:

$$R \circ R^{-1} = 1_X.$$

Stejně je tomu i u zobrazení. Čtenář pravděpodobně již slyšel termín *inverzní funkce*. Zde se nám tato znalost krásně propojuje se středoškolským učivem.

Poznámka 5.3.3. Inverzní zobrazení f^{-1} k f existuje právě tehdy, když f je **prosté** (pro připomenutí viz definice 4.3.4).

Některé příklady jsou níže.

(i) Funkce $f_1 : \mathbb{R} \to (0,\infty)$, kde $f_1(x) = e^x$; inverzní funkce $f_1^{-1} : \mathbb{R}^+ \to \mathbb{R}$ je $f_1^{-1}(x) = \ln x$.

(ii) Funkce $f_2 : \left\langle -\frac{\pi}{2}, \frac{\pi}{2} \right\rangle \to \langle -1,1 \rangle$, kde $f_2(x) = \sin x$; inverzní funkce $f_2^{-1} : \langle -1,1 \rangle \to \left\langle -\frac{\pi}{2}, \frac{\pi}{2} \right\rangle$ je $f_2^{-1}(x) = \arcsin x$,

(iii) Funkce $f_3 : \mathbb{R} \to \mathbb{R}$, kde $f_3(x) = x^3 - 1$; inverzní funkce je $f_3^{-1} : \mathbb{R} \to \mathbb{R}$ je $f_3^{-1}(x) = \sqrt[3]{x+1}$.

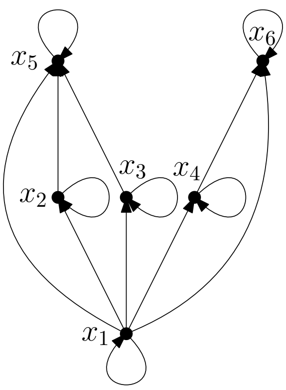
Je vidět, že složením libovolné f_i s f_i^{-1} dostaneme identitu $\left(f_i \circ f_i^{-1}\right)(x) = x$.

5.3.2 Relace uspořádání

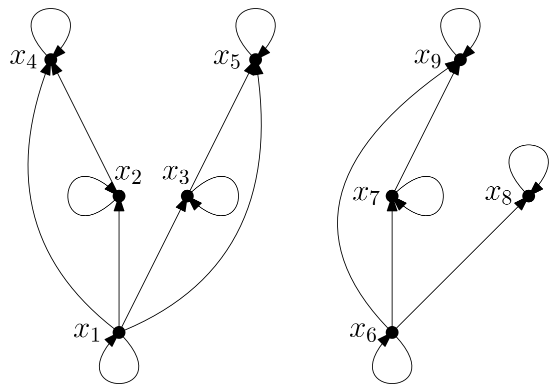
Relace lze dále klasifikovat podle jejich typů. Každý z nich se vyznačuje právě podle definovaných druhů v 5.3.1, do nichž spadají. Pro nás bude velmi podstatné tzv. *uspořádání*. (Vedle tohoto typu ještě existuje tzv. *relace ekvivalence*, o které si lze přečíst v příloze E.)

Definice 5.3.4 (Uspořádání)**.** Nechť R je relace na množině X. Řekneme, že R je relací *uspořádání* (též jen *uspořádání*), pokud je *reflexivní*, *antisymetrická* a *tranzitivní*.

Začněme opět příklady, ať víme, jak si takový typ relace vlastně představit. Mějme relace R_1 a R_2 na obrázcích 5.8 a 5.9. (Zkuste si sami rozmyslet, zda R_1,R_2 splňují podmínky uspořádání.)

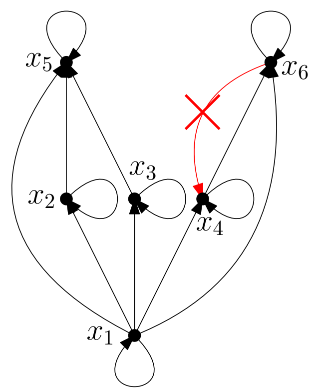


Obrázek 5.8: Relace uspořádání R_1 na šesti prvcích.

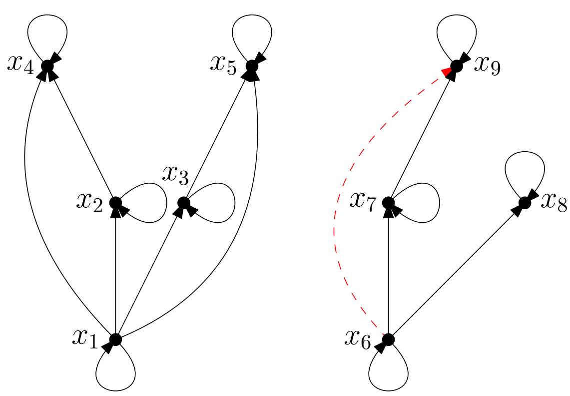


Obrázek 5.9: Relace uspořádání R_2 na devíti prvcích.

Naopak ukázky modifikací relací R_1,R_2 na obrázcích 5.10 a 5.11 **nejsou** uspořádáními.



Obrázek 5.10: Relace $R_1 \cup (x_4,x_6)$, která není uspořádáním.



Obrázek 5.11: Relace $R_2 \setminus (x_6,x_9)$, která není uspořádáním.

Příklad 5.3.5. Další příklady uspořádání:

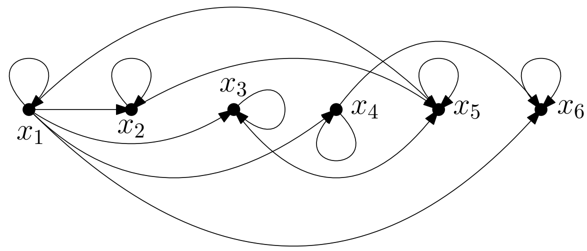
(i) Relace „$\leq$“ na množině $\mathbb{N}$ je uspořádání.

(ii) Relace „$\geq$“ na množině $\mathbb{R}$ je uspořádání.

(iii) Relace „$|$“ („býti dělitelem“) na množině $\mathbb{N}$ je uspořádání.

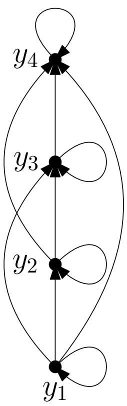
(iv) Relace „$\subseteq$“ na množině $\mathcal{P}(X)$ je uspořádání, kde X je konečná množina.

Zde si můžeme všimnout jisté redundance při zakreslování. Konkrétně šipky vyplývající z tranzitivity a reflexivity bychom v těchto případech mohli klidně vynechat a považovat za samozřejmé. Zároveň jsme cíleně zakreslili relace R_1 a R_2 tak, aby šipky vedly pouze nahoru, neboť to činí obrázek přehlednějším. (Toto funguje díky tomu, že v relaci uspořádání se nemohou vyskytnout „cykly“ kvůli podmínce antisymetrie a tranzitivity, nepočítáme-li „cykly“ z reflexivity.) Zkuste se schválně podívat na znázornění relace R_1 na obrázku 5.12 pro srovnání.

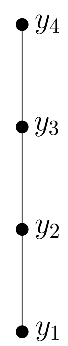


Obrázek 5.12: Relace R_1 zakreslená podle pořadí indexů prvků.

Tím se dostáváme k tzv. *Hasseovým diagramům*, které nám poskytují velmi komfortní reprezentaci uspořádání. Dosavadní způsoby reprezentace relací v sobě obsahovaly jistou míru libovůle, co do umístění prvků v diagramech, neboť důležité byly pouze šipky mezi nimi. Zde toto již neplatí, neboť umístěním prvků budeme určovat, které jsou společné v relaci. Přijmeme konvenci, že šipky mezi prvky povedou pouze směrem nahoru. Tzn. pokud xRy, pak x bude nakresleno níž oproti y. Na obrázku 5.13 máme zakreslené uspořádání na množině $\{y_1,y_2,y_3,y_4\}$.



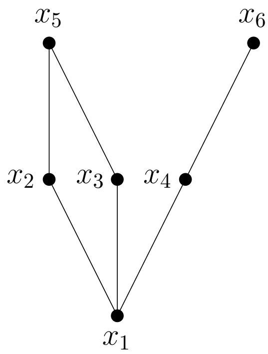
(a) Standardní zakreslení S



(b) Hasseův diagram S

Obrázek 5.13: Relace S zakreslená standardně a pomocí Hasseova diagramu.

Podobně můžeme zakreslit i relaci R_1 z obrázku 5.8 (viz obrázek 5.14).



Obrázek 5.14: Hasseův diagram relace R_1.

(Sekce inspirována [7], str. 44-48 a str. 55)

5.4 Speciálně o uspořádaných množinách

Uspořádání v matematice lze dále klasifikovat. Už jsme měli možnost vidět různé příklady tohoto typu relace, kdy naším primárním cílem bylo si ilustrovat jeho vlastnosti, jimiž je definována a ukázat si pro nás jejich výhodný jejich způsob zakreslování – *Hasseovými diagramy*. V této části se více zaměříme na vlastnosti uspořádání, zavedeme si další typy a především se podíváme na tzv. *dobře uspořádané množiny*.

V ohledu, v jakém se budeme dále uspořádáním věnovat, se nám bude lépe pracovat s následujícím termínem.

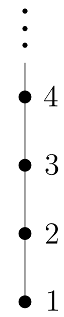
Definice 5.4.1 (Uspořádaná množina)**.** Nechť R je uspořádání na množině X. Pak uspořádanou dvojici (X,R) nazýváme *uspořádaná množina.*

Definice 5.4.2 (Lineární uspořádání)**.** Nechť (X,R) je uspořádaná množina. Pak R, resp. (X,R) nazýváme *lineárním uspořádáním*, resp. *lineárně uspořádanou množinou*, jestliže $\forall x,y \in X : xRy \vee yRx$.

Pojem *částečné uspořádání*, resp. *částečně uspořádaná množina* jsou používány naopak pro uspořádání, která nemusí být nutně lineární. Jedná se tedy pouze o obšírnější termín. Obecně platí, že každá lineárně uspořádaná množina je částečně uspořádanou, avšak ne každá částečně uspořádaná množina je lineárně uspořádanou.

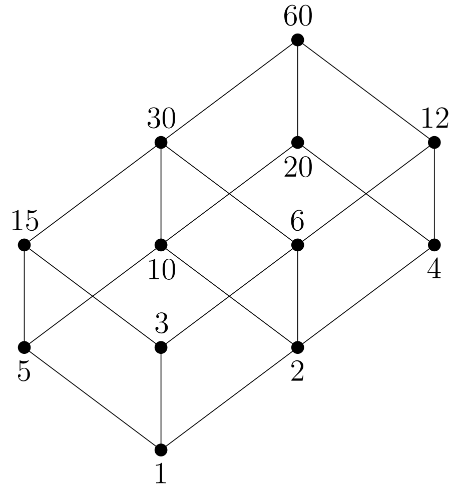
Příklad 5.4.3. Klasifikace některých známých uspořádání a jejich Hasseovy diagramy.

(i) $(\mathbb{N}, \leq)$ je lineárně uspořádaná množina.



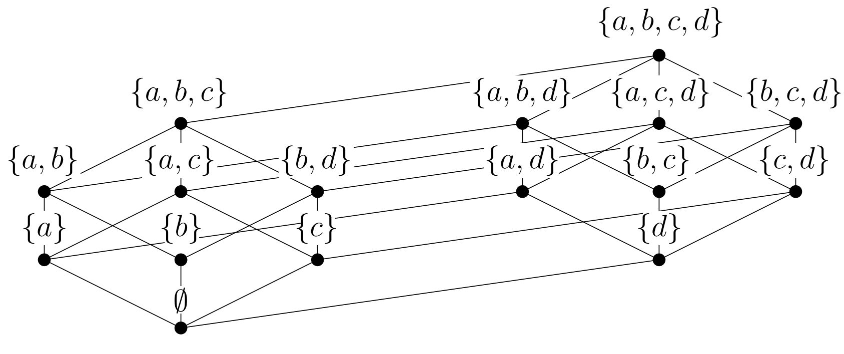
Obrázek 5.15: Diagram uspořádané množiny $(\mathbb{N}, \leq)$.

(ii) $(S, |)$, kde $S = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$ (množina všech dělitelů čísla 60), je částečně (nikoliv však lineárně) uspořádaná množina.



Obrázek 5.16: Diagram uspořádané množiny $(S, |)$.

(iii) $(\mathcal{P}(X), \subseteq)$, kde $X = \{a,b,c,d\}$, je částečně (nikoliv však lineárně) uspořádaná množina.

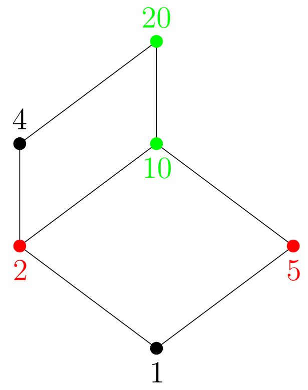


Obrázek 5.17: Diagram uspořádané množiny $(\mathcal{P}(X), \subseteq)$.

Lze si všimnout, že díky antisymetrii tvoří prvky jistou „hierarchii“. Např. v (i) v předešlém příkladu 5.4.3 můžeme vidět z obrázku 5.15, že každému prvku „předchází“ jiný prvek až na číslo 1. Podobně je tomu tak i u (ii) a (iii).

Definice 5.4.4 (Porovnatelné prvky)**.** Nechť (X,R) je uspořádaná množina. Řekneme, že prvky $x,y \in X$ jsou *porovnatelné*, pokud $xRy \vee yRx$.

Lineární uspořádaná množina (X,R) je tak jednoduše uspořádaná množina, kde jsou každé dva prvky porovnatelné.
Pro příklad porovnatelných prvků nemusíme chodit daleko. Vezměme si všechny třeba všechny dělitele čísla 20, tj. $(\{1,2,4,5,10,20\}, |)$, na obrázku 5.18 níže, kde je zeleně zvýrazněn příklad porovnatelných prvků a červeně příklad prvků, které nejsou porovnatelné.



Obrázek 5.18: Diagram uspořádané množiny $(\{1,2,4,5,10,20\}, |)$ se zvýrazněním porovnatelných a neporovnatelných prvků.

S porovnatelností prvků se pojí již trochu významově „užší“ termíny, které pro nás budou stěžejní.

Definice 5.4.5 (Minimální/maximální prvek, nejmenší/největší prvek)**.** Nechť $(X, \preceq)$ je uspořádaná množina. Mějme prvek $a \in X$. Prvek a nazveme

(i) *minimálním*, pokud $\forall x \in X, x \neq a : x \not\preceq a$.

(ii) *maximálním*, pokud $\forall x \in X, x \neq a : a \not\preceq x$.

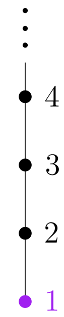
(iii) *nejmenším*, pokud $\forall x \in X : a \preceq x$.

(iv) *největším*, pokud $\forall x \in X : x \preceq a$.

Na první pohled nemusí být rozdíl v definici jednotlivých termínů zřejmý. Zkuste se však nad nimi zamyslet z pohledu porovnatelnosti prvků. Ve skutečnosti termíny *nejmenší a největší prvek* jsou „silnější“. Je-li např. prvek maximální, pak tvrdíme, že není s žádným z ostatních prvků množiny v relaci. To ale však neznamená, že je se všemi prvky porovnatelný. (Opět vyzývám čtenáře, aby si zkusil rozmyslet.) Podobně je tomu i pro minimální prvek. Naopak největší a nejmenší prvek jsou vždy s každým prvkem porovnatelné. Lépe bude rozdíl v těchto termínech vidět opět na příkladech.

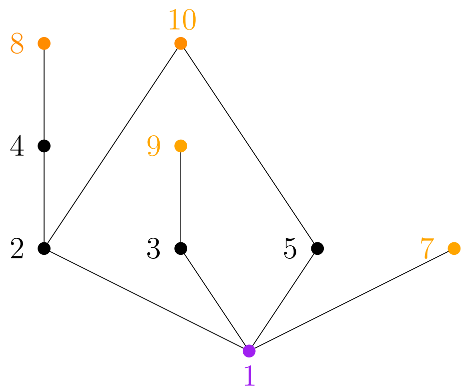
Příklad 5.4.6. Ukázky některých uspořádaných množin a jejich nejmenších/největších, resp. minimálních/maximálních prvků. Maximální/největší prvky jsou označeny oranžovou barvou a minimální/nejmenší prvky fialovou.

(i) Uspořádaná množina $(\mathbb{N}, \leq)$ má minimální prvek 1, ale nemá největší, ani maximální prvek.



Obrázek 5.19: Diagram uspořádané množiny $(\mathbb{N}, \leq)$ s minimálním prvkem.

(ii) Uspořádaná množina $(\{1,2,\ldots,10\}, |)$ má nejmenší prvek 1 a maximální prvky 7, 8, 9 a 10, ale nemá největší prvek.

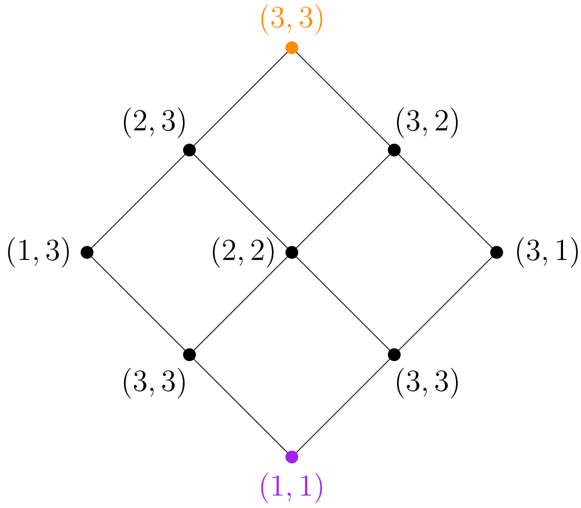


Obrázek 5.20: Diagram uspořádané množiny $(\{1,2,\ldots,10\}, |)$ s minimálním prvkem a dvěma maximálními prvky.

(iii) Uspořádaná množina $(A^2, \preceq)$, kde $A = \{a,b,c\}$, definovaná předpisem

$$\forall (x_1,x_2),(y_1,y_2) \in A^2 : \Big((x_1,x_2) \preceq (y_1,y_2) \Leftrightarrow x_1 \leq y_1 \wedge x_2 \leq y_2\Big)$$

má nejmenší prvek (1,1) největší prvek (3,3).



Obrázek 5.21: Diagram uspořádané množiny $(A^2, \preceq)$ s nejmenším prvkem a největším prvkem.

Ve skutečnosti si lze všimnout, že největší, resp. nejmenší prvek je vždy zároveň i maximální, resp. minimální. Opačné tvrzení však již neplatí.

5.5 Vlastnosti přirozených čísel

Podívejme se nyní blíže na vlastnosti přirozených čísel, které plynou z definice v sekci 5.2. Již jsme si ukazovali, jak lze axiomaticky zavést přirozená čísla pomocí Peanových axiomů (viz 5.1), které nám dávaly poměrně jednoznačnou představu, co od takové množiny požadujeme. Skutečně, množina přirozených čísel zavedená jako

$$0 = \emptyset, \quad 1 = \{0\}\,, \quad 2 = \{0{,}1\}\,, \quad 3 = \{0{,}1{,}2\}\,, \quad 4 = \{0{,}1{,}2{,}3\}\,, \quad \ldots$$

společně se zobrazením s (následník) definovaným předpisem $s(x) = x \cup \{x\}$ splňuje tyto axiomy. Mějme na paměti, že v rámci teorie množin **Peanovy axiomy** již nejsou v ZF axiomy, nýbrž věty (tvrzení, která lze odvodit z axiomů ZF). Jejich platnost zde dokazovat nebudeme, avšak budeme je v dalším textu používat. Důkazy lze najít v knize [6], str. 40-41 a str. 43-44.

Na konci sekce 5.2 jsme poukázali na to, že zavedení přirozených čísel použitým způsobem má za důsledek, že každý z prvků obsahuje všechny své předchůdce. To nám umožňuje zformulovat poznatek 5.5.1. Zároveň nám to poslouží jako ukázka využití indukce při studiu tohoto modelu přirozených čísel v ZF.

Lemma 5.5.1. *Nechť jsou dána přirozená čísla $n,m \in \mathbb{N}_0$. Pak platí:*

(i) $n \in \mathbb{N}_0 \Rightarrow n \subseteq \mathbb{N}_0$,

(ii) $m \in n \Rightarrow m \subseteq n$,

(iii) $n \notin n$.

Důkaz. Všechny body tohoto tvrzení samostatně dokážeme indukcí.

(i). Pro začátek ověříme platnost tvrzení pro nulu. To jistě platí, neboť $0 = \emptyset$ a prázdná množina je podmnožinou každé množiny, jak jsme si již dokázali v tvrzení 3.2.7, tedy i $0 \subseteq \mathbb{N}_0$.

Předpokládejme, že tvrzení platí pro jisté přirozené číslo n, tzn. $n \subseteq \mathbb{N}_0$. Ukážeme, že tvrzení platí i pro n^+. Protože $n \in \mathbb{N}_0$, pak $\{n\} \subseteq \mathbb{N}_0$, z čehož již plyne, že $n^+ = n \cup \{n\} \subseteq \mathbb{N}_0$, neboť sjednocením podmnožin je opět podmnožina. Z principu indukce tak (i) platí pro všechna $n \in \mathbb{N}_0$.

(ii). Definujme množinu

$$X = \{n \in \mathbb{N}_0 \mid \forall m \, (m \in n \Rightarrow m \subseteq n)\} \, .$$

Naším cílem je indukcí ukázat, že $X = \mathbb{N}_0$.

Určitě platí, že $0 \in X$. (Ačkoliv $\emptyset$ neobsahuje žádné prvky, podmínka přesto platí. Vysvětlení v sekci 3.2 v důkazu lemmatu 3.2.7.)

Předpokládejme, že $n \in X$. Ukážeme, že $n^+ \in X$. Vezměme si libovolný prvek $m \in n^+ = n \cup \{n\}$. Z toho vyplývá, že buď $m \in n$, nebo $m = n$. V prvním případě $m \in n$ z indukčního předpokladu platí $m \subseteq n$, tedy i $m \subseteq n \cup \{n\} = n^+$. V druhém případě $m = n$ platí totéž. Tím jsme ukázali, že $n^+ \in X$ a podle principu indukce tedy platí $X = \mathbb{N}_0$.

(iii). Pro nulu tvrzení platí. Opět předpokládejme, že tvrzení platí pro $n \in \mathbb{N}_0$, tj. $n \notin n$. Indukční krok dokážeme sporem. Pro spor nechť platí $n^+ \in n^+$. Pak z definice n^+ musí platit buď $n^+ \in n$, nebo $n^+ = n$. Použitím tvrzení (ii) v obou případech dostáváme, že $n^+ = n \cup \{n\} \subseteq n$. To znamená, že $\{n\} \subseteq n$, z čehož již odvodíme $n \in n$. To je však spor s indukčním předpokladem, že $n \notin n$. Tím dostáváme, že $n^+ \notin n^+$. □

(Převzato z [5], str. 86-87.)

Všimněte si, že bod (ii) jsme dokázali definováním množiny prvků, které splňují dokazované tvrzení a ukázali jsme, že taková množina jsou všechna přirozená čísla. Ostatní body (i) a (iii) jsme dokázali „běžnou“ indukcí. Jedná se však o ekvivalentní přístupy.

Je tak docela pěkně vidět, co v řeči množin znamená, když je nějaké přirozené číslo větší/menší než jiné.

Definice 5.5.2. Nechť n,$m \in \mathbb{N}_0$. Pak definujeme

(i) $m < n \overset{\text{def.}}{\Leftrightarrow} m \in n$,

(ii) $m \leq n \overset{\text{def.}}{\Leftrightarrow} m < n \lor m = n$,

(iii) $m > n \overset{\text{def.}}{\Leftrightarrow} n < m$,

(iv) $m \geq n \overset{\text{def.}}{\Leftrightarrow} n \leq m$.

O relaci „$\leq$“ jsme již v minulé sekci o uspořádáních 5.4 ukázali, že na $\mathbb{N}$ se jedni o uineární uspořádání (konkrétně v příkladu 5.4.3). Zde jsme s ní však nepracovali ve smyslu definice 5.5.2. Zkusme se tedy přesvědčit, že je takto definovaná relaci skutečně lineárním uspořádáním na $\mathbb{N}_0$ (pro připomenutí definice viz 5.3.4). Nejdříve si však zformulujme následující lemma, které později využijeme.

Lemma 5.5.3. *Nechť jsou dána přirozená čísla* $n,m \in \mathbb{N}_0$. *Pak platí:*

(i) $m < n \Leftrightarrow m \subset n$,

(ii) $m < n \vee m = n \vee m > n$.

Důkaz. (i). (⇒). Z definice máme $m \in n$. Platnost této implikace je pouze důsledkem lemmatu 5.5.1 (bodu (ii)) a faktu $m \notin m$ (bod (iii)).

(⇐). Postupujeme indukcí podle n. Zvolme si pevné $m \in \mathbb{N}_0$. Pro $n = 0$ lze vidět, že tvrzení platí.

Předpokládejme, že tvrzení platí pro n (a všechna m), tj. $m < n \Leftrightarrow m \subset n$. Zvolme $m \subset n^+$. Ukážeme, že z toho plyne $m < n^+$.

Ukažme nejprve, že $m \subseteq n$. Na to lze nahlédnout sporem. Kdyby platilo $n > m$, tzn. $n \in m$, pak by podle tvrzení (ii) v lemmatu 5.5.1 dostáváme $n \subseteq m$ a tedy i $n^+ \subseteq m$ (opět nemůže platit, že $n \in n$). To je však v rozporu s předpokladem, že $m \subset n^+$.

Již tedy víme, že $n \notin m$ a $m \subseteq n$. Z definice podmnožiny mohou nastat dva případy (pro připomenutí viz definice 3.2.5).

- $m \subset n$. Podle indukčního předpokladu platí $m < n$ a tedy i $m < n^+$.
- $m = n$. Pak z faktu $n < n^+$ plyne $m < n^+$.

V obou případech jsme tak dokázali indukční krok.

(ii). Důkaz je trochu složitější a proto jej zde vynecháme, nicméně čtenář jej může nalézt v knize [5], str. 88. □

(Převzato z [5], str. 87-88.)

Důsledek 5.5.4. $\forall n,m \in \mathbb{N}_0 : n \leq m \vee m \leq n$.

Důkaz. Přímo plyne z tvrzení (ii) lemmatu 5.5.3. □

Díky lemmatům 5.5.1, 5.5.3 a důsledku 5.5.4 můžeme již zformulovat větu 5.5.5. Důkaz lze nalézt v příloze D.

Věta 5.5.5. $(\mathbb{N}_0, \leq)$ *je lineárně uspořádaná množina.*

Co kdybychom uvážili relaci „<“ na $\mathbb{N}_0$? Striktně podle definice 5.3.4 by $(\mathbb{N}_0, <)$ nebyla uspořádaná množina, neboť „<“ není reflexivní. Nicméně zbývající vlastnosti jsou zachovány. V matematice se občas dále rozlišuje tzv. *ostré* a *neostré* uspořádání, kdy ostré oproti neostrému je *antireflexivní*, tj. pro všechna x z dané množiny platí $x \not R x$.

5.6 Aritmetika přirozených čísel

Již jsme si ukázali, že naše definice přirozených čísel je skutečně korektní a splňuje vlastnosti lineárního uspořádání vzhledem k relaci „≤“. Posledním krokem pro nás nyní je zavést základní početní operace a dokázat, že mají takové vlastnosti, na jaké jsme zvyklí. V této sekci si však jen ukážeme náznak, jak zavést tyto základní početní operace; důkazům jejich vlastností se již věnovat nebudeme. Zatím jsme se bavili v případě množin pouze o jejich struktuře, avšak vyhýbali se termínům jako *počet prvků*, *velikost množiny*, apod. Přitom přirozená čísla si člověk často spojí s **počtem nějakých objektů**. Intuitivní by tak bylo definovat tyto operace v tomto duchu. Alternativní zavedení pomocí následníků nabízí např. kniha [6], str. 48-57.

Zcela pochopitelně by čtenář mohl namítat, že pojem **„velikost množiny"** jsme nikterak formálně nedefinovali. Vzhledem k tomu, že v této sekci budeme pracovat pouze s konečnými[4] množinami, můžeme zatím termín počtu prvků chápat víceméně intuitivně, avšak později si tento koncept zobecníme v kapitole 6 v sekci 6.3. Velikost množiny X (resp. počet prvků) budeme značit $|X|$, kterou reprezentuje přirozené číslo z množiny $\mathbb{N}_0$.

Definice 5.6.1 (Součin přirozených čísel)**.** Nechť jsou dána přirozená čísla a,b,k. Pak definujeme *součin* čísel a a b

$$a \cdot b = k \overset{\text{def.}}{\Leftrightarrow} |a \times b| = |k|\,.$$

Pokud si vzpomeneme na kartézský součin množin (viz definice 4.1.1), zjistíme, že takové zavedení je celkem přirozené. Z kombinatorického hlediska to není nic jiného, než počítání všech možných uspořádaných dvojic. Např. součin přirozených čísel 3 a 5 tak dopovídá číslu 15 (protože existuje přesně 15 uspořádaných dvojic (a,b), kde $a \in 3 = \{0,1,2\}$ a $b \in 5 = \{0,1,2,3,4\}$).

Co kdybychom však za jedno z čísel vzali nulu? Z definice bychom tak dostali kartézský součin, kde jedna z množin by byla prázdná, tj. např. $\emptyset \times b$. Podle definice kartézského součinu by muselo platit:

$$\emptyset \times b = \{(x,y) \mid x \in \emptyset \wedge y \in b\}\,.$$

Avšak uspořádaná dvojice (x,y), která by splňovala podmínku $x \in \emptyset \wedge y \in b$ pochopitelně nemůže existovat, neboť x bereme z prázdné množiny. Tedy skutečně $\emptyset \times b = b \times \emptyset = \emptyset$, což znamená, že $0 \cdot b = b \cdot 0 = 0$, jak bychom předpokládali. Naše definice je tak skutečně rozumná.

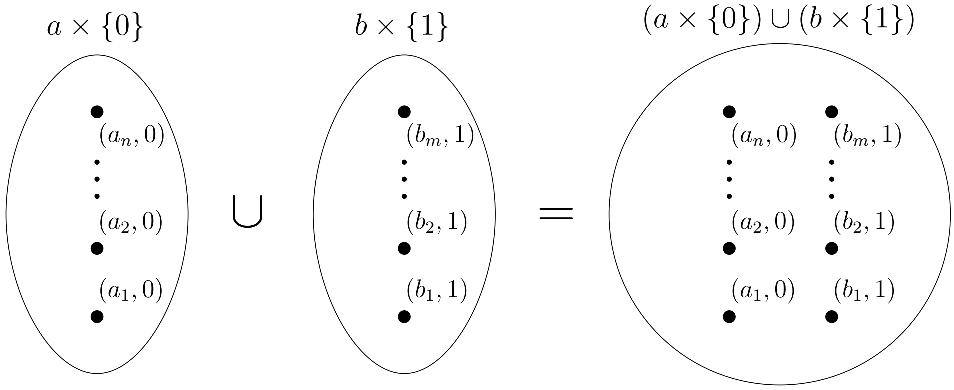
Přesuňme se k součtu. Zde nemůžeme položit $a + b = |a \cup b|$, neboť a a b nemusí být nutně disjunktní, tj. nemusí platit $a \cap b = \emptyset$. Prvky těchto množin je tak třeba určitým způsobem „odlišit". Toho docílíme v definici 5.6.2.

Definice 5.6.2 (Součet přirozených čísel)**.** Nechť jsou dána přirozená čísla a,b,k. Pak definujeme *součet* čísel a a b

$$a + b = k \overset{\text{def.}}{\Leftrightarrow} |(a \times \{0\}) \cup (b \times \{1\})| = |k|\,.$$

Kartézské součiny $a \times \{0\}$ a $b \times \{1\}$ zde zajišťují, že výsledné množiny každého z nich budou vzájemně disjunktní (druhá souřadnice se vždy bude lišit) a tedy velikost jejich sjednocení bude skutečně korespondovat s naší představou (viz obrázek 5.22).

[4]Konečnost a nekonečnost množiny později definujeme v kapitole 6 v sekci 6.2.



Obrázek 5.22: Grafické znázornění sjednocení množin $a \times \{0\}$ a $b \times \{1\}$.

Nyní bychom měli správně ukázat, že takto zavedené operace sčítání a násobení splňují vlastnosti jako *asociativita*, *komutativita*, *distributivita*, aj. Pro udržení jednoduchosti textu zde tuto pasáž vynecháme.

Kapitola 6

Porovnávání nekonečných množin

Na začátku celého tohoto textu jsme si položili otázku, zda má více prvků interval (0,1), nebo množina všech přirozených čísel $\mathbb{N}$. I přesto, co všechno jsme o množinách zjistili, stále nemáme způsob, jak na tuto otázku odpovědět. V této závěrečné kapitole se proto podíváme na to, jak v matematice zacházíme s nekonečnými množinami a co vlastně vůbec rozumíme pod pojmem „počet prvků“ v případě nekonečných množin.

6.1 Hilbertův hotel

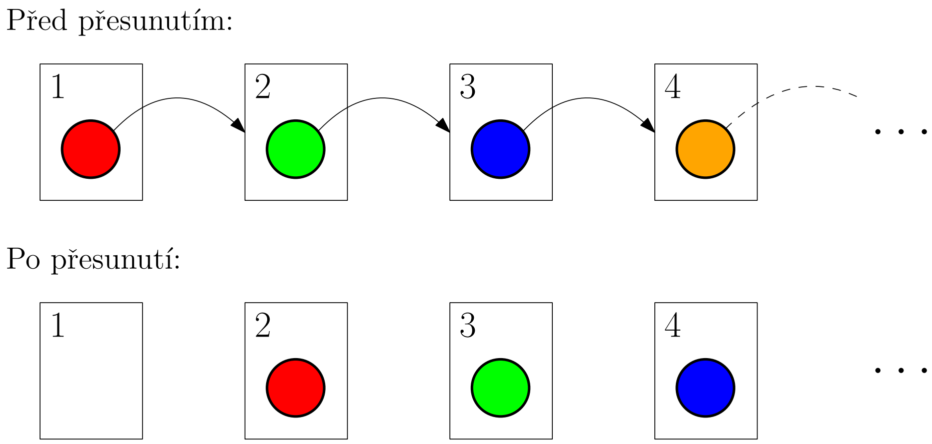
Jak jsme si již uvedli v historickém úvodu (konkrétně v podsekci 1.2.2), matematik Georg Cantor byl jedním z prvních, kteří se zabývali konceptem nekonečna v uvedeném smyslu, aniž by se ohlížel na předsudky, které plynuly o nekonečnu z naší intuice. Jeden takový případ jsme si již ukázali u pozorování Galilea Galilei (viz podsekce 1.1.1), který však naopak dospěl k závěru, že porovnáváním velikostí nekonečných množin se nemá smysl zabývat. Cantorovy úvahy o nekonečnu byly z počátku velmi kontroverzní a odmítané, ale dnes jsou již drtivou většinou matematické komunity uznávané. Cantorova teorie množin však dávala ve své době vzniknout různým „paradoxům nekonečna“[1], které ilustrovaly, jak neintuitivní může být práce s nekonečnem. Jedním z nejznámějších paradoxů tohoto typu je tzv. *Hilbertův hotel*, který je pojmenován po německém matematikovi DAVIDU HILBERTOVI[2] (1862-1943), jenž přišel s tímto myšlenkovým experimentem.

Zadání problému. *Představme si, že v jednom neznámém městě stojí hotel, kde pracuje matematiky znalý recepční. Hotel má jednu zvláštní vlastnost, a to sice, že má nekonečně mnoho pokojů. Všechny pokoje v hotelu jsou jednolůžkové postupně očíslované přirozenými čísly* $1,2,3,\dots$ *a hotel je plně obsazen. Recepční se postupně potýká s následujícími situacemi.*

[1] Uvozovky jsou zde uvedeny z důvodu, že dnes již tyto záležitosti za paradoxy nepovažujeme.

[2] D. Hilbert si v historii matematiky připsal mnohé zásluhy. Jako první uspokojivě vybudoval axiomatickou eukleidovskou geometrii a také zformuloval 23 nejdůležitějších (tehdy zatím nevyřešených) problémů matematiky, které prezentoval na druhém mezinárodním matematickém kongresu v Paříži v roce 1900, jímž nasměroval úsilí matematické komunity na další století. Některé z těchto problémů jsou dodnes otevřené a není na ně známá jednoznačná odpověď.

(i) Do hotelu přijde nový zákazník. Běžný recepční by nejspíše zákazníka poslal pryč s tím, že hotel je plný. Avšak tento recepční si uvědomí, že může nového zákazníka snadno ubytovat. Protože hotel je nekonečný, vymyká se principům platným u konečných množin. Není tak žádný problém každého z hostů požádat, aby se přesunul do vedlejšího pokoje. To znamená, že host v pokoji č. 1 se přesune do pokoje č. 2, host v pokoji č. 2 do pokoje č. 3, atd. Situaci lze sledovat na obrázku 6.1. Právě z důvodu, že hotel je nekonečný,



Obrázek 6.1: Situace před a po přesunutí hostů. (Převzato z [1] a upraveno.)

nemůže nastat situace, kdy by některý z hostů se již nemohl přesunout do nového pokoje (což naopak, jak je patrné, by nastalo u hotelu s konečně mnoha pokoji). Pro nového hosta se tak uvolní pokoj č. 1, kde může být ubytován.

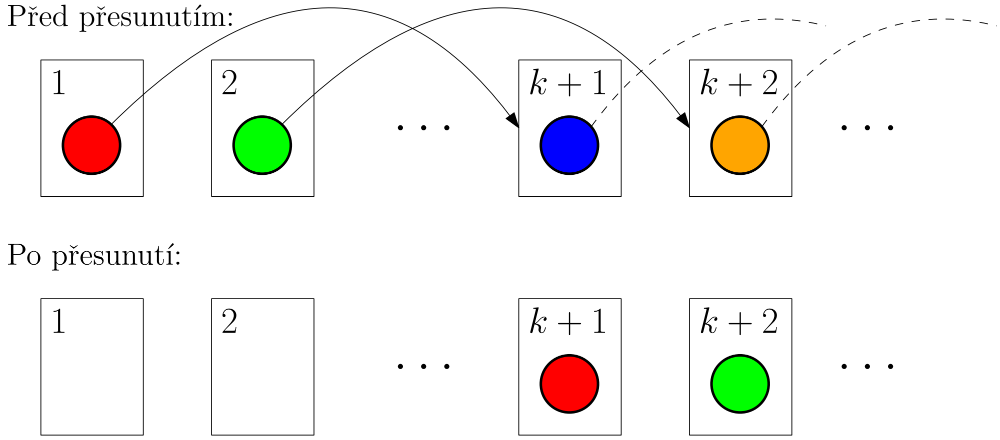
Jak bychom činnost recepčního mohli vyjádřit matematicky? Podíváme-li se na tuto akci obecněji, tak libovolný host v pokoji s číslem n se přesunul do pokoje s číslem $n+1$. Nejedná se tak o nic jiného, než o nobrazení (dokonce funkci) $\mathbb{N}$ do $\mathbb{N}$. Pokud bychom si jej označili f, pak $f : \mathbb{N} \to \mathbb{N}$, kde

$$f(n) = n + 1$$

Zobrazení f je jistě prosté (žádní dva hosté se nepřesunou do stejného pokoje) a není na (první pokoj zbude neobsazený).

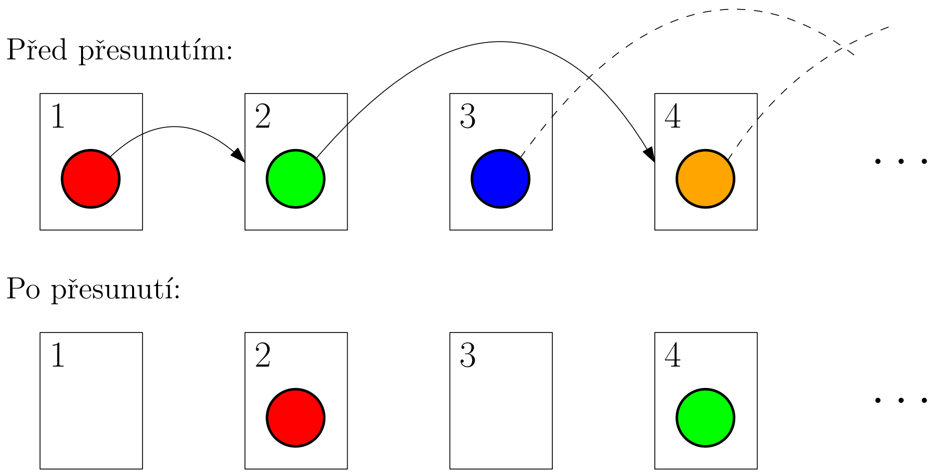
(ii) Do hotelu přijde obecně k nových hostů. Recepční se s tímto problémem může vypořádat obdobně jako v předešlém případě. Je tedy potřeba uvolnit k pokojů. V předešlém případě recepční požádal hosta v pokoji č. n o přesunutí do pokoje č. $n + 1$. Pro k nových hostů nám tak stačí požádat každého hosta o přesun do pokoje s číslem větším o k, tj. host v pokoji č. n se přesune do pokoje č. $n + k$ (viz obrázek 6.2). Analogicky i zde můžeme tuto akci popsat jako zobrazení $g : \mathbb{N} \to \mathbb{N}$, kde $g(n) = n + k$ (k je pevné). Zobrazení g je prosté, neboť hosté z různých pokojů se nikdy nepřesunou do pokoje se stejným číslem, a také není na, neboť čísla $1, 2, \dots, k$ nemají žádný vzor, tj. prvních k pokojů zůstane volných.

Ze situací *(i)* a *(ii)* lze vidět, že ačkoliv je hotel plně obsazen, recepční stále může ubytovávat nové hosty.



Obrázek 6.2: Situace před a po přesunutí k hostů. (Převzato z [1] a upraveno.)

(iii) Recepční tak může zajásat, neboť pro libovolný počet nových hostů vždy může uvolnit potřebný počet pokojů. Avšak při pohledu z okna si všimne, že před hotelem zaparkoval autobus. To by nebyl takový problém, neboť recepční již zná postup, jak uvolnit pokoje pro libovolný **konečný** počet nových hostů. Avšak tento autobus byl nekonečný s nekonečně mnoha sedadly očíslovanými přirozenými čísly $1, 2, \ldots$, kde každé bylo obsazeno turistou se zájmem o ubytování. Jak má nyní recepční postupovat? Postup popsaný výše mu zde bohužel již nepomůže. Nemůže požádat hosta v pokoji č. 1, aby se přesunul o nekonečně mnoho pokojů dál (pokoje jsou očíslované konečnými čísly). Bude třeba jiná strategie. Zde si však recepční může poradit takto: hosta v pokoji č. 1 požádá, aby se přesunul do pokoje č. 2; hosta v pokoji č. 2, aby se přesunul do pokoje č. 4; hosta v pokoji č. 3, aby se přesunul do pokoje č. 6; atd. Obecně host v pokoji č. n se přesune do pokoje s číslem $2n$ (viz obrázek 6.3). Jak můžeme vidět, touto akcí recepční



Obrázek 6.3: Situace po přesunutí hostů obecně z pokoje n do $2n$. (Převzato z [1] a upraveno.)

zaplnil všechny pokoje se **sudým** číslem a pokoje s lichým číslem jsou tak nyní volné. Nyní recepčnímu stačí, aby turistu sedícího na sedačce s číslem k ubytoval v pokoji č. $2k - 1$.

(iv) Mohlo by se zdát, že je již problémům konec. Avšak jednoho dne se recepční podíval z okna a viděl, že před hotelem parkuje nekonečně mnoho autobusů, kde každý z nich byl nekonečně dlouhý s nekonečně mnoha turisty. Každý s turistů se chce v hotelu ubytovat. Předešlý postup již fungovat nebude, neboť by bylo třeba pro každý z autobusů provést samostatné stěhování již ubytovaných hostů (iterací by tak muselo být nekonečně mnoho). Náš recepční je však matematicky zdatný a vzpomene si na fakt, že prvočísel je nekonečně mnoho (pro zvídavého čtenáře viz příloha A, tvrzení A.3.3).

$$2{,}3{,}5{,}7{,}11,\ldots$$

Jak mu to zde pomůže? Pro všechny ubytované hosty vezme první prvočíslo, což je 2, a každého z nich ubytuje následujícím způsobem. Hostovi v pokoji č. 1 přiřadí pokoj č. $2^1 = 2$, hostovi v pokoji č. 2 pokoj č. $2^2 = 4$, atd. Obecně hostovi v pokoji s číslem k je přiřazen pokoj č. 2^k. Pro všechny ubytované hosty tak vyčerpá všechny mocniny dvojky. Následně pro první autobus vezme prvočíslo 3 a nyní postup probíhá obdobně. Turista na sedadle s číslem k je ubytován v pokoji č. 3^k. Nejprve si uvědomme, že pro libovolná $n,m \in \mathbb{N}$ je $2^n \neq 3^m$, tzn. žádnému z turistů z prvního autobusu nemůže být přiřazen pokoj, který je již obsazený již ubytovaným hostem.

Obecně označíme-li si ℓ-té prvočíslo jako p_ℓ, pak pro $(\ell-1)$-tý autobus bude k-tému turistovi přiřazen pokoj p_ℓ^k. I zde bychom mohli ukázat, že zobrazení $h_\ell : \mathbb{N} \to \mathbb{N}$ pro $\ell \in \mathbb{N}$ je prosté a

$$\forall \ell_1,\ell_2 \in \mathbb{N}, \ell_1 \neq \ell_2 : h_{\ell_1}(\mathbb{N}) \cap h_{\ell_2}(\mathbb{N}) = \emptyset,$$

tj. množiny obrazů zobrazení h_{ℓ_1} a h_{ℓ_2} jsou pro různá ℓ_1,ℓ_2 disjunktní. Tímto způsobem tak recepční je schopný ubytovat všechny turisty, aniž by na některého z nich nezbyl žádný pokoj. Dokonce si můžeme všimnout, že některé pokoje i po ubytování zůstanou neobsazené. Např. pokoj č. 6, protože toto číslo není mocninou žádného prvočísla; jeho faktory jsou 2 a 3.

Pokud pomineme potenciálně nekonečný počet stížností od hostů kvůli neustálému stěhování a jiné další problémy, Hilbertův hotel nám krásně ilustruje myšlenku, že práce s nekonečnem může být dosti neintuitivní a i poměrně jednoduché principy platné při konečných počtech v případě nekonečna již neplatí. Sami jsme viděli, že i přesto, že byl hotel plně obsazen, nebyl problém problém zde ubytovat další nové hosty, a to ať uh v konečném nebo nekonečném počtu. Matematickou podstatu Hilbertova hotelu si blíže popíšeme v sekci 6.2.

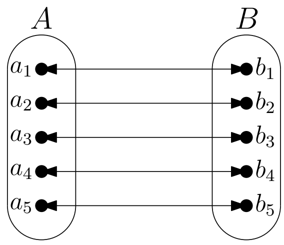
6.2 Porovnávání podle počtu prvků

Nekonečné množiny mají tedy dost pozoruhodné vlastnosti. V souvislosti s předešlou úvahou by nás tak mohlo napadnout, že při plně obsazeném hotelu je hostů „stejně mnoho“ jako pokojů. Ovšem z případu *(i)* jsme mohli vidět, že po přesunutí hostů do vedlejšího pokoje byly pak již obsazeny „pouze“ pokoje $2,3,\ldots$ a první tak zůstal volný. Pokud by toto byla výchozí situace, mohlo by se nám tak zdát, že hostů je méně, neboť v prvním pokoji žádný není. Avšak jediné, co se stalo je, že hosté změnili svůj pokoj, čímž se celkem přirozeně nemohl porušit jejich počet. Změnil se tedy počet hostů a pokojů, nebo jich je stejně mnoho?

Náš náhled se pochopitelně odráží od porovnávání velikostí konečných množin. U těch toto nečinní žádný problém, stačí spočítat jejich prvky. U nekonečných množin již prvky „spočítat“ nemůžeme. Existuje však ještě jeden způsob, který ve skutečnosti vůbec nevyžaduje schopnost počítání.

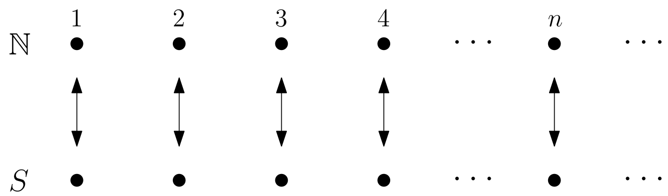
O domorodém kmenu a slepicích. *Představme si, že jistý domorodý kmen hledá nového náčelníka. Po několika vyřazovacích kolech zbyli poslední dva kandidáti. Ostatní členové kmene rozhodli, že náčelníkem se stane ten z kandidátů, který vlastní více slepic. Tento kmen je však matematicky velmi primitivní a jeho příslušníci umí počítat pouze do pěti. Oba dva kandidáti však mají ostře více jak pět slepic. Kmen se tedy rozhodl postupovat takto: každý z kandidátů přinese vždy jednu svoji slepici a tímto způsobem pokračují, dokud jednomu z nich slepice nedojdou. Ten, kterému dříve dojdou slepice, prohraje a druhý se tak stane náčelníkem.* [9]

Z tohoto příkladu je již nejspíše jasné, jak lze množiny porovnávat. Pokud mají dvě množiny stejný počet prvků, pak lze jednotlivé prvky „spárovat“. V matematické řeči náčelníci pouze sestrojují zobrazení z jedné množiny slepic do druhé. Toto dává jistě smysl v kontextu konečných množin. Pokud mají množiny stejně prvků, pak mezi nimi existuje bijekce (viz obrázek 6.4). Stejným způsobem



Obrázek 6.4: Bijekce mezi konečnými množinami A,B se stejným počtem prvků.

však můžeme porovnávat i nekonečné množiny! Zkusme si vzít např. množinu všech kladných sudých čísel $S = \{2k \mid k \in \mathbb{N}\}$ a přirozená čísla $\mathbb{N}$. Selský rozum by nám nejspíše napověděl, že sudých čísel musí být „méně“ než přirozených, neboť S nenáleží všechna lichá přirozená čísla, zatímco množině $\mathbb{N}$ náleží. Z jistého pohledu tomu tak může být, ale z „perspektivy“ bijekce nikoliv. Pokud uvážíme zobrazení $f : \mathbb{N} \to S$, kde pro $n \in \mathbb{N}$ je $f(n) = 2n$, můžeme se snadno přesvědčit, že f je bijekcí[3].



Obrázek 6.5: Bijekce mezi množinami S a $\mathbb{N}$.

[3]Skutečně, inverzní zobrazení je $f^{-1} : S \to \mathbb{N}$, kde $f^{-1}(n) = n/2$.

Příklad 6.2.1. Další příklady bijekcí mezi $\mathbb{N}$ a jinými množinami.

(i) Bijekce mezi $\mathbb{N}$ a kladnými lichými čísly: $f_1 : \mathbb{N} \to \{2k-1 \mid k \in \mathbb{N}\}$, kde $f_1(n) = 2n-1$.

(ii) Bijekce mezi $\mathbb{N}$ a druhými mocninami: $f_2 : \mathbb{N} \to \{n^2 \mid n \in \mathbb{N}\}$, kde $f_2(n) = n^2$.

(iii) Bijekce mezi $\mathbb{N}$ a prvočísly.

Všimněme si, že všechny (zatím) uvažované množiny byly všechny vlastní podmnožiny $\mathbb{N}$. Toto však u konečných množin provést nelze, neboť libovolná vlastní podmnožina je vždy „menší“ než původní množina (velikosti těchto množin se pak liší v počtu „chybějících“ prvků). V případě nekonečných množin toto však není žádnou překážkou. Archimédův logický axiom, že *celek je větší než část* tak skutečně patří pouze do oblasti konečných množin. Toto se zdá být jako pěkná charakteristika odlišující konečné a nekonečné množiny.

Do této chvíle jsme termín „konečná“ a „nekonečná“ množina chápali intuitivně bez formální definice. Vzhledem k jasnosti těchto termínů v použitých kontextech nejspíše nebyl problém s jejich chápáním. Avšak díky výše zmíněnému máme již dostupný nástroj, jak definovat nekonečnou množinu.

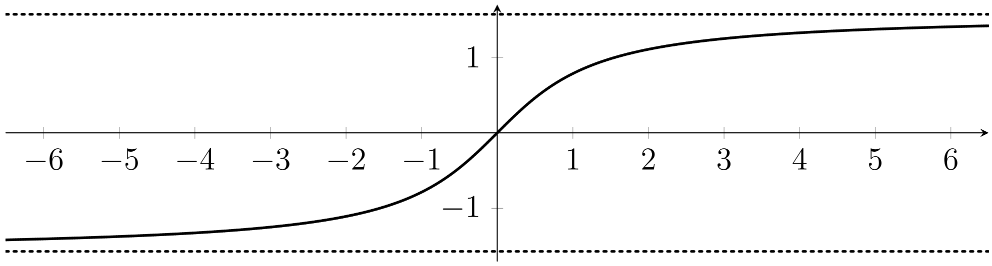
Definice 6.2.2 (Nekonečnost množiny)**.** Množinu libovolnou množinu X nazveme *nekonečnou*, pokud existuje vlastní podmnožina $X' \subset X$ (tj. $X' \subseteq X$ a $X' \neq X$) taková, že existuje bijektivní zobrazení $f : X \to X'$.

Jednoduše, množina je nekonečná, pokud existuje bijekce množiny na některou její vlastní podmnožinu. Nabízí se otázka, jak bychom mohli definovat konečnou množinu. Vzhledem k formalizaci „nekonečná množina“ v definici 6.2.2 bychom za konečnou množinu mohli jednoduše prohlásit množinu, která není nekonečná. Avšak tento termín můžeme zavést i více přirozeně. Pokud o množině řekneme, že je „konečná“, pak tím intuitivně rozumíme, že její počet prvků odpovídá nějakému přirozenému číslu, tj. $|A| = n$, kde $n \in \mathbb{N}_0$. Pokud si však vzpomeneme, přirozená čísla jsme si zaváděli pomocí množin, což znamená že se opět jedná o množiny. Za konečnou množinu tak můžeme prohlásit množinu, u níž **existuje bijekce na nějaké přirozené číslo**. (Pro úplnost bychom měli dokázat, že při této definici nemůže existovat množina, která by byla současně konečná a nekonečná, ale zde jej vynecháme.)

Pokud se nebudeme omezovat pouze na přirozená čísla, příklady zajímavých bijekcí najdeme i u reálných čísel $\mathbb{R}$.

Příklad 6.2.3. Ukázky bijekcí mezi množinou $\mathbb{R}$ některými jejími vlastními podmnožinami.

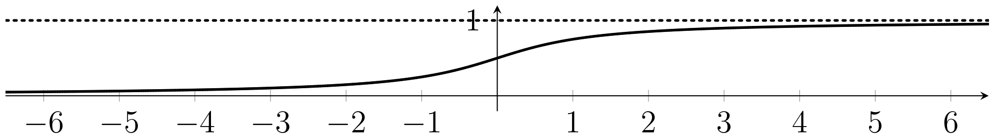
(i) Bijekce mezi $\mathbb{R}$ a intervalem $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$: $g_1 : \mathbb{R} \to \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, kde $g_1(x) = \operatorname{arctg} x$.



Obrázek 6.6: Graf funkce g_1.

(ii) Bijekce mezi $\mathbb{R}$ a intervalem $(0,1)$: $g_2 : \mathbb{R} \to (0,1)$, kde

$$g_2(x) = \frac{1}{\pi}\left(\operatorname{arctg} x + \frac{\pi}{2}\right)$$



Obrázek 6.7: Graf funkce g_2 („přeškálovaný" a posunutý graf arctg).

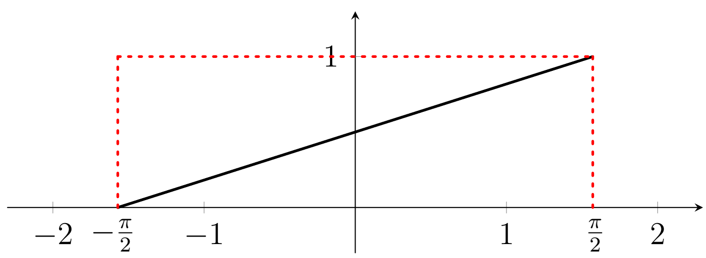
(iii) Stejně tak lze sestrojit bijekci z intervalu $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ do $\mathbb{R}$. Stačí vzít inverzní funkci ke g_2, tj. $g_3 : \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to \mathbb{R}$, kde $g_3(x) = g_1^{-1}(x) = \operatorname{tg} x$.

(iv) Bijekci můžeme sestrojit i mezi samotnými intervaly $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ a $(0,1)$. Tu můžeme nalézt složením funkcí g_3 a g_2, tj. $g_4 = g_3 \circ g_2$, protože

$$g_3 : \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to \mathbb{R} \text{ a } g_2 : \mathbb{R} \to (0,1)$$

Tedy celkově $g_4 : \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to (0,1)$, kde

$$g_4(x) = g_2(g_3(x)) = \frac{1}{\pi}\left(\underbrace{\operatorname{arctg}(\operatorname{tg} x)}_{\text{identita}} + \frac{\pi}{2}\right) = \frac{1}{\pi}\left(x + \frac{\pi}{2}\right) = \frac{1}{\pi}x + \frac{1}{2}.$$



Obrázek 6.8: Graf funkce g_4 (složení funkcí g_3 a g_2).

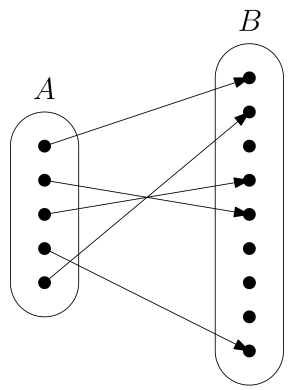
Lze vidět, že g_4 je skutečně bijekce, což ostatně plyne z bodu (iii) tvrzení 4.3.8 o vlastnostech skládání zobrazení.

(Převzato z [1], str. 4-5.)

Poznámka 6.2.4. Pochopitelně g_4 jsme mohli najít ihned, avšak tento složitější postup byl zvolen čistě pro ilustraci.

6.3 Spočetné a nespočetné množiny

V této sekci rozdělíme množiny na dva základní typy. Než tak však učiníme, zůstaneme ještě na chvíli u bijekcí mezi množinami, kterými jsme se zabývali v minulé sekci. Zde jsme se snažili ukázat souvislost mezi „velikostmi“ množin a existencí bijekce mezi nimi. V případě konečných množin však zcela běžně může nastat situace, kdy množiny mají různý počet prvků, tj. pokud $|A| = n$ a $|B| = m$, kde $n < m$. Je zřejmé, že bijekci mezi takovými množinami sestrojit nelze. Nicméně, stále můžeme sestrojit prosté zobrazení z A do B (viz obrázek 6.9).



Obrázek 6.9: Prosté zobrazení z množiny A do množiny B.

Takové zobrazení však nikdy nemůže být na. A naopak zobrazení z B do A může být na, ale nikdy ne prosté. Stejný princip platí i pro nekonečné množiny. V souvislosti s tímto si zavedeme následující termíny a značení.

Definice 6.3.1 (Subvalence a ekvipontence)**.** Nechť X a Y jsou libovolné množiny. Pak pokud

(i) existuje bijekce mezi X a Y, píšeme $X \approx Y$ (čteme „X je *ekvipotentní* Y“ nebo „X a Y mají *stejnou mohutnost*“.

(ii) existuje prosté zobrazení z X do Y, píšeme $X \preccurlyeq Y$ (čteme „X je *subvalentní* Y“ nebo „X má *menší nebo stejnou mohutnost* jako Y“).

(iii) platí $X \preccurlyeq Y$ a zároveň $X \not\approx Y$, píšeme $X \prec Y$ (čteme „X je *ostře subvalentní* Y“ nebo „X má *(ostře) menší mohutnost* než Y“).

Je vhodné podotknout, že pokud platí $X \approx Y$, pak $X \preccurlyeq Y$ i $Y \preccurlyeq X$, neboť bijekce je (z definice) prostá.[4]

[4]Opačná implikace, tj. $X \preccurlyeq Y \wedge Y \preccurlyeq X \Rightarrow X \approx Y$ platí též. Toto tvrzení se nazývá *Cantorova-Bernsteinova věta*. Její důkaz je však zcela nad rámec tohoto textu.

Z předchozích příkladů 6.2.1 a 6.2.3 bychom tak mohli zápis některých našich poznatků zkrátit jednoduše takto:

- $\mathbb{N} \approx \{2k - 1 \mid k \in \mathbb{N}\}$,
- $\mathbb{N} \approx \{n^2 \mid n \in \mathbb{N}\}$,
- $\mathbb{R} \approx (0,1)$, apod.

V definici 6.3.1 jsme použili slovo „mohutnost“. V případě konečných množin bychom tento termín nejspíše chápali ve smyslu **velikosti** množiny (tj. počtu prvků). U nekonečných množin zatím pouze víme, co znamená, že dvě množiny mají stejnou mohutnost, ale samotný termín nejsme schopni vysvětlit. Definice mohutnosti je však trochu složitější a zabývat se jí zde nebudeme. Zvídavý čtenář si však může nahlédnout do přílohy E pro přiblížení. Podrobněji se této problematice věnuje např. kniha [10], str. 167.

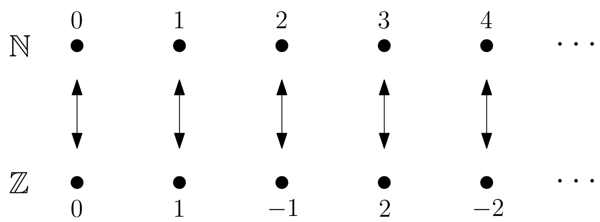
Podívejme se na trochu zajímavější korespondenci mezi celými a přirozenými čísly s nulou.

Věta 6.3.2. *Platí* $\mathbb{N}_0 \approx \mathbb{Z}$.

Důkaz. Pro důkaz sestrojíme bijekci mezi $\mathbb{N}_0$ a $\mathbb{Z}$. Zobrazení $f : \mathbb{N}_0 \to \mathbb{Z}$ definujeme předpisem

$$f(n) = \begin{cases} -n/2\,, & \text{pokud } 2 \mid n \\ (n+1)/2\,, & \text{jinak.} \end{cases}$$

Na obrázku 6.10 můžeme vidět, jakým způsobem spolu korespondují v f prvky $\mathbb{N}_0$ a $\mathbb{Z}$.



Obrázek 6.10: Znázornění zobrazení f.

Snadno se lze přesvědčit, že f je bijekce[5]. □

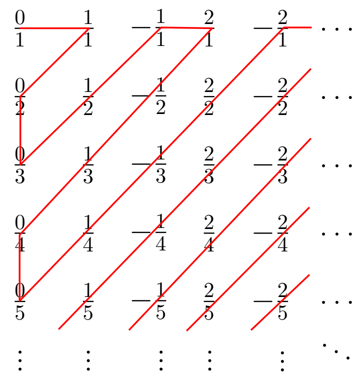
Překvapivější výsledek, ke kterému došel Georg Cantor, je ekvipotence množiny přirozených čísel $\mathbb{N}$ a racionálních čísel $\mathbb{Q}$. To může působit jako zarážející, neboť při pohledu na reálnou osu se zde racionální čísla vyskytují „četněji“ oproti přirozeným číslům, přesto však mezi těmito dvěma množinami existuje bijekce.

Věta 6.3.3. *Platí* $\mathbb{N} \approx \mathbb{Q}$.

[5] Jedná se vlastně o seřazení prvků $\mathbb{Z}$ do posloupnosti $0,1,-1,2,-2,\ldots$. Takto se standardně dokazuje, že množina má stejnou mohutnost jako $\mathbb{N}$.

Náznak důkazu. Uspořádejme všechna racionální čísla do „mřížky“ (viz obrázek 6.11). Začneme-li od zlomku $0/1$, tedy $f(0/1) = 1$. Pak lomená čára určuje pořadí, v němž zobrazíme dané prvky postupně na čísla $1,2,3,\dots$.

$$
\begin{array}{cccccc}
\frac{0}{1} & \frac{1}{1} & -\frac{1}{1} & \frac{2}{1} & -\frac{2}{1} & \cdots \\
\frac{0}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{2}{2} & -\frac{2}{2} & \cdots \\
\frac{0}{3} & \frac{1}{3} & -\frac{1}{3} & \frac{2}{3} & -\frac{2}{3} & \cdots \\
\frac{0}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{2}{4} & -\frac{2}{4} & \cdots \\
\frac{0}{5} & \frac{1}{5} & -\frac{1}{5} & \frac{2}{5} & -\frac{2}{5} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$



Obrázek 6.11: Znázornění zobrazovacího „algoritmu“ racionálních čísel na přirozená.

je možné sestrojit zobrazení $\mathbb{N}$ na[6] $\mathbb{Q}$. □

Definovaná subvalence „$\preccurlyeq$“ a ostrá subvalence „$\prec$“ v 6.3.1 nám může trochu naznačovat, že existují dvojice množin, které nemají stejnou mohutnost. S takovými jsme se zatím nesetkali v případě nekonečných množin. Jsou skutečně všechny nekonečné množiny stejně velké? Odpověď na tuto otázku jsme si již předložili v podsekci 1.2.2, kde jsme si zmínili, že Georg Cantor ukázal, že množina všech reálných čísel $\mathbb{R}$ má větší mohutnost než množina přirozených čísel $\mathbb{N}$. Způsob, kterým se tento fakt obvykle dokazuje, je dnes nazýván *Cantorova diagonální metoda*.

Věta 6.3.4. *Platí* $\mathbb{N} \prec \mathbb{R}$.

Důkaz. Důkaz rozdělíme na dvě části: $\mathbb{N} \not\approx \mathbb{R}$ a $\mathbb{N} \preccurlyeq \mathbb{R}$. Protože již víme, že $(0,1) \approx \mathbb{R}$, stačí dokázat $\mathbb{N} \not\approx (0,1)$.

Budeme postupovat sporem. Pro spor nechť existuje bijekce $f : \mathbb{N} \to (0,1)$. Obrazy jednotlivých přirozených čísel můžeme tak uspořádat do (očíslovaného) „seznamu“ $f(1), f(2), f(3), \dots$. Každé přirozené číslo tak „koresponduje“ s jistým desetinným číslem. Reálná čísla jsou jednoznačně určena svým desetinným rozvojem (a zakážeme-li periodu $\overline{9}$, jednoznačně svůj rozvoj určují).

$$
\begin{array}{rcccccc}
f(1) = & 0, & 4 & 6 & 1 & 1 & \dots \\
f(2) = & 0, & 9 & 9 & 4 & 2 & \dots \\
f(3) = & 0, & 5 & 1 & 0 & 6 & \dots \\
f(4) = & 0, & 7 & 2 & 7 & 2 & \dots
\end{array}
$$

Obrázek 6.12: Desetinné rozvoje obrazů přirozených čísel v f.

[6] Není prosté, neboť každé racionální číslo se v „seznamu“ vyskytuje nekonečně mnohokrát. Vynecháním opakovaných výskytů pak získáme prosté zobrazení.

Podle předpokladu musí být na tomto „seznamu“ (viz obrázek 6.12) **všechna** reálná čísla, protože každé je obrazem nějakého přirozeného čísla. Zaměřme se nyní na diagonálu tvořenou těmito desetinnými rozvoji (viz obrázek 6.13).

$$\begin{array}{rcccccc}
f(1) = & 0, & 4 & 6 & 1 & 1 & \dots \\
f(2) = & 0, & 9 & 9 & 4 & 2 & \dots \\
f(3) = & 0, & 5 & 1 & 0 & 6 & \dots \\
f(4) = & 0, & 7 & 2 & 7 & 2 & \dots
\end{array}$$

Obrázek 6.13: Diagonála tvořená obrazy v f.

Pokud bychom si číslice na diagonále uspořádali, přidáním „0,“ bychom opět dostali nějaký desetinný rozvoj čísla, jež si označíme x, tj. v tomto případě $x = 0{,}4902\dots$. Je takové číslo na našem seznamu? To nemůžeme vědět. Mohlo by se stát (při nešťastné volbě obrazů $f(1),f(2),\dots$), že číslice na diagonále budou tvořit periodu $\overline{9}$, kterou jsme vyloučili. My však z toho čísla můžeme vytvořit nový desetinný rozvoj. Definujme zobrazení $d : \{0,1,2,\dots,9\} \to \{0,1\}$ předpisem:

$$d(i) = \begin{cases} 1\,, & \text{pokud } i = 0 \\ 0\,, & \text{pokud } i \neq 0. \end{cases}$$

Uvažujme nyní číslo $x \in (0,1)$, jehož desetinný rozvoj je tvořený číslicemi na diagonále, které si označíme $i_1,i_2,i_3,\dots$, tzn. $x = 0{,}i_1,i_2,i_3,\dots$. Nové číslo x' definujeme desetinným rozvojem

$$0{,}d(i_1)d(i_2)d(i_3)\dots$$

Pokud má tedy číslo n ve svém obrazu $f(n)$ na n-tém místě (tedy na diagonále) svého desetinného rozvoje číslo různé od nuly, pak číslo x' bude mít na dané pozici nulu. Naopak pokud bude číslo na dané pozici číslo 0, pak x' zde bude mít číslo 1. Např. pro diagonálu na obrázku 6.13 výše bude $x' = 0{,}1101\dots$.

Číslo x' jistě nemůže obsahovat periodu $\overline{9}$. Přitom stále platí, že $x' \in (0,1)$ a podle předpokladu se musí nacházet v „seznamu“, resp. $\exists n \in \mathbb{N} : f(n) = x'$. Může toto nastat? Nemůže, a to z principu konstrukce! Číslo x' se totiž liší od každého čísla v seznamu (minimálně) v cifře na diagonále. Tzn. že x' nema v sobrazení f svůj vzor, což je spor s předpokladem, že f je bijekce, protože není na.

Z toho celkově plyne, že $\mathbb{N} \not\approx (0,1)$ a tedy $\mathbb{N} \not\approx \mathbb{R}$.

Mezi množinami $\mathbb{N}$ a $\mathbb{R}$ tedy neexistuje bijekce. K důkazu $\mathbb{N} \preccurlyeq \mathbb{R}$, stačí nalézt prosté zobrazení z $\mathbb{N}$ do $\mathbb{R}$. Protože $\mathbb{N} \subset \mathbb{R}$, stačí zvolit identitu, tedy $g : \mathbb{N} \to \mathbb{R}$, kde $g(n) = n$. □

Jak můžeme vidět, skutečně existují nekonečné množiny, které mají různé mohutnosti, a to $\mathbb{N}$ a $\mathbb{R}$. Tento poznatek nám dává základ pro následující klasifikaci množin.

Definice 6.3.5 (Spočetná a nespočetná množina)**.** Nechť X je libovolná množina. Pak říkáme, že X je

(i) *spočetná*, pokud $X \preccurlyeq \mathbb{N}$.

(ii) *nespočetná*, pokud $X \not\preccurlyeq \mathbb{N}$.

Množina X je tedy spočetná, pokud existuje prosté zobrazení X do $\mathbb{N}$ (resp. existuje bijekce na nějakou podmnožinu $\mathbb{N}$). Naopak pokud takové zobrazení X do $\mathbb{N}$ neexistuje, pak X nazýváme nespočetnou[7]. U konečných množin se můžeme přesvědčit, že **všechny jsou spočetné**; stačí spočítat jejich prvky.

Věta 6.3.6. *(i) Množiny přirozených čísel $\mathbb{N}$, celých čísel $\mathbb{Z}$ a racionálních čísel $\mathbb{Q}$ jsou spočetné.*

(ii) Množiny reálných čísel $\mathbb{R}$ a komplexních čísel $\mathbb{C}$ jsou nespočetné.

Důkaz. Triviálně platí $\mathbb{N} \preccurlyeq \mathbb{N}$. Zbývající části plynou z 6.3.2, 6.3.3 a 6.3.4. □

Podobně ostatní množiny zmíněné v příkladech 6.2.1 a 6.2.3 můžeme takto klasifikovat:

- množina $\{2k - 1 \mid k \in \mathbb{N}\}$ je spočetná,
- množina $\{p \mid p \text{ je prvočíslo}\}$ je spočetná,
- interval $(0,1)$ je nespočetný,
- interval $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ je nespočetný.

Takto se nám rozpadají množiny do dvou velkých skupin. Mohlo by se dokonce zdát, že pokud libovolná množina X není spočetná, tj. je nespočetná, pak nutně $X \approx \mathbb{R}$. Ve skutečnosti ale existují množiny, které jsou nespočetné, ale nemají stejnou mohutnost jako $\mathbb{R}$. S tímto nám pomůže tzv. *Cantorova věta.*

Věta 6.3.7 (Cantorova)**.** *Pro libovolnou množinu X platí*

$$X \prec \mathcal{P}(X).$$

K důkazu lze opět použít Cantorovu diagonální metodu. Všimněte si, že ve větě 6.3.7 uvažujeme spočetnou i nespočetnou množinu X. Zde již důkaz nemůžeme znázornit jako u věty 6.3.4, protože pro nespočetnou množinu X nelze její prvky seřadit do posloupnosti. Způsob důkazu se tak bude zdánlivě vymykat předešlému postupu, nicméně můžete si zkusit rozmyslet, že myšlenka je ve své podstatě stejná. Pro konečné množiny X lze nalézt důkaz této věty v příloze E, věta E.0.1.

Důkaz. Nejdříve ukážeme, že $X \not\approx \mathcal{P}(X)$ a pak $X \preccurlyeq \mathcal{P}(X)$. Pro spor předpokládejme, že existuje bijekce $f : X \to \mathcal{P}(X)$. Ukážeme, že f není na, tj. nalezneme prvek v $\mathcal{P}(X)$, který nemá v f vzor. Definujme množinu S takto:

$$S = \{x \in X \mid x \notin f(x)\}.$$

[7]Termíny „spočetný“ a „nespočetný“ v tomto kontextu vychází z faktu, že prvky spočetných množin lze „spočítat“, tedy lze je očíslovat přirozenými čísly. Naopak u nespočetných toto nelze.

Množina S tedy obsahuje všechny prvky x, které nenáleží svému obrazu v f (tedy odpovídající podmnožině množiny X). Podle předpokladu f je bijekce a tedy je na. To znamená, že $\exists s \in X : f(s) = S$, tedy S má vzor v f. Jak se ale ukáže, taková množina nemůže mít v f vzor. Pro prvek musí platit buď, že $s \in S$, nebo $s \notin S$.

- $s \in S$. Tzn. $s \in f(s)$. Z definice množiny S musí pro s platit, že $s \notin f(s) = S$, což je spor.
- $s \notin S$. Pak prvek s splňuje, že $s \in f(s)$ a podle definice množiny S platí $s \in S = f(s)$, čímž jsme též došli ke sporu[8].

V obou případech jsme dostali spor, tedy platí $X \not\approx \mathcal{P}(X)$.

Pro důkaz $X \preccurlyeq \mathcal{P}(X)$ můžeme definovat prosté zobrazení $g : X \to \mathcal{P}(X)$ předpisem $g(x) = \{x\}$. $\square$

Poznámka 6.3.8. Indukcí můžeme toto tvrzení rozšířit, tedy platí

$$X \prec \mathcal{P}(X) \prec \mathcal{P}(\mathcal{P}(X)) \prec \mathcal{P}(\mathcal{P}(\mathcal{P}(X))) \prec \dots$$

Tedy skutečně existuje nekonečně mnoho množin vzájemně různých mohutností. Speciálně, pro $X = \mathbb{N}$ máme

$$\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \prec \mathcal{P}(\mathcal{P}(\mathbb{N})) \prec \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) \prec \dots$$

Lze dokonce ukázat, že $\mathcal{P}(\mathbb{N}) \approx \mathbb{R}$, ale důkaz zde vynecháme.

Můžeme tak skutečně konstruovat stále „mohutnější“ množiny, čímž vzniká jistá „hierarchie“. S tou se však pojí netriviální otázka. V roce 1878 vyslovil Georg Cantor domněnku, že libovolná podmnožina reálných čísel je buď spočetná, nebo má stejnou mohutnost jako $\mathbb{R}$. ([5], str. 98.) Formálněji

$$\forall A \subseteq \mathbb{R}, A \text{ je nekonečná} : A \approx \mathbb{N} \vee A \approx \mathbb{R}.$$

Též ekvivalentně: *existuje množina X taková, že $\mathbb{N} \prec X \prec \mathbb{R}$?* Později byla tato domněnka nazvána *hypotézou kontinua.* Cantor a mnozí další členové tehdejší matematické komunity se snažili marně dokázat tuto domněnku. David Hilbert dokonce zařadil tuto otázku na první místo svého seznamu dvaceti tří problémů, který později prezentoval na druhém mezinárodním matematickém kongresu v Paříži v roce 1900.

Podstatný krok učinil v roce 1940 Kurt Gödel. Ukázalo se, že hypotézu kontinua není možné vyvrátit z axiomů ZF. Později v roce 1965 americký matematik Paul Cohen (1934-2007) dokázal, že hypotézu kontinua nelze z těchto axiomů ani dokázat. Z toho plyne, že se jedná o tzv. *nerozhodnutelné tvrzení.* Jejich existence byla díky Gödelovým objevům známa již dříve a souvisí s nimi tzv. *Gödelovy věty o neúplnosti* (viz historický úvod 1.2.4). Hypotéza kontinua je nezávislá na axiomech teorie množin, což znamená, že ji lze přijmout za axiom. Jejím přijetím do systému axiomů by však vznikla jiná nerozhodnutelná tvrzení v rámci této nové teorie. ([2], str. 101.)

[8] Jedná se o podobný spor, jako v Russellově paradoxu (viz podsekce 1.2.2).

Seznam použité literatury

[1] M. Rmoutil. *Logika a teorie množin. [online]*, Citováno 4. května 2022. Dostupné z: `https://www2.karlin.mff.cuni.cz/~rmoutil/NMTM503/TM.pdf`.

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

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

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

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

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

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

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

[9] L. Pick. *Strašidelné matematické paradoxy aneb S rozumem v koncích. [online]*, Citováno 1. května 2022. Dostupné z: `https://youtu.be/6Ti44xNaEm8`.

[10] Michael D. Potter. *Set theory and its philosophy: A critical introduction.* Clarendon, 2009. ISBN 9781423788850.

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

[12] *karlin.mff.cuni.cz. [online]*, Citováno 24. března 2022. Dostupné z: `https://www2.karlin.mff.cuni.cz/~portal/logika/?page=prim`.

Příloha A

Důkazy

V matematice se lze setkat s celou řadou různých tvrzení. Od primitivních, jejichž platnost je zřejmá až po složitější, nad jejichž platností je třeba se více zamyslet. Čtenář se nejspíše zatím spíše setkával s matematikou, která zahrnovala užívání jistých matematických postupů. Např. zjednodušování algebraických výrazů, řešení soustav rovnic, ověřování trigonometrických identit, aj. 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 používáme v matematice, které budeme dále v textu využívat.

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

- *Axiom.* Tvrzení, které považujeme za pravdivé a nedokazujeme jej. S axiomatikou jsme se již částečně seznámili v historické předmluvě (viz 1.2.4).
- *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.

Důkazem v matematice rozumíme určitou „posloupnost" výroků, z nichž logicky plyne nutná platnost tvrzení.

A.1 Důkaz přímý

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 2.1.11

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

Z tohoto faktu vyplývá, že pokud je každá z dílčích implikací pravdivá, pak je nutně pravdivá[1] i implikace $A \Rightarrow C$, kterou jsme chtěli dokázat[2].

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 použili jistou generalizaci. Předvedený jednořádkový 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] Víme-li tedy, že že platí $(A \Rightarrow B) \wedge (B \Rightarrow C)$, můžeme podle pravidla modus ponens přijmout za pravdivou $A \Rightarrow C$.

[2] 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* $x,y \in \mathbb{R}$ *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 [11], str. 79 a [12], 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 2.1.11):

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

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, musí platit $3 \mid y$. Pokud by totiž platilo $3 \nmid y$, pak $3 \nmid x \wedge 3 \nmid y$, z čehož by plynulo, že $3 \nmid xy$.
- $3 \nmid y$. 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[3], 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.2 Důkaz nepřímý

Některá tvrzení v matematice může být obtížné dokázat přímým důkazem. 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 2.1.11, 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.2.1. *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. Zde bude 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 $k \in \mathbb{Z}$. Prozkoumáme případ $x = 3k + 1$ (pro případ $x = 3k + 2$ je důkaz analogický). Pak

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

[3]Termín *bez újmy na obecnosti* (někdy zkráceně *BÚNO*) se v matematických textech používá v situacích, kdy může nastat více možností, avšak jejich důkazy jsou analogické, takže stačí probrat jednu z těchto možností.

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.2.2. *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 $x \notin A$, zřejmě $A \cup B \neq A$.
($\Leftarrow$). 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 [11], str. 111.)

A.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 2.1.11 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 2.1.11) 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, právě když platí její předpoklad, ale neplatí její závěr.

Tvrzení A.3.1. *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.

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

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 neplatí. To znamená, že znegované tvrzení je nepravdivé, což je spor s předpokladem, že je-li a sudé a b liché, pak $4 \mid (a^2 + 2b^2)$. Tedy platí původní tvrzení, což jsme chtěli dokázat. □

(Převzato z [11], str. 126) V případě důkazu sporem je asi nejznámější (a též i nejstarší dochovaný) důkaz, že číslo $\sqrt{2}$ je iracionální.

Tvrzení A.3.2. *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 znamená

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

O každém zlomku navíc 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 je možné 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. Při spočítání $(2l-1)^2$ vyjde liché číslo.) To znamená, 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. Proto nemůže neexistovat zlomek p/q, který by byl roven $\sqrt{2}$ a byl v základním tvaru. □

Tvrzení A.3.3. *Prvočísel je nekonečně mnoho.*

Důkaz. Pro spor naopak předpokládejme, 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.4 Důkaz matematickou indukcí

K této důkazové technice si na úvod ukažme příklad. Čtenáři si možná vzpomene na vzorec pro součet prvních n členů geometrické posloupnosti. Při jeho znalosti by tak pro nás neměl být problém určit součet

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

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

$$\begin{aligned} 2^0 &= 1 = 2 - 1, \\ 2^0 + 2^1 &= 3 = 4 - 1, \\ 2^0 + 2^1 + 2^2 &= 7 = 8 - 1, \\ 2^0 + 2^1 + 2^2 + 2^3 &= 15 = 16 - 1. \end{aligned}$$

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 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

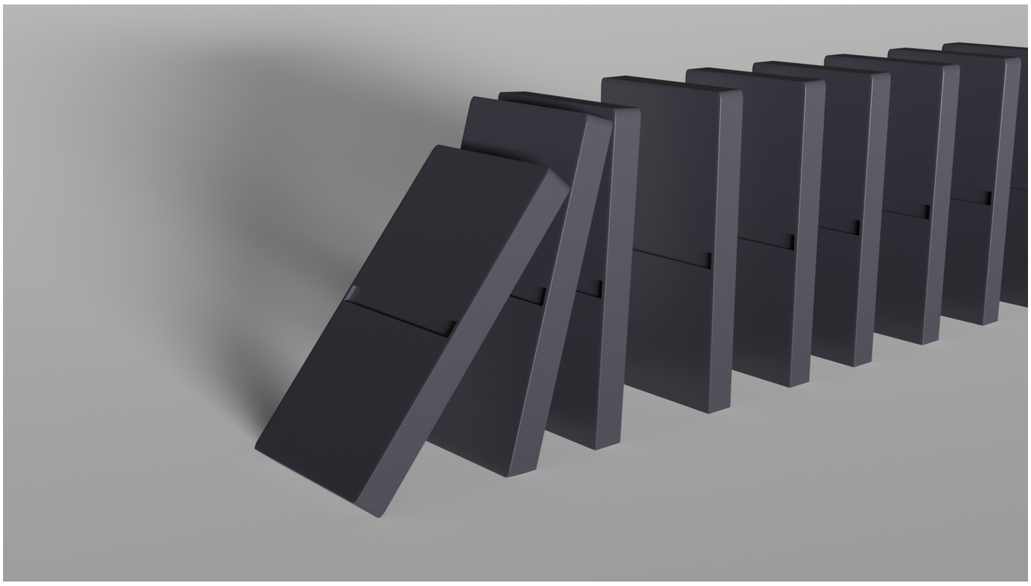
$$\sum_{k=0}^{n_0+1} 2^k = \sum_{k=0}^{n_0} 2^k + 2^{n_0+1}.$$

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), když tvrzení platí pro $n = 0$, pak platí i pro $n = 1$ (pro $n_0 = 0$). Pro $n = 1$ pak opět podle (ii) dostaneme, 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. Takto postupně dostaneme, že tvrzení tedy platí pro všechna $n \in \mathbb{N}$ (viz obrázek A.1).



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

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 [7], str. 32.)

Tento postup vychází z tzv. *principu matematické indukce*, který lze zformulovat jako větu.

Věta A.4.1 (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 [11], str. 144.)
Tuto větu v různých textech lze najít i v jiných formulacích. Uveďme si ještě jeden příklad.

Úmluva A.4.2. Při aplikaci indukčního předpokladu se někdy píše zkratka *I. P.*, čehož se budeme držet v dalším textu.

Tvrzení A.4.3. *Pro každé přirozené $n \geq 5$ platí $2^n > n^2$.*

Důkaz. Tvrzení dokážeme indukcí podle n.

- Pro nejmenší hodnotu $n = 5$ dostáváme $2^5 = 32 > 25 = 5^2$, 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 $2n_0^2 > (n_0 + 1)^2$.

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

  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 [11], str. 153.)

Tvrzení A.4.4. *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 $n_0 + 1$ prvcích. 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 také $X = T \cup T'$. 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. $B \in T$, 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[4] 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, celkový počet prvků je $2^{n_0} + 2^{n_0} = 2^{n_0+1}$, což jsme chtěli dokázat. □

[4] 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 4.3.

Příloha B

Dodatky k logice

V kapitole o výrokovém a predikátovém počtu jsme pracovali s výrokovými a později predikátovými formulemi, kde jsme si pouze neformálně vysvětlili, co pod těmito termíny rozumíme. Formálněji můžeme k těmto záležitostem přistoupit pomocí následující metadefinice.

Definice B.0.1 (Výroková a atomická formule)**.** Termíny definujeme rekurentně:

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

(ii) Jsou-li φ a ψ 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 [2], str. 14 a [5], str. 30).

Definice výrokové formule B.0.1 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 B.0.1 výrokovými formulemi. Podle (ii) jsou pak formulemi i výrazy

$$(A) \wedge (B)\ ,\ (A) \vee (C) \text{ a } \neg(B). \tag{B.1}$$

Nyní můžeme opakovaně použít (ii) k sestrojení dalších složitějších formulí. Tedy užitím formulí (B.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.

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

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 B.0.2. Mějme výraz

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

Ověřte, zda φ je výroková formule.

Řešení. Aby φ 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 φ_1 zřejmě je formulí, neboť A a C jsou atomické formule. Ovšem u φ_2 lze již vidět, že výraz nesplňuje definici výrokové formule, neboť u $\neg(C)$ chybí vnější závorky. Z bodu (iii) definice B.0.1 tedy plyne, že výraz φ **není výrokovou formulí**, neboť jej nelze získat pomocí pravidel (i) a (ii). □

Čtenáře možná již napadlo, že formule, které jsme sestrojili z definice B.0.1, jsou zapsány poměrně komplikovaně, především co do nadměrného používání závorek. Např. výraz

$$A \wedge \neg C, \tag{B.2}$$

není podle B.0.1 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 B.0.2, i při vypuštění uzávorkování u výrazu φ_2 by dávalo smysl interpretovat výraz

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

jako výrok „Jestliže platí A nebo B, pak neplatí C.“.

Příloha C

Dodatky k axiomům teorie množin

Ještě jedny známé vztahy pro množiny jsou tzv. *De Morganovy vzorce* (viz obrázek C.1), které si zde zformulujeme jako větu.

Věta C.0.1 (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 na pravé a levé straně jsou si rovny. Z axiomu extenzionality (ZF2) 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 platí $x \in \bigcap_{i=1}^{n} (A \setminus X_i)$. Z definice rozdílu množin (viz 3.2.2) musí podle předpokladu 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:

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

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 náleží množině $A \setminus X_i$ pro libovolné i, kde $1 \leq i \leq n$. Tj.

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

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.

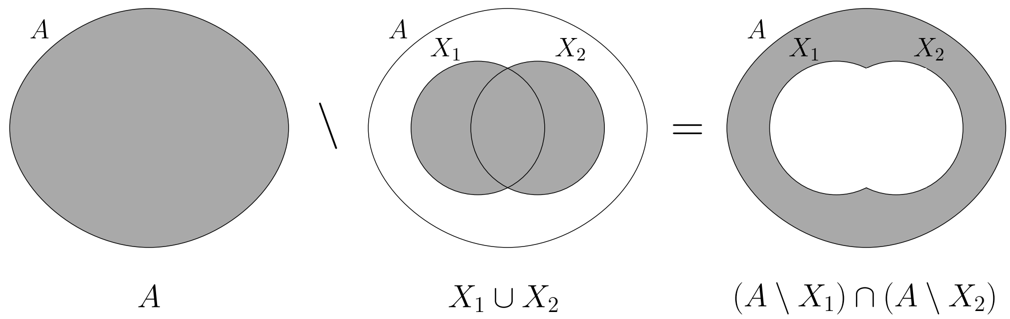
(⇐). Podobně ukážeme opačnou implikaci, tj. pokud $x \in \bigcap_{i=1}^{n} (A \setminus X_i)$, pak $x \in A \setminus (\bigcup_{i=1}^{n} X_i)$. Nechť je tedy dáno $x \bigcap_{i=1}^{n} (A \setminus X_i)$. Z předchozího již víme, že

$$\begin{aligned} x \in \bigcap_{i=1}^{n} (A \setminus X_i) &\Rightarrow \forall i \in \{1,\dots,n\} : x \in A \setminus X_i \\ &\Rightarrow x \in A \wedge \forall i \in \{1,\dots,n\} : x \notin X_i \\ &\Rightarrow x \in A \wedge x \notin \bigcup_{i=1}^{n} X_i \end{aligned}$$

a tedy

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

□



Obrázek C.1: De Morganovy vzorce pro $n = 2$.

C.1 Schéma axiomů nahrazení

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

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 4.3.1. V tomto případě můžeme tak φ chápat jako formuli udávající, zda obrazem prvku u je prvek v.

Druhá část

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

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 lze uvažovat „rozumné soubory“, které bez schématu axiomů nahrazení nejsou množinami. 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 φ 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.

C.2 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 $x \cap u = \emptyset$. Protože však pouze x' je prvkem u, pak musí nutně platit (protože $x' \neq \emptyset$), že $x' \cap u = \emptyset$. To ale neplatí!

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

neboť $x' \in x'$. Tzn. u tedy **nesplňuje** axiom fundovanosti a není tak množinou v ZF. Tím pádem nemůže být množina ani x' (kdyby ano, tak i u je množina podle axiomu dvojice (ZF3)).

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 „$\in$“ množin

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

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.

Příloha D

Dodatky k budování číselných množin

Věta D.0.1. $(\mathbb{N}_0, \leq)$ *je lineárně uspořádaná množina.*

Důkaz. Je-li množina $\mathbb{N}_0$ lineárně uspořádaná vzhledem k relaci „$\leq$“, pak tato relace musí být **reflexivní**, **antisymetrická** a **tranzitivní** (pro připomenutí viz definice 5.3.1) a dále každá dvojice prvků $n,m \in \mathbb{N}_0$ musí být porovnatelná, tj. $n \leq m \vee m \leq n$.

- **Reflexivita**. Z definice relace „$\leq$“ v 5.5.2 triviálně pro libovolné přirozené číslo n platí $n \leq n$.
- **Antisymetrie**. Nechť $n,m \in \mathbb{N}_0$, přičemž $n \leq m \wedge m \leq n$. Chceme ukázat, že $n = m$. Pokud platí $n \leq m \wedge m \leq n$, pak musí platit

  $$(n < m \vee n = m) \wedge (m < n \vee n = m) \text{ neboli } n = m \vee (n < m \wedge m < n).$$

  Případ $n < m \wedge m < n$ nemůže nastat, což lze ukázat sporem: nechť platí $n < m \wedge m < n$, tj. podle definice $n \in m \wedge m \in n$. Z bodu (i) lemmatu 5.5.3 by plynulo $n \subset m \wedge m \subset n$ a z tranzitivity inkluze máme $n \subset n$, což je spor.
- **Tranzitivita**. Nechť $n,m,\ell \in \mathbb{N}_0$, taková, že platí $n \leq m \wedge m \leq \ell$. Chceme ukázat, že $n \leq \ell$.

  Pokud platí $n = m$, $m = \ell$ nebo $n = \ell$, pak tvrzení jistě platí. Předpokládejme nyní, že $n \neq m \wedge m \neq \ell \wedge n \neq \ell$. Podle bodu (iii) lemmatu 5.5.3 dostáváme $n \subset m \wedge m \subset \ell$ a tedy $n \subset \ell$. Opět podle tvrzení (iii) odvodíme $n \leq \ell$.

Tedy relace „$\leq$“ na $\mathbb{N}_0$ je skutečně uspořádáním. Fakt, že toto uspořádání je lineární plyne přímo z důsledku 5.5.4. □

Příloha E

Dodatky k porovnávání nekonečných množin

Dodatečná ukázka Cantorova diagonálního argumentu při důkazu Cantorovy věty pro spočetné množiny.

Věta E.0.1. *Pro libovolnou spočetnou množinu X platí*

$$X \prec \mathcal{P}(X).$$

Důkaz. Ukážeme, že $X \not\approx \mathcal{P}(X)$ (případ $X \preccurlyeq \mathcal{P}(X)$ již známe). K tomu lze přistoupit sporem. Pro spor nechť $X \approx \mathcal{P}(X)$, tzn. existuje bijekce $f : X \to \mathcal{P}(X)$. Obdobně jako v důkazu věty 6.3.4, i zde ukážeme, že f není na. Obrazy prvků $x_i \in X$ tak můžeme „uspořádat" do „seznamu" $f(x_1)$,$f(x_2)$,$f(x_3)$,$\ldots$. Podmnožinu A můžeme z množiny sestrojit X tak, že pro každý z prvků množiny X určíme, zda náleží A či nikoliv. Označíme-li si případ $x \in A$ písmenem A a případ $x \notin A$ jako N, pak zmíněný „seznam" bychom mohli znázornit podobně jako na obrázku E.1.

$$X = \{x_1, x_2, x_3, x_4, x_5, \ldots\}$$

$$\begin{array}{lcccccc}
f(x_1): & A & N & A & N & A & \ldots \\
f(x_2): & N & N & A & A & N & \ldots \\
f(x_3): & A & N & N & N & N & \ldots \\
f(x_4): & N & A & N & A & N & \ldots \\
f(x_5): & A & N & N & N & A & \ldots
\end{array}$$

Obrázek E.1: Podmnožiny (obrazy) množiny X určené náležením každého z prvků.

Opět se zaměříme na diagonálu tohoto seznamu.

$$
\begin{array}{rcl}
 & & X = \{x_1, x_2, x_3, x_4, x_5, \ldots\} \\
f(x_1) & : & A \quad N \quad A \quad N \quad A \quad \ldots \\
f(x_2) & : & N \quad N \quad A \quad A \quad N \quad \ldots \\
f(x_3) & : & A \quad N \quad N \quad N \quad N \quad \ldots \\
f(x_4) & : & N \quad A \quad N \quad A \quad N \quad \ldots \\
f(x_5) & : & A \quad N \quad N \quad N \quad A \quad \ldots
\end{array}
$$

Obrázek E.2: Diagonála seznamu podmnožin množiny X.

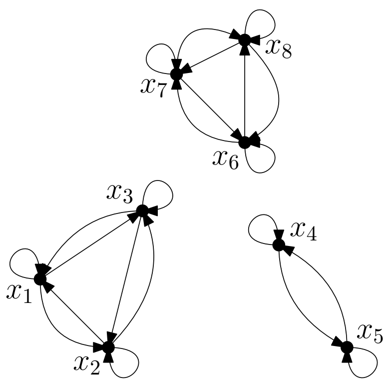
Zkonstruujeme množinu S tak, že každý prvek x na diagonále jí náleží právě tehdy, když nenáleží podmnožině (tedy obrazu $f(x)$) v příslušném řádku. Evidentně množina S je podmnožinou X. Zároveň se však od každé podmnožiny na seznamu liší minimálně v prvku na diagonále. To znamená, že S nemůže být na seznamu, čímž dostáváme spor. □

E.1 Relace ekvivalence

Zmíněné druhy relací nám dovolují definovat dva jejich nejdůležitější typy, jednomu z nichž se budeme dále přednostně věnovat. Začneme prvním z nich.

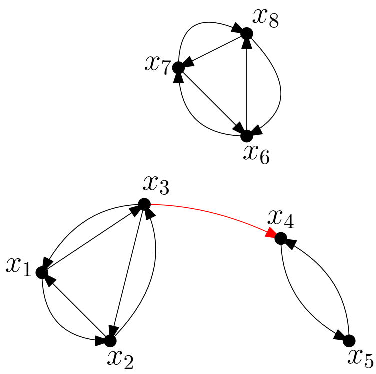
Definice E.1.1 (Relace ekvivalence)**.** Nechť R je relace na množině X. Řekneme, že R je *relací ekvivalence na* X (nebo jen *ekvivalencí na* X), pokud je *reflexivní*, *symetrická* a *tranzitivní*.

Ač se to nemusí zdát, tento typ relace má velmi příjemné vlastnosti. Jak si ji představit? Příkladem může být třeba relace R na množině $X = \{x_1, \ldots, x_7\}$ znázorněná na obrázku E.3 níže.



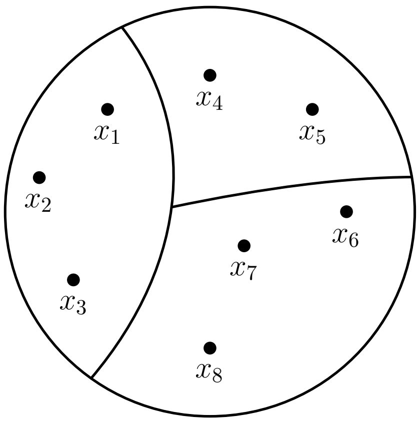
Obrázek E.3: Příklad relace ekvivalence R na X.

Pokud by však byl např. prvek x_3 v relaci prvkem x_4, pak by již R nebyla ekvivalencí, jak lze naopak vidět z obrázku E.4.



Obrázek E.4: Relace $R \cup (x_3,x_4)$ na X.

Všimněte si, že na obrázku E.3 jsou prvky rozděleny na „ostrůvky“, kde v rámci každého z nich jsou spolu všechny prvky v relaci[1]. (Zkuste si z definice rozmyslet, že to tak vždy musí být.) Zakreslovat relaci ekvivalence dosavadním způsobem se tak stává již celkem nevýhodným, neboť pro větší množství ekvivalentních prvků již zakreslovat všechny vztahy šipkami je v tomto případě poměrně zdlouhavý proces (např. pro 5 ekvivalentních prvků bychom museli kreslit 25 šipek). Úspornější a taktéž názornější pro nás bude si pouze schématicky rozdělit prvky do skupinek (relace mezi nimi z definice ekvivalence považujeme za samozřejmé), např. jako na obrázku E.5.



Obrázek E.5: Schématické znázornění ekvivalence R na X.

Definujme si nyní tyto „ostrůvky“ trochu formálněji.

Definice E.1.2 (Třída ekvivalence)**.** Nechť R je relace ekvivalence na množině X a nechť $x \in X$. Pak definujeme množinu

$$[x]_R = \{y \mid xRy\},$$

kterou nazýváme *třída ekvivalence R určená prvkem x*.

Třída ekvivalence $[x]_R$ jistého prvku x tak obsahuje všechny prvky, které jsou s x ekvivalentní, tj. v relaci R. Z příkladu výše je vidět že platí:

[1] U relace ekvivalence též říkáme, že prvky jsou spolu *ekvivalentní*.

- $[x_1]_R = [x_2]_R = [x_3]_R = \{x_1,x_2,x_3\}$,
- $[x_4]_R = [x_5]_R = \{x_4,x_5\}$,
- $[x_6]_R = [x_7]_R = [x_8]_R = \{x_6,x_7,x_8\}$.

Příklad E.1.3. Další příklady relací ekvivalence a jejich tříd.

(i) $(\mathbb{N}, =)$ (rovnost přirozených čísel) je relace ekvivalence, kde každý prvek tvoří samostatnou třídu ekvivalence.

$$\begin{aligned}
[1]_R &= \{1\} \\
[2]_R &= \{2\} \\
&\vdots
\end{aligned}$$

(ii) Relace *„mít stejnou paritu“*[2] na množině $\mathbb{Z}$ je relace ekvivalence o dvou třídách (sudá a lichá čísla).

$$\begin{aligned}
[1]_R &= \{-1,1,-3,3,-5,5,\dots\} \\
[2]_R &= \{0,-2,2,-4,4\dots\} \\
&\vdots
\end{aligned}$$

(iii) Relace „mít stejný zbytek po celočíselném dělení 5“ na množině $\mathbb{Z}$ je relace ekvivalence o pěti třídách (čísla 0–4 jako zbytek po celočíselném dělení).

$$\begin{aligned}
[0]_R &= \{0,5,10,\dots\} \\
[1]_R &= \{1,6,11,\dots\} \\
[2]_R &= \{2,7,12,\dots\} \\
[3]_R &= \{3,8,13,\dots\} \\
[4]_R &= \{4,9,14,\dots\}
\end{aligned}$$

(iv) Relace „mít stejnou absolutní hodnotu“ na množině $\mathbb{R}$ je relace ekvivalence, kde každá třída obsahuje prvek x a $-x$ pro všechna $x \in \mathbb{R}$.

$$\begin{aligned}
[0]_R &= \{0\} \\
[1]_R &= \{-1,1\} \\
[\sqrt{2}]_R &= \left\{\sqrt{2},-\sqrt{2}\right\} \\
[\sqrt[4]{30}]_R &= \left\{\sqrt[4]{30},-\sqrt[4]{30}\right\} \\
&\vdots
\end{aligned}$$

[2] Tzn. obě čísla jsou sudá nebo lichá.

E.2 Mohutnost množiny

V sekci jsme v definici subvalence a ekvipotence 6.3.1 zmínili pojem „mohutnost“ (ostatně zmínili jsme jej ue v historickém úvodu). Již víme, co je míněno pod tvrzením, že množina „má větší/stejnou mohutnost“ jako jiná množina. To nám však pouze dává představu, jak mohutnosti porovnávat. Jak tuto vlastnost množiny explicitně vyjádřit?

V případě konečných množin rozumíme pod „mohutností“ množiny jednoduše její velikost (tj. počet prvků), kterou reprezentuje nějaké přirozené číslo. U nekonečných množin je to však složitější. Nelze říci, že mohutnost je ∞. Podle této logiky by pak muselo platit např. $|\mathbb{N}| = |\mathbb{R}| = \infty$. To by však nebylo konzistentní s definicí, že dvě množiny mají stejnou mohutnost, když mezi nimi existuje bijekce, protože podle věty 6.3.4 víme, že $\mathbb{N} \prec \mathbb{R}$. Na mohutnost množiny lze nahlížet i trochu abstraktněji.

Pro lehčí pochopení se na chvíli přesuňme ke geometrii. Uvážíme-li relaci „být rovnoběžný s“, tj. „$\parallel$“ na množině všech přímek v rovině, jaké vlastnosti splňuje?

- **Reflexivita**. Každá přímka je rovnoběžná sama se sebou, tj. pro přímku p platí $p \parallel p$.
- **Symetrie**. Platí-li $p \parallel q$, pak platí i $q \parallel p$.
- **Tranzitivita**. Je-li přímka p rovnoběžná s přímkou q a zároveň q je rovnoběžná s přímkou r, pak určitě $p \parallel r$.

Tedy „$\parallel$“ je relací ekvivalence na množině přímek v rovině. Na základě tohoto poznatku, máme-li libovolnou přímku p, jaké přímky obsahuje třída ekvivalence $[p]_{\parallel}$? Budou to právě takové přímky, které jsou rovnoběžné s přímkou p. Jak bychom definovali *směr* přímky?

Uvážíme-li libovolnou třídu ekvivalence relace „$\parallel$“, pak přímky jí náležící mají vždy shodný směr. To znamená, že výběrem kterékoliv třídy ekvivalence je směr jednoznačně určen podle náležících přímek. Tedy celkově: za **směr** přímky p prohlásíme třídu ekvivalence $[p]_{\parallel}$.

Tato úvaha nám zde velmi pomůže. Ačkoliv sice netušíme, co je to mohutnost množiny, přesto dokážeme určit (v principu), zda libovolné množiny X a Y mají stejnou mohutnost, nebo nemají.

Lemma E.2.1. *Ekvipotence $\approx$ je relací ekvivalence*[3]*.*

Důkaz. Z definice relace ekvivalence stačí ověřit, že $\approx$ je reflexivní, symetrická a tranzitivní. Mějme libovolné množiny X,Y,Z.

- **Reflexivita**. Jistě platí $X \approx X$. Za bijekci stačí zvolit identitu 1_X.

[3] Zde se jedná o tzv. *třídovou relaci* na tzv. *univerzální třídě* (často označované $\mathbb{V}$), tedy „souhrnu“ všech množin. Tento „souhrn“ nemůže být množinou, neboť bychom tak došli ke sporu v ZF. Třídy představují v teorii množin „nadstavbu“ termínu množina. Obecně platí, že každá množina je třída, ale ne každá třída je množina. Pro hlubší pochopení doporučuji knihu [5], str. 45-50

- **Symetrie**. Pokud $X \approx Y$, pak existuje bijekce $f : X \to Y$. Protože f je bijekce, existuje inverzní zobrazení $f^{-1} : Y \to X$, které je též bijekcí. Tzn. platí i $Y \approx X$.

- **Tranzitivita**. Nechť $X \approx Y$ a zároveň $Y \approx Z$. Pišme $f : X \to Y$ a $g : Y \to Z$. Definujme zobrazení $h = g \circ f$. Podle tvrzení 4.3.8 je $h : X \to Z$ bijekce a tedy $X \approx Z$.

Tedy $\approx$ je relací ekvivalence. $\square$

Pro libovolnou množinu X tak třída ekvivalence $[X]_{\approx}$ obsahuje všechny množiny, které mají stejnou mohutnost jako X. Tzn.

$$\forall Y \in [X]_{\approx} : Y \approx X.$$

Víme tak, že každá z množin v libovolné třídě ekvivalence má stejnou mohutnost. Tuto třídu bychom pak mohli prohlásit za její mohutnost. V případě konečných množin, kde za mohutnost považujeme přirozené číslo, se jedná o alternativní pohled.

Mohutnosti představují v teorii množin tzv. *kardinální čísla*, která lze definovat způsobem popsaným výše. Jedná se tak o zobecnění myšlenky počtu prvků u konečných množin. Podobně jako na přirozených číslech, i na kardinálních číslech lze definovat smysluplnou aritmetiku.