Vysoké učení technické v Brně **Fakulta strojního inženýrství**

Jan Franců

MATEMATIKA I

Část 1

Základní pojmy

Verze 26. září 2021

1. Základní pojmy

V této části stručně uvedeme základní pojmy matematické logiky a teorie množin. Matematika se zabývá abstraktními pojmy, které vznikly zobecněním a idealizací reálných objektů a situací, například číslo, počet, bod, přímka, vektor, funkce, tvrzení, rovnice, minimum, řešení, atd. Abychom se nemuseli bavit o konkrétních objektech, používáme pojem množina a její prvky. Vlastnosti objektů popisujeme pomocí tvrzení, tzv. výroků. Pomocí logiky můžeme výroky skládat a pomocí pravidel formalizovat usuzování, tj. odvozování nových tvrzení.

Teorie množin a matematická logika jsou rozsáhlé matematické disciplíny, kterými se nebudeme do hloubky zabývat, intuitivně uvedeme jen vybrané pojmy a jejich základní vlastnosti, které budeme v dalším potřebovat. Většinu z toho již znáte ze střední školy, zde to jenom připomeneme a případně doplníme.

1A. Výroková logika

Pojem logika se v češtině běžně používá ve smyslu myšlenková cesta, která vede k určitým závěrům. Za jejího zakladatele je považován **Aristoteles**[1]. Jeho logiku ilustruje jednoduchý příklad: „Každý člověk je smrtelný.“ „Sokrates je člověk.“ proto „Sokrates je smrtelný.“

Jako vědní obor Matematická logika vznikla v 19. století. **Gerge Boole**[2] prosadil algebraické pojetí logiky a zavedl logické spojky: výroky se spojují pomocí spojek analogickým způsobem jako se počítá v algebře s čísly. K dalším tvůrcům booleovské logiky patří **John Venn**[3], mimo jiné zavedl tzv. Vennovy diagramy používané v teorii množin.

Za druhého zakladatele logiky je považován **G. Frege**[4], který výrokovou logiku rozšířil na tzv. predikátovou logiku, která se zabývá dokazováním matematických tvrzení. Zavedl v logice pojem tzv. predikátu, kvantifikátoru a výrokové formy. Domýšlel se, že s jeho logikou bude možné odvozovat všechna pravidla aritmetiky. Tyto představy se později ukázaly jako liché.

V roce 1901 Bertrand Russell[5] objevil tzv. **Russellův paradox**, který způsobil krizi v matematické logice a tzv. naivní teorii množin. Paradox uvedeme v odstavci 1.29. Logickou obdobou je tzv. **paradox lháře**, který byl znám již v antickém Řecku. Je to výrok, který není ani pravdivý ani nepravdivý. Jednou z řady jeho formulací je „Lhář řekl: Teď lžu“, nebo v matematice: „**Tato věta je nepravdivá**“. Předpokládáme-li, že výrok je pravdivý, dojdeme ke sporu, také předpoklad, že výrok je nepravdivý, vede ke sporu.

Řešením paradoxu je axiomatická teorie množin a logiky, která určuje jakým způsobem lze tvořit výroky i množiny, který takovéto výroky a množiny vytvořit nedovolí.

Jedním z nejvýznamnějších logiků všech dob je **Kurt Gödel**[6], jehož *Věta o úplnosti predikátové logiky prvního řádu* a *Věty o neúplnosti axiomatických formálních systémů s aritmetikou* výrazně ovlivnily vývoj matematiky.

[1] Aristoteles ze Stageiry (384–322 př. n. l.) řecký filozof, žák Platona a vychovatel Alexandra Makedonského.
[2] George Boole (1815–1864) britský matematik filozof zakladatel Booleovy algebry.
[3] John Venn (1834–1923) anglický matematik, logik a filozof.
[4] Gottlob Frege (1848–1925) německý matematik, logik a filozof.
[5] Bertrand Russell (1872–1970) britský matematik a logik, spisovatel, nositel Nobelovy ceny za literaturu.
[6] Kurt Gödel (1906–1978) matematik a logik, brněnský rodák, po studiích ve Vídni působil v USA.

Výroková logika

Základním pojmem logiky je **výrok**. Intuitivně ho lze definovat jako:

Definice 1.1. **Výrok** je sdělení (obvykle oznamovací věta), o němž má smysl uvažovat, zda je pravdivé nebo nepravdivé. Buď A výrok. Je-li A pravdivý, zapisujeme tuto skutečnost symbolicky $p(A) = 1$, je-li A nepravdivý, píšeme $p(A) = 0$. Symboly $0, 1$ se nazývají pravdivostní hodnoty výroku.

Výrok je tedy oznamovací věta, i když nejsme schopni rozhodnout, zda je pravdivá. Tázací ani rozkazovací věta není výrok. Výrok může obsahovat kromě slov také matematické značky.

Příklady 1.2. Určete pravdivost následujících výroků:

(a) $A :=$ „Platí $\frac{2}{\sqrt{2}} = \sqrt{2}$.“ (Pravdivý, tj. $p(A) = 1$, neboť $\frac{2}{\sqrt{2}} = \frac{2\sqrt{2}}{\sqrt{2}\sqrt{2}} = \frac{2\sqrt{2}}{2} = \sqrt{2}$.)

(b) $B :=$ „Číslo 51 je prvočíslo.“ (Nepravdivý, tj. $p(B) = 0$, neboť $51 = 3 \cdot 17$.)

Spojování výroků

Jednotlivé výroky lze spojovat ve složené výroky pomocí logických spojek. Předmětem studia výrokové logiky je studium závislosti pravdivostní hodnoty složeného výroku na způsobu spojení a na pravdivostních hodnotách jednotlivých výroků.

Výrok se nazývá **atomární**, nebo též **elementární**, neobsahuje-li logické spojky. Například výroky A, B Příkladu 1.2 jsou atomární. Pravdivost složeného výroku záleží na pravdivosti atomárních výroků. Rozhodování o pravdivosti atomárního výroku přísluší odpovídající vědecké disciplíně, která zkoumá shodu jeho obsahu s objektivní realitou.

Definice 1.3. (Logické spojky) Buď A výrok. **Negací výroku** A nazveme výrok $\neg A$, který má opačnou pravdivostní hodnotu, tj. $\neg A$ je nepravdivý, pokud výrok A je pravdivý a $\neg A$ je pravdivý, pokud A je nepravdivý. Negace se často značí také A', textově se píše non A. Definici negace lze také zapsat tabulkou:

$p(A)$	$p(\neg A)$
1	0
0	1

Pro spojování dvou výroků používáme logické spojky, zejména: **konjunkce** $\wedge$, **disjunkce** $\vee$, **implikace** $\Rightarrow$ a **ekvivalence** $\Leftrightarrow$. Tyto spojky definujeme tabulkou pravdivostních hodnot vypsáním všech existujících kombinací. Buďte A, B výroky, pravdivost výroků spojených těmito spojkami je dána tabulkou

$p(A)$	$p(B)$	$p(A \wedge B)$	$p(A \vee B)$	$p(A \Rightarrow B)$	$p(A \Leftrightarrow B)$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

V tabulce uvedeme název spojky, její označení, slovní vyjádření a logický význam.

název spojky	označení	slovní vyjádření	logický význam
konjunkce	$A \wedge B$	A a současně B	současně platí A i B
disjunkce	$A \vee B$	A nebo B	platí alespoň jeden z A, B
implikace	$A \Rightarrow B$	z A plyne B	jestliže platí A, potom platí B
ekvivalence	$A \Leftrightarrow B$	A právě tehdy, když B	buď oba A a B platí nebo oba neplatí

Při vyhodnocování pravdivostní hodnoty složeného výroku se zachovává následující pořadí operací: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$. Pokud chceme toto pořadí změnit, přidáme závorky.

Pro implikaci se užívá následující terminologie. V implikaci $A \Rightarrow B$ se výrok A nazývá **předpoklad** nebo **premisa** a B **závěr** implikace. Slovně lze implikaci $A \Rightarrow B$ vyjádřit také: A **je postačující podmínkou pro** B nebo B **je nutnou podmínkou pro** A. Připomeňme, že v případě, kdy A neplatí, implikace $A \Rightarrow B$ platí bez ohledu na pravdivost B.

Implikace $B \Rightarrow A$ se nazývá **obrácená implikace** a $\neg B \Rightarrow \neg A$ **obměněná implikace** k implikaci $A \Rightarrow B$. Například výrok „Nepršelo, tudíž jsme nezmokli.“ je obměnou implikace „Zmokli jsme, tudíž pršelo.“

Věta 1.4. Obměněná implikace $\neg B \Rightarrow \neg A$ **je ekvivalentní** původní implikaci $A \Rightarrow B$. Obrácená implikace $B \Rightarrow A$ **není ekvivalentní** implikaci $A \Rightarrow B$.

Důkaz. Tvrzení snadno ověříme pomocí tabulky pravdivostních hodnot výroků:

$p(A)$	$p(B)$	$p(A \Rightarrow B)$	$p(\neg B \Rightarrow \neg A)$	$p(B \Rightarrow A)$
1	1	1	1	1
1	0	0	0	1
0	1	1	1	0
0	0	1	1	1

Třetí a čtvrtý sloupec je stejný, pátý se od nich liší, tvrzení proto platí. □

Pro úplnost zmíníme ještě spojku **alternativa** $\veebar$, která má význam „buď A nebo B“. Výrok $A \veebar B$ je pravdivý pokud je pravdivý právě jeden z výroků A a B, tj. jeden z výroků je pravdivý a druhý nepravdivý.

Teoretický význam má **Shefferova**[7] **spojka** (Shefferova funkce nebo Shefferův symbol) $|$. Výrok $A|B$ je nepravdivý, jen když oba výroky A a B jsou pravdivé, tj. „neplatí A ani B“.

Poznámka 1.5.

(a) Jsou 4 možnosti pravdivosti dvou výroků: 11, 10, 01 a 00. Každý z uvedených 4 případů může dát pravdu nebo nepravdu. Proto všech možných logických spojek, které spojují dva výroky A, B je $2^4 = 16$.

(b) Říkáme, že systém spojek je **úplný**, pokud pomocí závorek a těchto spojek lze definovat každou z 16 možných spojek. Systém logických spojek $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ je úplný.

(c) Pro úplný systém spojek dvou výroků stačí jenom dvě spojky: negace a jedna ze spojek konjunkce, disjunkce a implikace.

(d) Lze dokázat, že všechny logické spojky lze popsat pomocí jediné spojky: Shefferovy funkce. Skutečně, $A|A$ dává negaci $\neg A$ a $(A|A)|(B|B)$ dává disjunkci $A \vee B$. Shefferova spojka proto tvoří nejmenší úplný systém.

[7] Henry Maurice Sheffer (1882–1964) americký logik.

(e) Analogicky existují logické spojky spojující tři výroky A, B, C. Protože je $2^3 = 8$ případů pravdivosti tří výroků, existuje $2^8 = 256$ možných logických spojek tří výroků. Známa je například spojka „**if** A **then** B **else** C“, která se používá v programování.

Příklad 1.6. Určete pravdivostní hodnotu výroku: $\big((2 \cdot 3 = 6) \vee (3 \cdot 4 = 11)\big) \Rightarrow (2 < 1)$.

Řešení: Jedná se o složený výrok, který je tvořen třemi atomárními výroky A, B, C, kde A je „$2 \cdot 3 = 6$“, B je „$3 \cdot 4 = 11$“ a C je „$2 < 1$“. Určíme jejich pravdivostní hodnoty. Zřejmě $p(A) = 1$, $p(B) = 0$ a $p(C) = 0$. Odtud plyne

$$p\Big(\big((2 \cdot 3 = 6) \vee (3 \cdot 4 = 11)\big) \Rightarrow (2 < 1)\Big) = p\big((1 \vee 0) \Rightarrow 0\big) = p(1 \Rightarrow 0) = 0.$$

Uvedený složený výrok je tedy nepravdivý.

Výrokové formy, proměnné a kvantifikátory

Matematické objekty s jednoznačně stanoveným významem, např. čísla 0, 1, π, $\sqrt{2}$, funkce (sin, exp,...), výroky, atd. nazýváme **konstanty**. Atomární výrok obvykle přisuzuje jednomu objektu-konstantě určitou vlastnost. Abychom mohli určitou vlastnost přisoudit více objektům, zavedeme **proměnné**, tj. objekty, které nemají jednoznačně stanovený význam, např. x, y, z. Proměnné zastupují konkrétní objekty. Tvrzení s proměnnou nazýváme **výrokovou formou**, která není výrokem, protože její pravdivost nelze posoudit, pokud neznáme hodnotu proměnné.

Z výrokové formy lze utvořit výrok tím, že všechny proměnné ve formě vážeme omezujícími podmínkami, které jednoznačně specifikující hodnoty všech proměnných. Tyto podmínky se nazývají kvantifikátory. Výroková forma pomocí proměnné tak umožňuje přisoudit vlastnost mnoha objektům, spojit tak konečně i nekonečně mnoho výroků do jednoho.

Definice 1.7. **Výroková forma** je tvrzení obsahující proměnné, z něhož se po dosazení konstant za proměnné stane výrok. Výrokovou formu A s proměnnou x označujeme $A(x)$.

Příklad 1.8. Tvrzení $A(x)$:= „$3x$ je sudé číslo“, je výroková forma s proměnnou x. Zvolíme-li $x = 1$, dostáváme výrok $A(x), x = 1$, zkráceně $A(1)$, který není pravdivý, tj. $p(A(x), x = 1) = 0$. Hodnota $x = 2$ dává výrok pravdivý, tj. $p(A(x), x = 2) = 1$.

U výrokové formy musíme určit, které hodnoty (objekty) proměnná zastupuje, tzv. obor proměnnosti M. Pro každou hodnotu proměnné tak dostáváme atomární výrok. Tyto výroky pak spojuje tzv. **kvantifikátor**. Nejčastěji používaný je **obecný** kvantifikátor $\forall$ zvaný také **univerzální** a **existenční** kvantifikátor $\exists$:

Definice 1.9. Nechť $A(x)$ je výroková forma s proměnnou x z oboru proměnnosti M. Potom:

Obecný kvantifikátor $\forall$ (čteme Pro každé) spojuje výroky $A(x)$ pro $x \in M$ konjunkcemi:

$\forall\, x \in M$ platí $A(x)$ znamená $\bigwedge\{A(x), x \in M\}$.

Existenční kvantifikátor $\exists$ (čteme Existuje) spojuje výroky $A(x)$ pro $x \in M$ disjunkcemi:

$\exists\, x \in M$, že platí $A(x)$ znamená $\bigvee\{A(x), x \in M\}$.

Příklad 1.10. Tvrzení $A(x)$:= „$3x$ je sudé číslo“, je výroková forma s proměnnou x. Zvolíme-li $x = 1$, dostáváme výrok $A(x), x = 1$, zkráceně zapíšeme $A(1)$, který není pravdivý, tj. $p(A(x), x = 1) = 0$, zatímco hodnota $x = 2$ dává výrok pravdivý $p(A(x), x = 2) = 1$.

Vezmeme-li obor proměnnosti proměnné x celá čísla, pro každé celé číslo x dostáváme výrok, například $A(0)$, $A(1)$, $A(-1)$, $A(2)$, atd. Tyto výroky jsou pravdivé pro sudá x a nepravdivé pro lichá x. S obecným kvantifikátorem $\forall$ dostáváme výrok:

„Pro každé celé x je číslo $3x$ sudé“,

který ovšem není pravdivý, protože neplatí pro lichá x. Pomocí existenčního kvantifikátoru dostaneme pravdivý výrok:

„Existuje celé x takové, že číslo $3x$ je sudé“,

protože platí například pro $x = 2$.

Poznámky 1.11.

(a) Kvantifikátorů lze utvořit libovolně mnoho. Vedle existenčního kvantifikátoru $\exists$ se užívá kvantifikátor $\exists!$ ve významu **existuje právě jeden**. Kvantifikátory lze vytvořit pomocí slovních spojení „alespoň“, „právě“, „nejvýše“, např. „existují právě dva“, „existují nejvýše tři“, „pro všechny s výjimkou jednoho“, atd.

(b) Výrokové formy mohou mít více proměnných, které lze různě kvantifikovat, přičemž **záleží** na jejich pořadí. Kvantifikací všech proměnných dostáváme výrok. V případě dvou za sebou jdoucích kvantifikátorů lze jejich pořadí zaměnit. Pokud je množina zřejmá z kontextu, lze ji vynechat.

Příklad 1.12. Zjistěte pravdivost následujících výroků:

$A :=$ „$\forall\, x \in \mathbb{R} \;:\; x^2 > 0$“ – slovně „Pro každé reálné číslo x platí $x^2 > 0$.“
(*Výrok neplatí, protože neplatí pro $x = 0$.*)

$B :=$ „$\exists\, n \in \mathbb{Z} \;:\; n^2 = 2$“ – slovně „Existuje celé číslo n, pro které platí $n^2 = 2$.“
(*Výrok neplatí, protože $\sqrt{2}$ není celé číslo.*)

$C :=$ „$\forall\, a \in \mathbb{R}\ \forall\, b \in \mathbb{R} \;:\; (a+b)^2 = a^2 + 2ab + b^2$“ (*Výrok platí.*)

$D :=$ „$\exists\, e \in \mathbb{R}\ \ \forall x \in \mathbb{R} \;:\; e \cdot x = x$“ (*Výrok platí, $e = 1$.*)

$E :=$ „$\forall\, x \in \mathbb{R}\ \ \exists\, q \in \mathbb{R} \;:\; x + q = 0$“ (*Výrok platí, $q = -x$.*)

$F :=$ „$\exists\, q \in \mathbb{R}\ \ \forall x \in \mathbb{R} \;:\; x + q = 0$“ (*Výrok neplatí.*)

Poznámka. Výroky E a F předchozích příkladů ukazují, že na pořadí kvantifikátorů záleží. V případě výroku E číslo q může být pro každé x jiné, výrok F vyžaduje existenci jednoho q takového, že rovnost platí pro všechna x, takové reálné číslo však neexistuje.

V případě dvou stejných kvantifikátorů za sebou lze jejich pořadí zaměnit: například výrok C je ekvivalentní s výrokem se stejnou výrokovou formou a s prohozenými kvantifikátory, tj. „$\forall\, b \in \mathbb{R}\ \forall\, a \in \mathbb{R} :\ (a+b)^2 = a^2 + 2ab + b^2$“.

Negace výroků s kvantifikátory

Aby výrok s obecným kvantifikátorem $\forall\, x$ neplatil, stačí najít jedno x, pro které vlastnost neplatí, proto při negaci výroku se kvantifikátor $\forall$ mění na $\exists$ a vlastnost se neguje. Aby výrok s kvantifikátorem $\exists x$ neplatil, vlastnost musí neplatit pro všechna x. Proto při negaci se kvantifikátor $\exists$ se mění na $\forall$ a vlastnost se neguje. V obou případech se přitom **obor proměnné x nemění**. V případě více kvantifikátorů se také **pořadí kvantifikátorů nemění**:

Věta 1.13. (**Negace výroků s kvantifikátory**)
Buď $A(x)$ výroková forma s proměnnou $x \in X$. Potom platí

(a) negací výroku „$\forall\, x \in X$ platí $A(x)$“ je výrok „$\exists\, x \in X$ že platí $\neg A(x)$“,

(b) negací výroku „$\exists\, x \in X$, že platí $A(x)$“ je výrok „$\forall\, x \in X$ platí $\neg A(x)$“,

kde $\neg A(x)$ je negace formy $A(x)$. Stejné pravidlo platí i pro výroky s více kvantifikátory.

Příklady 1.14. Negace výroku „Všichni studenti skupiny udělali zkoušku z Matematiky.“ je výrok „Existuje (alespoň jeden) student skupiny, který zkoušku z Matematiky neudělal.“

Negace výroku „Existuje student skupiny, který neudělal zkoušku z Fyziky.“ je výrok
„Všichni studenti skupiny zkoušku z Fyziky udělali.“

Podobně negací výroku se dvěma kvantifikátory:
„Existuje student skupiny, který udělal všechny zkoušky“
dostáváme výrok „Každý student skupiny alespoň jednu zkoušku neudělal“.

Vždy je splněno: buď platí výrok a negace výroku neplatí, nebo obráceně.

Příklad 1.15. Negujte výroky A, B, C, D, E, F z předchozího příkladu 1.12!

Řešení:
$\neg A :=$ „$\exists\, x \in \mathbb{R} \;:\; x^2 \leq 0$“ (*Výrok platí,* $x = 0$.)
$\neg B :=$ „$\forall\, n \in \mathbb{Z} \;:\; n^2 \neq 2$“ (*Výrok platí.*)
$\neg C :=$ „$\exists\, a \in \mathbb{R} \;\; \exists\, b \in \mathbb{R} \;:\; (a+b)^2 \neq a^2 + 2ab + b^2$“ (*Výrok neplatí.*)
$\neg D :=$ „$\forall\, e \in \mathbb{R} \;\; \exists\, x \in \mathbb{R} \;:\; e \cdot x \neq x$“ (*neplatí, Výrok např.* $e = 1$.)
$\neg E :=$ „$\exists\, x \in \mathbb{R} \;\; \forall\, q \in \mathbb{R} \;:\; x+q \neq 0$“ (*Neplatí*) ale změnou pořadí kvantifikátorů:
$\neg F :=$ „$\forall\, q \in \mathbb{R} \;\; \exists\, x \in \mathbb{R} \;:\; x + q \neq 0$“ (*Výrok platí.*)

Tautologie

Důležitým problémem je, zda různé výroky dávají stejné pravdivostní hodnoty. Složené výroky, které jsou vždy pravdivé se nazývají říká **tautologie**. Uveďme příklad:

Příklad 1.16. Šárka a Iva čekají na svoje kamarády Petra, Honzu a Jirku. Šárka tvrdí: Přijde-li Petr a Honza, přijde i Jirka. Iva říká: Já si myslím, že když přijde Petr a nepřijde Jirka, nepřijde ani Honza. Na to povídá Šárka: To ale říkáš totéž co já. Rozhodněte, zda obě skutečně říkají totéž.

Řešení: Nejprve vhodně označíme atomární výroky. Symbolem A označme výrok „Petr přijde“, symbolem B označme výrok „Honza přijde“ a dále C označme výrok „Jirka přijde“. V uvedeném označení mají výpovědi Šárky a Ivy tvar: $X := (A \wedge B) \Rightarrow C$, $Y := (A \wedge \neg C) \Rightarrow \neg B$. Aby Šárka a Iva říkaly totéž musí být výroky X, Y ekvivalentní. Sestavíme tabulku pravdivostních hodnot pro všechny možné kombinace pravdivosti výroků A, B, C.

A	B	C	$A \wedge B$	$A \wedge \neg C$	$X = (A \wedge B) \Rightarrow C$	$Y = (A \wedge \neg C) \Rightarrow \neg B$	$X \Leftrightarrow Y$
1	1	1	1	0	1	1	1
1	1	0	1	1	0	0	1
1	0	1	0	0	1	1	1
1	0	0	0	1	1	1	1
0	1	1	0	0	1	1	1
0	1	0	0	0	1	1	1
0	0	1	0	0	1	1	1
0	0	0	0	0	1	1	1

Z tabulky hodnot vyplývá, že $X \Leftrightarrow Y$, což znamená, že Šárka a Iva říkají skutečně totéž.

Definice 1.17. Výroková forma, jejíž proměnnými jsou výroky, se nazývá **tautologie**, pokud po dosazení libovolné kombinace pravdivostních hodnot výroků za proměnné dostáváme pravdivý výrok. Naopak, výroková forma, která je vždy nepravdivá se nazývá **kontradikce**. V ostatních případech se forma nazývá **splnitelná**.

Složené výroky A, B se nazývají **logicky ekvivalentní**, což zapisujeme $A = B$, když ve všech případech platí $A \Leftrightarrow B$. V tom případě výrok $A \Leftrightarrow B$ je tautologie.

Příklad 1.18. Formy $A \wedge B$ a $B \wedge A$ jsou logicky ekvivalentní, platí $(A \wedge B) = (B \wedge A)$ a forma $(A \wedge B) \Leftrightarrow (B \wedge A)$ je tautologie. Také $A \vee \neg A$ je tautologie a $A \wedge \neg A$ je kontradikce.

Další důležité tautologie uvádí následující věta:

Věta 1.19. Následující výrokové formy jsou tautologie:

(a) $(A \Rightarrow B) \Longleftrightarrow (\neg B \Rightarrow \neg A)$.

(b) $(A \Leftrightarrow B) \Longleftrightarrow \big((A \Rightarrow B) \wedge (B \Rightarrow A)\big)$.

(c) $\big((A \Rightarrow B) \wedge (B \Rightarrow C)\big) \Longrightarrow (A \Rightarrow C)$.

Důkaz. Tautologie (a) plyne z následující tabulky pravdivostních hodnot:

A	B	$A \Rightarrow B$	$\neg B \Rightarrow \neg A$	$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$
1	1	1	1	1
1	0	0	0	1
0	1	1	1	1
0	0	1	1	1

Tautologie (b) plyne z tabulky:

A	B	$A \Leftrightarrow B$	$A \Rightarrow B$	$B \Rightarrow A$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$	$(A \Leftrightarrow B) \Leftrightarrow ((A \Rightarrow B) \wedge (B \Rightarrow A))$
1	1	1	1	1	1	1
1	0	0	0	1	0	1
0	1	0	1	0	0	1
0	0	1	1	1	1	1

Tautologie (c) pro tři výroky plyne z tabulky:

A	B	C	$A \Rightarrow B$	$B \Rightarrow C$	$(A \Rightarrow B) \wedge (B \Rightarrow C)$	$A \Rightarrow C$	$((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	1	0	1	1
1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	0	1	1	1	1	1	1
0	0	0	1	1	1	1	1

Poznámky 1.20. Uvedené tautologie mají zásadní význam, tvoří základ teorie důkazů.

Tvrzení (a) říká, že důkaz implikace je ekvivalentní důkazu její obměněné implikace.

Tautologie (b) říká, že ekvivalenci dvou tvrzení dokážeme důkazem implikace a obrácené implikace.

Vlastnost (c) se nazývá **tranzitivita implikace**. Matematickou indukcí můžeme tvrzení (c) rozšířit na libovolný konečný počet výrokových proměnných $A_1, \ldots, A_n$, což lze vyjádřit:

$$[(A_1 \Rightarrow A_2) \wedge (A_2 \Rightarrow A_3) \wedge \ldots \wedge (A_{n-1} \Rightarrow A_n)] \Rightarrow (A_1 \Rightarrow A_n).$$

Pro negace složených výroků platí následující pravidla, která lze podobně dokázat pomocí tabulek pravdivostních hodnot:

Věta 1.21. Platí následující vztahy pro negace složených výroků:

(a) $\neg(\neg A) = A$ (zákon vyloučení třetího).

(b) $\neg(A \wedge B) = \neg A \vee \neg B$,

(c) $\neg(A \vee B) = \neg A \wedge \neg B$,

(d) $\neg(A \Rightarrow B) = A \wedge \neg B$,

(e) $\neg(A \Leftrightarrow B) = (A \vee B) \wedge (\neg A \vee \neg B) = (A \wedge \neg B) \vee (\neg A \wedge B)$.

Některé vlastnosti operací mají svůj název:

Definice 1.22. Buďte dány symboly operací $\circ$, $*$. Pak následující vztahy nazýváme:

(a) $a \circ b = b \circ a$ — **komutativní zákon**.

(b) $a \circ (b \circ c) = (a \circ b) \circ c$ — **asociativní zákon**.

(c) $a \circ (b * c) = (a \circ b) * (a \circ c)$ — **distributivní zákon**.

Také logické spojky splňují komutativní, asociativní a distributivní zákon:

Věta 1.23. Pro logické spojky $\wedge, \vee$ platí komutativní, asociativní a distributivní zákony:

(a) $A \wedge B = B \wedge A$, $\quad A \vee B = B \vee A$.

(b) $A \wedge (B \wedge C) = (A \wedge B) \wedge C$, $\quad A \vee (B \vee C) = (A \vee B) \vee C$,

(c) $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$, $\quad A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$.

1B. Důkazy v matematice

Úvahy dokazující tvrzení lze rozdělit na induktivní a deduktivní. **Deduktivní** úvahou nazýváme takovou úvahu, při níž z obecného tvrzení vyvozujeme platnost individuálního případu. Podstata dedukce je tedy v tom, že se zvláštní případ zahrnuje pod obecný princip. Matematické úvahy jsou převážně deduktivní.

Induktivní úvaha je opačný postup, kdy z jednotlivých případů odvodíme obecné pravidlo. V matematice lze induktivní postup využít, když jednotlivých případů je konečný (nepříliš velký) počet. Obvykle však matematická tvrzení zahrnují nekonečně mnoho případů, proto induktivní úvahu nelze použít. Ve fyzice a dalších vědách je induktivní postup obvyklý, z konečného počtu experimentů se usuzuje na obecné pravidlo.

Matematická tvrzení mají často tvar implikací nebo ekvivalencí. Ve větě tvaru $A \Rightarrow B$ se A nazývá **předpoklad** a B **tvrzení věty** nebo závěr. Existují tři základní možnosti důkazu implikace: přímý, nepřímý a sporem. V krátkosti si nyní vysvětlíme, jaký je logický základ těchto důkazů a v čem spočívají.

(a) Přímý důkaz. Chceme-li dokázat implikaci $A \Rightarrow B$ přímým důkazem, pak se pokusíme zkonstruovat tzv. řetězec implikací $A \Rightarrow A_1, A_1 \Rightarrow A_2, \ldots, A_n \Rightarrow B$. Podle Věty 1.19, části (c) odtud plyne $A \Rightarrow B$. Zápis řetězce implikací je zvykem zapisovat v kratším tvaru

$$A \Rightarrow A_1 \Rightarrow A_2 \Rightarrow \ldots \Rightarrow A_n \Rightarrow B.$$

(b) Nepřímý důkaz. Při nepřímém důkazu využijeme platnost tautologie (a) z Věty 1.19. Místo původní implikace dokazujeme obměněnou implikaci $\neg B \Rightarrow \neg A$ stejně jako v případě přímého důkazu.

(c) Důkaz sporem. Vycházíme z předpokladu, že implikace neplatí, tj. A platí a B neplatí, tj. $A \wedge \neg B$. Konstruujeme řetězec implikací $A \wedge \neg B \Rightarrow A_1, A_1 \Rightarrow A_2, \ldots, A_n \Rightarrow S$, až dojdeme k výroku S, který je logicky ve sporu s původním předpokladem nebo s nějakým evidentně pravdivým výrokem. Spor je situace, kdy nějaký výrok a jeho negace mají být současně pravdivé. Proto předpoklad, že implikace neplatí je nepravdivý, a proto implikace platí.

Poznámky. V matematice se využívá ještě **důkaz konstrukcí**, kdy existenci nějakého objektu dokážeme tím, že jeden konkrétní objekt zkonstruujeme. V případě, kdy se tvrzení týká konečně mnoha objektů nebo skupin objektů, lze tvrzení dokázat **rozborem všech případů**, neboli tzv. „dokonalou indukcí“.

Uvedené důkazové postupy demonstrujeme na příkladu.

Příklad 1.24. Dokažte přímo, nepřímo i sporem, že $\forall x \in \mathbb{N} : x \geq 2 \;\Rightarrow\; 6x + 3 > 13$.

Řešení: **(a) Přímý důkaz.** Důkaz využívá vlastnosti nerovností:

$$x \geq 2 \quad \Rightarrow \quad 6x \geq 12 \quad \Rightarrow \quad 6x + 1 \geq 12 + 1 \quad \Rightarrow \quad 6x + 1 \geq 13 \quad \Rightarrow \quad 6x + 3 > 13.$$

Uvedený řetězec implikací tvoří důkaz tvrzení.

(b) Nepřímý důkaz. Sestrojíme obměnu (kontrapozici) původní implikace

$$\forall x \in \mathbb{N}: \ 6x+3 \leq 13 \ \Rightarrow \ x < 2.$$

Toto tvrzení je logicky ekvivalentní původnímu tvrzení. Obměnu dokážeme přímým důkazem

$$6x+3 \leq 13 \quad \Rightarrow \quad 6x \leq 10 \quad \Rightarrow \quad x \leq \frac{10}{6} \quad \Rightarrow \quad x < 2.$$

(c) Důkaz sporem. Předpokládejme, že dokazované tvrzení neplatí. Pak je ale pravdivá jeho negace. Negace implikace má tvar

$$\exists x \in \mathbb{N}: x \geq 2 \ \wedge \ 6x+3 \leq 13.$$

Z tohoto předpokladu nyní plyne, že existuje $x \in \mathbb{N}$ takové, že

$$x \geq 2 \ \wedge \ 6x+3 \leq 13 \quad \Rightarrow \quad x \geq 2 \ \wedge \ 6x \leq 10 \quad \Rightarrow \quad x \geq 2 \ \wedge \ x \leq \frac{10}{6},$$

což je spor, neboť žádné $x \in \mathbb{N}$ vlastnost $x \geq 2 \ \wedge \ x \leq \frac{10}{6}$ nemá. Předpoklad, z něhož se řetězec implikací odvíjel, je tedy nepravdivý. To ale znamená, že je pravdivá jeho negace. Tato negace je však ekvivalentní původní implikaci.

Pěkným příkladem důkazu sporem je důkaz následující Eukleidovy[8] Věty o počtu prvočísel:

Věta 1.25. Prvočísel je nekonečně mnoho.

Důkaz. Předpokládejme, že všech prvočísel je konečně mnoho, označme je $p_1, p_2, p_3, \ldots, p_n$. Zkoumejme součin všech prvočísel $P = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n$. Číslo $P+1$ při dělení kterýmkoliv prvočíslem p_i dává zbytek 1, proto není dělitelné žádným z prvočísel $p_1, \ldots, p_n$. Číslo $P+1$ je proto dalším prvočíslem, což je ve sporu s předpokladem, že $p_1, \ldots, p_n$ jsou všechna prvočísla. Proto prvočísel je nekonečně mnoho. □

Speciálním, ale v matematice často používaným důkazem je důkaz pomocí principu matematické indukce. **Matematická indukce** je věta, která umožňuje provádět důkazy tvrzení týkajících se množiny přirozených čísel $\mathbb{N} = \{1, 2, 3, \ldots\}$.

Věta 1.26. (Matematická indukce) Buď $V(n)$ výroková forma proměnné $n \in \mathbb{N}$. Nechť platí výrok $V(1)$. Pokud pro každé $n \geq 1$ z platnosti výroku $V(n)$ plyne platnost výroku $V(n+1)$, potom výrok $V(n)$ platí pro všechna $n \in \mathbb{N}$. Postup lze zapsat symboly:

$$\Big(p\big(V(1)\big) = 1\Big) \wedge \Big(\forall n \in \mathbb{N}: p\big(V(n)\big) = 1 \implies p(V(n+1)) = 1\Big) \Rightarrow \forall n \in \mathbb{N}: p(V(n)) = 1.$$

Poznamenejme, že ačkoliv v názvu metody je slovo indukce, matematická indukce je metodou deduktivní, protože obecnou implikace $V(n) \Rightarrow V(n+1)$ dokazujeme z obecných pravidel.

Důkaz matematické indukce provedeme sporem:

Důkaz. Předpokládejme, že existuje číslo $n \in \mathbb{N}$, takové, že $V(n)$ neplatí. Odtud plyne, že množina $M = \{n; p\big(V(n)\big) = 0\}$ je neprázdná a symbolem m označme její nejmenší prvek.

[8] Eukleides z Alexandrie (325 -– asi 260 př. n. l.) řecký matematik a geometr, autor 13 knih „Základů“.

Protože $V(1)$ platí, je $m > 1$ a protože $m - 1 \notin M$ platí $V(m-1)$. Z indukčního předpokladu ale plyne, že $V(m)$ platí, což je spor. □

Poznámka 1.27. Důkaz tvrzení „$\forall n \in \mathbb{N}$ platí $V(n)$“ pomocí matematické indukce se skládá ze tří částí:

(a) Dokážeme, že platí výrok $V(1)$, tj. $p\big(V(1)\big) = 1$. V obecnějším případě platnost formule dokážeme pro nejmenší přípustné n. Nejčastěji je to právě číslo 1 nebo 0.)

(b) Dokážeme: pro každé $n \in \mathbb{N}$ platí: jestliže platí $V(n)$ potom platí také $V(n+1)$.

(c) Odvoláme se na Větu 1.26 o matematické indukci, podle které je nyní tvrzení $V(n)$ pravdivé pro každé přirozené číslo n.

Postup vysvětlíme na příkladu:

Příklad 1.28. Pro $a, b \in \mathbb{N}$ řekneme, že a dělí b a píšeme $a|b$, jestliže existuje číslo $c \in \mathbb{N}$ tak, že $b = ac$. Pomocí matematické indukce dokažte následující tvrzení „Pro každé přirozené n je číslo $6^{2n} - 8$ dělitelné sedmi“, zapsané symbolicky: „$\forall n \in \mathbb{N} : 7|(6^{2n} - 8)$“.

Důkaz. Označme výrok $V(n) = 7|(6^{2n} - 8)$. Tvrzení dokážeme ve třech krocích:

(a) Nejprve dokážeme, že tvrzení je pravdivé pro $n = 1$. Výrok $V(1)$ má tvar $7|(6^2 - 8)$. Protože $6^2 - 8 = 28 = 4 \cdot 7$, tvrzení pro $n = 1$ platí.

(b) Předpokládejme nyní, že tvrzení je pravdivé pro libovolné pevně zvolené číslo n. Dokažme, že potom tvrzení platí rovněž pro $n + 1$, tj. je třeba dokázat, že

$$\forall n \in \mathbb{N} : 7|(6^{2n} - 8) \;\Rightarrow\; 7|(6^{2(n+1)} - 8).$$

Číslo $6^{2(n+1)} - 8$ z výroku $V(n+1)$, jehož dělitelnost číslem 7 máme dokázat, upravíme:

$$6^{2(n+1)} - 8 = 6^{2n+2} - 8 = 6^2 \cdot 6^{2n} - 8 = 36 \cdot 6^{2n} - 8 = 35 \cdot 6^{2n} + (6^{2n} - 8).$$

První sčítanec součtu je dělitelný číslem 7, neboť $35 = 5 \cdot 7$, druhý je dělitelný 7 podle indukčního předpokladu. Oba sčítance jsou dělitelné 7, proto je i jejich součet je také dělitelný 7, což bylo potřeba dokázat.

(c) Podle Věty 1.26 o matematické indukci je tvrzení pravdivé pro každé přirozené číslo n. □

1C. Základní množinové pojmy

Vedle logiky základním kamenem matematiky je teorie množin. Za jejího zakladatele je považován G. Cantor[9]. Hlavní problematikou, kterou se teorie množin zabývala, byly otázky týkající se vlastností nekonečna, zejména srovnávání různých velikostí nekonečna. Ukázalo se však, že v teorii množin lze budovat i jiné matematické teorie, a to tak, že se každému matematickému objektu přiřadí určitá množina, která ho reprezentuje. V tomto smyslu se tzv. naivní teorie množin stala základem celé matematiky.

S jistou nadsázkou lze říci, že se teorie množin narodila 7. 12. 1873. Toho dne totiž G. Cantor nalezl odpověď na otázku, zda lze všechna reálná čísla z nějakého intervalu (a, b) seřadit do posloupnosti, tj. utvořit prosté zobrazení reálných čísel z intervalu (a, b) na množinu přirozených čísel. Ke svému překvapení zjistil, že takové zobrazení neexistuje.

Otázku, zda má smysl porovnávat nekonečné systémy podle velikosti, si položil například již v roce 1638 jeden z géniů té doby Galilei[10]. Ten vypsal řadu čísel $1, 2, 3, 4, \ldots$ a jejich druhých mocnin $1, 4, 9, 16, \ldots$ a uvědomil si, že mezi těmito množinami existuje vzájemně jednoznačné zobrazení. To by však znamenalo, že uvedené systémy čísel jsou stejně velké. Tento závěr se mu jevil naprosto absurdní. Popíral totiž jeden ze základních Eukleidových[11] logických axiomů, který říká, že celek je vždy větší než jeho část. Galilei proto dospěl k závěru, že pro nekonečné systémy nemá otázka o jejich velikosti žádný smysl. Na konci svého života sepsal Bolzano[12] matematicko-filozofické dílo *Paradoxy nekonečna*. Vyšlo posmrtně v roce 1851. V tomto díle dospěl na práh teorie množin.

Na přelomu 19. a 20. století se objevily paradoxy – rozpory mezi zákony, které způsobily krizi matematiky v logice i teorii množin. Je to již zmíněný Russellův[13] paradox. Nejprve uveďme tzv. **Holičův paradox**, který převádí paradox z oblasti teorie množin do životní situace:

> *Holič ze Sevilly holí právě ty ze sevillských mužů, kteří se neholí sami.* Pokusíme-li se odpovědět na otázku, zda holič holí sám sebe, dostaneme se do bludného kruhu. Pokud se sám neholí, tak se musí holit, protože holí ty, co se sami neholí. A naopak holí-li se sám, tak se holit nemůže, protože holí jen ty, kteří se sami neholí.

Russellův paradox 1.29. Buď A libovolná množina. Pak nastane právě jedna z možností buď $A \in A$ nebo $A \notin A$. Všechny množiny rozdělíme do dvou skupin: ty které jsou prvkem samy sebe, tj. $X = \{A \mid A \in A\}$, a ty, které nejsou prvkem samy sebe, tj. $Y = \{A \mid A \notin A\}$. Žádná množina však nemůže patřit do X i Y současně. Uvažme nyní Y. Protože Y je množina, musí sama ležet v X nebo Y. Připusťme nejprve $Y \in X$. Pak ale podle definice X platí $Y \in Y$, což je spor, neboť Y nemůže ležet v X i Y. Připusťme tedy, že $Y \in Y$. Pak ale z definice Y plyne $Y \notin Y$, což je rovněž spor, protože Y nemůže ležet a současně neležet v Y. Vzniká neřešitelná situace na úrovni intuitivní teorie množin. Pojem množiny v intuitivním smyslu se ukázal příliš široký. Problém spočívá ve tvorbě množin: nutno ji omezit jistými pravidly.

Tyto paradoxy v logice i v teorii množin si vynutily novou metodiku výstavby matematických teorií. Nejobvyklejší metodou se stala axiomatická výstavba. Množiny i výroky lze tvořit podle přesně specifikovaných pravidel.

[9] Georg Cantor (1845–1918) německý matematik a logik
[10] Galileo Galilei (1564–1642) italský astronom
[11] (Eukleides (325–260 př.n.l.) řecký matematik
[12] Bernard Bolzano (1781–1848) německy píšící filozof, matematik a teolog italského původu žijící v Praze.
[13] Bertrand Russell (1872–1970) britský matematik, logik, ...

Definice 1.30. (Intuitivní definice množiny)

(a) **Množina** je souhrn libovolných různých (navzájem rozlišitelných) objektů.

(b) Jednotlivé objekty nazveme **prvky množiny** a shrnování v jeden celek označíme pomocí složených závorek. V množinových závorkách **nezáleží na pořadí**, v jakém prvky zapíšeme. Nezáleží ani na tom, kolikrát prvek v množině zapíšeme. Pro přehlednost budeme zapisovat každý prvek pouze jednou.

(c) Množiny zpravidla označujeme velkými písmeny a jejich prvky malými písmeny.

(d) Zápis $a \in A$ znamená, že objekt a **je prvkem množiny** A.

(e) Zápis $a \notin A$ znamená, že a **není prvkem množiny** A.

(f) Řekneme, že **množiny** A, B **jsou si rovny**, pokud mají stejné prvky, a píšeme $A = B$.

(g) Řekneme, že množina A **je podmnožinou množiny** B, když každý prvek množiny A je prvkem množiny B, a píšeme $A \subset B$. Symbol $\subset$ se nazývá znak **inkluze** nebo také znak **podmnožiny**.

(h) Množinu lze zadat **výčtem prvků**, tj. napsáním seznamu, např. $\{1, 2, 3\}$ nebo pomocí **charakteristické vlastnosti**, např. $\{x \in \mathbb{N} : x \leq 3\}$.

(i) Symbolem $\emptyset$ označujeme množinu, která nemá žádný prvek. Nazýváme ji **prázdná množina**. Některé další často používané číselné množiny mají vlastní stálé označení.

Vedle symbolu $\subset$ se užívá i symbol $\supset$ (nadmnožina) ve významu $A \supset B$, právě když $B \subset A$.

Analogicky k nerovnostem $a \leq b$, $a < b$ někteří autoři místo $\subset$ píší symbol $\subseteq$, aby se zdůraznilo, že inkluze připouští i rovnost množin. Symbol $A \subset B$ potom má význam tzv. vlastní inkluze, kdy každý prvek z A je i v B a existuje prvek z B, který není v A. V tomto textu nebudeme rozlišovat vlastní inkluzi a rovnost množin a budeme psát jen $\subset$ nebo $\supset$.

Základní vlastnosti inkluze shrneme ve větě:

Věta 1.31. Pro libovolné množiny A, B, C platí:

(a) $\emptyset \subset A$.

(b) $A \subset A$.

(c) $A \subset B \wedge B \subset C \;\Rightarrow\; A \subset C$ — tzv. tranzitivita inkluze.

(d) $A \subset B \wedge B \subset A \;\Leftrightarrow\; A = B$.

Tvrzení (a) a (b) jsou zřejmá. Vlastnost (c) se nazývá tranzitivita inkluze. Tvrzení (d) má zásadní význam pro důkazy množinových rovností. Chceme-li dokázat, že $A = B$, tak postupujeme tak, že dokážeme obě inkluze $A \subset B$ a $B \subset A$. Odtud podle (d) plyne, že $A = B$.

Příklady 1.32. Rozhodněte, které z výroků jsou pravdivé:

- „Množina $\{\emptyset\}$ nemá žádný prvek“ (*Není pravdivý, množina má prvek $\emptyset$.*)
- „$\{1, 1\} = \{1\}$“ (*Platí, prvek může být zapsán víckrát.*)
- „$\{1\} \subset \{1\}$“ (*Platí.*)
- „$\{1, 2\} = \{2, 1\}$“ (*Platí, v zápisu množiny nezávisí na pořadí prvků.*)

Definice 1.33. Mezi množinami A, B definujeme následující základní operace:

(a) **průnik** $A \cap B := \{x \ : \ (x \in A) \wedge (x \in B)\}$.

(b) **sjednocení** $A \cup B := \{x \ : \ (x \in A) \vee (x \in B)\}$.

(c) **rozdíl množin** $A \setminus B := \{x \ : \mid (x \in A) \wedge (x \notin B)\}$.

(d) Pro množiny $A \subset M$ **doplněk (komplement)** A **v** M je rozdíl $M \setminus A = \{x \in M \mid x \notin A\}$.

Často se rozdíl množin místo $A \setminus B$ píše $A - B$.
Pokud je M daná základní množina místo $M \setminus A$ píšeme jen A^C.

Poznámka 1.34. Uvědomte si souvislost mezi logickými spojkami a množinovými operacemi. Nechť $A(x)$ a $B(x)$ jsou výrokové formy proměnné $x \in M$ a označme M_A a M_B množiny prvků $x \in M$, pro které jsou výroky A a B pravdivé, tj.

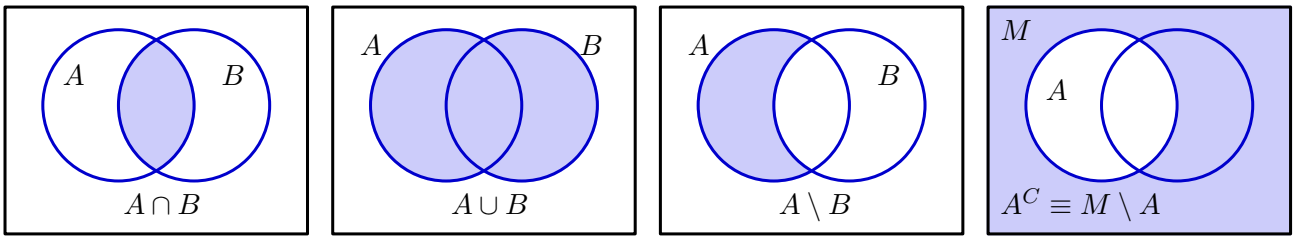
$$M_A = \{x \in M \mid p(A(x)) = 1\}\,, \qquad M_B = \{x \in M \mid p(B(x)) = 1\}$$

Potom Logické spojce konjunkce odpovídá množinová operace průnik, disjunkci sjednocení a negaci doplněk ve smyslu:

$$M_{A \wedge B} = M_A \cap M_B\,, \qquad M_{A \vee B} = M_A \cup M_B\,, \qquad M_{\neg A} = M \setminus M_A\,.$$

Vennovy diagramy

Množinové operace znázorňujeme pomocí tzv. **Vennových**[14] **diagramů**: množině odpovídá plošný útvary v rovině, nejčastěji kruh, elipsa nebo obdélník.



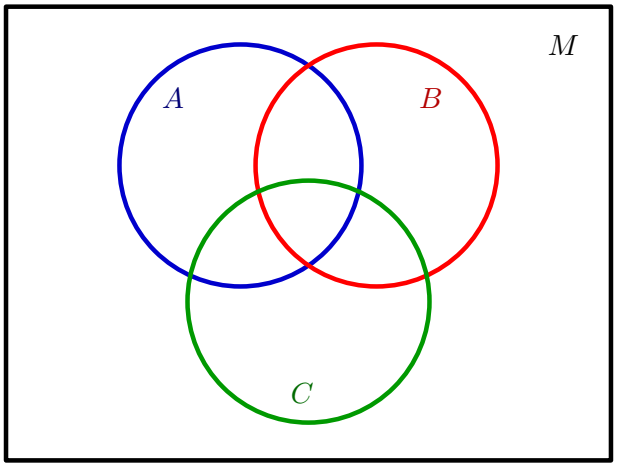
Obr. 1.1: Průnik $A \cap B$, sjednocení $A \cup B$, rozdíl $A \setminus B$ množin A, B a doplněk A v množině M.

Obrázky typu 1.1 zahrnují všechny možné situace dvou množin $A, B \subset M$. Kružnice rozdělují plochu na čtyři části. Každý prvek $x \in M$ má $2 \times 2 = 4$ možnosti: být nebo nebo nebýt prvkem množiny A a být nebo nebo nebýt prvkem množiny B. Pokud například množiny A, B jsou disjunktní, jejich průnik $A \cap B$ je potom množina prázdná.

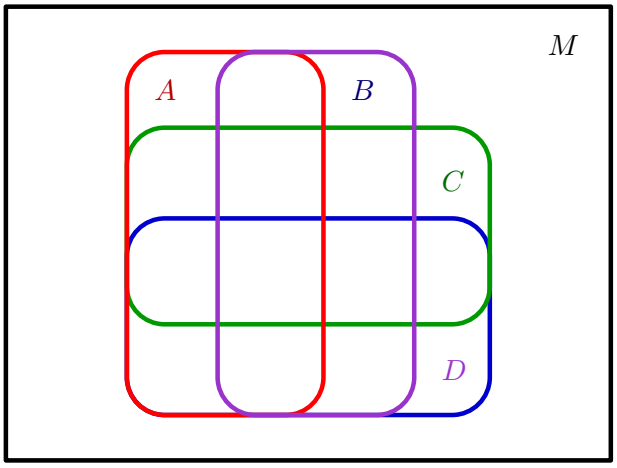
V případě tří množin $A, B, C \subset M$ je možných $2 \times 2 \times 2 = 8$ možností, které lze znázornit diagramem s třemi kružnicemi, viz Obr. 1.2, které obdélník M rozdělují na 8 částí.

V případě čtyř množin A, B, C, D je již situace složitější, protože potřebujeme množinu M rozdělit na 16 částí. Možné řešení je na Obr. 1.3. V každé části je jiná kombinace toho, zda prvek náleží nebo nenáleží jednotlivým množinám A, B, C, D.

[14] John Venn (1834–1923) anglický matematik a logik



Obr. 1.2: Vennův diagram tří množin.



Obr. 1.3: Vennův diagram čtyř množin

Vlastnosti množinových operací

Pro množinové operace platí analogické vlastnosti jako pro logické spojky:

Věta 1.35. Pro množinové operace $\cap$, $\cup$ platí komutativní, asociativní a distributivní zákon:

(a) $A \cap B = B \cap A, \qquad A \cup B = B \cup A,$

(b) $A \cap (B \cap C) = (A \cap B) \cap C, \qquad A \cup (B \cup C) = (A \cup B) \cup C,$

(c) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$

Ještě uveďme jeden důležitý pojem: množinu všech podmnožin množiny:

Definice 1.36. **Množina všech podmnožin** množiny A, tj. $\{X : X \subset A\}$ se označuje **$\exp(A)$** nebo 2^A. V případě konečné množiny A s n prvky, množina $\exp(A)$ má 2^n prvků.

Příklad. Jednoprvková množina $A = \{a\}$ má dvě podmnožiny, proto $\exp(A) = \{\emptyset, \{a\}\}$, dvojprvková $B = \{a, b\}$ má čtyři podmnožiny $\exp(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. Trojprvková množina $B = \{a, b, c\}$ už má 8 podmnožin, $\exp(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

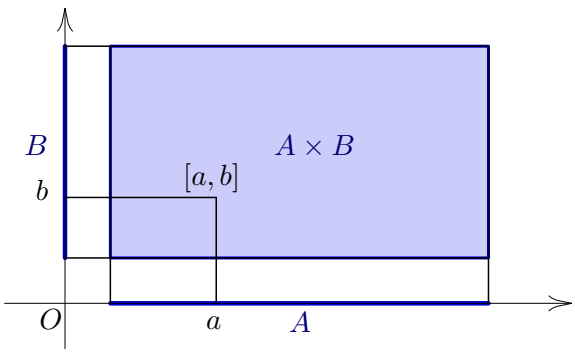
Obecně, je-li množina A konečná a má-li n (různých) prvků, potom $\exp(A)$ obsahuje 2^n různých podmnožin množiny A. Při tvoření podmnožin pro každý prvek máme dvě možnosti: buď v podmnožině bude nebo nebude, tj. máme $2 \cdot 2 \cdot \cdots \cdot 2 = 2^n$ různých podmnožin.

Kartézský součin množin

Připomeňme, že pro $a \neq b$ zápisy $\{a, b\}$ a $\{b, a\}$ označují stejnou dvojprvkovou množinu, na pořadí v zápisu nezávisí. Zápisy $[a, b]$ a $[b, a]$ určuje dvě různé uspořádané dvojice. Pro libovolné množiny A, B kartézský součin množin A, B je množina všech uspořádaných dvojic prvků z A a B, tj.

$$A \times B := \{[a, b] : (a \in A) \wedge (b \in B)\}.$$

V případě intervalů $A, B \subset \mathbb{R}$, kartézský součin $A \times B$ je obdélník, viz obr. 1.4.



Obr. 1.4: Kartézský součin dvou množin

Definice 1.37.

(a) **Uspořádaná dvojice** prvků a, b je dvojice prvků, kdy záleží na pořadí, zapisujeme $[a, b]$. Proto $[a, b]$ a $[b, a]$ jsou různé dvojice. Obecně **uspořádaná n-tice** je soubor n prvků, ve kterém je určeno, který prvek je první, druhý, ... n-tý, zapisujeme $[a_1, a_2, a_3, \ldots, a_n]$. Prvky v n-tici se mohou opakovat.

(b) **Kartézský součin** množin A a B je množina všech uspořádaných dvojic $[a, b]$:

$$A \times B = \{[a, b] \mid (a \in A) \wedge (b \in B)\}.$$

(c) Podobně zavedeme kartézský součin n množin $A_1, A_2, \ldots, A_n$:

$$A_1 \times A_2 \cdots \times A_n := \{[a_1, \ldots, a_n] \mid (a_1 \in A_1) \wedge (a_2 \in A_2) \wedge \ldots \wedge (a_n \in A_n)\}.$$

Jestliže množina A_i má k_i prvků, potom jejich kartézský součin má $k_1 k_2, \cdots, k_n$ prvků.

(d) Kartézský součin je asociativní: $(A \times B) \times C = A \times (B \times C)$.

(e) Kartézský součin však **není komutativní**, obecně rovnost $A \times B = B \times A$ **neplatí**

Místo $A \times A$ píšeme A^2, místo $A \times A \times A \times B \times C \times C$ můžeme psát $A^3 \times B \times C^2$.

1D. Základní číselné množiny

Uvedeme základní číselné množiny. Jsou to čísla přirozená $\mathbb{N}$, čísla celá $\mathbb{Z}$, čísla racionální $\mathbb{Q}$, čísla reálná $\mathbb{R}$ a čísla komplexní $\mathbb{C}$. Množiny lze seřadit pomocí inkluze $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Přirozená čísla

Přirozená čísla vznikla přirozeně, když lidé potřebovali určit počet určitých objektů, například kolik mají předmětů, ovcí, členů tlupy. Až později byly konstruovány další množiny čísel.

Definice 1.38. **Množinu přirozených čísel** označujeme $\mathbb{N} := \{1, 2, 3, 4, 5, 6, 7, \ldots\}$, její prvky označujeme obvykle písmeny m, n, i, j, k, l, lze užít i jiná písmena.

Množina $\mathbb{N}$ je uspořádaná: pro každá dvě různá čísla m, n platí buď $m < n$ nebo $n < m$.

Operace sčítání $m + n$ i násobení $m \cdot n$ (zkráceně $m\,n$) jsou definovány pro každá $m, n \in \mathbb{R}$.

Operace odčítání $m - n$ je definována jen tehdy, pokud $m > n$.

Operace dělení $m : n$ je definována pokud m je dělitelné n, tj. existuje $k \in \mathbb{N}$, že $m = n\,k$.

Formální matematická definice přirozených čísel je založena na tzv. Peanových[15] axiomech:

(a) Existuje číslo 1.

(b) Každé přirozené číslo n má následníka označeného $n + 1$.

(c) Neexistuje přirozené číslo, jehož následníkem by bylo číslo 1.

(d) Různá přirozená čísla mají různé následníky: pokud $n \neq m$, pak $n + 1 \neq m + 1$.

(e) Nechť nějakou vlastnost V splňuje číslo 1 a nechť pro každé číslo n platí: jestliže číslo n splňuje vlastnost V pak vlastnost V splňuje i následník $n + 1$. Potom vlastnost V splňují všechna přirozená čísla.

[15] Giuseppe Peano (1858–1932) italský matematik, filozof a logik

Axiom (e) zajišťuje platnost důkazů technikou matematické indukce.

Pojem množiny přirozených čísel není jednotný, jsou určité důvody přidat k přirozeným číslům nulu, obvykle se však nula za přirozené číslo nepovažuje. Přirozená čísla s nulou budeme označovat $\mathbb{N}_0 := \{0\} \cup \mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}$.

Celá čísla

Při směně předmětů lidé potřebovali rozlišit „Má dáti“, tj. dluh, a „Dal“, tj. abychom mohli čísla odečítat bez omezení, k přirozeným číslům přidáme nulu a čísla $-n$ opačná k přirozeným číslům. Tím vznikla celá čísla.

Definice 1.39. Množinu celých čísel $\mathbb{Z}$ dostaneme přidáním nuly a čísel opačných k přirozeným číslům:

$$\mathbb{Z} := \{1, 2, 3, \dots\} \cup \{0\} \cup \{-1, -2, -3, \dots\} = \{0, 1, -1, 2, -2, 3, -3, \dots\},$$

její prvky opět označujeme obvykle písmeny m, n, i, j, k, l.

Množina $\mathbb{Z}$ je také uspořádaná: $m > n$ jestliže $m - n > 0$, tj. $m - n \in \mathbb{N}$.

Operace sčítání $m + n$, odčítání $m - n$ i násobení $m\,n$ jsou definovány pro všechny dvojice celých čísel.

Operace dělení $m : n$ je definována pouze pro $n \neq 0$ a jen tehdy, jestliže m je dělitelné n, tj. existuje celé číslo $k \in \mathbb{Z}$, že $m = n\,k$.

Racionální čísla

Abychom mohli všechna čísla navzájem dělit (kromě dělení nulou), přidáme zlomky. Dostáváme tak racionální čísla:

Definice 1.40. Množinu racionálních čísel označujeme $\mathbb{Q}$. Je to množina zlomků (podílů) celých čísel s nenulovým jmenovatelem (dělitelem). Pro jednoznačnost vyjádření racionálního čísla požadujeme, aby jmenovatel zlomku $\frac{m}{n}$ byl přirozené číslo $n \in \mathbb{N}$, čitatel celé číslo $m \in \mathbb{Z}$ a čísla m, n byla nesoudělná: jejich největší společný dělitel $D(m, n)$ byl 1:

$$\mathbb{Q} := \left\{ \frac{m}{n} \;:\; m \in \mathbb{Z} \;\wedge\; n \in \mathbb{N} \;\wedge\; D(m, n) = 1 \right\}.$$

Racionální čísla označujeme obvykle písmeny $x, y, z, p, q, r, a, b, c, d, \dots$.

Množina $\mathbb{Q}$ je uspořádaná, $\frac{m_1}{n_1} < \frac{m_2}{n_2}$ pokud $m_1 n_2 < m_2 n_1$ ($n_1, n_2 > 0$ protože podle definice $n_1, n_2 \in \mathbb{N}$.

Operace sčítání $x + y$, odčítání $x - y$ a násobení $x\,y$ jsou definované pro každá dvě racionální čísla x, y. Operace dělení $x : y$ **je definována jen pro** $y \neq 0$.

Operace se zlomky

Je to sice učivo ze základní školy, najdou se však studenti, kteří tyto operace neovládají. Patří mezi ně například „střihači zlomků“ kteří počítají podle „svých pravidel“

$$\frac{\mathbf{1}}{\mathbf{2+3}} = \frac{\mathbf{1}}{\mathbf{2}} + \frac{\mathbf{1}}{\mathbf{3}}, \qquad \mathbf{(a+b)^{-1} = a^{-1} + b^{-1}}, \qquad \frac{\mathbf{a+b}}{\mathbf{c+d}} = \frac{\mathbf{a}}{\mathbf{c}} + \frac{\mathbf{b}}{\mathbf{d}}.$$

Dosazením konkrétních čísel za a, b, c, d snadno ověříte, že **výše uvedená „pravidla“ neplatí**.

Připomeňme **správná** pravidla pro počítání se zlomky:

Věta 1.41. Pro racionální, reálná i komplexní čísla a, b, c, d platí následující pravidla:

$$\frac{a}{b}+\frac{c}{d}=\frac{a\,d+b\,c}{b\,d}, \qquad \frac{a}{b}-\frac{c}{d}=\frac{a\,d-b\,c}{b\,d}, \qquad \frac{a}{b}\cdot\frac{c}{d}=\frac{a\,c}{b\,d} \qquad \text{pro } b\neq 0\,,\ d\neq 0,$$

$$\frac{\frac{a}{b}}{\frac{c}{d}} \equiv \frac{a}{b}:\frac{c}{d}=\frac{a}{b}\cdot\frac{d}{c}=\frac{a\,d}{b\,c} \quad \text{pro } b\neq 0\,,\ c\neq 0\,,\ d\neq 0.$$

Reálná čísla

Reálná čísla vycházejí z geometrické představy bodů na přímce. Odmocnina z většiny přirozených čísel $2, 3, 5, 6, 7, 8, \ldots$ není číslo přirozené ani racionální, leží však na číselné ose mezi racionálními čísly. Množinu reálných čísel tak dostaneme z množiny racionálních čísel „vyplněním děr“ mezi racionálními čísly pomocí tzv. iracionálních čísel, které nelze vyjádřit ve tvaru zlomku $\frac{m}{n}$, kde $m \in \mathbb{Z}$, $n \in \mathbb{N}$. Jsou to například odmocniny $\sqrt{2}, \sqrt[3]{3}, \sqrt{5}, \ldots$, jejich násobky, součiny a podíly, např. $\frac{1}{2}\sqrt{2}, \sqrt{5}/\sqrt{7}$ a také čísla π, e a mnoho dalších.

Definice 1.42. **Množinu reálných čísel** označujeme symbolem $\mathbb{R}$, jako u racionálních čísel její prvky obvykle označujeme písmeny $x, y, z, u, v, p, q, r, s, t, u, v, a, b, c, d, \ldots$

Pro libovolné $a, b \in \mathbb{R}$ splňující $a < b$ definujeme otevřené, uzavřené intervaly

$$(a,b) := \{x \in \mathbb{R} \ : \ a < x < b\} \qquad \langle a,b\rangle := \{x \in \mathbb{R} \ : \ a \le x \le b\},$$

a polouzavřené (polootevřené) intervaly

$$(a,b\rangle := \{x \in \mathbb{R} : a < x \le b\}\,, \qquad \langle a,b) := \{x \in \mathbb{R} : a \le x < b\}.$$

V případě „otevřeného“ konce připouštíme $a = -\infty$ nebo $b = \infty$, např. $(-\infty, b\rangle$ a (a, ∞).

Označíme $\mathbb{R}^+ := (0, \infty)$ a podobně $\mathbb{R}_0^+ := \langle 0, \infty)$, $\mathbb{R}^- := (-\infty, 0)$ a $\mathbb{R}_0^- := (-\infty, 0\rangle$.

Množinu reálných čísel rozšířenou o symboly $\pm\infty$ značíme $\mathbb{R}^* := \mathbb{R} \cup \{-\infty, \infty\}$.

Stejně jako u racionálních čísel reálná čísla tvoří množinu uspořádanou. Operace sčítání $x+y$, odčítání $x-y$, násobení $x\,y$ a dělení $x : y$ jsou definovány pro všechny dvojice reálných čísel, jen při dělení vyžadujeme $y \neq 0$.

Pro otevřený a uzavřený interval se užívají také hranaté závorky: $]a, b[$ znamená otevřený (a, b) a $[a, b]$ označuje uzavřený interval $\langle a, b\rangle$.

Maximum, supremum, minimum a infimum

Omezená (tj. ohraničená) podmnožina M množiny reálných čísel $\mathbb{R}$ může mít své maximum: je to největší prvek m množiny M, tj.

$$m := \max(M) \quad \Longleftrightarrow \quad m \in M \ \wedge\ \forall x \in M \ \text{ platí } \ x \le m.$$

Otevřený interval $(0, 2)$ však nemá maximum, protože pravá mez 2, kandidát na maximum, už není v M a nemůže být proto maximem. Abychom tuto nepříjemnost odstranili, zavedeme pojem supremum množiny, které je rovno maximu množiny v případě, že maximum existuje.

Supremum množiny nemusí být v dané množině. Je to tzv. „nejmenší horní závora“ množiny, tj. nejmenší číslo, které je větší nebo rovno než všechna čísla množiny M.

Omezená podmnožina také nemusí mít své minimum, například opět interval $(0, 2)$. Podobnými úvahami zobecněním pojmu minimum dostaneme pojem infimum množiny: je to „největší dolní závora“, tj. největší číslo, které je menší nebo rovno než všechna čísla množiny. Také infimum množiny v dané množině být nemusí.

Definice 1.43. Buď M neprázdná omezená podmnožina množiny reálných čísel $\mathbb{R}$. Potom:

(a) Číslo h je **horní závora** množiny M, jestliže $\forall x \in M$ platí $x \leq h$.

(b) Číslo s je **supremum** množiny M jestliže s je nejmenší horní závora, $s = \sup(M)$.

(c) Číslo d je **dolní závora** množiny M, jestliže $\forall x \in M$ platí $x \geq d$.

(d) Číslo i **je infimum** množiny M, jestliže i je největší dolní závora, píšeme $i = \inf(M)$.

(e) Pokud množina M není omezená shora, nemá horní závoru a položíme $\sup(M) = \infty$.

(f) Pokud množina M není omezená zdola, nemá dolní závoru a položíme $\inf(M) = -\infty$.

Příklady 1.44.

(a) Horní závorou otevřeného intervalu $I = (1, 5)$ je nekonečně mnoho, např. čísla $5, 6, 7, \ldots$, také 5.1 a 5.01. Nejmenší z nich je 5. Proto supremum itervalu je $\sup(I) = 5$. Podobně dolní závory jsou čísla, $-1, 0, 1, 0.9, \ldots$, největší z nich je číslo 1. Proto infimum intervalu je $\inf(I) = 1$. Maximum ani minimum otevřeného intervalu I neexistuje.

(b) Uzavřený interval $I = \langle 1, 5\rangle$ má stejné horní i dolní závory jako v předchozím příkladu. Proto supremum i maximum intervalu je $\sup(I) = \max(I) = 5$ a také infimum i minimum je $\inf(I) = \min(I) = 1$.

(c) Intervaly $I_1 = (1, 5\rangle$ a $I_2 = \langle 1, 5)$ mají stejné supremum $\sup(I_1) = \sup(I_2) = 5 = \max(I_1)$ a stejné infimum $\inf(I_1) = \inf(I_2) = \min(I_2) = 1$. maximum $\max(I_2)$ ani $\min(I_1)$ neexistují.

(d) Množina $M = \{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots\}$ má $\max(M) = \sup(M) = 1$, $\inf(M) = 0$ minimum nemá.

(e) Neomezený interval $J = (1, \infty)$ má $\sup(J) = \infty$, $\inf(J) = 1$, maximum ani minimum však nemá. Podobně neomezený interval $J = (-\infty, 3\rangle$ má $\sup(J) = \max(J) = 3$, infimum $\inf(J) = -\infty$, minimum nemá.

Poznámky 1.45.

(a) Definice suprema a infima jsou trochu složitější než definice maxima a minima, pojmy supremum a infimum, však mají lepší vlastnosti: vždy existují, zatímco maximum i minimum existovat nemusí.

(b) Pokud množina má maximum, je to současně i supremum a pokud existuje minimum, je to také infimum.

(c) Vztah $s = \sup(M)$ neprázdné množiny M znamená dvě vlastnosti:

(i) Pro každé $x \in M$ platí $x \leq s$,

(ii) Supremum s je nejmenší horní závora, tj. každé číslo menší než s není horní závorou: pro každé $\varepsilon > 0$ číslo $s - \varepsilon$ není horní závorou, protože existuje $x \in M$ že $x > s - \varepsilon$.

(d) Podobně vztah $i = \inf(M)$ neprázdné množiny M znamená dvě vlastnosti:

(i) Pro každé $x \in M$ platí $x \geq i$,

(ii) Infimum je největší dolní závorou: tj. každé číslo větší než i není dolní závorou: pro každé $\varepsilon > 0$ existuje $x \in M$ že $x > s - \varepsilon$.

Věta 1.46. Uvažujme libovolné podmnožiny M, M_1, M_2 množiny reálných čísel. Potom platí:

(a) Každá podmnožina M množiny reálných čísel $\mathbb{R}$ má svoje supremum a infimum.

(b) Jestliže existuje maximum $\max(M)$ množiny M, je to i supremum: $\sup(M) = \max(M)$.

(c) Jestliže existuje minimum $\min(M)$, je to i infimum: $\inf(M) = \min(M)$.

(d) Pro každou neprázdnou M a $x \in M$ platí $-\infty \leq \inf(M) \leq x \leq \sup(M) \leq \infty$.

(e) Platí $\sup(M_1 \cup M_2) = \max(\sup(M_1), \sup(M_2))$.

(f) Platí $\inf(M_1 \cup M_2) = \min(\inf(M_1), \inf(M_2))$.

Pokud $\sup(M_i) = \infty$, potom položíme $\max(\sup(M_1), \sup(M_2)) := \infty$.
Podobně v případě $\inf(M_i) = -\infty$ položíme $\max(\inf(M_1), \inf(M_2)) := -\infty$.

Poznámky 1.47.

(a) V Definici 1.43 jsme zavedli supremum a infimum neprázdné množiny. Jak zavést supremum prázdné množiny. Horní závorou prázdné množiny je každé reálné číslo. Nejmenší dolní závora proto neexistuje, ale infimum je $-\infty$, proto položíme $\sup(\emptyset) := -\infty$. Podobně dolní závorou prázdné množiny je každé reálné číslo. Největší dolní závora proto neexistuje, supremum je ∞ proto položíme $\inf(\emptyset) = \infty$.

(b) Stejný výsledek dostaneme, pokud chceme, aby vlastnost (c) z předchozí věty platila i pro případ prázdné množiny. Pokud $M_1 = \emptyset$ a $\sup(M_2) := m$, potom platí $M_1 \cup M_2 = M_2$, a proto $\sup(M_1 \cup M_2) = \sup(M_2) = m$. Podle podmínky (c) $\sup(\emptyset \cup M_2) \equiv m = \max(\sup(\emptyset), m)$ má platit pro každé m. To je splněno v případě $\sup(\emptyset) = -\infty$.

(c) Podobně lze odvodit, $\inf(\emptyset) = \infty$ je nutnou podmínkou, aby vlastnost (d) platila i pro případ prázdné množiny, tj. aby platilo $\inf(\emptyset \cup M_2) = \min(\inf(\emptyset), \inf(M_2)$ pro libovolné infimum množiny M_2.

Poznámky 1.48. (Dedekindovy řezy)

V teorii množin se reálná čísla zavádějí pomocí tzv. Dedekindových[16] řezů.

(a) **Dedekindovým řezem** (anglicky „cut“) nazveme dvojici (A, B) podmnožin racionálních čísel $\mathbb{Q}$, která vznikne „rozřezáním“ množiny racionálních čísel na dvě neprázdné části: dolní část A a její doplněk horní část $B = \mathbb{Q} \setminus A$, přičemž pro každé $a \in A$ a $b \in B$ platí $a < b$. Navíc požadujeme, že dolní část A nemá největší prvek. Řez je tak jednoznačně určen svou dolní částí A.

Množina A je tak vždy interval racionálních čísel od minus nekonečna, B pak interval racionálních čísel (větších než kterékoliv číslo z A) po nekonečno.

(b) Řezy lze rozdělit do dvou druhů:

(i) B má nejmenší prvek q, tj. $B = \langle q, \infty) \cap \mathbb{Q}$,

(ii) B nemá nejmenší prvek.

[16] Richard Dedekind (1831–1916) německý matematik.

Řezy prvního druhu ztotožníme s racionálním číslem q, které je nejmenším prvkem horní části B. Řez druhého druhu, kdy A nemá největší prvek a ani B nemá nejmenší prvek, definuje nové tzv. iracionální číslo. Například řez $A = \{q \in \mathbb{Q} \mid q < 2\}$ určuje racionální číslo 2, řez $A = \{q \in \mathbb{Q} \mid q^2 < 3\}$ definuje iracionální číslo $\sqrt{3}$.

(c) Řezy jsou uspořádané podle inkluze dolních částí, což dává uspořádání odpovídajících reálných čísel: jestliže $A_1 \subset A_2$, potom řekneme, že $a_1 \leq a_2$, kde a_i je reálné číslo určené řezem A_i. Číslo je kladné, pokud jeho dolní část A obsahuje interval $(-\infty, 0\rangle$.

(d) Dále nutno pomocí řezů definovat operace sčítání, odčítání, násobení i dělení reálných čísel. Potřeba ověřit, že definice nejsou ve sporu a operace mají požadované vlastnosti. Například součet dvou čísel určených řezy A_1, A_2 je určen řezem $\{x_1 + x_2 \mid x_1 \in A_1, x_2 \in A_2\}$.

(e) V teorii Dedekindových řezů symbol nekonečno ∞ odpovídá „řezu“ $(\mathbb{Q}, \emptyset)$ s prázdnou horní částí a symbol $-\infty$ řezu $(\emptyset, \mathbb{Q})$ s prázdnou dolní částí.

(f) Supremum množiny čísel je sjednocení dolních částí řezů všech čísel množiny a infimum množiny čísel je průnik dolních částí všech čísel množiny.

Komplexní čísla

Podnětem pro rozšíření množiny reálných čísel je fakt, že kvadratické rovnice $a\,x^2 + b\,x + c = 0$ s reálnými koeficienty a, b, c a záporným diskriminantem $D := b^2 - 4ac < 0$ nemají v oboru reálných čísel řešení.

Rozšíření spočívá v tom, že k reálné části x přidáme tzv. imaginární část y označenou tzv. **imaginární** jednotkou i. Komplexní číslo $z = [x, y]$ s reálnou složkou x a imaginární složkou y tak zapíšeme $z = x + \mathrm{i}y$. Komplexní čísla znázorňujeme jako vektory v tzv. komplexní Gaussově[17] rovině, na vodorovnou osu dáváme reálnou část x, na svislou osu imaginární část y. Komplexní číslo $z = x + \mathrm{i}y$ tak znázorňujeme jako vektor o souřadnicích (x, y).

Definice 1.49. Komplexní číslo $z = [x, y]$ lze reprezentovat uspořádanou dvojicí reálných čísel x, y, kde první složka x se nazývá **reálná část** a druhá y je **imaginární část** komplexního čísla z. Zapisujeme ho ve tvaru $z = x + \mathrm{i}y$, kde i označuje **imaginární jednotku**, která splňuje $\mathrm{i}^2 = -1$. Množinu komplexních čísel $\mathbb{C}$ lze ztotožnit s rovinou $\mathbb{R}^2$.

Komplexní číslo a jeho složky obvykle zapisujeme písmeny $z = [x, y] \equiv x + \mathrm{i}y$, také $w = [u, v] \equiv u + \mathrm{i}v$.

Komplexní čísla nelze „rozumně“ uspořádat, množina komplexních čísel $\mathbb{C}$ netvoří uspořádanou množinu jako čísla přirozená, celá, racionální a reálná.

Operace sčítání a odčítání jsou definovány po složkách: pro $z_i = [x_i, y_i] \equiv x_i + \mathrm{i}y_i$ položíme

$$z_1 + z_2 := [x_1 + x_2, y_1 + y_2] \equiv (x_1 + x_2) + \mathrm{i}(y_1 + y_2),$$
$$z_1 - z_2 := [x_1 - x_2, y_1 - y_2] \equiv (x_1 - x_2) + \mathrm{i}(y_1 - y_2).$$

Z rovností $\mathrm{i} \cdot 1 = 1 \cdot \mathrm{i} = \mathrm{i}$ a $\mathrm{i} \cdot \mathrm{i} = -1$ lze snadno odvodit pravidlo pro násobení:

$$z_1 \cdot z_2 := [x_1x_2 - y_1y_2, x_1y_2 + x_2y_1] \equiv (x_1x_2 - y_1y_2) + \mathrm{i}(x_1y_2 + x_2y_1)\,.$$

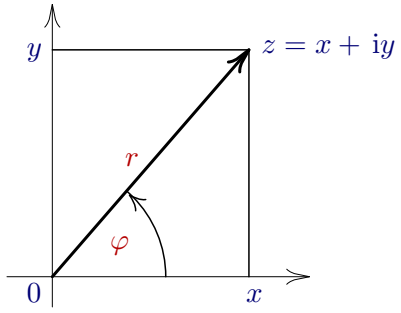
Číslo $\overline{z} := [x, -y] \equiv x - \mathrm{i}y$ se nazývá číslo **komplexně sdružené** k číslu $z = [x, y]$.

[17] Johann Carl Friedrich Gauss (1777–1855) německý matematik a fyzik

Vedle uvedeného algebraického zápisu $z = x + \mathrm{i}y$ komplexního čísla z se užívá také **goniometrický tvar**, který obsahuje velikost r vektoru (x, y) a jeho směr určený jednotkovým vektorem $(\cos\varphi, \sin\varphi)$ svírající s osou x orientovaný úhel φ, viz Obr. 1.5. Přitom platí

$$r = \sqrt{x^2 + y^2}, \quad x = r\,\cos\varphi, \quad y = r\,\sin\varphi\,.$$

Protože funkce sin a cos mají periodu 2π, orientovaný úhel φ je určen jednoznačně až na přičtení libovolného celého násobku 2π, tj. pro celé k úhly φ a $\varphi + 2k\pi$ určují stejné komplexní číslo z.

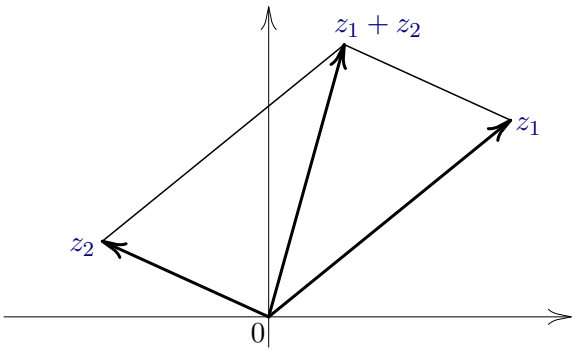


Obr. 1.5: Algebraický a goniometrický tvar komplexního čísla z.

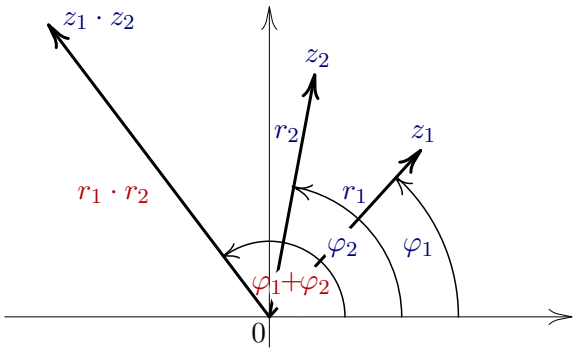
Sčítání komplexních čísel $z_1 + z_2$ odpovídá sčítání příslušných vektorů v rovině, viz Obr. 1.6.

Operace násobení je rozšířením operace násobení reálným číslem. Pokud $z_1 := [r, 0]$ je reálné číslo, potom součin je z_1 násobek vektoru z_2, tj. $z_1 \cdot z_2 = [r, 0] \cdot [x_2, y_2] = [rx_2, ry_2]$.

Pokud obě čísla mají imaginární složku, interpretace součinu je složitější. V goniometrickém tvaru součin $z = z_1 \cdot z_2$ komplexních čísel $z_i = x_i + \mathrm{i}y_i$ s velikostmi r_i a úhly φ_i má velikost r rovnou součinu velikostí $r = r_1 \cdot r_2$ a úhel φ je součet úhlů $\varphi = \varphi_1 + \varphi_2$, viz Obr. 1.7.



Obr. 1.6: Součet dvou komplexních čísel.



Obr. 1.7: Součin dvou komplexních čísel

Absolutní hodnotou čísla nazýváme jeho „vzdálenost“ od počátku, tj. od komplexní nuly $0 \equiv [0, 0]$. Je definována pro všechna čísla a je vždy kladné číslo nebo nula:

Definice 1.50. Pro nezáporné číslo (přirozené, celé, racionální i reálné) je absolutní hodnota $|x|$ stejné číslo x. Pro záporné číslo $x < 0$ je $|x| = -x$, tj. číslo kladné. Platí vzorec $|x| = \sqrt{x^2}$, který pro komplexní číslo $z = [x, y]$ podle Pythagorovy věty nutno doplnit na $|z| = \sqrt{x^2 + y^2}$. Platí také $|z|^2 = z \cdot \overline{z}$, kde $\overline{z} = [x, -y]$ je číslo komplexně sdružené.

Vlastnosti operací racionálních, reálných i komplexních čísel shrnuje následující věta:

Věta 1.51. Operace sčítání a násobení na celých, racionálních, reálných i komplexních číslech z_i jsou asociativní, komutativní:

$$(z_1+z_2)+z_3 = z_1+(z_2+z_3), \quad (z_1\cdot z_2)\cdot z_3 = z_1\cdot(z_2\cdot z_3)\,, \quad z_2+z_1 = z_1+z_2, \quad z_2\cdot z_1 = z_1\cdot z_2$$

a jsou spojeny distributivním zákonem:

$$z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3\,, \quad (z_1 + z_2) + z_3 = z_1 \cdot z_3 + z_2 \cdot z_3\,.$$

Pro absolutní hodnotu součinu platí $|x \cdot y| = |x| \cdot |y|$.
Pro absolutní hodnotu součtu platí tzv. trojúhelníková nerovnost $|x + y| \leq |x| + |y|$.

Kvaterniony

Uveďme ještě další rozšíření komplexních čísel. Přidáním imaginární složky k reálnému číslu jsme získali komplexní čísla, které lze reprezentovat uspořádanou dvojicí reálných čísel se speciálním násobením.

Dalším rozšířením čísel jsou čísla zvaná **kvaterniony**. Lze je reprezentovat pomocí čtveřic reálných čísel (a, b, c, d). K reálné a imaginární složce označené jednotkou $\mathrm{i} = (0, 1, 0, 0)$ přidáme další dvě imaginární složky $\mathrm{j} = (0, 0, 1, 0)$ a $\mathrm{k} = (0, 0, 0, 1)$. Kvaternion určený čtveřicí (a, b, c, d) lze tak zapsat jako $a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}$.

Operace sčítání kvaternionů je sčítání po složkách jako sčítání vektorů:

$$(a_1, b_1, c_1, d_1) + (a_2, b_2, c_2, d_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2, d_1 + d_2);$$

nebo v zápisu pomocí komplexních jednotek

$$(a_1 + b_1\,\mathrm{i} + c_1\,\mathrm{j} + d_1\,\mathrm{k}) + (a_2 + b_2\,\mathrm{i} + c_2\,\mathrm{j} + d_2\,\mathrm{k}) = (a_1 + a_2) + (b_1 + b_2)\,\mathrm{i} + (c_1 + c_2)\,\mathrm{j} + (d_1 + d_2)\,\mathrm{k}\,.$$

Násobení je určeno vzájemným součinem 1 a imaginárních jednotek i, j, k:

$$\begin{array}{llll} 1 \cdot 1 = 1\,, & 1 \cdot \mathrm{i} = \mathrm{i}\,, & 1 \cdot \mathrm{j} = \mathrm{j}\,, & 1 \cdot \mathrm{k} = \mathrm{k}\,, \\ \mathrm{i} \cdot 1 = \mathrm{i}\,, & \mathrm{i} \cdot \mathrm{i} = -1\,, & \mathrm{i} \cdot \mathrm{j} = \mathrm{k}\,, & \mathrm{i} \cdot \mathrm{k} = -\mathrm{j}\,, \\ \mathrm{j} \cdot 1 = \mathrm{j}\,, & \mathrm{j} \cdot \mathrm{i} = -\mathrm{k}\,, & \mathrm{j} \cdot \mathrm{j} = -1\,, & \mathrm{j} \cdot \mathrm{k} = \mathrm{i}\,, \\ \mathrm{k} \cdot 1 = \mathrm{k}\,, & \mathrm{k} \cdot \mathrm{i} = \mathrm{j}\,, & \mathrm{k} \cdot \mathrm{j} = -\mathrm{i}\,, & \mathrm{k} \cdot \mathrm{k} = -1\,. \end{array}$$

Absolutní hodnota kvaternionu je $|a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}| = \sqrt{a^2 + n^2 + c^2 + d^2}$.

Operace sčítání kvaternionů je asociativní a komutativní, operace násobení je asociativní ale není komutativní.

Množina kvaternionů se označuje $\mathbb{H}$ podle svého objevitele Hamiltona[18] Kvaterniony se užívají k popisu rotace v $\mathbb{R}^3$ i $\mathbb{R}^4$.

1E. Relace

Definice 1.52. Buďte A, B neprázdné množiny, které nemusí být různé. **Binární relací $\mathcal{R}$ mezi množinami** A, B nazveme libovolnou podmnožinu $\mathcal{R}$ kartézského součinu $A \times B$

$$\mathcal{R} \subset A \times B := \{[a, b] \ : \ a \in A \ \wedge \ b \in B\}\,.$$

Je-li $A = B$ mluvíme o **binární relaci na množině** A.
Binární relace $\mathcal{R}$ určuje dvě význačné množiny:
Definiční obor relace $\mathcal{R}$: $\mathcal{D}(\mathcal{R}) := \{a \in A \mid \exists\, b \in B : [a, b] \in \mathcal{R}\}$,
Obor hodnot relace $\mathcal{R}$: $\mathcal{H}(\mathcal{R}) := \{b \in B \mid \exists\, a \in A : [a, b] \in \mathcal{R}\}$.

[18] William Rowan Hamilton (1805–1865) byl irský matematik, fyzik a astronom.

Vztah $[a,b] \in \mathcal{R}$ se také často zapisuje $a\mathcal{R}b$.

Příkladem binární relace je tzv. *relační databáze*, která strukturuje data ve formě tabulek. Například relace $\mathcal{R} \subset A \times B$, kde A je množina zaměstnanců, B množina vozidel a relace $\mathcal{R}$ vyjadřuje, kdo s kterým vozidlem má právo jezdit.

V matematice užíváme relace např. rovnost $=$, nerovnosti $<$, $\leq$, $>$, $\geq$.

Binární relace $\mathcal{R}$ na množině A mohou mít řadu významných vlastností. Nejdůležitější z nich popíšeme v následující definici:

Definice 1.53. Buď $\mathcal{R}$ binární relace na množině A. Řekneme, že relace $\mathcal{R}$ je

(a) **reflexivní**, pokud $\forall a \in A$ platí $[a,a] \in \mathcal{R}$,

(b) **symetrická**, pokud $\forall a,b \in A$ platí $([a,b] \in \mathcal{R}) \Rightarrow ([b,a] \in \mathcal{R})$,

(c) **antisymetrická**, pokud $\forall a,b \in A$ platí $([a,b] \in \mathcal{R}) \wedge ([b,a] \in \mathcal{R}) \;\Rightarrow\; (a = b)$,

(d) **tranzitivní**, pokud $\forall a,b,c \in A$ platí $(([a,b] \in \mathcal{R}) \wedge ([b,c] \in \mathcal{R})) \;\Rightarrow ([a,c] \in \mathcal{R})$,

(e) **ekvivalence**, pokud je reflexivní, symetrická a tranzitivní.

Příklad. Na množinách $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ máme přirozenou relaci $\mathcal{R}$ neostré nerovnosti „$\leq$“ definovanou $[x,y] \in \mathcal{R}$ jestliže $x \leq y$. Tato relace je reflexivní, antisymetrická a tranzitivní. Ostrá nerovnost „$<$“ je tranzitivní, není však symetrická ani antisymetrická ani reflexivní.

Příklad. Mezi konečnými podmnožinami množiny $\mathbb{N}$ můžeme zavést relaci $\mathcal{R}$ počtu prvků: $[A,B] \in \mathcal{R}$ pokud množiny A a B mají stejný počet prvků. Tato relace je reflexivní, symetrická a tranzitivní, je proto ekvivalencí.

Definice 1.54. Buď $\mathcal{R} \subset A \times B$. Relaci $\mathcal{R}^{-1}$ nazveme **relací inverzní** k relaci $\mathcal{R}$, pokud je podmnožinou $B \times A$ a platí $[b,a] \in \mathcal{R}^{-1}$ právě když $[a,b] \in \mathcal{R}$.

Příklad. Relace „$\geq$“ je inverzní k relaci „$\leq$“ a „$>$“ je inverzní k relaci „$<$“. Je-li relace $\mathcal{R}$ na množině A symetrická, $\mathcal{R}^{-1} = \mathcal{R}$.

Pojem binární relace lze zobecnit na relaci mezi více množinami:

Definice 1.55. *n-ární relací* rozumíme podmnožinu kartézského součinu $A_1 \times A_2 \times \cdots A_n$, kde $A_1, A_2, \ldots, A_n$ jsou neprázdné, ne nutně navzájem různé množiny.

1F. Zobrazení

Zobrazení je základním pojem matematiky. Po formální stránce je to relace $\mathcal{F}$, ve které pro každé $a \in A$ existuje nejvýše jedno $b \in B$, že $[a,b] \in \mathcal{F}$. Jazykem matematiky to zapisujeme:

Definice 1.56. **Zobrazením** z množiny A do množiny B nazveme relaci $\mathcal{F}$, která splňuje

$$\forall\, a \in A\; \forall\, b_1, b_2 \in B \quad \text{platí} \quad (([a,b_1] \in \mathcal{F}) \;\wedge\; ([a,b_2] \in \mathcal{F})) \quad \Longrightarrow \quad b_1 = b_2.$$

Místo $\mathcal{F} \subset A \times B$ píšeme $f\colon A \to B$ a místo $[a,b] \in \mathcal{F}$ píšeme $b = f(a)$ nebo $a \mapsto f(a)$.
Prvek a se nazývá **vzor** prvku b v zobrazení f a b říkáme **obraz** prvku a v zobrazení f.
Funkcí obvykle rozumíme zobrazení, kde množina B je číselná.

Pojem definiční obor a obor hodnot relace přeneseme na zobrazení:

Definice 1.57. Všechna $a \in A$, pro které existuje $b \in B$ takové, že $f(a) = b$, tj. $[a, b] \in \mathcal{F}$, tvoří množinu, které říkáme **definiční obor** zobrazení f a značíme $\mathcal{D}(f)$.

Všechna $b \in B$, pro které existuje $a \in A$ takové, že $f(a) = b$, tj. $[a, b] \in \mathcal{F}$, tvoří množinu, které říkáme **obor hodnot** zobrazení f a značíme ji $\mathcal{H}(f)$.

Pokud obor hodnot zobrazení f je částí definičního oboru g, zobrazení lze skládat:

Definice 1.58. (**Skládání zobrazení**) Buďte A, B, C množiny a $f : A \to B$ a $g : B \to C$ zobrazení. Jestliže $\mathcal{H}(f) \subset \mathcal{D}(g)$, potom existuje zobrazení $g \circ f : A \to C$ definované vztahem $\forall\, x \in \mathcal{D}(f)\,,\ (g \circ f)(x) = g(f(x))$, které nazýváme **zobrazení složené**. Zápis $g \circ f$ čteme „g po f“ .

Důležitými vlastnostmi zobrazení jsou následující pojmy:

Definice 1.59. Zobrazení $f : A \to B$ (definované na celém A, tj. $\mathcal{D}(f) = A$) nazveme

(a) **prosté** neboli **injektivní** nebo **injekce**, jestliže každý obraz má jenom jeden vzor, tj.

$$\forall\, a_1, a_2 \in A \ \ \forall\, b \in B \quad \text{platí} \quad b = f(a_1),\ b = f(a_2) \ \Rightarrow\ a_1 = a_2\,.$$

(b) **na** neboli **surjektivní** nebo **surjekce**, jestliže obor hodnot funkce je celá množina B, tj. $\mathcal{H}(f) = B$.

(c) **vzájemně jednoznačné** neboli **bijektivní** nebo **bijekce**, jestliže zobrazení je injektivní i surjektivní. Říkáme, že f je **bijekce** množin A a B.

Skládání zobrazení (pokud je definované) je asociativní: $(f \circ g) \circ h = f \circ (g \circ h)$.

Každá binární relace $\mathcal{R} \subset A \times B$ má svoji inverzní relaci $\mathcal{R}^{-1} \subset B \times A$. Pro bijektivní zobrazení $f : A \to B$ stejným způsobem definujeme inverzní zobrazení $f^{-1} : B \to A$.

Definice 1.60. Buď $f : A \to B$ vzájemně jednoznačné zobrazení mezi množinami A a B. Potom zobrazení f^{-1} nazveme **zobrazením inverzním** k zobrazení f, jestliže příslušná relace $\mathcal{F}^{-1}$ je inverzní k relaci $\mathcal{F}$, tj.

$$\forall\, a \in A \ \ \forall\, b \in B \quad \text{platí} \quad f^{-1}(b) = a \iff f(a) = b\,.$$

Pokud zobrazení f definované na $\mathcal{D}(f) \subset A$ je prosté ale není na, potom lze definovat inverzní zobrazení f^{-1} s definičním oborem $\mathcal{D}(f^{-1}) = \mathcal{H}(f)$ a oborem hodnot $\mathcal{H}(f^{-1}) = \mathcal{D}(f)$.

Poznámky 1.61.

(a) Skládání zobrazení (pokud je definované) je asociativní: $(h \circ g) \circ f = h \circ (g \circ f)$, není však komutativní, jestliže $g \circ f$ je definované, $f \circ g$ nemusí být vůbec definované.

(b) Zvláštním případem zobrazení je identické zobrazení I_M na množině M. Je to zobrazení z M do M, které „nic nedělá“, tj. $\mathcal{D}(\mathrm{I}_M) = \mathcal{H}(\mathrm{I}_M) = M$ a $\mathrm{I}_M(x) = x\,,\ \forall\, x \in M$.

(c) Identické zobrazení I_M je bijektivní z M na M, má inverzní zobrazení, které je stejné, tj. $(\mathrm{I}_M)^{-1} = \mathrm{I}_M$. Působí jako neutrální prvek: pro $f : A \to B$ platí $f = \mathrm{I}_B \circ f = f \circ \mathrm{I}_A$.

(d) Inverzní zobrazení k zobrazení $f : A \to B$ můžeme definovat vztahy $f^{-1} \circ f = \mathrm{I}_A\,,$ $f \circ f_{-1} = \mathrm{I}_B$.

(e) Zobrazení F nazveme **rozšířením** neboli **extenzí** zobrazení f a obráceně řekneme, že zobrazení f je **zúžením** neboli **restrikcí** zobrazení F, pokud $\mathcal{D}(f) \subset \mathcal{D}(F)$ a platí $F(x) = f(x)$ pro všechna $x \in \mathcal{D}(f)$.

1G. Mohutnost množin

Která ze dvou množin má víc prvků? V případě konečných množin stačí porovnat počty prvků obou množin. V případě nekonečných množin je situace složitější, nelze mluvit o počtu prvků, místo toho mluvíme o **mohutnosti** množiny. Mohutnost množiny porovnáváme pomocí prostého zobrazení:

Definice 1.62. **(Mohutnost množin)**

(a) Řekneme, že množina A má **stejnou nebo menší mohutnost** než množina B, pokud existuje prosté zobrazení, které každému prvku z A přiřadí jeden prvek z B. (Prosté znamená, že různým prvkům množiny A přiřadí různé prvky množiny B).

(b) Řekneme, že množiny A a B mají **stejnou mohutnost**, pokud existuje prosté zobrazení z A do B a také existuje prosté zobrazení z B do A.

(c) Řekneme, že množina A má **menší mohutnost** než množina B, pokud existuje prosté zobrazení z A a do B, ale **neexistuje** prosté zobrazení z B do A.

Poznámky 1.63.

(a) Platí: Množiny A, B mají stejnou mohutnost, pokud existuje bijektivní, tj. vzájemně jednoznačné zobrazení z A do B.

(b) Uvedenou definici lze uplatnit i na konečné množiny. Přitom platí: pokud konečné množiny mají stejné mohutnosti, mají i stejný počet prvků.

(c) Pro konečné množiny platí: *Množina A, která je vlastní podmnožinou B (tj. $A \subset B$ a v B existují prvky, které nejsou v A), má méně prvků, tj. A má menší mohutnost než B.*

(d) V případě nekonečných množin tato vlastnost neplatí: například množina přirozených čísel má více prvků než množina přirozených čísel, přitom, jak uvidíme, obě množiny mají stejnou mohutnost. Kvůli tomuto paradoxu podle Galilea nemá smysl porovnávat počet prvků nekonečných množin.

Povšimněme si některých nekonečných množin, které mají stejnou mohutnost jako množina přirozených čísel $\mathbb{N}$, tedy množiny, jejichž prvky lze „oindexovat“ přirozenými čísly, tj. seřadit do posloupnosti. Přitom jedna může být vlastní podmnožinou druhé a přesto má stejnou mohutnost. Je to je například množina všech kladných sudých čísel $\{2, 4, 6, 8, 10, \dots\}$, kdy bijekcí je zobrazení $n \mapsto 2n$.

Také množinu všech celých čísel $\mathbb{Z}$ lze „oindexovat“ přirozenými čísly, pokud ji seřadíme do posloupnosti $\{0, -1, 1, -2, 2, -3, 3, -4, 4, -5, 5, \dots\}$.

Překvapivější však je, že stejnou mohutnost má i množina všech racionálních čísel $\mathbb{Q}$, což lze dokázat následovně. Racionální čísla zapíšeme ve tvaru $\frac{p}{q}$, kde p je celé, q přirozené a p, q jsou nesoudělná, číslo 0 zapíšeme jako $\frac{0}{1}$. Každému číslu $\frac{p}{q}$ nyní přiřadíme tzv. *výšku* $r = |p| + q$.

Protože počet racionálních čísel s danou výškou r je konečný, čísla seřadíme do posloupnosti nejprve podle výšky r a pak podle čitatele p: nejdříve vypíšeme všechna čísla s výškou $r = 1$, pak s výškou $r = 2$, $r = 3$, $r = 4$, atd. Tímto způsobem sestavíme posloupnost, která obsahuje všechna racionální čísla:

$$\left\{\frac{0}{1}, \frac{-1}{1}, \frac{1}{1}, \frac{-2}{1}, \frac{-1}{2}, \frac{1}{2}, \frac{2}{1}, \frac{-3}{1}, \frac{-1}{3}, \frac{1}{3}, \frac{3}{1}, \frac{-4}{1}, \frac{-3}{2}, \frac{-2}{3}, \frac{-1}{4}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \frac{-5}{1}, \ldots, \frac{5}{1}, \ldots\right\}.$$

Definice 1.64. Nekonečné množiny, které mají stejnou mohutnost jako množina přirozených čísel $\mathbb{N}$, se nazývají **spočetné**.

Množiny konečné a spočetné se dohromady označují termínem **nejvýše spočetné**.

Množinu M, která má nekonečně mnoho prvků, ale neexistuje prosté zobrazení mezi množinou M a množinou přirozených čísel $\mathbb{N}$, nazýváme množinou **nespočetnou**.

Z definice plyne následující tvrzení:

Věta 1.65. Podmnožina spočetné množiny je nejvýše spočetná, tj. konečná nebo spočetná. Množina je nespočetná, pokud obsahuje nespočetnou podmnožinu.

Existuje nespočetná množina? Například reálná čísla nebo jenom interval reálných čísel tvoří nespočetnou množinu:

Věta 1.66. Interval reálných čísel $\langle 0, 1)$ je nespočetná množina.

Důkaz. Předpokládejme opak, tj. že interval $\langle 0, 1)$ je spočetná množina. Každé číslo z tohoto intervalu lze zapsat ve tvaru nekonečného desetinného rozvoje, který začíná nulou a po desetinné tečce pokračuje nekonečnou posloupností číslic $c_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Každá taková posloupnost určuje právě jedno reálné číslo z intervalu $\langle 0, 1)$. Toto vyjádření reálného čísla je jednoznačné s výjimkou čísel končících samými nulami a samými devítkami, které určují stejné číslo, například rozvoje $0.19999999999\ldots$, $0.20000000000\ldots$ určují stejné reálné číslo 0.2, proto rozvoje se samými devítkami můžeme vyloučit.

Předpokládejme tedy, že všechna reálná čísla z intervalu $\langle 0, 1)$ zapsané ve tvaru nekonečného desetinného rozvoje lze seřadit do posloupnosti:

$$\begin{aligned}
a_1 &= 0.a_{11}a_{12}a_{13}a_{14}a_{15}\ldots a_{1n}\ldots,\\
a_2 &= 0.a_{21}a_{22}a_{23}a_{24}a_{25}\ldots a_{2n}\ldots,\\
a_3 &= 0.a_{31}a_{32}a_{33}a_{34}a_{35}\ldots a_{3n}\ldots,\\
a_4 &= 0.a_{41}a_{42}a_{43}a_{44}a_{45}\ldots a_{4n}\ldots,\\
a_5 &= 0.a_{51}a_{52}a_{53}a_{54}a_{55}\ldots a_{4n}\ldots,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
a_n &= 0.a_{n1}a_{n2}a_{n3}a_{n4}a_{n5}\ldots a_{nn}\ldots,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.
\end{aligned}$$

Sestrojme nyní číslo $b = 0.b_1b_2b_3b_4 \dots b_n \dots$ takto: je-li číslice $a_{ii} = 1$, klademe $b_i = 2$, je-li $a_{ii} \neq 1$, klademe $b_i = 1$. Číslo b takto sestrojené je různé od všech čísel a_i (od a_1 se liší v první číslici za desetinnou tečkou, od a_2 se liší v druhé číslici za desetinnou tečkou, atd.). Protože číslo $b \in \langle 0, 1)$, mělo by být ve vypsaném seznamu, tzn. mělo by být některým z čísel a_i, ale není, což je spor. Proto interval $\langle 0, 1)$ a tudíž i množina $\mathbb{R}$ jsou nespočetné množiny. □

Důsledkem předchozí věty je skutečnosti, že každá množina obsahující neprázdný interval je nespočetná, nespočetná je i množina reálných čísel, množina komplexních čísel, atd.

1H. Algebraické struktury

Pokud nechceme akceptovat intuitivní definice jako matice je „tabulka čísel uspořádaných do řádků a sloupců“ a funkce je „předpis, který x přiřazuje y . . . “, pojem zobrazení nám umožňuje korektně zavést řadu dalších pojmů:

Reálná matice s m řádky a n sloupci je zobrazení $A\colon \{1, \dots, m\} \times \{1, \dots, n\} \to \mathbb{R}$.

Reálná funkce reálné proměnné je zobrazení $f\colon \mathbb{R} \to \mathbb{R}$.

Také základní pojem „operace“ je definován pomocí pojmu relace a zobrazení:

Definice 1.67. **Binární operací** na množině A nazveme zobrazení f

$$f : A \times A \to A\,, \qquad f \ : \ [a_1, a_2] \mapsto f(a_1, a_2) = a_3\,,$$

přičemž místo $f(a_1, a_2) = a_3$ nebo $[a_1, a_2, a_3] \in \mathcal{F}$ píšeme $a_1 * a_2 = a_3$.
Symbol $*$ lze nahradit jinými znaky např. $\star, \circ, \bullet, \dots$.
V obecnějším pojetí **n-ární operací** z $A_1 \times A_2 \times \cdots \times A_n$ do A_0 rozumíme zobrazení

$$f\colon A_1 \times A_2 \times \cdots \times A_n \to A_0.$$

Často $A_1 = A_2 = \cdots = A_n = A_0 = A$, potom mluvíme o n-ární operaci na množině A.

Poznámky 1.68. Operace může mít $n = 0, 1, 2, 3, \dots$ tzv. **argumentů**. Operaci s jedním argumentem nazýváme **unární**, například operace opačná hodnota $-r$ čísla r. Operace se dvěma argumenty se nazývá **binární**, například součet dvou čísel. Operace se třemi argumenty se nazývá **ternární**, například smíšený součin vektorů, viz Kapitola 3 Analytická geometrie. Přitom konstanty 0 a 1 nemají žádný argument, lze je považovat za **nulární** operaci.

Definice 1.69. **Algebraickou strukturou** rozumíme množinu A spolu s nějakými operacemi, které jsou na ní definované.

Poznámky 1.70. (Definice operace na množině A zajišťuje, že libovolné užití operace nevede nikdy k „vyběhnutí“ z množiny A, říkáme, že struktura je pro tyto operace uzavřená.

Vyšetřováním obecných vlastností algebraických struktur se zabývá část matematiky zvaná **algebra**. Základní strukturou studovanou v algebře je grupa, uveďme její definici:

Definice 1.71. Algebraická struktura s množinou G a binární operací $*$ se nazývá **grupou**, jestliže platí:

- **(G1)** Pro všechna $a, b, c \in G$ platí $(a * b) * c = a * (b * c)$.
- **(G2)** Existuje prvek $e \in G$, že pro každé $a \in G$ platí $a * e = e * a = e$.
- **(G3)** Pro každé $a \in G$ existuje $b \in G$, že platí $a * b = b * a = e$.

Poznámky 1.72.

(a) Vlastnost (G1) je asociativita operace, (G2) dává **existenci neutrálního prvku** a (G3) **existenci opačného prvku**

(b) Existenci neutrálního prvku – vlastnost (G2) – lze považovat za nulární operaci a existenci opačného prvku – (G3) – za unární operaci.

(c) Příkladem grupy je množina celých čísel $\mathbb{Z}$ s operací sčítání: neutrálním prvkem je prvek 0, každý prvek a ma inverzní $-a$. Podobně množiny racionálních $\mathbb{Q}$, reálných $\mathbb{R}$ i komplexních $\mathbb{C}$ čísel s operací sčítání jsou grupy. Protože sčítání čísel je komutativní, tyto grupy se nazývají komutativní.

(d) Také množina nenulových racionálních čísel $\mathbb{Q} \setminus \{0\}$, nenulových reálných čísel $\mathbb{R} \setminus \{0\}$, množina nenulových komplexních čísel $\mathbb{C} \setminus \{0\}$ s operací násobení jsou komutativní grupy. Neutrálním prvkem je číslo 1 a inverzním prvkem k číslu a je číslo inverzní $a^{-1} = 1/a$.

(e) Množina všech bijektivních zobrazení z M do M s operací skládání tvoří také grupu. Neutrálním prvkem je identické zobrazení I_M, inverzním prvkem je inverzní zobrazení. Tato grupa však není komutativní. V případě $M = \{1, 2, 3, \ldots, n\}$ dostáváme grupu **permutací** množiny M.

Důležitou algebraickou strukturou s dvěmi operacemi je těleso:

Definice 1.73. **Těleso** je algebraická struktura s množinou $\mathbb{T}$ s prvky x a dvěma operacemi sčítání $+$ a násobení $\cdot$, které splňují následující axiomy:

1. Množina $\mathbb{T}$ s operací součtu $+ : \mathbb{T} \times \mathbb{T} \to \mathbb{T}$ je **komutativní grupa**:

- Operace je **asociativní**: $\forall\, a, b, c \in \mathbb{T}$ platí $(a + b) + c = a + (b + c)$,
- Existuje neutrální prvek **nula** 0: $\forall\, a \in \mathbb{T}$ platí $a + 0 = 0 + a = a$,
- Pro každé $a \in \mathbb{T}$ existuje **opačný** prvek $-a$ splňující $a + (-a) = (-a) + a = 0$,
- Operace je **komutativní**: $\forall\, a, b \in \mathbb{T}$ platí $b + a = a + b$.

2. Množina $\mathbb{T}$ s operací násobení $\cdot : \mathbb{T} \times \mathbb{T} \to \mathbb{T}$ splňuje:

- Násobení je **asociativní**: $\forall\, a, b, c \in \mathbb{T}$ platí $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- Existuje neutrální prvek **jednotka** 1: $\forall\, a \in \mathbb{T}$ platí $a \cdot 1 = 1 \cdot a = a$.
- Pro každé $a \in \mathbb{T}$, $a \neq 0$ existuje **inverzní prvek** a^{-1} splňující $a \cdot a^{-1} = a^{-1} \cdot a = 1$.
- Operace *cdot* je **komutativní**: $\forall\, a, b \in \mathbb{T}$ platí $b \cdot a = a \cdot b$.

3. Obě operace jsou spojeny **distributivními zákony**:

- Pro každé $a, b, c \in \mathbb{T}$ platí $a \cdot (b + c) = a \cdot b + a \cdot c$.
- Pro každé $a, b, c \in \mathbb{T}$ platí $(a + b) \cdot c = a \cdot c + b \cdot c$.

Poznámky 1.74.

(a) Množina racionálních čísel $\mathbb{Q}$, reálných čísel $\mathbb{R}$ i komplexních čísel $\mathbb{C}$ jsou tělesa.

(b) Existují i konečná tělesa, například množina $\{0, 1, 2, 3, \ldots, p-1\}$, kde p je prvočíslo $p = 2, 3, 5, 7, 11, \ldots$ a operace jsou zbytkové třídy po dělení prvočíslem p: výsledek operace sčítání i násobení bereme jako zbytek po dělení prvočíslem p. Například pro $p = 5$ je to množina $\{0, 1, 2, 3, 4\}$ s operacemi $1 + 2 = 3$, $2 + 3 = 0$, $3 + 4 = 2$, $2 \cdot 3 = 1$, $3 \cdot 4 = 2$.

(c) V definici požadujeme, že násobení je komutativní. Množina kvaternionů $\mathbb{H}$ je tzv. nekomutativní těleso: splňuje všechny axiomy tělesa kromě komutativnosti násobení.

(d) Jde o typický postup matematické **abstrakce**: obecný popis a vlastnosti abstraktní algebraické struktury může být využit v jednotlivých strukturách. Například vlastnosti grupy lze uplatnit pro číselné množiny $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ s operací sčítání.

Na závěr uveďme velmi důležitou strukturu, která se nazývá **lineární prostor**.

Definice 1.75. Lineární prostor (také **vektorový prostor**) nad tělesem $\mathbb{T}$, je množina X prvků $\mathrm{x}, \mathrm{y}, \mathrm{z}, \ldots$ s operacemi součtu $+$ a skalárního násobku jestliže:

1. Množina X s binární operací součtu $+ : X \times X \to X$ tvoří **grupu**:
- Pro každé $\mathrm{x}, \mathrm{y}, \mathrm{z} \in X$ platí $(\mathrm{x} + \mathrm{y}) + \mathrm{z} = \mathrm{x} + (\mathrm{y} + \mathrm{z})$ – (asociativní zákon).
- Existuje prvek nula $0 \in X$ splňující: $\forall\, \mathrm{x} \in X$ platí $\mathrm{x} + 0 = 0 + \mathrm{x} = \mathrm{x}$.
- Ke každému $\mathrm{x} \in X$ existuje opačný prvek $(-\mathrm{x})$ takový, že $\mathrm{x} + (-\mathrm{x}) = (-\mathrm{x}) + \mathrm{x} = 0$.
- Operace sčítání $+$ je **komutativní**: tj. $\forall\, \mathrm{x}, \mathrm{y} \in X$ platí $\mathrm{y} + \mathrm{x} = \mathrm{x} + \mathrm{y}$.

2. Operace skalárního násobku $\mathbb{T} \times X \to X$ je:
- Asociativní: – Pro každé $\alpha, \beta \in \mathbb{T}$, $\mathrm{x} \in X$ platí $(\alpha, \beta)\mathrm{x} = \alpha(\beta \mathrm{x})$.
- Pro každé $\mathrm{x} \in X$ a jednotku 1 tělesa $\mathbb{T}$ platí: $1\mathrm{x} = \mathrm{x}$.

3. Obě operace jsou spojeny **distributivními zákony**:
- Pro každé $\alpha, \beta \in \mathbb{T}$ a každé $\mathrm{x} \in X$ platí $(\alpha + \beta)\mathrm{x} = \alpha\,\mathrm{x} + \beta\,\mathrm{x}$.
- Pro každé $\alpha \in \mathbb{T}$ a každé $\mathrm{x}, \mathrm{y} \in X$ platí $\alpha(\mathrm{x} + \mathrm{y}) = \alpha\,\mathrm{x} + \alpha\,\mathrm{y}$.

Poznámky 1.76.

(a) V lineárním prostoru je tělesem $\mathbb{T}$ obvykle množina reálných čísel $\mathbb{R}$, případně množina komplexních čísel $\mathbb{C}$.

(b) Těleso reálných i komplexních čísel jsou lineární prostory. Prvky lineárních prostorů jsou obvykle vektory (odtud častý název vektorový prostor), ale i matice stejného typu, reálné funkce nad stejným intervalem a pod.