1. Základy matematiky

1A. Výroková logika

Logika se v češtině běžně používá ve smyslu myšlenková cesta, která vede k určitým závěrům. Logika patří k základům matematiky. Jako vědní obor Matematická logika vznikla v 19. století. Jejím zakladatelem byl anglický matematik G. Boole (1815–1864). Boole prosadil algebraické pojetí logiky a zavedl logické spojky. K dalším tvůrcům booleovské logiky patřil J. Venn (1834–1923). Rozšířením této tzv. výrokové logiky je predikátová logika, která se zabývá dokazováním matematických tvrzení. Její vznik je spjat s německým matematikem G. Fregem (1848–1925). Frege zavedl v logice pojem kvantifikátoru. Jedním z nejvýznamnějších logiků všech dob byl brněnský rodák Kurt Gödel (1906–1978), jehož věta o úplnosti predikátové logiky prvního řádu a věty o neúplnosti axiomatických formálních systémů s aritmetikou výrazně ovlivnily vývoj matematiky.

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

Definice 1.1. **Výrok** je tvrzení, o němž má smysl říci, 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**.

Výrok je tedy oznamovací věta, i když nejsme schopni rozhodnout, zda je pravdivá. Tázací ani rozkazovací věta není výrok.

Příklad 1.2. Rozhodněte o pravdivosti následujících výroků:
(a) $A :=$ „Platí $\dfrac{2}{\sqrt{2}} = \sqrt{2}$.“ (b) $B :=$ „Číslo 51 je prvočíslo.“

Řešení: (a) Zřejmě $p(A) = 1$, neboť $\dfrac{2}{\sqrt{2}} = \dfrac{2\sqrt{2}}{\sqrt{2}\,\sqrt{2}} = \dfrac{2\sqrt{2}}{2} = \sqrt{2}$. (b) Zřejmě $p(B) = 0$, neboť $51 = 3 \cdot 17$.

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

Výrok se nazývá **elementární**, nebo též atomární, neobsahuje-li logické spojky. Například výroky A, B jsou atomární. 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 A', který má opačnou pravdivostní hodnotu, tj. A' je nepravdivý, pokud výrok A je pravdivý a A' je pravdivý pokud A je nepravdivý. Negace se často značí také **non** A nebo $\neg A$. Definici negace lze také zapsat tabulkou:

$p(A)$	$p(A')$
1	0
0	1

. (1.1)

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

(1.2)

V následující tabulce uvedeme název spojky, její označení, slovní vyjádření a odpovídající 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 aspoň jeden z A, B
implikace	$A \Rightarrow B$	jestliže A, pak B	z A plyne B
ekvivalence	$A \Leftrightarrow B$	A právě tehdy, když B	A a B jsou ekvivalentní

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

Speciálně 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. Implikace $B' \Rightarrow A'$ se nazývá **obměnou implikace** nebo **obměněnou implikací** a je ekvivalentní původní implikaci $A \Rightarrow B$. Pozor, implikace $B \Rightarrow A$ se nazývá **obrácená implikace**, ale **není ekvivalentní** implikaci $A \Rightarrow B$.

Pro úplnost uveďme ještě spojkou **alternativa** $\veebar$, která má význam „buď A, nebo B“ a je pravdivá pokud je pravdivý právě jeden z výroků A a B. Teoretický význam má **Shefferův symbol** $|$, který je pravdivý jenom, když oba výroky A a B jsou nepravdivé.

Poznámky: Všech možných logických spojek, které spojují dva výroky A, B je 16. Říkáme, že systém spojek je **úplný**, když stačí k definování všech 16-ti spojek, tj. pomocí závorek a spojek lze popsat libovolnou logickou situaci. Systém logických spojek $'$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ je úplný.

Lze dokázat, že k vytvoření úplného systému stačí vzít pouze dvě spojky: negaci a jednu ze spojek $\wedge, \vee, \Rightarrow$. Dokonce lze dokázat, že všechny logické spojky lze popsat pomocí jediné spojky: Shefferova symbolu.

Analogicky existují logické spojky spojující tři výroky A, B, C. Všeobecně je známa například spojka „**if** A **then** B **else** C“ používaná v programování.

Příklad: 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 $p\Big(\big((2 \cdot 3 = 6) \vee (3 \cdot 4 = 11)\big) \Rightarrow (2 < 1)\Big) = p\big((1 \vee 0) \Rightarrow 0\big) = p(1 \Rightarrow 0) = 0$. Složený výrok je tedy nepravdivý.

Výrokové formy, proměnné a kvantifikátory

Matematické objekty s jednoznačně stanoveným významem, např. 0, 1, π, $\sqrt{2}$ nazýváme **konstanty**. Objekty, které nemají jednoznačně stanovený význam, např. x, y, z, nazýváme **proměnné**.

Definice 1.4. **Výroková forma** je tvrzení obsahující proměnné, z něhož se po dosazení konstant za proměnné stane výrok. Výrokovou formu A s proměnnou x můžeme zapsat $A(x)$

Příklad: Tvrzení $A :=$ „$3x$ je sudé“, je výroková forma. Zvolíme-li $x = 1$, pak $p(A, x = 1) = 0$, zatímco pro $x = 2$ je $p(A, x = 2) = 1$. Při zápisu výrokové formy $A(x) :=$ „$3x$ je sudé“ lze psát $p(A(1)) = 0$, $p(A(2)) = 1$.

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.

Definice 1.5. V matematice se nejčastěji používají následující dva kvantifikátory:
1. **obecný kvantifikátor**, který se označuje $\forall$ a čte se **„pro každé“** a
2. **existenční kvantifikátor** $\exists$, který má význam **„existuje aspoň jeden“**.

Tyto kvantifikátory doplňují proměnnou a množinu, například „$\forall\, x \in X$ platí $A(x)$“ nebo „$\exists\, x \in X$, že platí $A(x)$“, kde X je množina a $A(x)$ výroková forma s proměnnou x.

Výrokové formy mohou mít více proměnných, které lze různě kvantifikovat, přičemž **záleží** na pořadí. Kvantifikací všech proměnných dostáváme výrok. Pokud je množina zřejmá z kontextu, lze ji vynechat.

Příklad 1.6. Zjistěte pravdivost následujících výroků:

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

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

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

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

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

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

Kvantifikátorů existuje nekonečně mnoho. Příkladem dalšího kvantifikátoru je kvantifikátor $\exists!$ s významem **existuje právě jeden**. Podobně existují kvantifikátory právě dva, právě tři, atd. Nejběžněji používané kvantifikátory využívají slovních spojení aspoň, právě a nejvýše.

Negace výroků s kvantifikátory

Při negaci výroku se kvantifikátor $\forall$ mění na $\exists$, kvantifikátor $\exists$ na $\forall$ **(množina se přitom nemění)** a následující výroková forma se neguje:

Věta 1.7. (**Negace výroků s kvantifikátory**) Buď $A(x)$ výroková forma s proměnnou $x \in X$, potom

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

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

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

Příklad: Negací výroku „Všichni studenti skupiny udělali zkoušku z Matematiky.“ dostaneme výrok „Existuje (alespoň jeden) student skupiny, který zkoušku z Matematiky neudělal.“

Podobně negací výroku se dvěma kvantifikátory: „Existuje (alespoň jeden) student skupiny, který udělal všechny zkoušky“ dostáváme výrok „Každý student skupiny alespoň jednu zkoušku neudělal“, přičemž vždy platí výrok a negace výroku neplatí, nebo obráceně.

Příklad 1.8. Negujte výroky A, B, C, D, E, F z předchozího příkladu!

Řešení:

(a) $A' :=$ „$\exists\, x \in \mathbb{R} \;:\; x^2 \leq 0$“ – (*platí*, $x = 0$)

(b) $B' :=$ „$\forall\, n \in \mathbb{Z} \;:\; n^2 \neq 2$“ – (*platí*)

(c) $C' :=$ „$\exists\, a, b \in \mathbb{R} \;:\; (a+b)^2 \neq a^2 + 2ab + b^2$“ (*neplatí*)

(d) $D' :=$ „$\forall\, e \in \mathbb{R}\; \exists x \in \mathbb{R} \;:\; e \cdot x \neq x$“ (*neplatí, např.* $e = 1$)

(e) $E' :=$ „$\exists\, x \in \mathbb{R}\; \forall\, q \in \mathbb{R} \;:\; x + q \neq 0$“ (*neplatí*); a změnou pořadí kvantifikátorů:

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

Tautologie

Důležitým problémem je také rovnost výroků, zda říkají totéž, uveďme příklad:

Příklad 1.9. 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 provedeme vhodné označení atomárních výroků. Symbolem A označme výrok „Petr přijde“, symbolem B označme výrok „Honza přijde“ a dále C označme výrok „Jirka přijde“. V provedeném označení mají výpovědi Šárky a Ivy tvar: $X := (A \wedge B) \Rightarrow C$ a $Y := (A \wedge C') \Rightarrow B'$. Aby Šárka a Iva říkaly totéž musí být $X \Leftrightarrow Y$ tautologie. Sestavíme tabulku pravdivostních hodnot.

A	B	C	$A \wedge B$	$A \wedge C'$	X	Y	$X \Leftrightarrow Y$
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 1.10. 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 nepravdivý bez ohledu na pravdivost jeho částí 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 $A \Leftrightarrow B$; tj. je to tautologie.

Příklad: 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. Další důležité tautologie uvádí následující věta:

Věta 1.11. Následující výrokové formy jsou tautologie:

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

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

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

Poznámky: Uvedené tautologie mají zásadní význam. Tvoří základ teorie důkazů.

Tvrzení a říká, že důkaz implikace je ekvivalentní důkazu její obměny.

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

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

Část c říká, že důkaz ekvivalentnosti dvou tvrzení dokážeme důkazem implikace a obrácené implikace.

Pro negace složených výroků platí následující pravidla:

Věta 1.12. Platí následující vztahy pro negace složených výroků:

(a) $(A')' = A$ — (zákon vyloučení třetího).

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

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

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

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

Některé vlastnosti operací mají svůj název:

Definice 1.13. Buďte dány symboly $\circ$, $*$. Pak následující zákony 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**.

I logické spojky splňují výše uvedené zákony:

Věta 1.14. 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

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.

Poznámka. 1.15. Při důkazu tvrzení v matematice můžeme postupovat třemi způsoby:

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 1.11, části (b) odtud plyne $A \Rightarrow B$. Zápis řetězce implikací je zvykem zapisovat v kratším tvaru

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

Nepřímý důkaz. Při nepřímém důkazu využijeme platnost tautologie (a) z Věty 1.11. Implikaci $B' \Rightarrow A'$ potom dokazujeme přímým důkazem.

Důkaz sporem. Vycházíme z předpokladu, že implikace neplatí, tj. $p(A \wedge B') = 1$ a konstruujeme řetězec implikací $A \wedge B' \Rightarrow A_1, A_1 \Rightarrow A_2, \ldots, A_n \Rightarrow S$, až dojdeme k výroku S, který logicky popírá původní předpoklad, nebo nějaký evidentně pravdivý výrok. Spor je situace, kdy nějaký výrok a jeho negace mají být současně pravdivé. Proto předpoklad, že implikace neplatí je nepravdivý, a proto implikace platí.

Uvedené důkazové postupy budeme nyní demonstrovat na příkladu.

Příklad 1.16. Dokažte přímo, nepřímo i sporem, že $\forall x \in \mathbb{N} : x \geq 2 \;\Rightarrow\; 6x + 3 > 13$.

Řešení:

(a) Přímý důkaz. Jednotlivé kroky důkazu vyžadují elementární znalosti o vlastnostech 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 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

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

(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

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

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.

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 $\mathbb{N} = \{1, 2, 3, \ldots\}$. Důkaz matematické indukce provedeme sporem.

Věta 1.17. (Matematická indukce) Buď $V(n)$ výroková forma proměnné $n \in \mathbb{N}$.

$$\Big(p\big(V(1)\big) = 1\Big) \wedge \Big(\forall k \in \mathbb{N} : p\big(V(k)\big) = 1 \implies p(V(k+1)) = 1\Big) \Rightarrow \forall n \in \mathbb{N} : p(V(n)) = 1. \qquad (1.3)$$

Důkaz. Tvrzení dokážeme sporem. Předpokládejme, že existuje číslo $k \in \mathbb{N}$, takové, že $p\big(V(k)\big) = 0$. Odtud plyne, že množina $M = \{k; p\big(V(k)\big) = 0\}$ je neprázdná a symbolem m označme její nejmenší prvek. Protože $p\big(V(1)\big) = 1$ je $m > 1$ a protože $m - 1 \notin M$ platí $p\big(V(m-1)\big) = 1$. Z indukčního předpokladu ale plyne $p\big(V(m)\big) = 1$, což je spor.

Poznámka. 1.18. Důkaz tvrzení „$\forall n \in \mathbb{N} : p\big(V(n)\big) = 1$“ pomocí matematické indukce se skládá ze tří částí:

(a) Dokážeme, že je $p\big(V(1)\big) = 1$.
(Pozn. Obecněji platí, že dokážeme platnost formule pro nejmenší přípustné n a nejčastěji je to právě číslo 1.)

(b) Dokážeme, že platí implikace $\forall k \in \mathbb{N} : p(V(k)) = 1 \Rightarrow p(V(k+1)) = 1$.

(c) Odvoláme se na Větu 1.17 o matematické indukci, podle které je nyní tvrzení $V(n)$ pravdivé pro každé přirozené číslo n.

Postup vysvětlíme na příkladu:

Příklad 1.19. Řekneme, že a dělí b a píšeme $a|b$, když existuje číslo c tak, že $b = ac$. Pomocí matematické indukce dokažte následující tvrzení „$\forall k \in \mathbb{N} : 7|6^{2k} - 8$“.

Důkaz. Tvrzení dokážeme ve třech krocích:

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

(b) Předpokládejme nyní, že tvrzení je pravdivé pro libovolné pevně zvolené číslo k a dokažme, že platí rovněž pro $k + 1$. Označme $V(k+1) = 7|6^{2(k+1)} - 8$. Je třeba dokázat, že

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

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

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

První člen součtu $(6^{2k} - 8) + 35 \cdot 6^{2k}$ je dělitelný číslem 7 podle indukčního předpokladu, dělitelnost druhého členu je zřejmá, neboť $7|35$. Protože jsou číslem 7 dělitelné oba členy je jím dělitelný i jejich součet a to bylo třeba dokázat.

(c) Podle Věty 1.17 o matematické indukci je tvrzení pravdivé pro každé přirozené číslo n.

Deduktivní úvahou nazýváme takovou úvahu, při níž z obecného tvrzení vyvozujeme zvláštní, individuální. Podstata dedukce je tedy v tom, že zvláštní případ zahrnuje pod obecný princip. Matematické úvahy jsou převážně deduktivní.

1C. Základní množinové pojmy

Vedle logiky základním kamenem matematiky je teorie množin. Za jejího zakladatele je považován německý matematik G. Cantor (1845–1918). Základní 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 modelovat i jiné matematické teorie a to tak, že se každému matematickému objektu přiřadí určitá množina, která ho reprezentuje. V tomto smyslu se 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) spočítat v tom smyslu, že je lze bijektivně zobrazit na množinu všech 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, Galileo Galilei. 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 bijekce. To by však znamenalo, že jsou uvedené systémy čísel stejně velké. Tento závěr se mu jevil naprosto absurdní. Popíral totiž jeden ze základních Eukleidových 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 B. Bolzano (1781–1848) 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 v teorii množin antinomie (rozpory mezi zákony), které si vynutily novou metodiku výstavby matematických teorií. Nejobvyklejší metodou se stala axiomatická výstavba.

Definice 1.20. (intuitivní)

(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) Negace výroku $a \in A$ píšeme $a \notin A$.

(f) Řekneme, že **množiny** A, B **jsou si rovny**, když mají tytéž prvky. Pak píšeme $A = B$.

(g) Řekneme, že množina A **je podmnožinou množiny** B, když každý prvek množiny A je prvkem množiny B. Pak 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**.

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

Někdy se místo $\subset$ píše symbol $\subseteq$, aby se zdůraznilo, že inkluze připouští i možnost rovnosti množin a zatímco symbol $A \subset B$ má význam tzv. vlastní inkluze, tj. každý prvek z A je i v B a existuje prvek z B, který není v A analogicky k nerovnostem $a \leq b$ a $a < b$.

Základní vlastnosti inkluze shrneme ve větě:

Věta 1.21. Pro libovolné množiny A, B, C platí:

(a) $\emptyset \subset A$.

(b) $A \subset A$.

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

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

Tvrzení a a b jsou zřejmá a c znamená tranzitivitu inkluze. Tvrzení d má zásadní význam pro důkazy množinových rovností. Chceme-li dokázat, že $A = B$, tak postupujeme tak, že dokážeme, že $A \subset B$ a $B \subset A$.

Odtud podle (d) již plyne, že $A = B$.

Příklad: 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.*)

Russelův paradox (1903). 1.22. Následující úvaha je typickým příkladem, který se objevil na počátku 20. století v souvislosti se třetí krizí matematiky. Buď A libovolná množina. Pak nastane právě jedna z možností buď $A \in A$ nebo $A \notin A$.

Všechny množiny rozdělíme do dvou skupin $X = \{A; A \in A\}$, $Y = \{B; B \notin B\}$. Je zřejmé, že žádná množina nemůže patřit do X i Y současně a že X, Y jsou také množiny. 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.

Definice 1.23. 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** $A \setminus B := \{x \ : \ x \in A \wedge x \notin B\}$.

(d) Pro množiny A, B **doplněk (komplement)** A **v** Z je rozdíl $Z \setminus A$.

Často se rozdíl množin místo $A \setminus B$ píše $A - B$.
Pokud je Z daná základní množina místo $Z \setminus A$ píšeme jenom A^c.

Věta 1.24. 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) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$

Definice 1.25. Množina všech podmnožin množiny A, tj. $\{X \ : \ X \subset A\}$ se označuje $\exp(A)$ nebo 2^A.

Příklad: Pro $A = \{a, b, c\}$ je $\exp(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.
Obecně, je-li množina A konečná a má n prvků, potom $\exp(A)$ má 2^n prvků.

Kartézský součin Jak v teorii množin zavést kartézský součin množin? Uspořádanou dvojici prvků a, b definujeme jako množinu $[a, b] := \{\{a\}, \{a, b\}\}$. Pro libovolné množiny A, B pak 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 tomto pojetí pro kartézský součin neplatí asociativní zákon: $A \times (B \times C) \neq (A \times B) \times C$, protože uvedené množiny mají jiné prvky. Například pro $A = \{a\}, B = \{b\}, C = \{c\}$ je $A \times (B \times C) = \{[a, [b, c]]\}$ a $(A \times B) \times C = \{[[a, b], c]\}$.

Proto pro praxi zavedeme dohodu, že vnitřní závorky odbouráme. Pak můžeme psát $A \times B \times C = \{[a, b, c]\}$ a asociativní zákon bude platit i pro kartézský součin. Pojem uspořádané dvojice, trojice, atd. a kartézského součinu množin budeme užívat intuitivně bez vnitřních závorek:

Definice 1.26.

(a) **Uspořádaná dvojice** prvků a, b je dvojice prvků, kdy záleží na pořadí, zapisujeme $[a, b]$, tj. $[a, b]$ 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 $[a, b]$, kde $a \in A$ a $b \in B$:

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

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

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

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

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

V tomto pojetí už kartézský součin je asociativní. Kartézský součin však **není komutativní,** $A \times B \neq B \times A$.

1D. Základní číselné množiny

Za základní číselné množiny považujeme čísla přirozená $\mathbb{N}$, čísla celá $\mathbb{Z}$, čísla racionální $\mathbb{Q}$, čísla reálná $\mathbb{R}$ a čísla komplexní $\mathbb{C}$, která lze seřadit pomocí inkluze $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Přirozená čísla Vycházíme z množiny přirozených čísel. Formální matematická definice přirozených čísel je založena na tzv. Peanových axiomech:

(a) Existuje číslo 1.

(b) Každé přirozené číslo a má následníka, označeného jako $S(a)$.

(c) Neexistuje přirozené číslo, jehož následníkem by byla 0.

(d) Různá přirozená čísla mají různé následníky: pokud $a \neq b$, pak $S(a) \neq S(b)$.

(e) Pokud nějakou vlastnost splňuje jak číslo 0, tak i každé číslo, které je následníkem nějakého čísla, které tuto vlastnost splňuje, pak tuto vlastnost splňují všechna přirozená čísla. (Tento axiom zajišťuje platnost důkazů technikou matematické indukce.)

Pojem množiny přirozených čísel však není jednotný, jsou určité důvody přidat nulu k přirozeným číslům, obvykle se však nula za přirozené číslo nepovažuje.

Definice 1.27. Nekonečnou **množinu přirozených čísel** označujeme $\mathbb{N} := \{1, 2, 3, 4, 5, 6, 7, \dots\}$, její prvky označujeme obvykle písmeny m, n, i, j, k, lze užít i jiná písmena.

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

Operace sčítání $m + n$ i násobení $m \cdot n$ (zkráceně $m\,n$) je definována pro každé dvě přirozená čísla m, n.

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

Operace dělení $m : n$ je definována, jen pokud n **„dělí“** m, tj. existuje $k \in \mathbb{N}$, že $m = nk$.

Někdy se k přirozeným číslům přidává i nula, pak píšeme $\mathbb{N}_0 := \{0\} \cup \mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Celá čísla Abychom mohli čísla odečítat bez omezení, přidáváme záporná celá čísla a nulu:

Definice 1.28. **Množinu celých čísel** $\mathbb{Z}$ dostaneme přidáním nuly a celých záporných čísel:

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

její prvky opět označujeme obvykle písmeny m, n, i, j, k. Množina $\mathbb{Z}$ je také uspořádaná.

Operace sčítání $m + n$, násobení mn i odčítání $m - n$ jsou definována všechny dvojice celých čísel.

Operace dělení $m : n$ je definována jen pro $n \neq 0$ a pokud n **„dělí“** m, tj. existuje $k \in \mathbb{N}$, že $m = nk$.

Racionální čísla Abychom odstranili omezení na dělení, přidáme zlomky. Dostáváme tak racionální čísla:

Definice 1.29. **Množinu racionálních čísel** označujeme $\mathbb{Q}$. Je to vlastně množina všech zlomků, s nenulovým jmenovatelem. Pro jednoznačnost vyjádření požadujeme, aby ve jmenovateli zlomku m/n bylo přirozené číslo $n > 0$ a aby čísla m a 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 také uspořádaná.

Operace sčítání $x + y$, odčítání $x - y$ a násobení xy jsou definované pro každé dvě celá čísla x, y.

Operace dělení $x : y$ je definována, pokud $y \neq 0$.

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 „pravidel“:

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

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

Připomeňme „správná“ pravidla:

Věta 1.30. Pro racionální reálná i komplexní čísla a, b, c, d platí následující pravidla:

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

$$\frac{\frac{a}{b}}{\frac{c}{d}} \equiv \frac{a}{b}:\frac{c}{d}=\frac{a}{b}\cdot\frac{d}{c}=\frac{ad}{bc} \qquad \text{pro } b\neq 0 \text{ a } c\neq 0 \text{ a } d\neq 0.$$

Reálná čísla Odmocnina z většiny přirozených čísel $2, 3, 5, 6, 7, \ldots$ není číslo přirozené, ani racionální, leží však na číselné ose mezi racionálními čísly. Množinu reálných čísel tak dostaneme z racionálních čísel „vyplněním“ děr mezi racionálními čísly pomocí tzv. iracionálních čísel, které nelze vyjádřit zlomkem $\frac{m}{n}$, kde $m \in \mathbb{Z}$, $n \in \mathbb{N}$. Jsou to například odmocniny $\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots$, a také čísla π, e a další.

Reálná čísla vycházejí z geometrické představy bodů na přímce. Matematická definice zavadí reálná čísla pomocí tzv. Dedekindových řezů. Uveďme hlavní myšlenku. Řezem nazveme množinu racionálních čísel $\mathbb{Q}$ „rozřezanou“ na podmnožinu A a její doplněk $\mathbb{Q}\setminus A$ tak, že pro každé $a \in A$ a $b \in \mathbb{Q}\setminus A$ platí $a < b$. Množina A je tak vždy interval racionálních čísel od $-\infty$. Všechny řezy lze rozdělit do tří druhů:

(a) A má maximální prvek $q \in \mathbb{Q}$ — tj. $A = (-\infty, q\rangle \cap \mathbb{Q}$,

(b) $\mathbb{Q}\setminus A$ má minimální prvek $q \in \mathbb{Q}$ — potom $A = (-\infty, q) \cap \mathbb{Q}$,

(c) A nemá maximální prvek ani $\mathbb{Q}\setminus A$ nemá minimální prvek.

Řezy prvního druhu ztotožníme s racionálním číslem q, které je maximem A. Řezy druhého druhu nebudeme uvažovat, protože by určovaly stejné racionální číslo q. Řez, kde A nemá největší prvek, ani $\mathbb{Q}\setminus A$ nemá nejmenší prvek, definuje nové tzv. iracionální číslo r. Například řez $A := (-\infty, 0) \cup \{q \in \mathbb{Q} \ : \ q^2 \leq 2\}$ tak definuje tzv. iracionální číslo $\sqrt{2}$. Řezy prvního a třetího druhu jsou uspořádané podle inkluze, což dává uspořádání odpovídajících reálných čísel.

Výjimečné řezy, kde $A = \emptyset$ a $A = \mathbb{Q}$ nepovažujeme za reálná čísla, první odpovídá symbolu $-\infty$, druhý symbolu ∞. Dále nutno pomocí řezů definovat operace sčítání, odčítání, násobení i dělení reálných čísel.

Definice 1.31. **Množinu reálných čísel** označujeme symbolem $\mathbb{R}$, jako u racionálních čísel její prvky obvykle označujeme písmeny $x, y, z, p, q, r, a, b, c, d, \ldots$

Pro $-\infty < a < b < \infty$ definujeme otevřené, uzavřené intervaly

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

a polouzavřené (polootevřené) intervaly $(a, b\rangle := \{x \in \mathbb{R} : a < x \leq b\}$ a $\langle a, b) := \{x \in \mathbb{R} : a \leq x < b\}$. V případě „otevřeného“ konce připouštíme $a = -\infty$ nebo $b = \infty$.

Podmnožiny se označují $\mathbb{R}^+ := (0, \infty)$ 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 $-\infty, \infty$ 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 xy a dělení $x : y$ jsou definovány pro všechny dvojice reálných čísel, jen při dělení $y \neq 0$.

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

Maximum, supremum, minimum a infimum

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

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

Otevřený interval $(0, 2)$ tak nemá maximum, protože pravá mez 2, kandidát na maximum, už není v M a nemůže být proto maximum. Abychom tuto nepříjemnost odstranili, zavedeme pojem supremum, které je rovno maximu, v případě, že maximum existuje. Je to nejmenší „horní závora“, tj. 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: je to největší „dolní závora“, tj. číslo menší nebo rovno než všechna čísla množiny M.

Definice 1.32. Buď M neprázdná omezená podmnožina množiny reálných čísel $\mathbb{R}$. Potom řekneme:

(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, píšeme $s = \sup M$.
(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 horní závora, píšeme $i = \inf M$.
(e) Pokud množina M není omezená (ohraničená) shora, položíme $\sup(M) = \infty$.
(f) Pokud množina M není omezená (ohraničená) zdola, položíme $\inf(M) = -\infty$.
(g) V případě prázdné množiny $M = \emptyset$ položíme $\sup(M) = -\infty$ a $\inf(M) = \infty$.

Definice suprema a infima je složitější než definice maxima a minima, pojmy supremum a infimum mají však lepší vlastnosti: vždy existují.

Věta 1.33. Uvažujme libovolné podmnožiny $M, M_1, M_2, \ldots$ množiny reálných čísel.

(a) Každá podmnožina M množiny reálných čísel $\mathbb{R}$ má svoje supremum a infimum.
(b) Pro každou neprázdnou M platí $-\infty \leq \inf(M) \leq \sup(M) \leq \infty$.
(c) Platí $\sup(M_1 \cup M_2) = \max(\sup(M_1), \sup(M_2))$.
(d) Platí $\inf(M_1 \cup M_2) = \min(\inf(M_1), \inf(M_2))$.

Komplexní čísla Podnětem pro rozšíření reálných čísel byla skutečnost, že kvadratické rovnice $a\,x^2 + b\,x + c = 0$ s reálnými koeficienty v případě záporného diskriminantu $D := b^2 - 4ac < 0$ nemají v oboru reálných čísel řešení. Rozšíření spočívá v tom, že k reálné části přidáme tzv. imaginární část. Komplexní čísla tak nelze znázornit na reálné přímce, ale v tzv. komplexní rovině.

Definice 1.34. Komplexní číslo $z = [x, y]$ lze reprezentovat uspořádanou dvojici reálných čísel x, y, kde x se nazývá **reálná část** a y je **imaginární část**. Zapisujeme ho ve tvaru $z = x + \mathrm{i}y$, kde i označuje jednotku imaginární části často nepřesně psané $\mathrm{i} = \sqrt{-1}$. Množinu komplexních čísel $\mathbb{C}$ lze ztotožnit s rovinou $\mathbb{R}^2$.
Komplexní číslo a jeho složky obvykle zapisujeme písmeny $z \equiv [x, y] \equiv x + \mathrm{i}y$, také $w \equiv [u, v] \equiv u + \mathrm{i}v$.
Komplexní čísla nelze „rozumně“ uspořádat, množina komplexních čísel $\mathbb{C}$ netvoří uspořádanou množinu.
Operace sčítání a odčítání jsou definovány po složkách: pro $z_i \equiv [x_i, y_i] \equiv x_i + \mathrm{i}y_i$ 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 vlastnosti $\mathrm{i} \cdot 1 = 1 \cdot \mathrm{i} = \mathrm{i}$ a $\mathrm{i} \cdot \mathrm{i} = -1$ lze odvodit pravidlo pro násobení:

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

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

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

Absolutní hodnota „Vzdálenost“ čísla od nuly nazýváme absolutní hodnotou.

Definice 1.35. Pro nezáporné číslo (celé, racionální i reálné) číslo 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 $z = [x, y]$ nutno doplnit na $|z| = \sqrt{x^2 + y^2}$, také platí $|z| = \sqrt{z \cdot \overline{z}}$.

Věta 1.36. Operace sčítání a násobení na reálných i komplexních číslech jsou asociativní, komutativní a jsou spojeny distributivním zákonem. Pro absolutní hodnotu platí $|xy| = |x| \cdot |y|$ a $|x + y| \leq |x| + |y|$.

1E. Relace

Definice 1.37. Buďte dvě neprázdné množiny A a B, které nemusí být různé. **Binární relací $\mathcal{R}$ mezi množinami** A, B nazveme libovolnou podmnožinou $\mathcal{R}$ 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 $\mathcal{R}$: $\mathcal{D}(\mathcal{R}) := \{a \in A \ \exists\, b \in B : [a,b] \in \mathcal{R}\}$

Obor hodnot relace $\mathcal{R}$: $\mathcal{H}(\mathcal{R}) := \{b \in B \ \exists\, a \in A : [a,b] \in \mathcal{R}\}$.

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.

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

Definice 1.38. Buď $\mathcal{R}$ binární relace na množině A. Nazveme ji

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

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

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

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

(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 $x < y$. Tato relace je reflexivní, antisymetrická a tranzitivní. Neostrá nerovnost „$<$“ je tranzitivní, není symetrická ani reflexivní.
Příklad: Mezi konečnými množinami $\mathbb{N}$ 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 1.39. 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 1.40. **n-ární relací** rozumíme libovolnou podmnožinu kartézského součinu $A_1 \times A_2 \times \cdots A_n$, kde $A_1, A_2, \ldots, A_n$ jsou neprázdné ne nutně různé množiny.

1F. Zobrazení

Zobrazení je základním pojmem v matematice. 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 následovně:

Definice 1.41. **Zobrazením** z množiny A do množiny B nazveme relaci $\mathcal{F}$, která splňuje

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

Místo $\mathcal{F} \subset A \times B$ užíváme zápisu $f\colon A \to B$ a místo $[a,b] \in \mathcal{F}$ píšeme $b = f(a)$, nebo $a \mapsto f(a)$.
Prvek a se přitom 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 1.42. 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 $\mathcal{H}(f)$.

Definice 1.43. (**Skládání zobrazení**) Buďte A, B, C množiny a $f : A \to B$ a $g : B \to C$ zobrazení. Pokud $\mathcal{H}(f) \subset \mathcal{D}(g)$ existuje složené zobrazení $g \circ f : A \to C$ definované vztahem $(g \circ f)(x) = g(f(x)),\ \forall\, x \in \mathcal{D}(f)$.

Důležitými vlastnostmi zobrazení jsou následující pojmy:

Definice 1.44. 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.

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

(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 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 1.45. 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.

$$\forall\, a \in A\ \ \forall\, b \in B\ :\ f^{-1}(b) = a\ \Longleftrightarrow f(a) = b\,.$$

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

Poznámky:

(a) Skládání zobrazení (pokud je definované) je asociativní: $(f \circ g) \circ h = f \circ (g \circ h)$, není však komutativní, $g \circ f$ 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 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 $f = \mathrm{I}_A \circ f = f \circ \mathrm{I}_B$.

(d) Inverzní zobrazení můžeme definovat vztahem $f^{-1} \circ f = \mathrm{I}_B$ a $f \circ f_{-1} = \mathrm{I}_B$.

Další úvahy budeme provádět pro následující **číselné množiny**: množinu **přirozených čísel** $\mathbb{N}$, množinu **celých čísel** $\mathbb{Z}$, množinu **racionálních čísel** $\mathbb{Q}$ a množinu **reálných čísel** $\mathbb{R}$.

1G. Mohutnost množin

Která ze dvou množin má víc prvků? V případě konečných množin stačí porovnat počty prvků obou množin. V případě nekonečných množin se množiny porovnávají pomocí bijektivního zobrazení:

Příklad: V případě bijekce každému prvku množiny A odpovídá právě jeden prvek množiny B; jsou-li množiny A a B konečné, mají nutně stejný počet prvků; jsou-li nekonečné a existuje-li mezi nimi bijekce, můžeme také říci, že mají „stejně“ prvků, přesněji říkáme, že mají stejnou **mohutnost**.

Povšimněme si některých množin, které mají stejnou mohutnost jako množina přirozených čísel $\mathbb{N}$, tedy jejich prvky lze přirozenými čísly oindexovat. 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 $a \mapsto 2a$.

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

Překvapivé však je, že stejnou mohutnost má i množina všech racionálních čísel $\mathbb{Q}$, což lze dokázat následovně: racionální číslo 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 konkrétní výškou je konečný, jejich oindexování definujeme tak, že nejdříve vypíšeme všechna čísla s výškou $r = 1$, pak s výškou $r = 2$, $r = 3$, $r = 4$, atd. Tímto způsobem dostaneme posloupnost, která obsahuje všechna racionální čísla:

$$\left\{\frac{0}{1},\ \frac{-1}{1}, \frac{1}{1},\ \frac{-2}{1}, \frac{-1}{2}, \frac{1}{2}, \frac{2}{1}\ \frac{-3}{1}, \frac{-1}{3}, \frac{1}{3}, \frac{3}{1}\ \frac{-4}{1}, \frac{-3}{2}, \frac{-2}{3}, \frac{-1}{4}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1},\ \frac{-5}{1}, \dots \frac{5}{1},\ \frac{-6}{1}, \dots\right\}$$

Definice 1.46. Nekonečné množiny se stejnou mohutností jako $\mathbb{N}$ se nazývají **spočetné**. Množiny konečné a spočetné se dohromady označují termínem **nejvýše spočetné**.
Množiny, které mají nekonečně mnoho prvků, ale bijekce s přirozenými čísly neexistuje nazýváme množiny **nespočetné**.

Příklad: Dokažme nyní, že množina všech reálných čísel $\mathbb{R}$ není spočetná, tj. je nespočetná. Stačí ovšem, když dokážeme, že je nespočetná nějaká část množiny $\mathbb{R}$, tedy např. interval $[0, 1)$. Předpokládejme opak, tzn. že všechna čísla z intervalu $[0, 1)$ lze nějak uspořádat do nekonečné posloupnosti

$$\begin{aligned}
a_1 &= 0, a_{11}a_{12}a_{13}a_{14}\dots a_{1n}\dots\\
a_2 &= 0, a_{21}a_{22}a_{23}a_{24}\dots a_{2n}\dots\\
a_3 &= 0, a_{31}a_{32}a_{33}a_{34}\dots a_{3n}\dots\\
a_4 &= 0, a_{41}a_{42}a_{43}a_{44}\dots a_{4n}\dots\\
&\dots\\
a_n &= 0, a_{n1}a_{n2}a_{n3}a_{n4}\dots a_{nn}\dots\\
&\dots
\end{aligned}$$

kde $a_{ik} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ je k-tá číslice v desetinném vyjádření čísla a_i.

Sestrojme nyní číslo $b = 0, b_1b_2b_3b_4\dots b_n\dots$ takto: je-li $a_{ii} = 1$, 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 čárkou, od a_2 se liší v druhé číslici za desetinnou čárkou, atd.). Protože ale $b \in [0, 1)$, mělo by být ve vypsaném seznamu, tzn. mělo by být některým z čísel a_i, což je spor. Interval $[0, 1)$ a tudíž i množina $\mathbb{R}$ jsou nespočetné množiny.

1H. Algebraické struktury

Pojem zobrazení nám umožňuje korektně (pokud nechceme akceptovat intuitivní definice jako matice je „tabulka čísel uspořádaných do řádků a sloupců“ a funkce je „předpis“) 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 1.47. **Binární operací** na množině A nazveme zobrazení f z $A\times A$ do A

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

přičemž místo $f(a_1,a_2)=a$ nebo $[a_1,a_2,a]\in\mathcal{F}$ píšeme $a_1 * a_2 = a$ a symbol $*$ lze nahradit $\star,\circ,\bullet,\dots$.

V obecnějším pojetí **n-ární operací** z $A_1\times A_2\times\cdots\times A_N$ do A rozumíme zobrazení

$$f\colon A_1\times A_2\times\cdots\times A_n\to A_{n+1}.$$

Často $A_1=A_2=\cdots=A_n=A_{n+1}$, potom mluvíme o n-ární operaci na množině A.

Poznámky: Operace může mít $n=1,2,3,\dots$ tzv. argumentů. Pro $n=1$ příkladem **1-ární** operace zvané **unární** je opačná hodnota $-r$ reálného čísla r. Pro $n=2$ se operace nazývá **binární**, příkladem je součet dvou čísel. Pro $n=3$ se 3-ární operací nazývá **ternární**, atd. Také konstanty, například 0 a 1 lze považovat za $n=0$ **nulární** operaci.

Definice 1.48. **Algebraickou strukturou** rozumíme množinu A spolu s nějakými operacemi na ní.

Poznámky: Definice operace na množině A zajišťuje, že neomezené užití operace nevede nikdy k „vyběhnutí“ z množiny A, říkáme, že struktura je 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 1.49. Algebraická struktura s množinou G a binární operací $*$ se nazývá **grupou**, jestliže platí:

(G1) Pro všechna $a,b,c\in G$ platí $(a*b)*c=a*(b*c)$ (**asociativita**)

(G2) Existuje prvek $e\in G$, že pro každé $a\in G$ platí $a*e=e*a=e$ (**existence neutrálního prvku**)

(G3) Pro každé $a\in G$ existuje $b\in G$, že platí $a*b=b*a$ (**existence opačného prvku**)

Poznámky:

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

(b) Příkladem grupy je množina celých čísel $\mathbb{Z}$ s operací sčítání: neutrálním prvkem je prvek 0, prvku inverzním k prvku a je $-a$. Podobně množiny racionálních $\mathbb{Q}$, reálných $\mathbb{R}$ i komplexních $\mathbb{C}$ čísel s operací sčítání jsou grupy. Protože sčítání čísel je komutativní, grupy jsou komutativní.

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

(d) 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 komutativní není.

Jde o typický postup matematické **abstrakce**: abstraktní popis algebraických struktur pak může být využit v jednotlivých problémech. Například vlastnosti grupy lze uplatnit pro číselné množiny $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ s operací sčítání. Důležité jsou i struktury s dvěma operacemi jakou je okruh, těleso.