ČÍSELNÉ OBORY

Jaroslav Beránek

0. Úvod

Tento text je určen pro studenty pedagogického asistentství matematiky pro základní školy. Jedná se o přehledný studijní materiál doplňující základní studijní literaturu v disciplíně Algebra 3. Pro studium textu je nutno předpokládat znalosti základů algebry (množinové operace a jejich vlastnosti, binární relace a jejich vlastnosti, relace uspořádání a uspořádané množiny, relace ekvivalence a rozklad množiny, binární algebraické operace a jejich vlastnosti, algebraické struktury a jejich homomorfismy). Standardní je rovněž označení základních číselných množin:
$\boldsymbol{N}$ – množina všech přirozených čísel (samozřejmě včetně čísla nula)
$\boldsymbol{Z}$ – množina všech celých čísel
$\boldsymbol{Q}$ – množina všech racionálních čísel
$\boldsymbol{R}$ – množina všech reálných čísel
$\boldsymbol{C}$ – množina všech komplexních čísel.
U množin $\boldsymbol{Z, Q, R}$ budeme užívat i označení $\boldsymbol{Z^+, Q^+, R^+}$ a $\boldsymbol{Z^-, Q^-, R^-}$, označující podmnožinu všech kladných, resp. záporných čísel daného číselného oboru. Bude-li do této podmnožiny zařazena i nula, doplníme označení indexem nula, např. $\boldsymbol{Z_0^+, Q_0^-}$.

1. Přirozená čísla

Jednou ze základních charakteristik množiny všech přirozených čísel je to, že každé přirozené číslo má svého bezprostředního následovníka (pro každé $n \in \boldsymbol{N}$ je to číslo $n + 1$). Tento „fakt“ znají už žáci na 1. stupni ZŠ a je často didakticky využíván při výuce. Existence následovníka využijeme při teoretickém zavedení množiny přirozených čísel. Nejprve axiomaticky definujeme tzv. Peanovu množinu a potom ukážeme, že tato množina je univerzálním modelem množiny všech přirozených čísel.

Axiomy Peanovy množiny P :

(A1) Ke každému prvku x množiny P existuje jeho následovník, který budeme označovat $x^{|}$.
(A2) v množině P existuje prvek $e \in P$, který není následovníkem žádného prvku množiny P.
(A3) Různé prvky mají různé následovníky.
(A4) *Axiom úplné indukce*. Nechť $M \subseteq P$. Jestliže platí:
a) $e \in M$,
b) $(\forall\, x \in P)\ x \in M \Rightarrow x^{|} \in M$,
pak $M = P$.

Věta 1.1. Nechť $x \in P$, pak platí:
(1) $x \neq x^{|}$,
(2) $x \neq e \Rightarrow (\exists\, u \in P)\ x = u^{|}$.

Část (1) předchozí věty říká, že každý prvek je různý od svého následovníka. Ze druhé části pak plyne, že každý prvek x Peanovy množiny s výjimkou prvku e je následovníkem nějakého prvku $u \in P$. Tento prvek u budeme nazývat předchůdce prvku x a značit ${}^{/}x$.

Věta 1.2. Peanova množina je nekonečná množina.

Definice 1.3: Nechť $a \in P$ je libovolný prvek. Nechť množina $U(a) \subseteq P$ je pro každý prvek $a \in P$ definována takto:

(1) $a \in U(a)$,

(2) $x \in U(a) \Rightarrow {}^{/}x \in U(a)$ (pokud ${}^{/}x$ existuje).

Pak množinu $U(a)$ budeme nazývat úsek Peanovy množiny příslušný k prvku a .

Poznámka 1.4. Je zřejmé, že pro každé $a \in P$ je příslušný úsek $U(a)$ konečná množina.

Poznámka 1.5. Z předchozího plyne, že Peanovu množinu můžeme považovat za teoretický model množiny přirozených čísel. V tomto případě prvek e je roven číslu 1, následovník $x^{/}$ je roven číslu $x + 1$ a modely úseků příslušných ke každému přirozenému číslu chápanému jako prvek množiny P si lze představit takto: $U(1) = \{1\}$, $U(2) = \{1, 2\}$, $U(3) = \{1, 2, 3\}$, $U(4) = \{1, 2, 3, 4\}$ atd. Je zřejmé, že počet prvků každého úseku je určen přirozeným číslem, jemuž daný úsek přísluší. Proto i v dalším textu je možné představit si porovnávání prvků Peanovy množiny (relaci uspořádání v množině P) i operace sčítání a násobení v množině P pomocí množiny přirozených čísel. I když teoretický postup je opačný (z obecné teorie v množině P plynou speciální vlastnosti v množině přirozených čísel), jako model množiny P jsou přirozená čísla velmi vhodná.

Relace uspořádání v množině *P*

Definice 1.6: Nechť $a, b \in P$. Pak platí: $a \leq b \Leftrightarrow a \in U(b)$.

Poznámka 1.7. Je zřejmé, že $\leq$ z definice 1.6. je reflexivní, antisymetrická a tranzitivní, jedná se tedy skutečně o uspořádání v množině P. Pro každé dva různé prvky a, b množiny P vždy platí právě jeden ze vztahů $a \in U(b)$, $b \in U(a)$, proto je uspořádání $\leq$ lineární. Hasseovským diagramem uspořádané množiny $(P, \leq)$ je řetězec s nejmenším prvkem e. Dále poznamenejme, že zápis $a < b$ označuje tzv. ostré uspořádání , tedy $a \leq b$ a současně $a \neq b$.

Věta 1.8. Nechť $a, b \in P$. Pak platí:

(1) $(\forall\, a \in P)\ a < a^{/}$**;**

(2) Mezi prvky $a, a^{/}$ neexistuje žádný prvek x množiny P s vlastností $a < x < a^{/}$);

(3) Množina $(P, \leq)$ je dobře uspořádaná množina.

Operace sčítání v množině *P*

Věta 1.9. Na množině P existuje právě jedna operace + taková, že pro každou dvojici x, y prvků množiny P platí:

(1) $x + e = x^{/}$ **,**

(2) $x + y^{/} = (x + y)^{/}$ **.**

Definice 1.10. Operace + z předchozí věty se nazývá operace sčítání v množině P .

Věta 1.11. Operace + je v množině P asociativní a komutativní.

Věta 1.12. V grupoidu $(P, +)$ platí zákony o odečítání, tj. pro každé tři prvky x, y, z množiny P platí implikace $x + y = x + z \Rightarrow y = z$.

Věta 1.13. Nechť $x, y \in P$. Pak nastane právě jeden z následujících tří případů:
(1) $x = y$,
(2) existuje $p \in P$ s vlastností $x = y + p$,
(3) existuje $q \in P$ s vlastností $y = x + q$.

Operace sčítání je spojena s relací uspořádání řadou vztahů. Některé jsou uvedeny v následující větě.

Věta 1.14. Nechť $x, y, z, u, v \in P$. Pak platí:
(1) $x < y \Leftrightarrow x + z < y + z$,
(2) $x \leq y \Leftrightarrow x + z \leq y + z$,
(3) $x \leq y, u \leq v \Rightarrow x + u \leq y + v$,
(4) $x < y \Rightarrow x^{|} \leq y$.

Operace násobení v množině *P*

Věta 1.15. Na množině P existuje právě jedna operace $\cdot$ taková, že pro každou dvojici x, y prvků množiny P platí:
(1) $x \cdot e = x$,
(2) $x \cdot y^{|} = x \cdot y + x$.

Definice 1.16. Operace $\cdot$ z předchozí věty se nazývá operace násobení v množině P.

Poznámka 1.17. Pokud v zápise početních operací v množině P nepoužijeme závorky, má operace násobení přednost před operací sčítání. Rovněž se v zápisech velmi často vynechává označení $\cdot$ operace násobením tj. místo $x \cdot y$ píšeme jenom xy.

Věta 1.18. Operace $\cdot$ je v množině P asociativní, komutativní, má neutrální prvek (prvek e) a s operací sčítání je svázána distributivním zákonem:

$$x, y, z \in P: x \cdot (y + z) = x \cdot y + x \cdot z .$$

Operace násobení je spojena s relací uspořádání řadou vztahů. Některé jsou uvedeny v následující větě (zajímavá je analogie s obdobnými vztahy pro sčítání). Poznamenejme ještě, že tvrzení (3) následující věty říká, že v grupoidu $(P, \cdot)$ platí zákony o krácení.

Věta 1.19. Nechť $x, y, z, u, v \in P$. Pak platí:
(1) $x < y \Leftrightarrow x \cdot z < y \cdot z$,
(2) $x \leq y \Leftrightarrow x \cdot z \leq y \cdot z$,
(3) $x \cdot z = y \cdot z \Rightarrow x = y$
(4) $x \leq y, u \leq v \Rightarrow x \cdot u \leq y \cdot v$.

Věta 1.20. Algebraická struktura $(P, +, \cdot)$ je komutativní polookruh s jedničkou.

Poznámka 1.21. Z definice množiny P a popsaných vlastností relace uspořádání a operací sčítání a násobení v této množině vyplývá, že polookruh všech přirozených čísel $(\boldsymbol{N}, +, \cdot)$ je jedním z možných modelů polookruhu $(P, +, \cdot)$. Roli prvku e hraje číslo *1*, následovníkem čísla x je číslo $x + 1$, úsek množiny $\boldsymbol{N}$ příslušný číslu n obsahuje všechna přirozená čísla od čísla 1 po číslo $n - 1$ atd.

Poznámka 1.22. Jako problémová se jeví otázka, kolik modelů polookruhu $(P, +, \cdot)$ existuje, tzn. zda jsou přirozená čísla určena jednoznačně, resp. zda vůbec nějaký model množiny P existuje. Existenci modelu množiny P a tím i existenci přirozených čísel lze snadno ukázat; jde o kardinální čísla konečných množin. Těm se budeme věnovat v dalším textu. Odpovědí na otázku počtu modelů Peanovy množiny je tvrzení, že těchto modelů je nekonečně mnoho, všechny jsou ale navzájem izomorfní. Proto lze tvrdit, že přirozená čísla lze definovat až na izomorfismus jediným možným způsobem. Důležitou větu o tomto izomorfismu nyní uvedeme:

Věta 1.23. (O jednoznačnosti přirozených čísel) Nechť $\boldsymbol{N_1}, \boldsymbol{N_2}$ jsou dvě množiny přirozených čísel (dva modely Peanovy množiny). Pak existuje právě jedna bijekce $f: \boldsymbol{N_1} \to \boldsymbol{N_2}$ s vlastností

$$\forall\, x \in \boldsymbol{N_1} : f(x') = [f(x)]' \ .$$

Přirozená čísla jako kardinální čísla konečných množin

V této části se omezíme pouze na konečné množiny. I když v obecné teorii množin jsou studována i kardinální čísla nekonečných množin, pro účely konstrukce oboru všech přirozených čísel se nekonečnými množinami nemusíme zabývat.

Víme, že dvě množiny jsou ekvivalentní, jestliže existuje bijekce (vzájemně jednoznačné zobrazení) jedné na druhou. Tato relace ekvivalence na systému všech konečných množin $\mathcal{M}$ (označujeme ji $\sim$) je ekvivalencí v relačním smyslu (zřejmě je reflexivní, symetrická a tranzitivní). Proto generuje jednoznačným způsobem rozklad $\mathcal{M}|_{\sim}$ na systému všech konečných množin $\mathcal{M}$. Třídy rozkladu $\mathcal{M}|_{\sim}$ se nazývají kardinální čísla. Kardinálním číslem konečné množiny M tedy rozumíme třídu rozkladu $\mathcal{M}|_{\sim}$, která obsahuje množinu M. Místo označení kardinální číslo množiny M se často užívá též pojmu mohutnost množiny M (píšeme card M). Nyní definujeme přirozená čísla jako kardinální čísla konečných množin.

Popíšeme-li výše uvedenou konstrukci populárně (a matematicky ne zcela přesně), pak kardinální číslo konečné množiny M je systém množin, který kromě dané množiny M obsahuje všechny množiny (nekonečně mnoho), které mají tentýž počet prvků jako množina M. Tato jediná společná vlastnost všech těchto množin, tj. stejný počet prvků, je vyjádřena přirozeným číslem, které je kardinálním číslem množiny M definováno. Ve školské matematice na ZŠ proto říkáme, že přirozená čísla vyjadřují počty prvků konečných množin.

Přechod od struktury $(P, +, \cdot)$ k jejímu modelu $(\boldsymbol{N}, +, \cdot)$ lze popsat takto: Nechť $n \in P$ je libovolný prvek Peanovy množiny. Úsek množiny P příslušný k prvku n je množina $U(n) = \{e, e', e'', e''', \ldots, {}'n, n\}$. Tato množina je konečná, proto jistě náleží do některé třídy rozkladu $\mathcal{M}|_{\sim}$. Tato třída rozkladu je kardinálním číslem konečné množiny $U(n)$ a odpovídající přirozené číslo je číslo n. Lze tedy tvrdit, že úsek $U(n)$ obsahuje právě n prvků. Odtud prvku e odpovídá číslo *1*, prvku e' číslo *2*, prvku e'' číslo *3* atd. přirozené uspořádání přirozených čísel lze pak definovat ve shodě s definicí porovnávání prvků Peanovy množiny (každé číslo náležející do $U(n)$ je menší nebo rovno číslu n).

Jiná situace je u definice obou základních operací sčítání a násobení. I když lze tyto operace definovat stejným způsobem jako v abstraktní Peanově množině, z metodických důvodů se obě operace zavádějí odlišně, na základě množinových operací.

Definice 1.24. (Sčítání kardinálních čísel) Nechť A, B jsou konečné množiny, nechť platí $A \cap B = \phi$. Pak definujeme

$$\text{card } A + \text{card } B = \text{card } (A \cup B) .$$

Definice 1.25. (Násobení kardinálních čísel) Nechť A, B jsou konečné množiny.
Pak definujeme

$$\text{card } A \cdot \text{card } B = \text{card } (A \times B) .$$

Poznámka 1. 26. Lze ukázat, že obě operace definované definicemi 1.24. a 1.25. mají všechny vlastnosti, které očekáváme od operací sčítání a násobení přirozených čísel. Povšimněme si nyní omezující podmínky $A \cap B = \phi$ v definici 1.5. V případě jejího vypuštění bude pro součet kardinálních čísel množin A, B platit vztah $\text{card } A + \text{card } B \geq \text{card } (A \cup B)$, přičemž číslo na levé straně této neostré nerovnosti je obecně větší než číslo na pravé straně o počet prvků průniku obou množin. Platí tedy rovnost

$$\text{card } A + \text{card } B - \text{card } (A \cap B) = \text{card } (A \cup B) .$$

Z teoretického hlediska se jedná o princip inkluze a exkluze pro $n = 2$. Pokud jsou tedy množiny A, B disjunktní, pak $\text{card } (A \cap B) = 0$ a předchozí rovnost přejde v definici sčítání kardinálních čísel podle definice 1.5.

2. Celá čísla

Obecná teorie

Definice 2.1. Nechť $(G, \cdot), (H, \cdot)$ jsou grupoidy (dále budeme k označení grupoidů užívat pouze symbol nosné množiny). Řekneme, že grupoid G lze vnořit do grupoidu H, jestliže existuje injektivní homomorfismus f grupoidu G do grupoidu H.

Věta 2.2. Nechť G je komutativní grupoid. Pak jsou následující výroky ekvivalentní:
(1) Grupoid G je asociativní a platí v něm zákony o krácení.
(2) Grupoid G lze vnořit do nějaké grupy.

Poznámka 2.3. Důkaz této věty je konstruktivní, obsahuje konstrukci tzv. podílové grupy Γ grupoidu G. Tuto konstrukci nyní popíšeme:

Vyjdeme z kartézského součinu $G \times G$. Nechť na $G \times G$ je definována binární relace $\sim$ definovaná takto:

$$[a, b] \sim [c, d] \Rightarrow a \cdot d = b \cdot c \text{ pro každé dvě dvojice z } G \times G. \qquad (1)$$

Tato relace $\sim$ je ekvivalence, existuje tedy rozklad $G \times G \,|_{\sim}$. Množinu tříd rozkladu $G \times G \,|_{\sim}$ označme Γ. Na množinovém systému Γ definujme nyní binární operaci o následujícím způsobem. Nechť $[a, b], [c, d]$ jsou reprezentanti dvou tříd systému Γ . Pak platí

$$[a, b] \; o \; [c, d] = [a \cdot c, b \cdot d]. \qquad (2)$$

Grupoid (Γ, o) je faktoroidem grupoidu $(G, \cdot)$. Lze dokázat, že algebraická struktura (Γ, o) je dokonce grupa. Tato grupa se nazývá podílová grupa grupoidu $(G, \cdot)$. Vnoření $\psi : G \to \Gamma$ grupoidu G do grupy Γ je definováno pro každý prvek $g \in G$ předpisem

$$\psi (g) = \{[g \cdot x, x]; x \in G\}. \qquad (3)$$

Je-li místo multiplikativního označení (operace $\cdot$) užito označení aditivního (operace +), pak

definiční vztahy (1), (2), (3) přejdou do tvaru:

$$[a, b] \sim [c, d] \Rightarrow a + d = b + c \text{ pro každé dvě dvojice z } G \times G, \quad (4)$$

$$[a, b] \, o \, [c, d] = [a + c, b + d] \ , \quad (5)$$

$$\psi(g) = \{[g + x, x]; x \in G\}. \quad (6)$$

Místo označení podílová grupa pak říkáme rozdílová grupa.

Celá čísla

Definice 2.4. Rozdílová grupa pologrupy $(\boldsymbol{N}, +)$ se nazývá aditivní grupa celých čísel $(\boldsymbol{Z}, +)$.

Poznámka 2.5. Při konstrukci grupy $(\boldsymbol{Z}, +)$ postupujeme podle obecné konstrukce. Výchozím kartézským součinem je $\boldsymbol{N} \times \boldsymbol{N}$, relace $\sim$ je definována vztahem (4) pro $G = \boldsymbol{N}$; operace o, kterou budeme označovat symbolem +, tj. stejně jako sčítání čísel přirozených (zřejmě nebude docházet k nedorozumění), je pak definována pomocí vztahu (5), tedy

$$[a, b] + [c, d] = [a + c, b + d]. \quad (7)$$

Celá čísla jsou podle této konstrukce třídami rozkladu $\boldsymbol{N} \times \boldsymbol{N} \,|_{\sim}$. Vnoření $\psi : \boldsymbol{N} \to \boldsymbol{Z}$ grupoidu $\boldsymbol{N}$ do grupy $\boldsymbol{Z}$ je definováno analogicky jako v (6), tedy pro každý prvek $n \in \boldsymbol{N}$ předpisem

$$\psi(n) = \{[n + x, x]; x \in \boldsymbol{N}\}.$$

Poznámka 2.6. V dalším textu o celých číslech je nutno rozlišovat mezi případem, kdy $[a, b]$ bude označovat tuto jednu konkrétní uspořádanou dvojici přirozených čísel a případem, kdy bude hrát roli reprezentující dvojice nějakého celého čísla. V tomto druhém případě budeme užívat tučného označení $\boldsymbol{[a, b]}$. Platí tedy např. $\boldsymbol{[4, 2]} = \{[3, 1], [4, 2], [5, 3], [6, 4], ...\}$. Celé číslo je vždy reprezentováno nekonečnou množinou navzájem ekvivalentních uspořádaných dvojic přirozených čísel. Podle dohodnutého označení je nutno také rozlišovat následující vztahy: Např. pro uspořádané dvojice $[5, 3], [6, 4]$ platí $[5, 3] \neq [6, 4], [5, 3] \sim [6, 4]$, pro dvě celá čísla $\boldsymbol{[5, 3]}, \boldsymbol{[6, 4]}$ ale platí rovnost $\boldsymbol{[5, 3]} = \boldsymbol{[6, 4]}$, protože obě tyto dvojice jsou reprezentanty téže třídy rozkladu systému $\boldsymbol{N} \times \boldsymbol{N} \,|_{\sim}$. Poznamenejme, že v dalším textu budeme pro zjednodušení označovat celá čísla velkými tučnými písmeny, např. $\boldsymbol{A}, \boldsymbol{B}$, ... Toto označení není v rozporu s uvedenou konstrukcí; vždy lze přejít k reprezentaci pomocí uspořádaných dvojic, např. $\boldsymbol{A} = \boldsymbol{[a_1, a_2]}$, $\boldsymbol{B} = \boldsymbol{[b_1, b_2]}$, ...

Operace s celými čísly a jejich vlastnosti

Poznámka 2.7. Sčítání celých čísel je, jak již bylo zmíněno v poznámce 2.2., definováno předpisem

$$\boldsymbol{[a, b] + [c, d] = [a + c, b + d].}$$

Věta 2.8. Operace + z předchozí poznámky 2.7. je komutativní, asociativní, má neutrální prvek $\boldsymbol{0}$ reprezentovaný dvojicí $\boldsymbol{[n, n]}$ pro libovolné $n \in \boldsymbol{N}$ a ke každému celému číslu $\boldsymbol{A} = \boldsymbol{[a, b]}$ existuje právě jedno opačné číslo $\boldsymbol{-A = [b, a].}$

Věta 2.9. Algebraická struktura $(\boldsymbol{Z}, +)$ je komutativní grupa, ve které platí zákony o dělení, tj rovnice $\boldsymbol{A + X = B}$ má vždy řešení v množině $\boldsymbol{Z}$ pro každá dvě celá čísla $\boldsymbol{A, B.}$

Věta 2.10. V grupě $(\boldsymbol{Z}, +)$ platí zákony o krácení (v aditivní symbolice zákony o odečítání) a existuje právě jedna inverzní operace k operaci sčítání. tato operace se nazývá odčítání a je definována vztahem $\boldsymbol{A - B = A + (-B)}$.

Poznámka 2.11. Z předchozí věty a věty 2.1. lze odvodit početní pravidlo pro operaci odčítání:

$$\boldsymbol{[a, b] - [c, d] = [a + d, b + c].}$$

Povšimněme si, že v definici odčítání vystupují na pravé straně pouze součty přirozených čísel, tzn. operace odčítání je neomezeně definovaná a tedy algebraická struktura $(\boldsymbol{Z}, -)$ je grupoid. Tento grupoid není pologrupou, protože operace odčítání zřejmě není asociativní ani komutativní.

Definice 2.12. Na množině $\boldsymbol{Z}$ definujme binární operaci $\cdot$ následujícím způsobem:

$$\boldsymbol{[a, b] \cdot [c, d] = [ac + bd, ad + bc].}$$

Tuto operaci nazveme násobením v množině celých čísel. Tato operace je v množině $\boldsymbol{Z}$ neomezeně definovaná, struktura $(\boldsymbol{Z}, \cdot)$ je tedy grupoid.

Věta 2.13. Grupoid $(\boldsymbol{Z}, \cdot)$ je asociativní, komutativní a má neutrální prvek $\boldsymbol{1}$ reprezentovaný dvojicí $\boldsymbol{[n+1, n]}$ pro libovolné $n \in \boldsymbol{N}$.

Věta 2.14. V grupoidu $(\boldsymbol{Z}, \cdot)$ platí omezený zákon o krácení, tzn. pro každá tři celá čísla $x, y, z, x \neq 0$ platí implikace $x \cdot y = x \cdot z \Rightarrow y = z$.

Věta 2.15. Operace násobení je v množině celých čísel svázána s operací sčítání distributivním zákonem, tj.

$$\boldsymbol{A, B, C \in Z:\ A \cdot (B + C) = A \cdot B + A \cdot C.}$$

Věta 2.16. Algebraická struktura $(\boldsymbol{Z}, +, \cdot)$ je komutativní okruh s jedničkou charakteristiky nula, který není tělesem. V tomto okruhu neexistují vlastní dělitelé nuly, je to tedy obor integrity.

Poznámka 2.17. V oboru integrity všech celých čísel $(\boldsymbol{Z}, +, \cdot)$ platí řada tvrzení, běžně užívaných při výpočtech. Uveďme některé příklady.

Věta 2.18. Nechť $\boldsymbol{A, B, C \in Z}$. Pak platí:
(1) $\boldsymbol{-(-A) = A}$;
(2) $\boldsymbol{-(A + B) = (-A) + (-B)}$;
(3) $\boldsymbol{-(A - B) = B - A}$;
(4) $\boldsymbol{(A - (B - C) = (A + C) - B}$;
(5) $\boldsymbol{(-A) \cdot B = A \cdot (-B) = -(A \cdot B)}$.

Relace uspořádání v množině celých čísel

Definice 2.19. Nechť $\boldsymbol{A = [a, b]}$ je celé číslo. Řekneme, že toto číslo je kladné a píšeme $\boldsymbol{A > 0}$, právě když platí $a > b$. Je-li $a = b$, pak číslo $\boldsymbol{A = 0}$; ve zbývajícím případě pro $a < b$ říkáme, že celé číslo $\boldsymbol{A}$ je záporné a píšeme $\boldsymbol{A < 0}$.

Poznámka 2.20. Je zřejmé, že jeden z předchozích případů vždy musí nastat. Každé celé číslo je tedy buďto kladné nebo záporné nebo je rovno nule. Existuje tedy rozklad množiny všech celých čísel na čísla kladná, nulu a čísla záporná. Ve shodě s běžnou terminologií zavádíme i označení $A \leq 0$ a říkáme, že číslo A je nekladné, resp. v případě $A \geq 0$ je toto číslo nezáporné.

Definice 2.21. Nechť A, B jsou celá čísla. Řekneme, že $A < B$, právě když platí $A - B < 0$. Je-li $A - B = 0$, pak $A = B$; ve zbývajícím případě pro $A - B > 0$ pak platí $A > B$.

Poznámka 2.22. Je zřejmé, že i v předchozí definici jeden z případů vždy musí nastat. Relace uspořádání všech celých čísel je tedy lineární. I zde se běžně užívá i neostrá nerovnost $A \leq B$ pro případ $A - B \leq 0$ a analogicky $A \geq B$ pro případ $A - B \geq 0$.

Věta 2.23. Nechť A je celé číslo. Pak platí:
(1) $A > 0 \Rightarrow -A < 0$.
(2) $A < 0 \Rightarrow -A > 0$.

Věta 2.24. Nechť A, B jsou kladná celá čísla. Potom jejich součet $A + B$ i součin $A \cdot B$ jsou také kladná celá čísla.

Poznámka 2.25. Výše definovaná relace uspořádání v množině všech celých čísel je spojena s operacemi v této množině řadou vztahů. Uveďme alespoň některé.

Věta 2.26. Nechť A, B, C, D jsou libovolná celá čísla. Pak platí:
(1) Jestliže $A > B$ a $C < 0$, potom $AC < BC$;
(2) Jestliže $A + C > B + C$, potom $A > B$;
(3) Jestliže $AC > BC$ a $C > 0$, potom $A > B$;
(4) Jestliže $AC > BC$ a $C < 0$, potom $A < B$;
(5) Jestliže $A > B$ a $C > D$, potom $A + C > B + D$;
(6) Jestliže $A > B$ a $C > D$ a $C > 0$ a $B > 0$, potom $A \cdot C > B \cdot D$.

Věta 2.27. Nechť A, B jsou libovolná celá čísla, přičemž $B \neq 0$. Pak existuje jednoznačně určená dvojice celých čísel Q, R (přičemž $0 \leq R < |B|$) s vlastností $A = B \cdot Q + R$. Číslo A se nazývá dělenec, číslo B dělitel, číslo Q je podíl (někdy též neúplný podíl) a číslo R je zbytek. Proces nalezení čísel Q, R se nazývá dělení se zbytkem v množině celých čísel.

Definice 2.28. Absolutní hodnotu $|A|$ celého čísla A definujeme takto:
(1) Je-li $A \geq 0$, pak $|A| = A$;
(2) Je-li $A < 0$, pak $|A| = -A$.

Věta 2.29. Nechť A, B jsou libovolná celá čísla, pak platí:
(1) $|A| = |-A|$;
(2) $A \leq |A|$;
(3) $|A|^2 = A^2$;
(4) $|A \cdot B| = |A| \cdot |B|$;
(5) $|A + B| \leq |A| + |B|$;
(6) $|A - B| \geq |A| - |B|$.

Poznámka 2.30. Vnoření $\psi : \boldsymbol{N} \to \boldsymbol{Z}$ grupoidu $\boldsymbol{N}$ do grupy $\boldsymbol{Z}$ je definováno podle poznámky 2.2. pro každý prvek $n \in \boldsymbol{N}$ předpisem $\psi(n) = \{[n + x, x];\ x \in \boldsymbol{N}\}$. Každé celé kladné (tj. přirozené) číslo n je tedy reprezentováno dvojicí $\boldsymbol{[n + x, x]}$, číslo nula je reprezentováno dvojicí $\boldsymbol{[x, x]}$ a každé celé záporné číslo $-n$ je reprezentováno dvojicí $\boldsymbol{[x, n + x]}$.

3. Racionální čísla

Obecná teorie

Definice 3.1. Nechť $R = (R, +, \cdot)$, $S = (S, +, \cdot)$ jsou okruhy. Řekneme, že okruh R lze vnořit do okruhu S, jestliže existuje injektivní homomorfismus f okruhu R do okruhu S.

Věta 3.2. Nechť $(R, +, \cdot)$ je komutativní okruh. Pak jsou následující výroky ekvivalentní:
(1) V okruhu $(R, +, \cdot)$ platí omezený zákon o krácení, tzn.

$$\forall x, y, z \in R, x \neq 0:\ x \cdot y = x \cdot z \Rightarrow y = z\ .$$

(2) Okruh R lze vnořit do tělesa.

Poznámka 3.3. Důkaz této věty je konstruktivní, obsahuje konstrukci tzv. podílového tělesa T okruhu R. Tuto konstrukci nyní popíšeme:

Vyjdeme z kartézského součinu $R \times R - \{0\}$, který označíme M a budeme nazývat množina všech zlomků okruhu R. Nechť na M je definována binární relace $\sim$ definovaná takto:

$$[a, b] \sim [c, d] \Rightarrow a \cdot d = b \cdot c \text{ pro každé dvě dvojice z množiny } M. \qquad (8)$$

Tato relace $\sim$ je ekvivalence na M, existuje tedy rozklad $M\,|_{\sim}$. Množinu tříd rozkladu $M\,|_{\sim}$ označme T. Na množinovém systému T definujme nyní binární operace sčítání a násobení následujícím způsobem. Nechť $[a, b], [c, d]$ jsou reprezentanti dvou tříd systému T. Pak platí

$$[a, b] + [c, d] = [ad + bc, bd], \quad [a, b] \cdot [c, d] = [ac, bd] \qquad (9)$$

Lze dokázat, že algebraická struktura $(T, +, \cdot)$ je těleso. Toto těleso se nazývá podílové těleso okruhu R. Nulou tohoto tělesa je třída $\{[0, r];\ r \in R\}$, jedničkou třída $\{[r, r];\ r \in R\}$. Vnoření $\psi : R \to T$ okruhu R do tělesa T je definováno pro každý prvek $r \in R$ předpisem

$$\psi(r) = \{[r \cdot x, x];\ x \in R\}. \qquad (10)$$

Racionální čísla

Definice 3.4. Podílové těleso okruhu $(\boldsymbol{Z}, +, \cdot)$ se nazývá těleso racionálních čísel $(\boldsymbol{Q}, +, \cdot)$.

Poznámka 3.5. Při konstrukci tělesa $(\boldsymbol{Q}, +, \cdot)$ postupujeme podle obecné konstrukce. Výchozím kartézským součinem je $M = \boldsymbol{Z} \times \boldsymbol{Z} - \{0\}$, relace $\sim$ je definována vztahem (8) pro $R = \boldsymbol{Z}$. Protože se podle obecné teorie jedná o zlomky, budeme uspořádané dvojice z množiny M zapisovat jako zlomky, tedy místo $[a, b]$ budeme psát $\frac{a}{b}$. Odtud je také zřejmé, proč se v množině M pro druhé složky všech dvojic nepřipouští číslo nula. Operace sčítání a násobení jsou definovány vztahy (9); po vyjádření pomocí zlomků tedy

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}\ .$$

Racionální čísla jsou podle této konstrukce třídami rozkladu $M\,|_{\sim}$. Vnoření $\psi : \boldsymbol{Z} \to \boldsymbol{Q}$ okruhu $\boldsymbol{Z}$ do tělesa $\boldsymbol{Q}$ je definováno analogicky jako v (10), tedy pro každý prvek $z \in \boldsymbol{Z}$ předpisem

$$\psi(z) = \{\frac{z \cdot x}{x}; x \in \boldsymbol{Z} - \{0\}\}.$$

Analogicky jako u celých čísel budeme rozlišovat jeden konkrétní zlomek od racionálního čísla. Tučným označením $\frac{\boldsymbol{a}}{\boldsymbol{b}}$ budeme označovat stav, kdy tento zlomek bude reprezentovat racionální číslo, zatímco běžným způsobem $\frac{a}{b}$ budeme označovat tento jeden konkrétní zlomek. Platí tedy např. $\frac{\boldsymbol{3}}{\boldsymbol{4}} = \{\frac{3}{4}, \frac{6}{8}, \frac{3}{12}, \frac{-21}{-28}, \ldots\}$. Poznamenejme, že v dalším textu budeme pro zjednodušení označovat racionální čísla velkými tučnými písmeny, např. ***A, B,*** .... Toto označení není, tak jako u celých čísel, v rozporu s uvedenou konstrukcí; vždy lze přejít k reprezentaci pomocí uspořádaných dvojic, např. $\boldsymbol{A} = \frac{\boldsymbol{a}_1}{\boldsymbol{a}_2}$, $\boldsymbol{B} = \frac{\boldsymbol{b}_1}{\boldsymbol{b}_2}$, ... Obě operace sčítání a násobení lze pak užitím tohoto označení psát jako

$$\frac{\boldsymbol{a}}{\boldsymbol{b}} + \frac{\boldsymbol{c}}{\boldsymbol{d}} = \frac{\boldsymbol{ad + bc}}{\boldsymbol{bd}}, \qquad \frac{\boldsymbol{a}}{\boldsymbol{b}} \cdot \frac{\boldsymbol{c}}{\boldsymbol{d}} = \frac{\boldsymbol{ac}}{\boldsymbol{bd}} .$$

Věta 3.6. Operace sčítání v množině věech racionálních čísel je komutativní, asociativní, má neutrální prvek, ke každému racionálnímu číslu existuje právě jedno číslo opačné a platí zákony o dělení. Algebraická struktura $(\boldsymbol{Q}, +)$ je tedy komutativní grupa.

Poznámka 3.7. V grupě $(\boldsymbol{Q}, +)$ platí analogické vlastnosti a vztahy jako v grupě $(\boldsymbol{Z}, +)$, není tedy nutné je na tomto místě znovu uvádět. Poznamenejme jen, že neutrálním prvkem je číslo $\boldsymbol{0}$ reprezentované třídou $\frac{\boldsymbol{0}}{\boldsymbol{b}}$ a opačným racionálním číslem k číslu $\frac{\boldsymbol{a}}{\boldsymbol{b}}$ je číslo $-\frac{\boldsymbol{a}}{\boldsymbol{b}}$, které lze reprezentovat buďto třídou $\frac{\boldsymbol{-a}}{\boldsymbol{b}}$ nebo třídou $\frac{\boldsymbol{a}}{\boldsymbol{-b}}$.

Poznámka 3.8. Analogicky jako pro celá čísla lze zavést operaci odčítání jako přoïčtení opačného prvku, tedy $\boldsymbol{A - B = A + (-B)}$. Takto lze snadno odvodit běžně užívaný vztah pro odčítání zlomků:

$$\frac{\boldsymbol{a}}{\boldsymbol{b}} - \frac{\boldsymbol{c}}{\boldsymbol{d}} = \frac{\boldsymbol{ad - bc}}{\boldsymbol{bd}} .$$

Poznámka 3.9. Operace odčítání má v množině všech racionálních čísel tytéž vlastnosti jako v množině celých čísel (tj. není komutativní ani asociativní).

Poznámka 3.10. Nyní se budeme věnovat operaci násobení v množině všech racionálních čísel. Připomeneme definici: $\frac{\boldsymbol{a}}{\boldsymbol{b}} \cdot \frac{\boldsymbol{c}}{\boldsymbol{d}} = \frac{\boldsymbol{ac}}{\boldsymbol{bd}}$.

Věta 3.11. Operace násobení v množině $\boldsymbol{Q}$ je komutativní, asociativní a má neutrální prvek. Tímto neutrálním prvkem je číslo $\boldsymbol{1}$ reprezentované třídou zlomků $\frac{\boldsymbol{a}}{\boldsymbol{a}}$. Algebraická struktura

$(\boldsymbol{Q}, \cdot)$ je komutativní monoid. Operace násobení je distributivní vzhledem k operaci sčítání v množině všech racionálních čísel.

Poznámka 3.12. Budeme-li zkoumat i existenci inverzních prvků a platnost zákonů o dělení vzhledem k operaci násobení v množině $\boldsymbol{Q}$, snadno zjistíme, že jediným prvkem, který neumožňuje platnost těchto vlastností, je číslo 0. Po jeho odstranění z množiny $\boldsymbol{Q}$ můžeme vyslovit následující větu.

Věta 3.13. (1) Algebraická struktura $(\boldsymbol{Q} - \{0\}, \cdot)$ je komutativní grupa.
(2) Algebraická struktura $(\boldsymbol{Q}, +, \cdot)$ je komutativní těleso.

Poznámka 3.14. Inverzním prvkem k racionálnímu číslu $\frac{a}{b}$ je číslo $\frac{b}{a}$. Toto číslo vždy jednoznačně existuje ($b \neq 0$ podle konstrukce racionálních čísel a $a \neq 0$ podle předpokladu z poznámky 3.7. a věty 3.3.), nazývá se převrácené číslo k číslu $\frac{a}{b}$ a označuje $\left(\frac{a}{b}\right)^{-1}$. Při označení racionálního čísla $\boldsymbol{A}$ se převrácené číslo kromě zápisu $\boldsymbol{A^{-1}}$ zapisuje též $\frac{1}{A}$. V množině $\boldsymbol{Q} - \{0\}$ jsme nyní připraveni k definici operace dělení.

Definice 3.15. Dělení v množině $\boldsymbol{Q} - \{0\}$ je definováno jako násobení převráceným číslem, tj. $\boldsymbol{A : B = A \cdot B^{-1}}$. Vyjádřeno pomocí definice operace násobení a převráceného čísla dostáváme

$$\frac{a}{b} : \frac{c}{d} = \frac{ad}{bc} .$$

Poznámka 3.16. Připomeňme znovu, že existence převráceného čísla i operace dělení jsou neomezeně definovány v množině $\boldsymbol{Q} - \{0\}$, tedy že skutečně nemůže dojít k „dělení nulou“. Pro operace dělení a násobení platí rovněž řada vlastností, z nichž uvedeme např.:

Věta 3.17. Nechť $\boldsymbol{A, B, C \in Q}$. Pak platí:
(1) $(\boldsymbol{A^{-1}})^{-1} = \boldsymbol{A}$;
(2) $(\boldsymbol{A \cdot B})^{-1} = \boldsymbol{A^{-1} \cdot B^{-1}}$;
(3) $(\boldsymbol{A \cdot B^{-1}})^{-1} = \boldsymbol{B \cdot A^{-1}}$;
(4) $(\boldsymbol{A \cdot B^{-1}}) \cdot \boldsymbol{C}^{-1} = \boldsymbol{A \cdot (B \cdot C)^{-1}}$;
(5) $\boldsymbol{A \cdot (B \cdot C}^{-1})^{-1} = \boldsymbol{(A \cdot C) \cdot B^{-1}}$.

Relace uspořádání v množině racionálních čísel

Definice 3.18. Nechť $\boldsymbol{A} = \frac{a}{b}$ je racionální číslo. Řekneme, že toto číslo je kladné a píšeme $\boldsymbol{A} > 0$, právě když platí a i b jsou buďto obě současně kladná celá čísla nebo obě současně záporná celá čísla. . Je-li $a = 0$, pak číslo $\boldsymbol{A} = \boldsymbol{0}$; ve zbývajícím případě (jedno z čísel a, b je kladné celé číslo a jedno záporné) říkáme, že racionální číslo $\boldsymbol{A}$ je záporné a píšeme $\boldsymbol{A} < 0$.

Poznámka 3.19. Je zřejmé, že jeden z předchozích případů vždy musí nastat. Každé racionální číslo je tedy buďto kladné nebo záporné nebo je rovno nule. Existuje tedy rozklad množiny všech racionálních čísel na čísla kladná, nulu a čísla záporná. Ve shodě s běžnou terminologií zavádíme i označení $A \leq 0$ a říkáme, že číslo A je nekladné, resp. v případě $A \geq 0$ je toto číslo nezáporné.

Definice 3.20. Nechť A, B jsou racionální čísla. Řekneme, že $A < B$, právě když platí $A - B < 0$. Je-li $A - B = 0$, pak $A = B$; ve zbývajícím případě pro $A - B > 0$ pak platí $A > B$.

Poznámka 3.21. Je zřejmé, že i v předchozí definici jeden z případů vždy musí nastat. Relace uspořádání všech racionálních čísel je tedy lineární. I zde se běžně užívá i neostrá nerovnost $A \leq B$ pro případ $A - B \leq 0$ a analogicky $A \geq B$ pro případ $A - B \geq 0$.

Poznámka 3.22. Pro relaci uspořádání v množině racionálních čísel a její spojení s operacemi v množině Q platí analogické vztahy jako v množině celých čísel, stejně je definována i absolutní hodnota racionálního čísla. Vzhledem k tomu, že $(Q, +, \cdot)$ je komutativní těleso, nemá smysl v množině racionálních čísel zavádět dělení se zbytkem. Platí však zajímavá vlastnost relace uspořádání racionálních čísel, která v množinách přirozených ani celých čísel platit nemohla.

Definice 3.23. Relace uspořádání v množině racionálních čísel je hustě uspořádaná, tzn.

$$\forall x, y \in Q, x \neq y; \exists z \in Q: x < z < y .$$

Poznámka 3.24. Definice hustého uspořádání říká, že „mezi každá dvě různá racionální čísla lze vložit další racionální číslo“. Z teorie uspořádaných množin z toho plyne, že uspořádaná množina Q nemá skoky. Vysvětlení této skutečnosti ponecháme na teorii konstrukce reálných čísel.

Desetinné rozvoje racionálních čísel

Poznámka 3.25. Je zřejmé, že racionální čísla nevyjadřujeme výlučně ve tvaru zlomku, např. velmi často se setkáváme s jejich vyjádřením pomocí desetinných rozvojů.

Věta 3.26. Každé racionální číslo lze vyjádřit pomocí desetinného rozvoje, přičemž tento desetinný rozvoj je buďto ukončený nebo je periodický. Ukončený je právě tehdy, je-li dané racionální číslo tvaru $\frac{a}{2^p \cdot 5^q}$, tj. obsahuje-li rozklad jeho jmenovatele na prvočinitele pouze prvočísla *2* nebo *5*.

Poznámka 3.27. Převod zápisu racionálního čísla ze zlomku na desetinný rozvoj provádíme dělením čitatele jmenovatelem; opačný převod buďto přechodem na desetinný zlomek a úpravou (v případě konečného rozvoje) nebo užitím součtu konvergentní geometrické řady.

4. Reálná čísla

Poznámka 4.1. Protože $(\boldsymbol{Q}, +, \cdot)$ je komutativní těleso, tzn. ze strukturálního hlediska „nejbohatší“ strukturou, nelze již provést její „zlepšení“. Proto konstrukce reálných čísel nemůže být provedena pomocí podílových struktur; lze dokázat, že konstrukcí podílového tělesa racionálních čísel nedostaneme již nic nového. Těleso reálných čísel musí být konstruováno na jiné bázi. K tomu lze využít uspořádaných množin; buďto teorii řezů pocházející od R. Dedekinda nebo teorii úplných metrických prostorů. Zde využijeme Dedekindových řezů. Nejprve opět základní přehled teorie.

Obecná teorie

Definice 4.2. Nechť $(E, \leq)$ je lineárně uspořádaná množina. Dvojice $\alpha = (A, B), A \subseteq E, B \subseteq E$ se nazývá řez v množině E, jestliže platí:
(1) $A \cup B = E$, $A \neq \emptyset$, $B \neq \emptyset$,
(2) $x \in A \wedge y \in B \Rightarrow x < y$,
(3) $A \cap B = \emptyset$.

Poznámka 4.3. Systém $\{A, B\}$ tvoří tedy rozklad množiny E; množina A je dolní skupina řezu α a množina B je horní skupina řezu α.

Poznámka 4.4. (Typy řezů). Nechť $\alpha = (A, B)$ je řez v množině E. Pak mohou nastat následující čtyři případy.
Řez 1. druhu: Množina A obsahuje největší prvek a množina B neobsahuje nejmenší prvek;
Řez 2. druhu: Množina A neobsahuje největší prvek a množina B obsahuje nejmenší prvek;
Řez 3. druhu: Množina A neobsahuje největší prvek a množina B neobsahuje nejmenší prvek;
Řez 4. druhu: Množina A obsahuje největší prvek a množina B obsahuje nejmenší prvek.
Protože řezy 1. a 2. druhu popisují v podstatě tutéž situaci, budeme je tedy v dalším textu ztotožňovat. Každá lineárně uspořádaná množina proto může mít pouze řezy 1., 3. a 4. druhu.

Definice 4.5. Řez 3. druhu z poznámky 4.3. se nazývá mezera v lineárně uspořádané množině, řez 4. druhu z poznámky 4.3. se nazývá skok v lineárně uspořádané množině.

Věta 4.6. Lineárně uspořádaná množina, která obsahuje alespoň dva prvky, je hustě uspořádaná, právě když nemá skoky.

Příklady: a) řez 1. druhu: $E = \boldsymbol{Q}$; $A = \{x \in \boldsymbol{Q}: x \leq 1\}$, $B = \{x \in \boldsymbol{Q}: x > 1\}$;
b) řez 3. druhu: $E = \boldsymbol{Q}$; $A = \{x \in \boldsymbol{Q}: x^2 < 2\}$, $B = \{x \in \boldsymbol{Q}: x^2 > 2\}$;
c) řez 4. druhu: $E = \boldsymbol{Z}$; $A = \{x \in \boldsymbol{Z}: x \leq 1\}$, $B = \{x \in \boldsymbol{Z}: x \geq 2\}$.

Definice 4.7. Lineárně uspořádaná množina se nazývá spojitě uspořádaná, právě když nemá skoky ani mezery.

Definice 4.8. Nechť $(R, \leq)$, $(S, \leq)$ jsou lineárně uspořádané množiny. Zobrazení $f : R \to S$ se nazývá vnoření $(R, \leq)$ do $(S, \leq)$, jestliže platí:
(1) f je injektivní;
(2) $\forall x, y \in R: x \leq y \Rightarrow f(x) \leq f(y)$.
Někdy se pro toto zobrazení f užívá též označení izotonní zobrazení.

Věta 4.9. Každou lineárně uspořádanou množinu lze vnořit do lineárně uspořádané množiny bez mezer.

Věta 4.10. Nechť $(R, \leq)$ je lineárně uspořádaná množina. Označme S množinu všech řezů 1. a 3. druhu v množině R. Nechť na S je definováno uspořádání takto:

$$\alpha = (A, B),\ \beta = (C, D),\ \alpha, \beta \in S:\ \alpha \leq \beta \Leftrightarrow A \subseteq C.$$

Pak S je lineárně uspořádaná množina, která neobsahuje mezery.

Definice 4.11. Lineárně uspořádaná množina $(S, \leq)$ z předchozí věty se nazývá normální obal lineárně uspořádané množiny $(R, \leq)$.

Poznámka 4.12. Ztotožníme-li prvky množiny R s řezy 1. druhu v R, pak normální obal množiny R se skládá z prvků množiny R a mezer v R.

Označení 4.13. Nechť $(E, \leq)$ je lineárně uspořádaná množina. Pro každý prvek $m \in E$ budeme její podmnožinu $\{x \in E: x \leq m\}$ označovat $(m]$.

Věta 4.14. Nechť $(R, \leq)$ je lineárně uspořádaná množina a nechť $(S, \leq)$ je její normální obal. Uvažujme všechny řezy 1. druhu v množině R (podle poznámky 4.4. je každému prvku $r \in R$ přiřazen právě jeden řez 1. druhu, kde prvek r je největším prvkem dolní skupiny příslušného řezu). Označme $\alpha = (A, B)$ libovolný řez 1. druhu v množině R, nechť $r \in R$ je největší prvek množiny A. Definujme nyní zobrazení $f: R \to S$ takto: Pro každý prvek $r \in R$ nechť je jeho obrazem řez $f(r)$ v množině S definovaný takto:

$$f(r) = (\ (r],\ R - (r]\ ).$$

Pak zobrazení $f: R \to S$ je vnoření $(R, \leq)$ do $(S, \leq)$.

Reálná čísla

Poznámka 4.15. Z teorie racionálních čísel víme, že $(\boldsymbol{Q}, <)$ je lineárně uspořádaná množina, která nemá skoky (uspořádání je husté). Lze však snadno dokázat, že obsahuje mezery, např. $\sqrt{2}$ je zcela jistě číslo, které není racionální (nelze ho vyjádřit pomocí zlomku).

Věta 4.16. V lineárně uspořádané množině $(\boldsymbol{Q}, <)$ existují pouze řezy 1. a 3. druhu. Řezy 1. druhu odpovídají racionálním číslům a řezy 3. druhu mezerám v uspořádané množině $(\boldsymbol{Q}, <)$.

Definice 4.17. Normální obal lineárně uspořádané množiny $(\boldsymbol{Q}, <)$ je lineárně uspořádaná množina $(\boldsymbol{R}, <)$. Podle věty 4.10. lineárně uspořádaná množina $(\boldsymbol{R}, <)$ neobsahuje mezery, existují v ní tedy pouze řezy 1. druhu.

Věta 4.18.
(1) Lineárně uspořádaná množina $(\boldsymbol{R}, <)$ je spojitě uspořádaná (neobsahuje mezery).
(2) $\forall x, y \in \boldsymbol{R}, x < y;\ \exists z \in \boldsymbol{Q}: x < z < y$.

Definice 4.19. V uspořádané množině $(\boldsymbol{Q}, <)$ odpovídají řezy 1. druhu racionálním číslům a řezy 3. druhu (tj. mezery) odpovídají číslům iracionálním. Každá mezera v uspořádané množině $(\boldsymbol{Q}, <)$ tedy určuje právě jedno iracionální číslo. Označíme-li množinu všech iracionálních čísel $\boldsymbol{I}$, pak platí $\boldsymbol{R} = \boldsymbol{Q} \cup \boldsymbol{I}$.

Poznámka 4.20. Protože lineárně uspořádaná množina $(\boldsymbol{R}, <)$ neobsahuje mezery, . lze konstatovat, že každý bod číselné osy je obrazem právě jednoho reálného čísla a naopak, každé reálné číslo lze jednoznačně znázornit na číselné ose. Uvedené skutečnosti plynou i z axiomů spojitosti, známých z axiomatické teorie výstavby geometrie. Tyto axiomy jsou dva, Archimédův a Cantorův. Zejména Cantorův axiom, podle něhož průnik do sebe zařazených úseček je neprázdný, podstatně přispívá k představě obrazů reálných čísel na číselné ose.

Uspořádání v množině reálných čísel

Poznámka 4.21. Připomeňme, že reálná čísla jsou sjednocením racionálních řezů 1. a 3. druhu, tj. každé reálné číslo je racionálním řezem. V případě řezu 1. druhu jde o číslo racionální, v případě řezu 3. druhu jde o číslo iracionální.

Definice 4.22. Nechť $\alpha = (A, B)$, $\beta = (C, D)$ jsou řezy v množině $\boldsymbol{Q}$ (tj. dvě reálná čísla). Pak platí:

$$\alpha \leq \beta \Leftrightarrow A \subseteq C .$$

Definice 4.23. Nechť $\boldsymbol{Q}^+ = \{r \in \boldsymbol{Q}: r > 0\}$, tj. $\boldsymbol{Q}^+$ označuje množinu všech kladných racionálních čísel. Pak řez $(\boldsymbol{Q} - \boldsymbol{Q}^+, \boldsymbol{Q}^+)$ je reálné číslo, které označíme symbolem 0 a nazýváme nulou. Číslo $a \in \boldsymbol{R}$ je kladné, je-li $a > 0$, číslo $a \in \boldsymbol{R}$ je záporné, je-li $a < 0$.

Operace v množině reálných čísel

Definice 4.24. Nechť $a = (A, B)$, $b = (C, D)$ jsou libovolná reálná čísla. Položme nyní $C_2 = \{\alpha + \beta ; \alpha \in B, \beta \in D\}$, $C_1 = \boldsymbol{Q} - C_2$. Pak $C = (C_1, C_2)$ je reálné číslo, které nazveme součtem reálných čísel a, b a značíme $a + b$.

Věta 4.25. Nechť $a, b, c,$ jsou libovolná reálná čísla. Nechť platí $a < b$. Potom platí také nerovnost $a + c < b + c$. (Uspořádání reálných čísel je monotonní vzhledem ke sčítání).

Věta 4.26. Operace sčítání je v množině všech reálných čísel komutativní, asociativní, má neutrální prvek a platí zákony o dělení (rovnice $a + x = b$ má řešení pro libovolná reálná čísla a, b). Algebraická struktura $(\boldsymbol{R}, +)$ je komutativní grupa.

Definice 4.27. Z předchozí věty plyne, že rovnice $a + x = b$ má řešení pro libovolná reálná čísla a, b. Toto řešení píšeme ve tvaru $x = b - a$ a nazveme rozdílem reálných čísel a, b. příslušná operace se nazývá odčítání reálných čísel.

Definice 4.28. Nechť $a = (A, B)$, $b = (C, D)$ jsou libovolná reálná čísla. Položme nyní: $C_2 = \{\alpha \cdot \beta ; \alpha \in B, \beta \in D\}$, $C_1 = \boldsymbol{Q} - C_2$. Pak $C = (C_1, C_2)$ je reálné číslo, které nazveme součinem reálných čísel a, b a značíme $a \cdot b$.

Věta 4.29. Nechť $a, b, c,$ jsou libovolná reálná čísla. Pak platí:
(1) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$;
(2) $(-a) \cdot (-b) = a \cdot b$;
(3) $a \cdot b = 0$ právě tehdy, je-li $a = 0$ nebo $b = 0$.

Věta 4.30.

(1) Algebraická struktura $(\boldsymbol{R} - \{0\}, \cdot)$ je komutativní grupa.
(2) Algebraická struktura $(\boldsymbol{R}, +, \cdot)$ je komutativní těleso.

Věta 4.31. (Věta o supremu a infimu) Nechť M je libovolná neprázdná podmnožina množiny reálných čísel. Pak platí:
(1) Je-li M zdola ohraničená, existuje $inf_{\boldsymbol{R}} M$;
(2) Je-li M shora ohraničená, existuje $sup_{\boldsymbol{R}} M$.

Věta 4.32. (Vnoření racionálních čísel do čísel reálných)
Nechť $a \in \boldsymbol{Q}$. Označme $\boldsymbol{R_a} = \{x \in \boldsymbol{R}: x \leq a\}$. Pak zobrazení $f: \boldsymbol{Q} \to \boldsymbol{R}$ definované předpisem

$$f(a) = (\boldsymbol{R_a}, \boldsymbol{R} - \boldsymbol{R_a})$$

je izomorfní vnoření lineárně uspořádané množiny $\boldsymbol{Q}$ do lineárně uspořádané množiny $\boldsymbol{R}$.

Poznámka 4.33. Z matematické analýzy jsou známy následující definice:
(1) Posloupnost $\{a_n\}_{n=1}^{\infty}$ je cauchyovská, jestliže ke každému $\varepsilon > 0$ existuje přirozené číslo n_0 s vlastností, že pro každou dvojici přirozených čísel $m, n > n_0$ platí $|a_m - a_n| < \varepsilon$.
(2) Posloupnost $\{a_n\}_{n=1}^{\infty}$ je konvergentní s limitou L, jestliže ke každému $\varepsilon > 0$ existuje přirozené číslo n_0 s vlastností, že pro každé přirozené číslo $n > n_0$ platí $|a_n - L| < \varepsilon$.

Je zřejmé, že každá konvergentní posloupnost je cauchyovská, opak obecně neplatí. V metrickém prostoru $\boldsymbol{R}$ je ale každá cauchyovská posloupnost konvergentní, to znamená, že $\boldsymbol{R}$ je úplným metrickým prostorem. Této teorie úplných prostorů lze využít též ke konstrukci tělesa reálných čísel místo teorie řezů. Nyní následuje několik didaktických poznámek.

Poznámka 4.34. Již na střední škole se setkají studenti s důkazem, že číslo $\sqrt{2}$ nelze vyjádřit ve tvaru zlomku, tzn. že kromě čísel racionálních existují ještě čísla iracionální, přičemž iracionálními čísly jsou téměř všechny odmocniny, hodnoty goniometrických funkcí, logaritmů atd. Studentům však většinou chybí názorná geometrická představa; velmi těžko odlišují pojmy mezera a skok na číselné ose. Tyto pojmy, známé již ze starověké matematiky, jsou přitom ke správnému pochopení reálných čísel nezbytné. Nyní uvedeme dva modely reálných čísel, aritmetický a geometrický. S oběma se setká již žák základní školy. Aritmetickým modelem je pro něj množina všech čísel, geometrickým modelem číselná osa. Izomorfismus obou modelů umožňuje nerozlišovat mezi číslem a jeho obrazem na číselné ose. Aritmetický model je častější, geometrický model je přitom názornější a pro zavádění reálných čísel na školách vhodnější.

Množina $\boldsymbol{R}$ je:
- *uspořádaná* , tj. pro každá dvě $x, y \in \boldsymbol{R}$ nastane právě jeden z případů $x < y, x = y, x > y$;
- *hustá*, tj. $\forall x, y \in \boldsymbol{R}, x < y, \exists z \in \boldsymbol{R}: x < z < y$;
- *archimedovská*, tj. $\forall x, y \in \boldsymbol{R}, 0 < x < y, \exists n \in \boldsymbol{N}: x(n-1) \leq y < xn$;
- *spojitá*, tj. každá neprázdná shora ohraničená množina $M \subset \boldsymbol{R}$ má supremum.

V geometrickém modelu lze předchozí čtyři tvrzení formulovat názorněji:

- Jsou-li X, Y dva body na ose o, nastává právě jeden z případů: $X = Y$, X leží vlevo od Y, Y leží vlevo od X.
- Mezi každými dvěma různými body existuje bod.

- Jestliže B je vnitřním bodem úsečky AX a jestliže na polopřímce AX sestrojíme posloupnost bodů $B_1 = B, B_2, B_3$, ... tak, že postupně nanášíme úsečku AB (tedy úsečka AB_n je n-násobek úsečky AB), pak po jistém počtu kroků překročíme bod X (bod X bude prvkem jisté úsečky $B_{k-1}B_k$).
- Na číselné ose nejsou skoky (díry).

Aritmetický model množiny $\boldsymbol{R}$ je méně přehledný, lze v něm však uskutečňovat všechny aritmetické operace a dobře rozlišovat mezi racionálním a iracionálním číslem.

Od historie k dnešku

Poznámka 4.35. Problém důkazu existence iracionálních čísel je velmi starý. Již v antickém Řecku se objevila tzv. první krize matematického myšlení, která se týkala „nesouměřitelnosti úseček“. V tehdejší matematice byla známá racionální čísla i to, že jakékoliv racionální číslo lze přesnou geometrickou konstrukcí zobrazit na číselné ose. Společně se znalostí hustoty uspořádání racionálních čísel byl tehdy všeobecně přijímán názor, že jiná čísla než racionální neexistují, že každé číslo lze vyjádřit zlomkem a že každý bod číselné osy je obrazem nějakého racionálního čísla. Objev faktu, že v jakémkoliv čtverci jsou jeho strana a úhlopříčka tzv. nesouměřitelné a že délku úhlopříčky nelze vyjádřit zlomkem (má-li strana čtverce délku a, má úhlopříčka délku $\sqrt{2}\,a$), způsobil v tehdejší době doslova pozdvižení, neboť nebylo známo, jak vzniklý problém vyřešit. Z teorie už víme, že princip nesouměřitelnosti znamená to, že lineárně uspořádaná množina racionálních čísel obsahuje mezery. Vyřešení problému nesouměřitelnosti, tj. zavedení iracionálních čísel, mohlo být úspěšně teoreticky ukončeno až mnohem později, po uznání aktuálního nekonečna v díle Bernarda Bolzana.

Připomeneme nyní Cantorův axiom spojitosti, známý z geometrie. Podle něj je průnik do sebe zařazených úseček neprázdný. Po uznání aktuálního nekonečna a s tím souvisejícím zavedení limitních procesů do matematiky lze dokázat, že při nekonečném počtu do sebe zařazených úseček je průnikem pouze jednoprvková množina. Při nekonečném počtu do sebe zařazených úseček na číselné ose je tedy průnikem jediné číslo. Proto je možné iracionální číslo, které je mezerou na číselné ose (racionálním řezem 3. druhu), definovat jako průnik nekonečně mnoha do sebe zařazených úseček na číselné ose. Levé krajní body těchto úseček tvoří rostoucí shora ohraničenou posloupnost racionálních čísel, která proto musí mít limitu. Analogicky pravé krajní body tvoří klesající zdola ohraničenou posloupnost racionálních čísel, která musí mít rovněž limitu. Obě tyto limity se rovnají a jejich hodnota je hledané iracionální číslo. Uvedeme dva příklady:

a) Nechť (A, B), $A = \{x \in \boldsymbol{Q}: x^2 < 2\}$, $B = \{x \in \boldsymbol{Q}: x^2 > 2\}$ je řez třetího druhu v množině $\boldsymbol{Q}$. Budeme postupně volit čísla z množiny A i B tak, aby čísla množiny A tvořila rostoucí posloupnost a čísla z množiny B klesající posloupnost. Tyto dvojice čísel budou krajními body vnořených intervalů, kterými budeme postupně stále přesněji aproximovat hodnotu zvolené mezery (řezu 3. druhu).

$1^2 = 1;$	$2^2 = 4,$	tedy	$1 < \sqrt{2} < 2$
$(1,4)^2 = 1,96;$	$(1,5)^2 = 2,25\,,$	tedy	$1,4 < \sqrt{2} < 1,5$
$(1,41)^2 = 1,9881;$	$(1,42)^2 = 2,0164\,,$	tedy	$1,41 < \sqrt{2} < 1,42$
$(1,414)^2 = 1,999396;$	$(1,415)^2 = 2,002225\,,$	tedy	$1,414 < \sqrt{2} < 1,415$
$(1,4141)^2 = 1,99967881;$	$(1,4143)^2 = 2,00024449\,,$	tedy	$1,4141 < \sqrt{2} < 1,4143$

atd.

Uvedený proces aproximace je nekonečný a číslo $\sqrt{2}$ je tak postupně určováno se stále větší přesností. Při praktickém počítání v praxi se spokojíme s přesností, která postačuje k řešení matematických problémů.

b) Proces postupné aproximace iracionálního čísla lze i programovat. Příkladem může být přibližné určení čísla Eulerova čísla *e*. Víme, že $2 < e < 4$. Dále z matematické analýzy víme, že platí: $\lim_{n\to\infty} (1+\frac{1}{n})^n = e$, $\lim_{n\to\infty} (1+\frac{1}{n})^{n+1} = e$, přičemž první z těchto posloupností $\left\{\left(1+\frac{1}{n}\right)^n\right\}_{n=1}^{\infty}$ je rostoucí s prvním členem *2*, druhá z těchto posloupností $\left\{\left(1+\frac{1}{n}\right)^{n+1}\right\}_{n=1}^{\infty}$ je klesající s prvním členem *4*. Obecně tedy můžeme Eulerovo číslo aproximovat pro $n \in \boldsymbol{N}$ pomocí nerovností

$$(1+\frac{1}{n})^n < e < (1+\frac{1}{n})^{n+1} .$$

Závěrečné poznámky k reálným číslům

A) Surdické výrazy

Poznámka 4.36. Surdické výrazy jsou reálná čísla tvaru $a \pm \sqrt{b}$, kde *a, b* jsou nezáporná racionální čísla, *b* není druhou mocninou žádného racionálního čísla. Jedná o velmi starou problematiku - vzorce pro úpravu surdických výrazů znal již ve 12. století indický matematik Bháskara. Pro úpravu surdických výrazů platí vztahy: (předpokládáme, že $a > \sqrt{b} \geq 0$)

$$\sqrt{a+\sqrt{b}} \pm \sqrt{a-\sqrt{b}} = \sqrt{2(a \pm \sqrt{a^2-b})}\ , \qquad \sqrt{a \pm \sqrt{b}} = \sqrt{\frac{a+\sqrt{a^2-b}}{2}} \pm \sqrt{\frac{a-\sqrt{a^2-b}}{2}}\ .$$

Pomocí uvedených dvou vztahů se některé výrazy s odmocninami téměř „zázračně“ upraví, např. výraz $\sqrt{3+2\sqrt{2}} - \sqrt{3-2\sqrt{2}}$. Zde $a = 3,\ b = 8$, podle prvního ze vzorců je výsledek roven *2*. Takto lze upravovat i odmocniny z vyšších čísel, např. $\sqrt{100-2\sqrt{2499}} = \sqrt{51} - 7$, $\sqrt{31+\sqrt{600}} = 5 + \sqrt{6}$, $\sqrt{x+y+2\sqrt{xy}} + \sqrt{x+y-2\sqrt{xy}} = 2\sqrt{x}$.

Poznámka 4.37. Nyní se budeme věnovat úpravám výrazu $X = \sqrt[3]{\sqrt{a}+b} - \sqrt[3]{\sqrt{a}-b}$. Pokud $\sqrt[3]{a-b^2}$ je racionální číslo, pak lze po umocnění výrazu *X* na třetí a úpravě psát $X^3 = 2b - 3\sqrt[3]{a-b^2}\,X$, což je rovnice, ze které lze hodnota *X* vypočítat. Např. ve výrazu $\sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2}$ je $a = 5,\ b = 2$. Rovnice je potom tvaru $X^3 = 4 - 3X$, odkud je jeden kořen $X = 1$ ihned patrný včetně toho, že další reálná řešení tato rovnice nemá. Dodejme ještě, že obdobný rozbor lze provést i v případě, kdy ve výrazu *X* je mezi odmocninami znaménko plus.

B) Algebraická a transcendentní čísla

Definice 4.38. Algebraické číslo je takové reálné číslo, které je kořenem nějakého polynomu s racionálními koeficienty. Z množiny všech polynomů, jejichž je dané algebraické číslo kořenem, vybereme polynom s nejnižším stupněm. Tento stupeň polynomu je také stupněm tohoto algebraického čísla.

Poznámka 4.39. Každé racionální číslo je algebraické. Algebraická je však i řada iracionálních čísel. Např. číslo $\sqrt{2}$ je algebraické, neboť je řešením rovnice $x^2-2 = 0$. Z poznatků algebry a geometrie plyne, že pomocí kružítka a pravítka (bez stupnice) lze sestrojit právě a jen ty úsečky, jejichž délky jsou algebraická čísla stupně mocniny dvou. Z toho plyne neřešitelnost některých geometrických úloh jako je kvadratura kruhu, trisekce úhlu či duplikace krychle (tři klasické problémy antické matematiky).

Věta 4.40.
(1) Označme A množinu všech algebraických čísel. Pak $(A, +, \cdot)$ je komutativní těleso.
(2) Kořeny polynomu, jehož koeficienty jsou algebraická čísla, jsou opět algebraická čísla.

Definice 4.41. Transcendentní číslo je takové reálné číslo, které není kořenem žádné algebraické rovnice s racionálními koeficienty.

Poznámka 4.42. Důkaz existence transcendentních čísel přinesl v roce 1840 francouzský matematik Joseph Liouville. Je zřejmé, že transcendentní čísla musí být iracionální, jejich iracionalita je však „jiného typu“ než např. u surdických čísel, která jsou algebraická. I když od roku 1840 byla známa existence transcendentních čísel, po řadu let se nedařilo dokázat transcendentnost dvou významných iracionálních čísel π a e. Až v roce 1873 dokázal Hermite transcendentnost čísla e a v roce 1882 Ferdinand von Lindemann transcendentnost čísla π.

Poznámka 4.43. Lze dokázat, že v jistém smyslu většina iracionálních čísel je transcendentních. Abychom si udělali alespoň obecnou představu o transcendentních číslech, uvedeme výsledek, který dokázali v roce 1934 Gelfand a Schneider.

Věta 4.44. Nechť α, β jsou algebraická reálná čísla, nechť β je iracionální číslo a nechť $\alpha \neq 0$, $\alpha \neq 1$. Potom všechna čísla tvaru α^{β} jsou transcendentní.

Příklad 4.45. Podle předchozí věty 4.14. mezi transcendentní čísla patří například čísla $2^{\sqrt{2}}$, $3^{\sqrt{5}}$, $\left(\sqrt[3]{7}\right)^{(2+\sqrt{3})}$, $\left(1+\sqrt{3}\right)^{\sqrt{2}}$, ...

5. Komplexní čísla

Věta 5.1. Těleso reálných čísel lze vnořit do tělesa, ve kterém má rovnice $x^2 + 1 = 0$ řešení.

Poznámka 5.2. Důkaz je konstruktivní. Konstrukci tohoto tělesa popíšeme. Označme $\boldsymbol{C}$ kartézský součin $\boldsymbol{R} \times \boldsymbol{R}$, tzn. $\boldsymbol{C} = \boldsymbol{R} \times \boldsymbol{R} = \{[a, b]; a \in \boldsymbol{R}, b \in \boldsymbol{R}\}$. Na množině $\boldsymbol{C}$ definujme operace sčítání a násobení takto:

$$[a, b] + [c, d] = [a + c, b + d],$$

$$[a, b] \cdot [c, d] = [ac - bd, ad + bc].$$

Lze ukázat, že $(\boldsymbol{C}, +, \cdot)$ je těleso. Neutrálním prvkem vzhledem operaci sčítání je $[0, 0]$, neutrálním prvkem vzhledem operaci násobení je $[1, 0]$; opačným prvkem k prvku $[a, b]$ je

dvojice $[-a, -b]$, převráceným prvkem k prvku $[a, b]$, kde $a^2 + b^2 \neq 0$, je uspořádaná dvojice $\left[\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right]$. Platí $[0, 1] \cdot [0, 1] = [-1, 0]$, tj. $[0, 1]^2 + [1, 0] = [0, 0]$. Nechť nyní $f: \boldsymbol{R} \to \boldsymbol{C}$ je zobrazení definované pro každé reálné číslo $r \in \boldsymbol{R}$ předpisem $f(r) = [r, 0]$. Pak f je vnoření tělesa $(\boldsymbol{R}, +, \cdot)$ do tělesa $(\boldsymbol{C}, +, \cdot)$.

Definice 5.3. Těleso $(\boldsymbol{C}, +, \cdot)$ se nazývá těleso komplexních čísel.

Poznámka 5.4. Z předchozí definice plyne, že rovnice $A + X = B$ má v oboru komplexních čísel vždy jednoznačné řešení $X = B - A$ a také rovnice $A \cdot X = B$ má za podmínky $A \neq [0, 0]$ v oboru komplexních čísel vždy jednoznačné řešení $X = \frac{B}{A}$. V oboru komplexních čísel tedy lze neomezeně odčítat i dělit (kromě „dělení nulou“). Snadno lze odvodit příslušné vztahy:

$$[a, b] - [c, d] = [a - c, b - d],$$

$$\frac{[a,b]}{[c,d]} = \left[\frac{ac + bd}{c^2 + d^2}, \frac{bc - ad}{c^2 + d^2}\right], \quad [c, d] \neq 0.$$

Poznámka 5.5. Ve smyslu poznámky 5.2. lze ztotožnit každé reálné číslo r s komplexním číslem $[r, 0]$. Zápis $[0, 1]^2 + [1, 0] = [0, 0]$ tedy skutečně znamená, že rovnice $x^2 + 1 = 0$ má v množině všech komplexních čísel řešení. Tímto řešením je komplexní číslo $[0, 1]$. Toto číslo ale nemůže být reálné; zavádíme pro něj označení i a nazýváme ho komplexní jednotka. Protože z definice obou operací sčítání a násobení lze psát každé komplexní číslo $[a, b]$ ve tvaru $[a, b] = [a, 0] + [0, b] = [a, 0] + [b, 0] \cdot [0, 1]$, lze při uvedeném ztotožnění a označení psát $[a, b] = a + bi$.

Definice 5.6. Zápis $\alpha = a + bi$ se nazývá algebraický tvar komplexního čísla $\alpha = [a, b]$. Číslo a se nazývá reálná část komplexního čísla α, číslo b se nazývá imaginární část komplexního čísla α. . Je-li $a = 0$, říkáme, že číslo α je ryze imaginární. Reálná část komplexního čísla α se někdy také označuje $Re\alpha$, imaginární část komplexního čísla α se někdy také označuje $Im\alpha$.

Poznámka 5.7. Vzhledem k rovnosti $i^2 = -1$ platí pro mocniny čísla i následující vztahy:

$$i^n = i \text{ pro } n \equiv 1 \pmod 4,$$
$$i^n = -1 \text{ pro } n \equiv 2 \pmod 4,$$
$$i^n = -i \text{ pro } n \equiv 3 \pmod 4,$$
$$i^n = 1 \text{ pro } n \equiv 0 \pmod 4.$$

V algebraickém tvaru lze potom zapsat všechny čtyři základní operace takto:

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

$$(a + bi) - (c + di) = (a - c) + (b - d)i,$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i,$$

$$\frac{a + bi}{c + di} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2} i.$$

Věta 5.8. V množině všech komplexních čísel $\boldsymbol{C}$ neexistuje relace uspořádání.

Definice 5.9. Nechť $\alpha = a + bi$ je komplexní číslo. Pak komplexní číslo $\overline{\alpha} = a - bi$ se nazývá komplexně sdružené číslo k číslu α. Nezáporné reálné číslo $|\alpha| = \sqrt{a^2 + b^2}$ se nazývá absolutní hodnota komplexního čísla α.

Věta 5.10. Nechť α, β jsou komplexní čísla, pak platí:

(1) $|\alpha| = 0 \Leftrightarrow \alpha = 0$;

(2) $|-\alpha| = |\alpha|$;

(3) $|\alpha + \beta| \leq |\alpha| + |\beta|$;

(4) $|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$;

(5) $|\alpha - \beta| \geq \big||\alpha| - |\beta|\big|$;

(6) $\dfrac{|\alpha|}{|\beta|} = \left|\dfrac{\alpha}{\beta}\right|$ pro $\beta \neq 0$;

(7) $|\alpha|^2 = \alpha \cdot \overline{\alpha}$;

(8) $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$;

(9) $\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$;

(10) $Re\,\alpha = \dfrac{1}{2}(\alpha + \overline{\alpha})$, $Im\,\alpha = -\dfrac{i}{2}(\alpha - \overline{\alpha})$.

Poznámka 5.11. Víme už, že v oboru všech komplexních čísel lze provádět všechny čtyři základní operace sčítání, odčítání, násobení a dělení (kromě dělení nulou). Nyní se budeme zabývat mocninami a odmocninami komplexních čísel. K tomu ale musíme zavést vhodnější vyjádření komplexního čísla než je algebraický tvar. Znázorníme-li každé komplexní číslo $a + bi$ geometricky v tzv. Gaussově rovině, bude jeho obraz ležet v bodě s kartézskými souřadnicemi $[a, b]$. Z matematické analýzy je však známo ještě vyjádření polohy bodu pomocí polárních souřadnic. V těchto souřadnicích se kartézské průměty na osy x, y nahradí vzdáleností daného bodu od počátku soustavy souřadnic a orientovaným úhlem, který svírá průvodič spojující daný bod s počátkem soustavy souřadnic s polopřímkou vyjadřující kladný směr osy x. Např. bod $[1, 1]$ má v polárních souřadnicích vyjádření $\sqrt{2}\,(\cos 45° + \sin 45°)$, bod $[-\sqrt{3}, 1]$ má v polárních souřadnicích vyjádření $2(\cos 150° + \sin 150°)$, atd. Vyjádříme-li tímto způsobem komplexní číslo, řekneme, že jsme ho vyjádřili v goniometrickém tvaru. Komplexní číslo $\alpha = a + bi$ je tedy v goniometrickém tvaru $\alpha = r(\cos \varphi + i \sin \varphi)$. V tomto vyjádření $r = |\alpha|$ a úhel φ určíme pomocí znalostí a, b a znalostí zavedení goniometrických funkcí pomocí jednotkové kružnice.

Věta 5.12. Nechť $\alpha = r(\cos \varphi + i \sin \varphi)$, $\beta = s(\cos \psi + i \sin \psi)$, $\beta \neq 0$ jsou komplexní čísla. Pak platí:

(1) $\alpha \cdot \beta = rs(\cos(\varphi + \psi) + i \sin(\varphi + \psi))$,

(2) $\dfrac{\alpha}{\beta} = \dfrac{r}{s}(\cos(\varphi - \psi) + i \sin(\varphi - \psi))$.

Poznámka 5.13. Pro libovolné komplexní číslo existuje jeho *n*-tá mocnina. Je-li dané číslo vyjádřeno v algebraickém tvaru, lze užít binomickou větu, kde mocniny čísla *i* převádíme podle poznámky 5.7. Je-li ve tvaru goniometrickém, užijeme tzv. Moivreovu větu. Tento postup bývá početně snazší.

Věta 5.14. (Moivreova). Nechť $\alpha = r(\cos \varphi + i \sin \varphi)$ je libovolné komplexní číslo, nechť $n \in \boldsymbol{N}$. Pak platí:

$$\alpha^n = r^n(\cos n\varphi + i \sin n\varphi).$$

Poznámka 5.15. Nyní obrátíme pozornost k odmocninám komplexních čísel. Protože v oboru $\boldsymbol{C}$ neexistuje relace uspořádání, nemá smysl uvažovat o kladných či záporných komplexních číslech, a proto pro každé $n \in \boldsymbol{N}$ existuje *n*-tá odmocnina z komplexního čísla α. Označíme-li tuto odmocninu z , platí pro ni vztah $z = \sqrt[n]{\alpha}$, tedy $z^n = \alpha$. Poslední rovnice je však rovnicí binomickou, jejíž řešení je z algebry známé. Víme dokonce, že tato rovnice má *n* řešení, protože těleso komplexních čísel je algebraicky uzavřené. Existuje tedy celkem *n* odmocnin *n*-tého řádu z komplexního čísla α.

Věta 5.16. Nechť je dána binomická rovnice $z^n = \alpha$.. Číslo α vyjádříme v goniometrickém tvaru jako $\alpha = r(\cos \varphi + i \sin \varphi)$, pak řešení dané rovnice je:

$$z_k = \sqrt[n]{r}\left(\cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n}\right), \; k = 0, 1, \ldots, n-1.$$

Poznámka 5.17. Postupným konstruováním jednotlivých číselných oborů od polookruhu čísel přirozených až k tělesu komplexních čísel jsme dospěli ke struktuře, která je z algebraického hlediska „nejbohatší“. I když v $\boldsymbol{C}$ neexistuje uspořádání, lze provádět všechny čtyři základní operace (kromě dělení nulou) a pro každé komplexní číslo existuje jeho mocnina i odmocnina libovolného řádu. Těleso komplexních čísel je algebraicky uzavřené, tedy každý polynom stupně *n* má v $\boldsymbol{C}$ právě *n* kořenů (počítáme-li každý tolikrát, kolik je jeho násobnost). Proto již z praktického hlediska nemá větší význam zkoumat další možnosti rozšíření tělesa komplexních čísel. I když existuje rozšíření na těleso kvaternionů, není účelné se na tomto místě touto problematikou zabývat.

Dodatky

6. Cyklické grupy

Poznámka 6.1. V dalším textu budeme někdy (nebude-li možno dojít k nedorozumění) algebraické struktury označovat pouze symbolem jejich nosné množiny, tzn. např. místo označení grupy $(G, +)$ budeme psát pouze *G*.

Poznámka 6.2. Nechť *G* je grupa. Ze základního kurzu algebry víme, že průnik libovolného počtu podgrup grupy *G* je rovněž podgrupa grupy *G* **.**

Věta 6.3. Nechť *G* je grupa, nechť *M* je libovolná podmnožina množiny *G*. Symbolem $\langle M \rangle$ označme průnik všech podgrup v *G*, které obsahují množinu *M*. Pak $\langle M \rangle$ je nejmenší podgrupa v *G* (z hlediska její mohutnosti), obsahující množinu *M*.

Definice 6.4. Podgrupa $\langle M \rangle$ se nazývá podgrupa generovaná množinou *M*. Je-li $M = \{a\}$, pak budeme psát $\langle a \rangle$ a hovořit o podgrupě generované prvkem *a* .

Příklad 6.5. $G = \{1, 2, 3\}$, $S(G) = \{e, a, b, c, d, f\}$ je grupa všech permutací množiny *G*, kde:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Sestavíme operační tabulku grupy $(S(G), o)$, kde *o* je operace skládání permutací:

$\circ$	e	a	b	c	d
			f		
e	e	a	b	c	d
a	f				
b	a	e	d	f	b
c	c				
d	b	c	e	a	f
f	d				
	c	b	f	d	e
	a				
	d	f	a	e	c
	b				
	f	d	c	b	a
	e				

Grupa $(S(G), \circ)$ má tyto podgrupy:

$$H_1 = \{e\},\ H_2 = \{e, a\},\ H_3 = \{e, b\},\ H_4 = \{e, f\},\ H_5 = \{e, c, d\},\ H_6 = S(G).$$

Pak platí:

$$\langle e \rangle = H_1,\ \langle a \rangle = H_2,\ \langle b \rangle = H_3,\ \langle c \rangle = \langle d \rangle = H_5,\ \langle f \rangle = H_4,\ \langle \{a, b\} \rangle = H_6 .$$

Věta 6.6. Nechť *G* je grupa, nechť $a \in G$. Potom $\langle a \rangle = \{a^k;\ k \in \mathbf{Z}\}$.

Definice 6.7. Grupa *G*, která je generovaná jedním prvkem, tj. $G = \langle a \rangle$, se nazývá cyklická grupa. Prvek *a* se nazývá základní prvek cyklické grupy.

Příklad 6.8.

a) Grupa $G = \{1, -1, i, -i\}$ čtvrtých odmocnin z jedné je cyklická, základními prvky jsou buď i nebo $-i$.
b) Grupa $(\mathbf{Z}, +)$ je cyklická, základními prvky jsou buď 1 nebo -1.
c) Grupa $(\mathbf{Z}_m, +)$ je cyklická, základní prvek je C_1.

Definice 6.9. Nechť *G* je konečná grupa. Pak počet prvků této grupy se nazývá řád grupy *G* .

Věta 6.10. (Lagrange) V libovolné konečné grupě *G* je řád této grupy *G* dělitelný řádem každé její podgrupy.

Věta 6.11. Nechť $G = \langle a \rangle$ je konečná cyklická grupa řádu n (tzn. $G = \{e = a^0, a^1, a^2, ..., a^{n-1}\}$). Pak prvek a^k je základním prvkem grupy $G \Leftrightarrow NSD(k, n) = 1$.

Příklad 6.12. Grupa $(\boldsymbol{Z}_6, +)$ je cyklická grupa řádu 6, základními prvky jsou C_1 nebo C_5.

7. Faktorové struktury

Definice 7.1. Nechť $(G, \cdot)$ je grupoid. Nechť $X, Y \subseteq G$. Pak součinem množin X, Y rozumíme množinu $X \cdot Y = \{z; z = x \cdot y; x \in X, y \in Y\}$. Je-li jedna z množin X, Y jednoprvková, např. $X = \{x\}$, pak místo zápisu $\{x\} \cdot Y$ budeme psát pouze $x \cdot Y$ nebo stručně xY.

Definice 7.2. Nechť $(G, \cdot)$ je grupoid, nechť Ω je rozklad na množině G. Pak Ω nazveme vytvořující rozklad na grupoidu G, jestliže pro každé dvě třídy $X, Y \in \Omega$ existuje třída $Z \in \Omega$ s vlastností $X \cdot Y \subseteq Z$. Položíme-li $X \circ Y = Z$, pak $(\Omega, \circ)$ je grupoid, který nazýváme faktoroid grupoidu G (nebo krátce faktorgrupoid).

Příklad 7.3. a) Nechť $(G, \cdot)$ je libovolný grupoid. Pak nejhrubší rozklad $\Omega_1 = \{G\}$ i nejjemnější rozklad $\Omega = \{\{g\}; g \in G\}$ jsou vytvořující.
b) Nechť m je pevné přirozené číslo větší než dvě. Nechť $\boldsymbol{Z}_m = \{C_0, ..., C_{m-1}\}$ je rozklad množiny $\boldsymbol{Z}$ na zbytkové třídy. Pak tento rozklad je vytvořující a $(\boldsymbol{Z}_m, +)$ je faktorgrupoid grupoidu $(\boldsymbol{Z}, +)$.

Definice 7.4. Nechť $(G, \cdot)$ je grupoid, nechť $\equiv$ je relace ekvivalence na G. Pak $\equiv$ je relace kongruence na grupoidu $(G, \cdot)$, jestliže platí

$$a \equiv b \Rightarrow a \cdot c \equiv b \cdot c, \; c \cdot a \equiv c \cdot b \text{ pro libovolné } a, b, c \in G.$$

Věta 7.5. Nechť $(G, \cdot)$ je grupoid, nechť $\equiv$ je relace ekvivalence na G. Pak jsou následující výroky ekvivalentní:
(1) Relace $\equiv$ je kongruence na $(G, \cdot)$;
(2) $a \equiv b, c \equiv d \Rightarrow a \cdot c \equiv b \cdot d$ pro libovolné $a, b, c, d \in G$.

Věta 7.6. Nechť $(G, \cdot)$ je grupoid, nechť $\equiv$ je relace ekvivalence na G ,nechť Ω je rozklad na G příslušný ekvivalenci $\equiv$. Pak relace $\equiv$ je kongruence na grupoidu $(G, \cdot)$, právě když Ω je vytvořujícím rozkladem.

Věta 7.7. Nechť $(G, \cdot)$ je grupa, nechť $(H, \cdot)$ je podgrupa grupy G. Pak $\{a \cdot H; a \in G\}$, resp. $\{H \cdot a; a \in G\}$ jsou rozklady na G.

Definice 7.8. Nechť H je podgrupa grupy G. Pak rozklad $\{a \cdot H; a \in G\}$, resp. $\{H \cdot a; a \in G\}$ se nazývá levý, resp. pravý rozklad grupy G podle podgrupy H. Označení: $G/_l H$, $G/_p H$. Třída $a \cdot H$, resp. $H \cdot a$ tohoto rozkladu se nazývá levá, resp. pravá třída prvku a vzhledem k podgrupě H.

Poznámka 7.9. Z předchozího plynou následující důsledky:
1. $a \in a \cdot H, a \in H \cdot a$ (neboť $a = a \cdot e = e \cdot a, e \in H$),

2. $H \in G/_l H,\ H \in G/_p H$ (neboť $H = e \cdot H = H \cdot e$),
3. $x \in a \cdot H \Leftrightarrow x \cdot H = a \cdot H$ (tedy každá levá třída je určena libovolným svým prvkem; podobně pro pravé třídy),
4. $H \cdot H = H$.

Věta 7.10. Nechť *(G, ·)* je grupa, nechť *(H, ·)* je podgrupa grupy *G*, nechť $a, b \in G$. Pak platí:
(1) *a, b* patří do jedné třídy $G/_l H \Leftrightarrow a^{-1} \cdot b \in H$,
(2) *a, b* patří do jedné třídy $G/_p H \Leftrightarrow b \cdot a^{-1} \in H$.

Věta 7.11. Nechť *(G, ·)* je grupa, nechť *(H, ·)* je podgrupa grupy *G*, nechť $a, b \in G$ jsou libovolné prvky. Pak existují následující bijektivní zobrazení $f: a \cdot H \to H \cdot a$, $g: a \cdot H \to b \cdot H$, $h: G/_l H \to G/_p H$.

Poznámka 7.12. Třídy rozkladu jsou stejně početné vzhledem k dané grupě. Všechny třídy rozkladu (pravé i levé) jsou stejně početné vzhledem k libovolnému prvku. Počet tříd v levém i pravém rozkladu vzhledem ke stejné podgrupě je stejný.

Definice 7.13. Podgrupa *H* grupy *G* se nazývá invariantní podgrupa (někdy též normální dělitel), jestliže pro každý prvek $a \in G$ platí $a \cdot H = H \cdot a$.

Věta 7.14. Nechť *(G, ·)* je grupa, nechť *(H, ·)* je podgrupa grupy *G*. pak jsou následující výroky ekvivalentní:
(1) *H* je normální dělitel,
(2) $h \in H,\ g \in G$ libovolně $\Rightarrow\ g^{-1} \cdot h \cdot g \in H$,
(3) $g \in G$ libovolně $\Rightarrow\ g^{-1} \cdot H \cdot g = H$,
(4) $G/_l H = G/_p H$,
(5) $G/_l H,\ G/_p H$ jsou vytvořující rozklady na grupě *G*.

Poznámka 7.15. Je-li *H* je normální dělitel v grupě *G*, pak $G/_l H = G/_p H$. Proto se v tomto případě užívá pouze označení G/H. Rozklad G/H je vytvořujícím rozkladem na *G*. Poznamenejme ještě, že v komutativní grupě je každá podgrupa invariantní.

Poznámka 7.16. Z teorie cyklických grup víme, že řádem konečné grupy je počet prvků této grupy. Dále je dokazována Lagrangeova věta, podle které v konečné grupě je její řád dělitelný řádem každé její podgrupy. Odtud mj. plyne, že konečná grupa, jejíž počet prvků je prvočíslo, má pouze dvě podgrupy: triviální a sebe samu. Pro každou (konečnou) podgrupu *H* konečné grupy *G* dále platí, že počet prvků ve všech třídách rozkladů $G/_l H,\ G/_p H$ je stejný a je roven počtu prvků podgrupy *H*, a že počet tříd rozkladů $G/_l H,\ G/_p H$ je rovněž stejný.

Definice 7.17. Nechť *H* je podgrupa konečné grupy *G*. Pak systémy $G/_l H,\ G/_p H$ mají stejný počet tříd, který se nazývá index podgrupy *H* v grupě *G*.

Věta 7.18. Nechť *H* je podgrupa konečné grupy *G*. Pak řád grupy *G* je součinem řádu podgrupy *H* a indexu podgrupy *H* v grupě *G*. (Důsledkem je Lagrangeova věta.)

Věta 7.19. Nechť *(H, ·)* je invariantní podgrupa grupy *(G, ·)*. Pak faktorgrupoid $(G/H, \circ)$ je grupa. Jednotkovým prvkem této grupy je třída *H* a pro libovolné $x, y \in G$ platí:

$$(x \cdot H) \circ (y \cdot H) = (x \cdot y) \cdot H, \qquad (x \cdot H)^{-1} = x^{-1} \cdot H.$$

Definice 7.20. Nechť *(H, ·)* je invariantní podgrupa grupy *(G, ·)*. Pak faktorgrupoid *(G/H , ∘)* se nazývá faktorgrupa grupy *G* podle normální podgrupy *H*.

Věta 7.21. Všechny vytvořující rozklady na grupě jsou právě rozklady grupy vytvořené jejími invariantními podgrupami, tedy jediné faktorgrupoidy grupy jsou její faktorgrupy.

Příklad 7.22. V příkladu 6.1. byla uvedena grupa *(S(G), ∘)* permutací tříprvkové množiny a všechny její podgrupy. Uvažujme dvě z nich, a to nejprve podgrupu $H = \{e, a\}$ a potom podgrupu $K = \{e, c, d\}$. Platí:

a) $S(G)/_l H = \{\{e, a\}, \{b, c\}, \{d, f\}\}$, $S(G)/_p H = \{\{e, a\}, \{b, d\}, \{c, f\}\}$, tj. $S(G)/_l H \neq S(G)/_p H$. Podgrupa *H* není invariantní. Řád podgrupy *H* je *2*, její index je *3*.

b) $S(G)/_l K = \{\{e, c, d\}, \{a, b, f\}\}$, $S(G)/_p K = \{\{e, c, d\}, \{a, b, f\}\}$, tedy $S(G)/_l K = S(G)/_p K$. Podgrupa *K* je tedy invariantní a platí $S(G)/K = \{\{e, c, d\}, \{a, b, f\}\}$. Řád podgrupy *K* je *3*, její index je *2*. Označme nyní třídy rozkladu *S(G)/K*, např. $E = \{e, c, d\}$, $A = \{a, b, f\}$, pak faktorgrupa *(S(G)/K , ∘)* grupy *(S(G), ∘)* je určena operační tabulkou

∘	*E*	*A*
E	*E*	*A*
A	*A*	*E*

Definice 7.23. Nechť *(R , +, ·)* je okruh. Neprázdná množina $I \subseteq R$ se nazývá ideál okruhu *R*, jestliže platí:
(1) $i, j \in I \Rightarrow i - j \in I$,
(2) $i \in I, r \in R \Rightarrow i \cdot r \in I, r \cdot i \in I$.

Poznámka 7.24. Platí, že *(I , +, ·)* je podokruh okruhu *(R , +, ·)* a *(I , +)* je invariantní podgrupa grupy *(R , +)*. Rozklad *(R , +)/(I , +)* budeme značit pouze *R/I*. Poznamenejme dále, že každý okruh obsahuje dva základní ideály, a to nulový ideál $\{0_R\}$ a nevlastní ideál *R*.

Věta 7.25. Nechť *R* je okruh, *I* jeho ideál. Pak rozklad *R/I* je vytvořující rozklad na grupoidu *(R , ·)*.

Věta 7.26. Nechť *R* je okruh, *I* jeho ideál. Pak *(R/ I , +, ·)* je okruh, jehož operace jsou definovány následujícím způsobem: Nechť *a, b* jsou libovolné prvky množiny *R*. Pak platí

$$(a + I) + (b + I) = (a + b) + I, \qquad (a + I) \cdot (b + I) = (a \cdot b) + I.$$

Definice 7.27. Nechť *R* je okruh, *I* jeho ideál. Pak okruh *(R/ I , +, ·)* se nazývá faktorokruh okruhu *R* podle ideálu *I*.

Věta 7.28. Nechť *(R , +, ·)* je okruh a Ω vytvořující rozklad na grupoidech *(R , +)* i *(R , ·)*, tentýž na obou těchto grupoidech. Nechť $I \in \Omega$ je ta třída, která obsahuje 0_R. Pak *I* je ideál okruhu *R* a platí $R/I = \Omega$.

Definice 7.29. Nechť *R* je okruh, *I* jeho ideál. Řekneme, že prvky $a, b \in R$ jsou kongruentní podle ideálu *I* , jestliže platí $a - b \in I$. Píšeme $a \equiv b\ (I)$.

Věta 7.30. Nechť R je okruh, I jeho libovolný ideál. Kongruence podle ideálu I je kongruence na grupoidech $(R, +)$ i $(R, \cdot)$, rozklad příslušný této kongruenci je R/I.

Věta 7.31. Nechť $(R, +, \cdot)$ je okruh. Pak všechny kongruence na grupoidech $(R, +)$ i $(R, \cdot)$ jsou kongruencemi podle některého ideálu okruhu R. Každý faktorokruh okruhu R je tedy faktorokruhem podle některého ideálu. okruhu R.

8. Svazy a Booleovy algebry

Definice 8.1. Svazem nazýváme algebraickou strukturu $S = (S, \wedge, \vee)$ se dvěma binárními operacemi průsek ($\wedge$) a spojení ($\vee$), které splňují pro každé tři prvky $a, b, c \in S$ následující podmínky:

(1) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$, $a \vee (b \vee c) = (a \vee b) \vee c$,
(2) $a \wedge b = b \wedge a$, $a \vee b = b \vee a$,
(3) $a \wedge a = a$, $a \vee a = a$,
(4) $a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$.

Poznámka 8.2. Svaz lze také definovat jako uspořádanou množinu $(S, \leq)$, v níž pro každé dva prvky a, b existuje jejich infimum (ozn. $\wedge$) a supremum (ozn. $\vee$).

Definice 8.3. Svaz $(S, \wedge, \vee)$ se nazývá:

(1) distributivní, jestliže pro každé $a, b, c \in S$ platí $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$,
(2) modulární, jestliže pro každé $a, b, c \in S$ splňující $a \leq c$ platí $a \vee (b \wedge c) = (a \vee b) \wedge c$,
(3) komplementární, jestliže má nejmenší prvek 0 a největší prvek 1 a ke každému prvku $a \in S$ existuje jeho komplement, tj. prvek $b \in S$ s vlastností $a \vee b = 1$, $a \wedge b = 0$,
(4) booleovský, je-li distributivní a komplementární (pak jsou komplementy určeny jednoznačně),
(5) úplný, jestliže pro každou podmnožinu množiny S (i nekonečnou) existuje její supremum a infimum.

Definice 8.4. Svaz, který je úplný, distributivní a komplementární (doplňkový), se nazývá Booleova algebra.

Poznámka 8.5. Booleovu algebru je možno definovat přímo, bez využití svazové interpretace. To je obsahem následující definice.

Definice 8.6. Nechť B je neprázdná množina, na níž jsou definovány dvě binární operace $+, \cdot$ a jedna unární operace $`$ (doplněk), splňující pro každé $x, y, z \in B$ následující axiomy (symbol pro násobení $\cdot$ budeme bez újmy na srozumitelnosti často vynechávat):

(1) $x + y = y + x$, $x y = y x$
(2) $x + (y + z) = (x + y) + z$, $x(y z) = (x y) z$
(3) $x \cdot (y + z) = (x y) + (x z)$, $x + (y z) = (x + y) \cdot (x + z)$
(4) $x + 0 = x$, $x \cdot 1 = x$
(5) $x + x` = 1$, $x \cdot x` = 0$.

Pak algebraická struktura $(B, +, \cdot)$ se nazývá Booleova algebra.

Poznámka 8.7. V interpretaci Booleovy algebry pomocí svazů je operace sčítání (ozn.+) jiným označením operace spojení (ozn. $\vee$) a operace násobení (ozn. $\cdot$) jiným označením operace průsek (ozn. $\wedge$). Pro „počítání“ v Booleově algebře platí kromě axiomů z definice řada zajímavých pravidel. Některé z nich jsou obsahem následující věty:

Věta 8.8. Nechť $(B, +, \cdot)$ je Booleova algebra, nechť $x, y \in B$. Pak platí:

(1) $(x`)` = x$,

(2) $1` = 0$ , $0` = 1$,

(3) $x + x = x$, $x \cdot x = x$,

(4) $x + 1 = 1$, $x \cdot 0 = 0$,

(5) $(x + y)` = x` \cdot y`$ , $(x \cdot y)` = x` + y`$,

(6) $x + (x \cdot y) = x$, $x \cdot (x + y) = x$,

(7) $x + (x` \cdot y) = x + y$ , $x \cdot (x` + y) = x \cdot y$,

(8) $x + y = 0 \Leftrightarrow x = 0$ a $y = 0$, $x \cdot y = 1 \Leftrightarrow x = 1$ a $y = 1$,

(9) $x = y \Leftrightarrow x y` + x` y = 0$,

(10) $x = y \Leftrightarrow (x + y`) \cdot (x` + y) = 1$.

Poznámka 8.9. V Booleově algebře platí princip duality: Nechť φ je platná formule Booleovy algebry. Jestliže v této formuli nahradíme operaci sčítání násobením a naopak, operaci násobení sčítáním, a dále zaměníme prvky *0, 1,* dostaneme opět platnou formuli Booleovy algebry. Jako ilustrace může sloužit předchozí definice a věta.

Poznámka 8.10. Existují dva nejvýznamnější modely Booleovy algebry, a to množinová algebra a algebra pravdivostních hodnot výroků.

a) Množinová algebra. Nechť M je neprázdná množina. Nosičem B Booleovy algebry bude systém 2^M všech podmnožin množiny M, roli operace sčítání bude hrát operace sjednocení množin a roli operace násobení bude hrát operace průnik množin. Jako doplněk prvku Booleovy algebry bude vystupovat doplněk množiny v množině M. Prvkem *0* bude prázdná množina, prvkem *1* základní množina M.

b) Algebra pravdivostních hodnot výroků. $B = \{0, 1\}$, jako operace sčítání bude figurovat disjunkce výroků, jako násobení bude figurovat konjunkce výroků. Roli doplňku bude hrát negace výroku, prvkem *0* bude nepravdivý výrok, prvkem *1* pravdivý výrok.

V tomto smyslu lze konstatovat, že množinová algebra i algebra pravdivostních hodnot výroků mají tentýž matematický základ.

Příklad 8.11. Zjednodušte zápis množiny:

$$(A \cap E \cap C) \cup [(D \cap A)` \cup B]` \cup (E \cap C` \cap A) \cup [(B \cup D)` \cap A]` .$$

Řešení: Zadaný zápis množiny přepíšeme do Booleovy algebry. Dostaneme booleovský výraz, který upravíme:

$aec + [(da)` + b]` + ec`a + [(b + d)`a] = ae(c + c`) + dab` + b`d`a = ae + ab`(d + d`) = ae + ab` = a(e + b`)$.

Po zpětném přepisu do symboliky množinové algebry dostaneme hledané zjednodušení:

$$A \cap (E \cup B`) .$$