Západočeská univerzita v Plzni

FAKULTA PEDAGOGICKÁ

KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

KONSTRUKCE ČÍSELNÝCH OBORŮ

BAKALÁŘSKÁ PRÁCE

Magdaléna ŠŤASTNÁ

Přírodovědná studia, Matematická studia

Vedoucí práce: *Mgr. Martina KAŠPAROVÁ, Ph.D.*

Plzeň 2013

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, dne 28. 6. 2013 _____

Magdaléna Šťastná

Poděkování:

Na tomto místě bych ráda poděkovala vedoucí bakalářské práce Mgr. Martině Kašparové, Ph.D. za odborné vedení, cenné rady, připomínky a v neposlední řadě i za trpělivost a čas, který mi věnovala.

OBSAH

Úvod

Ve své bakalářské práci se věnuji konstrukci číselných oborů. Moje práce je členěna do čtyř kapitol, které se postupně věnují vzniku jednotlivých číselných oborů. V jednotlivých kapitolách je vždy prvních pár řádků věnováno obecnému popisu číselného oboru, kterého se daná kapitola týká. Moje práce je strukturována tak, aby jednotlivé číselné obory šly za sebou tak, jak je toho využíváno v jejich konstrukcích, a pokud nebude uvedeno jinak, jsou všechny věty a definice převzaty z publikací, které jsou uvedeny seznamu použité literatury.

Z hlediska historie můžeme vznik číselných oborů rozdělit do několika základních období. V prvním z nich se lidé omezovali pouze na primitivní matematiku. Číselné zprávy se před několik desítkami tisíc let uchovávaly pomocí uzlíků na provazech, oblázky, lasturami či zářezy do dřevěných holí či kostí. Vzhledem k tomu, že se jedná o způsoby, které měly za úkol v první řadě popsat počet předmětů a podávat informace o množství, vystačili si tehdy naši předkové s tím, co dnes nazýváme množinou přirozených čísel.

Již staří Egypťané používali ve svých matematických textech to, čemu říkáme egyptský zlomek. Avšak i řečtí a indičtí matematikové studovali tento typ čísel, který bychom dnes nazvali kladnými racionálními čísly. Nejznámějším dílem, kde se zlomky vyskytují, jsou Euklidovy Základy, jejichž vznik je datován zhruba do roku 300 před naším letopočtem.

Nejstarší známou zmínku o použití iracionálních čísel máme z doby mezi 800-500 lety před naším letopočtem z Indie. Avšak první důkazy o existenci iracionálních čísel souvisejí s objevem nesouměřitelných úseček ve starém Řecku. Důkaz nesouměřitelnosti strany a úhlopříčky ve čtverci nebo pětiúhelníku je připisován pythagorejcům. Říká se že Hippasus z Metapontu byl tím, kdo objevil iracionální čísla, když se snažil reprezentovat poměr mezi délkou úhlopříčky a stranou čtverce jako poměr dvou přirozených čísel.

Se zápornými čísly poprvé pracovali čínští matematikové přibližně v prvním století před naším letopočtem, kteří pomocí černě a červeně zbarvených tyčinek vyjadřovali na početní desce záporné a kladné koeficienty soustav lineárních rovnic, jejichž algoritmický způsob řešení objevili. První zmínka z Evropy byla z Řecka z 3.

století našeho letopočtu. K úplnému uznání záporných čísel došlo v evropské matematice až po objevu postupu řešení kubických rovnic v 16. století.

V historii se objevují nejprve kladná čísla, poté záporná a komplexní, později pak různé druhy hyperkomplexních čísel. Vznik jednotlivých číselných oborů můžeme popsat řadou: $\mathbb{N} \rightarrow \mathbb{Q}^{+} \rightarrow \mathbb{R}^{+} \rightarrow \mathbb{Z}^{-}, \mathbb{Q}^{-}, \mathbb{R}^{-} \rightarrow \mathbb{C}$.

Konstrukce množiny celých, resp. racionálních čísel jsou v této práci provedeny Kurošovou konstrukcí z 30. let minulého století. Reálná čísla se konstruují metodou Dedekindových řezů, které jsou pojmenovány podle Richarda Dedekinda, který na rozdíl od svých současníků, kteří zakládali konstrukci reálných čísel na nekonečných řadách, založil svou teorii na myšlence tzv. řezů[1] v racionálních číslech, které od sebe oddělují racionální a iracionální čísla.

[1] Metodou Dedekindových řezů se budeme blíže zabývat ve čtvrté kapitole.

KAPITOLA 1

Přirozená čísla

Přirozená čísla jsou, vedle některých geometrických poznatků, jedním z nejstarších matematických objektů, kterými se lidé zaobírají. Přirozená čísla vznikla hlavně jako potřeba popsat počet předmětů, nebo podat informaci o množství. Matematici se snažili několik století zpracovat axiomaticky teorii přirozených čísel. Toto se podařilo až italskému matematikovi Guiseppe Peanovi (1858 - 1932) na přelomu 19. a 20. století.

1.1 Peanovy axiomy

Peanovy axiomy jsou pojmenovány na počest italského matematika G. Peana, který jako první vytvořil axiomatizaci přirozených čísel vyhovující dnešním požadavkům na přesnost. Tyto axiomy zavádějí přirozená čísla pomocí pojmu následovník. Peanových aximomů je celkem devět (budeme značit A1-A9), kde prvních pět axiomů určuje množinu přirozených čísel a zbylé čtyři vymezí početní operace.

Předtím zavedeme značení dále používaných symbolů. Písmeny $a, b, \dots, x, y, z$ budeme značit proměnné pro přirozená čísla. Pro operaci „následovník“ použijeme symbol „′“, operaci „sčítání“ označíme „ + “. Pro operaci „násobení“ použijeme znak „ . “ a pro označení rovnosti použijeme „ = “. Dále budeme používat znaky „=“, „≠“, „∈“, „⊂“ v jejich obvyklém významu a také běžné znaky predikátového kalkulu.

Axiomy budeme formulovat následovně:

(A1) Množina $\mathbb{N}$ přirozených čísel je neprázdná.

$$(\exists\, x \in \mathbb{N})\; x = 1$$

(A2) Pokud prvek náleží množině přirozených čísel, pak do této množiny patří i jeho následovník.

$$(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})\; y = x'$$

(A3) Číslo 1 není následovník žádného prvku.

$$(\forall x \in \mathbb{N})\; x' \neq 1$$

(A4) Operace „následovník“ je bijektivní zobrazení.

$$(\forall x \in \mathbb{N})\; (\forall y \in \mathbb{N})\; x' = y' \Rightarrow x = y$$

(A5) Jestliže máme libovolnou množinu $R \subset \mathbb{N}$ takovou, že $1 \in R$, a navíc pro každé $x \in R$ také $x' \in R$, potom platí $R = \mathbb{N}$ (tento axiom nám říká, že množinu přirozených čísel tvoří právě prvek 1 a jeho následovníci).

$$\{R \subset \mathbb{N} \wedge [1 \in R \wedge ((\forall x \in R)(\exists y \in R)\ y = x')]\} \Rightarrow R = \mathbb{N}$$

Následující axiomy definují sčítání a násobení:

(A6) $(\forall x \in \mathbb{N})\ x + 1 = x'$

(A7) $(\forall x \in \mathbb{N})\ (\forall y \in \mathbb{N})\ x + y' = (x + y)'$

(A8) $(\forall x \in \mathbb{N})\ x.1 = x$

(A9) $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})\ x.y' = x.y + x$

(Podle [Bot11], str. 30.)

Na základě předchozích axiomů, můžeme nyní formulovat základní věty o sčítání a násobení přirozených čísel.

1.2 Vlastnosti operace sčítání a násobení přirozených čísel

Věta 1.2.1 (Věta o sčítání přirozených čísel):

Pro každá dvě přirozená čísla x, y, resp. pro každá tři přirozená čísla x, y, z platí, že:

I. Součet $x + y$ je jednoznačně definován.
II. $x + y = y + x$ (Věta o komutativnosti sčítání)
III. $(x + y) + z = x + (y + z)$ (Věta o asociativnosti sčítání)
IV. $x + z = y + z \Rightarrow x = z$ (Věta o krácení vzhledem ke sčítání)

Přirozená čísla $(\mathbb{N}, +)$ tvoří komutativní pologrupu s krácením vzhledem k operaci sčítání.

Věta 1.2.2 (Věta o násobení přirozených čísel):

Mějme libovolná čísla $x, y, z \in \mathbb{N}$. Potom platí, že:

I. Součin $x.y$ je jednoznačně definován.
II. $x.1 = x$ (Vlastnost jedničky-axiom A8)
III. $x.y = y.x$ (Věta o komutativnosti násobení)

IV. $x.(y.z) = (x.y).z$ (Věta o asociativnosti násobení)

V. $x.z = y.z \Rightarrow y = x$ (Věta o krácení vzhledem k násobení)

Přirozená čísla $(\mathbb{N},\cdot)$ tvoří komutativní pologrupu s krácením mající jednotkový prvek, kterým je číslo 1, tj. $(\mathbb{N},\cdot,1)$ je komutativní monoid s krácením.

Věta 1.2.3 (Věta o distributivnosti)

Mějme libovolná čísla $x, y, z \in \mathbb{N}$. Potom platí, že:

I. $x.(y+z) = x.y + x.z$ (Věta o distributivnosti zleva)

II. $(y+z).x = y.x + z.x$ (Věta o distributivnosti zprava)

Přirozená čísla $(\mathbb{N},+,\cdot)$ tvoří komutativní polookruh s jednotkovým prvkem.

Příklad 1.2.1

Je-li dáno mn čísel a_{ij}, kde $1 \leq i \leq m, 1 \leq j \leq n$, z oboru, v němž platí zákony asociativní a komutativní, a označíme-li

$$\sum_{j=1}^{n} a_{1j} = b_1, \sum_{j=1}^{n} a_{2j} = b_2, \ldots, \sum_{j=1}^{n} a_{mj} = b_m,$$

$$\sum_{i=1}^{m} a_{i1} = c_1, \sum_{i=1}^{m} a_{i2} = c_2, \ldots, \sum_{i=1}^{m} a_{in} = c_n,$$

pak

$$\sum_{i=1}^{m} b_i = \sum_{j=1}^{n} c_j$$

Dokažte!

(Převzato z [Hru53], str. 107/68.)

Daná čísla a_{ij} si lze představit jako prvky matice typu *m* x *n*.

$$\begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \ldots & a_{m.n} \end{pmatrix}$$

Součty b_i jsou součty čísel v *i*-tém řádku a c_j součty čísel v *j*-tém sloupci matice. Zadání úlohy pak můžeme interpretovat jako důkaz toho, že součet prvků v matici je stejný, ať sčítáme prvky po řádcích nebo po sloupcích.

$$\sum_{i=1}^{m} b_i = b_1 + b_2 + \cdots + b_m = \sum_{j=1}^{n} a_{1j} + \sum_{j=1}^{n} a_{2j} + \cdots + \sum_{j=1}^{n} a_{mj} =$$

$$= (a_{11} + a_{12} + \cdots + a_{1n}) + (a_{21} + a_{22} + \cdots + a_{2n}) + \cdots + (a_{m1} + a_{m2} + \cdots + a_{mn})$$

Sčítání přirozených čísel je komutativní a asociativní, proto lze postupným užitím těchto vlastností prvky $a_{21}, a_{31}, \ldots, a_{m1}$ „přemístit“ k prvku a_{11}, podobně čísla $a_{22}, a_{32}, \ldots, a_{m2}$ k členu a_{12} atd. až $a_{2n}, a_{3n}, \ldots, a_{mn}$ k členu a_{1n}. Je tedy

$$\sum_{i=1}^{m} b_i = (a_{11} + a_{21} + \cdots + a_{m1}) + (a_{12} + a_{22} + \cdots + a_{m2}) + \cdots +$$

$$+(a_{1n} + a_{2n} + \cdots + a_{mn}) =$$

$$= \sum_{i=1}^{m} a_{i1} + \sum_{i=1}^{m} a_{i2} + \cdots + \sum_{i=1}^{m} a_{in} = c_1 + c_2 + \cdots + c_n = \sum_{j=1}^{n} c_j$$

1.3 Uspořádání přirozených čísel

V této kapitole budeme definovat uspořádání množiny přirozených čísel. Dále si zde ukážeme také některé jeho vlastnosti. Začneme definicí relace být ostře menší a být menší nebo roven.

Pozn. Připomeňme, že relací *R* rozumíme libovolnou podmnožinu kartézského součinu množin. V našem případě budeme relací rozumět binární relaci na nějaké množině $\mathbb{A}$, tj. nějakou podmnožinu množiny všech uspořádaných dvojic $\langle x, y\rangle \in \mathbb{A} \times \mathbb{A} = \{\langle x, y\rangle; x \in \mathbb{A} \wedge y \in \mathbb{A}\}$

Definice 1.3.1 (Relace být ostře menší)

$$(\forall x, y \in \mathbb{N})\ x < y \iff (\exists n \in \mathbb{N}) x + n = y$$

Říkáme, že přirozené číslo x je ostře menší než přirozené číslo y (značíme $x < y$), právě tehdy když existuje přirozené číslo n takové, že $x + n = y$.

Definice 1.3.2 (Relace být menší nebo roven)

Říkáme, že přirozené číslo x je menší nebo rovno přirozenému číslu y (značíme $x \leq y$), právě tehdy když $x < y$ nebo $x = y$.

Analogicky můžeme definovat pojem být ostře větší a být větší nebo roven:

Definice 1.3.3 (Relace být ostře větší)

$$(\forall x, y \in \mathbb{N})\ x > y \iff (\exists n \in \mathbb{N}) x = y + n$$

Říkáme, že přirozené číslo x je ostře větší než přirozené číslo y (značíme $x > y$), právě tehdy když existuje přirozené číslo n takové, že $x = y + n$.

Definice 1.3.4 (Relace být větší nebo roven)

Říkáme, že přirozené číslo x je větší nebo rovno přirozenému číslu y (značíme $x \geq y$), právě tehdy když $x > y$ nebo $x = y$.

Než budeme moci uvést další definice, připomeneme několik dalších pojmů:

Definice 1.3.5 (relace reflexivní, antireflexivní)

Relace R je reflexivní, jestliže pro libovolné $a \in \mathbb{A}$, platí $\langle a, a\rangle \in R$.

Relace R je antireflexivní, jestliže pro libovolné $a \in \mathbb{A}$, platí $\langle a, a\rangle \notin R$.

Definice 1.3.6 (relace symetrická, antisymetrická, silně antisymetrická)

Relace R je symetrická, jestliže $\forall a, b \in \mathbb{A}\ \langle a, b\rangle \in R \Rightarrow \langle b, a\rangle \in R$.

Relace R je antisymetrická, jestliže $\forall a, b \in \mathbb{A}\ \langle a, b\rangle \in R\ , \langle b, a\rangle \in R \Rightarrow a = b$.

Relace R je silně antisymetrická, jestliže $\forall a, b \in \mathbb{A}\ \langle a, b\rangle \in R \Rightarrow\ \langle b, a\rangle \notin R$.

Definice 1.3.7 (relace tranzitivní)

Relace je tranzitivní, jestliže $\forall a, b, c \in \mathbb{A}\ \langle a, b\rangle \in R\ \wedge \langle b, c\rangle \in R \Rightarrow \langle a, c\rangle \in R$.

Definice 1.3.8 (relace ekvivalence)

Relaci, která je reflexivní, symetrická a tranzitivní nazveme relací ekvivalence.

Definice 1.3.9 (relace uspořádání, uspořádaná množina)

Uspořádáním na množině rozumíme binární relaci na množině, která je reflexivní, antisymetrická a tranzitivní. Množinu spolu s relací nazveme uspořádanou množinou. Uspořádání dané relací $\leq$, resp. $\geq$ budeme nazývat přirozené uspořádání.

Věta 1.3.1 (Vlastnosti uspořádání)

Ostré uspořádání $(<, >)$ na množině přirozených čísel $\mathbb{N}$ je antireflexivní, silně antisymetrické a tranzitivní. Přirozené uspořádání $(\leq, \geq)$ na množině přirozených čísel $\mathbb{N}$ je relací reflexivní, antisymetrickou a tranzitivní.

Věta 1.3.2 (Monotonie uspořádání)

Relace ostrého i přirozeného uspořádání jsou monotónní vůči sčítání i násobení, tj.

$$(\forall x, y, z \in \mathbb{N})\ x < y \Longrightarrow x + z < y + z$$

(přičítání stejného čísla k oběma stranám nerovnosti) a

$$(\forall x, y, z \in \mathbb{N})\ x < y \Longrightarrow x.z < y.z$$

(násobení obou stran nerovnosti stejným číslem), resp.

$$(\forall x, y, z \in \mathbb{N})\ x \leq y \Longrightarrow x + z \leq y + z \text{ a } x \leq y \Longrightarrow x.z \leq y.z$$

Věta 1.3.3 (Trichotomičnost relace)

Relace ostrého uspořádání na množině přirozených čísel $\mathbb{N}$ je trichotomická,

tj. platí pro libovolná čísla $x, y \in \mathbb{N}$ právě jedna z možností $x < y \vee x = y \vee x > y$.

Důsledek věty 1.3.3:

Přirozené uspořádání $\leq$ na množině $\mathbb{N}$ je lineární.

1.4 Matematická indukce a dobře uspořádaná množina

Matematická indukce je, jako velice důležitá charakteristika přirozených čísel, díky svému principu výborným způsobem, jak dokázat nějaké tvrzení. Při důkazu matematickou indukcí dokazujeme, že (1) vlastnost platí pro nějaké malé přirozené číslo, pro nějž má vlastnost smysl, (2) platí-li nějaká vlastnost pro n-tý prvek, platí tato vlastnost i pro prvek $n + 1$. Aplikujeme-li tento postup na důkaz tvrzení, že lze sečíst

libovolné konečné množství čísel. Zjistíme, že jedno číslo lze sečíst, tj. platí (1). Dále že jde sečíst i n čísel. Jejich součet označme a a nechť $(n+1)$-ní číslo je b. Součet $n+1$ čísel je podle předchozí formulace $a+b$. Podle principu matematické indukce, lze sečíst i $n+1$ prvků. Avšak z tohoto principu plyne, že lze sečíst libovolné, ale konečné, množství prvků. Princip matematické indukce je využíván nejen při dokazování, ale také při tvorbě definic.

Definice 1.4.1 (dobře uspořádaná množina)

Řekneme, že uspořádaná množina $(M, \leq)$je dobře uspořádanou množinou, jestliže každá její neprázdná podmnožina $R \subseteq M$ má nejmenší prvek, tj. existuje $1_R \in R$ takové, že $1_R \leq x$ pro každé $x \in R$.

Věta 1.4.1

Množina přirozených čísel $\mathbb{N}$ spolu s přirozeným uspořádáním $\leq$, $(\mathbb{N}, \leq)$, je dobře uspořádaná.

Základní vlastnosti dobře uspořádaných množin:

I. V každé podmnožině dobře uspořádané množiny existuje nejmenší prvek.

II. Každá lineárně uspořádaná konečná množina je dobře uspořádaná.

KAPITOLA 2

Celá čísla

Celá čísla jsou množina, která obsahuje přirozená čísla, nulu a záporná čísla. Tuto množinu v matematice označujeme $\mathbb{Z}$ podle německého Zahlen (čísla). Celá čísla tvoří nekonečnou, ale spočetnou množinu.

Množina celých čísel $\mathbb{Z}$ je uzavřená vzhledem k operaci sčítání a násobení, tedy součet dvou celých čísel je opět celé číslo a podobně i násobení dvou celých čísel získáme také celé číslo. Navíc množina celých čísel je uzavřená i pro operaci odčítání, na rozdíl od množiny přirozených čísel. Tato množina ovšem není uzavřena vzhledem k operaci dělení, neboť podíl dvou celých čísel už celé číslo být nemusí.

2.1 Celá čísla jako dvojice přirozených čísel

Vyjdeme z množiny přirozených čísel $\mathbb{N}$, jejíž prvky budeme označovat malými písmeny. Pro prvky z množiny celých čísel $\mathbb{Z}$ budeme používat označení velkými písmeny, tj. $A, B, \dots, X, Y, Z$. Pro operace s celými čísly budeme používat znaky zavedené v kapitole 1.1. Z prvků množiny přirozených čísel $\mathbb{N}$ budeme tvořit uspořádané dvojice. Pokud a_1, a_2 jsou dvě čísla z množiny $\mathbb{N}$, budeme tuto dvojici označovat $[a_1, a_2] = A$. Čísla a_1, a_2 v symbolu $[a_1, a_2]$ budeme nazývat složky celého čísla. Celé číslo je jednoznačně určeno svými dvěma složkami, ale daným celým číslem nejsou jeho složky jednoznačně určeny. Například celé číslo 2 je jednoznačně určeno dvojicí $[3,1]$, ale také $[5,3]$ určuje celé číslo 2, takže číslo 2 neurčuje složky jednoznačně.

Zavedení celého čísla jako uspořádané dvojice přirozených čísel zdůvodníme v kapitole 2.4.

Definice 2.1.1

Uspořádané dvojice čísel z množiny přirozených čísel $\mathbb{N}$ nazýváme celými čísly, jestliže jsou pro ně definovány vztahy „rovná se“, „menší než“, „větší než“ a početní výkony zvané sčítání a násobení takto:

$$A = B \text{ právě tehdy, když } a_1 + b_2 = a_2 + b_1$$
$$A < B \text{ právě tehdy, když } a_1 + b_2 < a_2 + b_1$$
$$A > B \text{ právě tehdy, když } a_1 + b_2 > a_2 + b_1$$
$$A + B = [a_1 + b_1, a_2 + b_2]$$
$$A.B = [a_1.b_1 + a_2.b_2, a_1.b_2 + a_2 b_1]$$

(Podle [Hru53] str. 155)

Věta 2.1.1 (Různé tvary téhož celého čísla)

Každé celé číslo lze psát v různých tvarech. Je-li $[a_1, a_2]$ jeden tvar celého čísla, je $[a_1 + x, a_2 + x]$, kde x je libovolné přirozené číslo, jiný tvar téhož celého čísla.

Věta 2.1.2 (Vlastnosti vztahu „rovná se“)

Vztah „rovná se“ definovaný mezi celými čísly (viz definice 2.1.1), je relací ekvivalence, tj.

$\forall A \in \mathbb{Z}$ $A = A$

$\forall A, B \in \mathbb{Z}$ $A = B \Rightarrow B = A$

$\forall A, B, C \in \mathbb{Z}$ $A = B \wedge B = C \Rightarrow A = C$

Důkaz vlastnosti $A = A$:

Podle vztahu $A = B$ právě tehdy, když $[a_1, a_2] = [b_1, b_2]$, který jsme uvedli v definici 2.1.1, můžeme psát: $a_1 + b_2 = a_2 + b_1$. Tento vztah je podle komutativního zákona možné upravit na $a_1 + b_2 = b_1 + a_2$. Pokud je

$a_1 = b_1$ a $a_2 = b_2$, pak předchozí rovnost platí a zřejmě $A = A$.

Jestliže $b_1 = a_1 + x$ a $b_2 = a_2 + x$, pak je rovnost $a_1 + b_2 = b_1 + a_2$ také splněna a $[b_1, b_2]$ je jen jiný tvar celého čísla $[a_1, a_2]$ a opět $A = A$.

(Podle [Hru53], str. 156)

Věta 2.1.3

Vztahy „menší než“ a „větší než“, které jsou definované mezi celými čísly (viz definice 2.1.1) mají tyto vlastnosti:

Je-li $A > B$, je $B < A$. (antireflexivita)

Jsou-li A, B dvě libovolná celá čísla, platí mezi nimi právě jeden ze vztahů:

$A = B$, $A < B$, A$> B$. (Trichotomičnost)

Je-li $A < B$a $B < C$, je $A < C$ (Tranzitivita)

Věta 2.1.4

Vztahy „menší než“ a „větší než“, které jsou definované mezi celými čísly (viz definice2.1.1) nezávisí výběru reprezentanta.

Příklad 2.1.1

Dvojice [1, 2] a [6, 7] určují totéž celé číslo A, podobně dvojice [3, 1] a [6, 4] představují stejné číslo B. Ukažte, že vztah mezi čísly A, B nezávisí na jejich reprezentantech.

Nyní porovnáme čísla $A,\ B$. Připomeňme, viz definice 2.1.1, že $A < B \Leftrightarrow a_1 + b_2 < a_2 + b_1$

Nyní si zvolíme reprezentanty čísel A, B podle zadání. V prvním případě porovnáme čísla A, B, pro reprezentanty $A = [1,2], B = [3,1]$. Vzhledem k tomu, že $a_1 + b_2 = 1 + 1 = 2$ je menší než $5 = 2 + 3 = a_2 + b_1$, je $A < B$.

Ve druhém případě použijeme následující tvary $A = [6,7], B = [6,4]$. Postup je stejný jako v prvním případě: $a_1 + b_2 = 6 + 4 = 10 < 13 = 7 + 6 = a_2 + b_1$. Opět platí, že $A < B$.

2.2 Vlastnosti operace sčítání a násobení celých čísel

2.2.1 Sčítání celých čísel

Množina celých čísel $\mathbb{Z}$ má, na rozdíl od množiny přirozených čísel $\mathbb{N}$, jednu důležitou vlastnost. Zvolíme-li si dvě celá čísla, existuje nějaké jiné celé číslo, které nazýváme rozdíl dvou celých čísel. Tuto vlastnost můžeme vyjádřit větou:

Věta 2.2.1.1

Jsou-li A, B dvě libovolná celá čísla, vždy existuje jediné celé číslo X tak, že

$$A + X = B$$

Definice 2.2.1.1 (Rozdíl celých čísel)

Jsou-li dána celá čísla A, B, pak celé číslo X, pro které platí $A + X = B$, se nazývá rozdíl čísel B, A. Píšeme:

$$X = B - A$$

Definice 2.2.1.2 (Číslo opačné)

Celá čísla $[a_1, a_2], [a_2, a_1]$ se nazývají čísla opačná. Přechod od čísla původního k číslu opačnému se jmenuje změna znaménka. Opačné číslo $[a_2, a_1]$ k číslu $A = [a_1, a_2]$ zapisujeme

$$\boldsymbol{A} = -A$$

Věta 2.2.1.2 (Odčítání celých čísel)

Odečítat číslo A je totéž jako přičítat opačné číslo $\boldsymbol{A}$.

Na základě této věty není nutné v oboru celých čísel zavádět odčítání jako zvláštní početní úkon, neboť podle ní lze každé odčítání převést na sčítání.

Věta 2.2.1.3

Opačným číslem k opačnému číslu je původní číslo.

Abychom mohli vyslovit nejdůležitější vlastnosti sčítání, je nyní vhodné zavést označení pro význačný prvek množiny celých čísel, kterým je nula.

Věta 2.2.1.4 (Číslo opačné samo k sobě)

V množině celých čísel $\mathbb{Z}$ existuje jediné číslo, které je samo k sobě opačné. Toto číslo je tvaru $[x, x]$, kde x je přirozené číslo.

Definice 2.2.1.3 (Číslo nula)

Celé číslo tvaru $[x, x]$ nazveme nula, značit ho budeme 0.

Věta 2.2.1.5 (Vlastnosti sčítání celých čísel)

Sčítání celých čísel, definované mezi celými čísly (viz definice 2.1.1), se řídí zákonem komutativním a asociativním, tj. pro všechna celá čísla A, B, C platí :

$$A + B = B + A \qquad \text{(komutativnita)}$$

$$A + (B + C) = (A + B) + C \qquad \text{(asociativita)}$$

Dále pro sčítání celých čísel platí vlastnosti:

$$A + C = B + C \Rightarrow A = B$$

$$A + 0 = A - 0 = A$$

$$A + \boldsymbol{A} = 0$$

Věta 2.2.1.6 (Jednoznačnost sčítání celých čísel)

Součet dvou celých čísel nezávisí na tvaru sčítanců, neboli součtem dvou celých čísel je opět celé číslo, které je oběma sčítanci jednoznačně určeno, neboť stejní sčítanci v různých tvarech dávají týž součet.

Příklad 2.2.1.1:

Zvolte různé tvary nějakých celých čísel A a B a ukažte, že je jejich součet určen jednoznačně, tj. nezávisí na reprezentantech sčítanců.

Zvolíme si dvě celá čísla $A = [8,5], B = [4,2]$:

$$A + B = [8 + 4,5 + 2] = [12,7] = C$$

Nyní zvolme jiné tvary stejných celých čísel $A = [13,10], B = [5,3]$

$$A + B = [13 + 5,10 + 3] = [18,13] = D$$

Zbývá ukázat, že dvojice [12, 7] a [18, 13] jsou různé tvary stejného celého čísla, a tedy *C* = *D*. Podle definice 2.1.1 rovnosti dvou celých čísel by muselo platit, že $18 + 7$ je rovno $13 + 12$. Zřejmě $25 = 25$ a proto $[18,13] = [12,7]$, tj. $C = D$.

Věta 2.2.1.7 (Monotonie sčítání celých čísel)

Sčítání celých čísel se řídí zákonem monotonie, tj. pro každá tři celá čísla A, B, C platí:

$$\text{Je-li } A < B, \text{ je } A + C < B + C.$$

Jelikož sčítání celých čísel se řídí zákonem komutativním, asociativním a má neutrální a inverzní prvek, tak celá čísla $(\mathbb{Z}, +)$ tvoří komutativní grupu,

2.2.2 Násobení celých čísel

Číslo 1 je význačným prvkem množiny přirozených čísel, uveďme jeho celočíselnou podobu, tj. definujme celé číslo 1 jako dvojici přirozených čísel.

Definice 2.2.2.1 (Číslo jedna)

Celé číslo tvaru $[x+1, x]$ nazveme jedna a označíme 1.

Věta 2.2.2.1

Násobení celých čísel (viz definice 2.1.1) se řídí zákonem komutativním a asociativním, tj. pro všechna celá čísla A, B, C platí:

$$A.B = B.A$$

$$A.(B.C) = (A.B).C$$

Dále pro násobení celých čísel platí následující pravidla:

$$A.C = B.C \Rightarrow A = B$$

$$A.1 = A$$

$$A.0 = 0$$

Je-li $A.B = 0$, je buď $A = 0$, nebo $B = 0$.

Násobení celých čísel je operací s krácením, neutrálním a agresivním prvkem, navíc v něm dle poslední vlastnosti nejsou dělitelé nuly.

Věta 2.2.2.2 (Jednoznačnost násobení)

Součin dvou celých čísel nezávisí na tvaru činitelů, neboli součinem dvou celých čísel je opět celé číslo, které je danými činiteli jednoznačně určeno, neboť stejní činitelé v různých tvarech dávají týž součin.

Příklad 2.2.2.1

Zvolíme si dvě celá čísla $A = [5,2], B = [7,3]$.

$$A.B = [5.7 + 2.3, 5.3 + 2.7] = [41,29] = C$$

Zvolíme jiné dva reprezentanty čísel A, B tak, že $A = [4,1], B = [5,1]$.

$$A.B = [4.5 + 1.1, 4.1 + 1.5] = [21,9] = D$$

Podle definice 2.1.1 rovnosti dvou celých čísel platí $[21,9] = [41,29]$ právě tehdy, když $21 + 29$ je rovno $9 + 41$. Pokud čísla sečteme, získáme vztah $50 = 50$. Z této rovnosti vyplývá, že $C = D$.

Věta 2.2.2.3 (Změna znaménka)

Změní-li se znamení některého činitele, změní se znaménko součinu.

Důsledek:

Změní-li se znaménko obou činitelů, součin se nezmění.

Protože násobení celých čísel se řídí komutativním a asociativním zákonem, má neutrální prvek, ale nemá prvek inverzní, tvoří celá čísla $(\mathbb{Z},\cdot)$ komutativní pologrupu s jednotkovým prvkem, kterým je číslo 1.

Věta 2.2.2.4 (Distributivní zákon)

Sčítání a násobení celých čísel se řídí zákonem distributivním, tj. pro každá tři celá čísla A, B, C platí:

$$A.(B + C) = A.B + A.C$$

Celá čísla $(\mathbb{Z}, +,\cdot)$ tvoří komutativní okruh, protože struktura $(\mathbb{Z}, +)$ je komutativní grupou, struktura $(\mathbb{Z},\cdot)$ tvoří komutativní pologrupu a mezi operacemi sčítání a násobení platí distributivní zákon. O struktuře celých čísel $(\mathbb{Z}, +,\cdot)$ říkáme, že tvoří komutativní obor integrity, neboť celá čísla $(\mathbb{Z}, +,\cdot)$ tvoří komutativní okruh, ve kterém nemáme netriviální dělitele nuly. Tato struktura není tělesem, protože pro operaci násobení $\mathbb{Z} - \{0\}$ nemáme inverzní prvek.

2.3 Uspořádání celých čísel

Definice 2.3.1 (Číslo kladné, nekladné, záporné a nezáporné)

Číslo A, pro které platí $A > 0$, se nazývá kladné. Číslo A, pro které platí $A < 0$, se nazývá záporné. Číslo A, pro které platí $A \geq 0$, se nazývá nezáporné. Číslo A, pro které platí $A \leq 0$, se nazývá nekladné.

Věta 2.3.1 (Opačné číslo)

Číslo A je kladné tehdy a jen tehdy, když $a_1 > a_2$. Číslo A je záporné tehdy a jen tehdy, když $a_1 < a_2$.

Důsledek:

Jsou-li dvě opačná čísla navzájem různá, je jedno kladné a druhé záporné.

Změnou znaménka se z kladného čísla stane číslo záporné a naopak. Proto o dvou číslech, z nichž jedno je kladné a druhé záporné říkáme, že mají opačná znaménka.

Věta 2.3.2

Součin dvou kladných čísel je kladný. Součin dvou čísel, z nichž jedno je záporné a druhé kladné, je záporný. Součin dvou záporných čísel je kladný.

Důkaz:

Je-li $A > 0$ a $B > 0$, je podle věty 2.3.1 $a_1 > a_2, b_1 > b_2$. Pak existuje číslo y takové, že $b_1 = b_2 + y$. Z nerovnosti $a_1 > a_2$ plyne, že $a_1.y > a_2.y$ a odtud $a_1.b_2 + a_1.y + a_2.b_2 > a_1.b_2 + a_2.b_2 + a_2.y$. Dále $a_1.(b_2 + y) + a_2.b_2 > a_1.b_2 + a_2.(b_2 + y) \Rightarrow a_1.b_1 + a_2.b_2 > a_1.b_2 + a_2.b_1$. To podle věty 2.3.1 znamená, že $A.B > 0$, tedy že součin $A.B$ je kladný.

(Podle [Hru53], str.165)

Změna znaménka u některého z kladných činitelů má podle důsledku věty 2.3.1 za následek, že tento činitel se stane záporným. Podle věty 2.2.2.3 se tím změní také znaménko součinu, který se stane záporným.

Změna znaménka u obou činitelů podle důsledku věty 2.2.2.3 nemá na znaménko součinu vliv.

Věta 2.3.3

Jsou-li A, B dvě celá čísla taková, že $A < B$, a je-li C kladné celé číslo, pak $A.C < B.C$. Naproti tomu, je-li C záporné celé číslo, pak $A.C > B.C$.

Věta 2.3.4

Přirozeně uspořádaná množina přirozených čísel je uspořádána podobně jako přirozeně uspořádaná množina celých kladných čísel. Při tom slovy přirozeně uspořádaná množina rozumíme uspořádanou množinu jednak přirozených čísel, v níž $m \prec n$ značí totéž jako $m < n$, a jednak celých kladných čísel, v níž $A \prec B$, značí totéž jako $A < B$.

Zavedením dvojic přirozených čísel a vhodnými definicemi rovnosti, nerovností a početních operací sčítání a násobení jsme získali nový číselný obor, jehož prvky se nazývají celá čísla. V tomto oboru lze provádět operaci odčítání bez jakéhokoli omezení. Tento obor je sjednocením tří disjunktních množin:

a) Množina celých kladných čísel, kterou můžeme ztotožnit s množinou čísel přirozených.
b) Jednoprvková množina obsahující nulu.
c) Množina celých záporných čísel.

V následujícím textu se budeme podrobněji věnovat tomu, proč jsme celá čísla zavedli jako dvojice přirozených čísel, jak jsme přislíbili na začátku této kapitoly.

2.4 Vnoření komutativní pologrupy do grupy

2.4.1 Faktorizace pologrupy

Ke konstrukci grupy z pologrupy potřebujeme zavést postup rozkladu množiny na třídy podle nějaké ekvivalence neboli faktorizaci množiny na třídy. Konstrukci faktorizace užíváme jak u množin, tak i u celých algebraických struktur, nás však teď budou zajímat hlavně grupy.

Použijeme faktorizaci na množině $\mathbb{Z}$ spolu s operacemi sčítání a násobení. Řekněme, že dvě celá čísla jsou ekvivalentní, pokud dávají stejný zbytek po dělení dvěma. Platí, že navzájem jsou ekvivalentní všechna sudá a také všechna lichá čísla. Takto vzniklá faktorová množina má dva prvky, množinu všech sudých a všech lichých čísel. Ze sčítání a násobení celých čísel můžeme odvodit operace sčítání a násobení na faktorové množině. Označíme-li 0 nějakého reprezentanta všech sudých čísel a 1 reprezentanta množiny všech lichých čísel, lze na faktorové množině definovat součet $0 \oplus 0 = 0,\ 1 \oplus 0 = 0 \oplus 1 = 1,\ 1 \oplus 1 = 0$.

Ke konstrukci grupy z pologrupy, v našem případě $(\mathbb{Z}, +)$ z $(\mathbb{N}, +)$, potřebujeme definovat binární operaci tak, aby splňovala axiomy grupy. Relace ekvivalence, kterou později použijeme k rozkladu kartézského součinu $\mathbb{N} \times \mathbb{N}$ nosné množiny $(\mathbb{N}, +)$, musí zachovávat binární operaci pologrupy.

Abychom toto mohli realizovat, musí daná relace být nejen relací ekvivalence, ale musí mít též další „dobrou vlastnost". Proto zavedeme následující definici.

Definice 2.4.1.1 (Kongruence pologrupy)

Mějme libovolnou pologrupu $\boldsymbol{G}$ = (G,·) . Potom relaci ekvivalence ~ na množině G nazveme kongruencí pologrupy $\boldsymbol{G}$, jestliže pro libovolné prvky $x_1, x_2, y_1, y_2 \in$ G platí: Pokud $x_1 \sim y_1$ a současně $x_2 \sim y_2$, potom také $x_1 \cdot x_2 \sim y_1 \cdot y_2$. Říkáme, že relace~ je kompatibilní s operací · nebo alternativně, že ~ zachovává operaci ·.

Věta 2.4.1.1 (Kongruenace pologrupy)

Mějme libovolnou pologrupu $\boldsymbol{G}$ = (G,·) a na ní kongruenci ~ . Potom lze na množině G/~ zavést operaci · tak, že pro libovolné $[x]\sim, [y]\sim \in G/\sim$ platí, že $[x]\sim \cdot [y]\sim = [x.y]\sim$ a navíc algebraická struktura $\boldsymbol{G}$/~=(G/~,·) je opět pologrupa.

2.4.2 Věta o vnoření komutativní pologrupy do grupy

V následujících řádcích budeme zjišťovat, za jakých podmínek můžeme do pologrupy přidat další prvky s odpovídajícím výsledky operace tak, abychom získali grupu, neboli kdy lze komutativní pologrupu rozšířit na grupu. Postupovat budeme tak, že nejprve sestrojíme grupu a po tom do ní pologrupu vnoříme.

Definice 2.4.2.1 (Vnoření pologrupy G do pologrupy H)

Jestliže máme dvě pologrupy G= (G, *) a H= (H, ∘). Pak zobrazení $f: G \to H$, které splňuje podmínku, že pro libovolné prvky $x, y \in G$ platí

$f(x * y) = f(x) \circ f(y)$,

nazýváme homomorfismem. Jestliže je navíc zobrazení injektivní, nazýváme ho vnořením.

Ve skutečnosti vnoření jedné pologrupy do druhé koresponduje s postupem rozšíření jedné pologrupy na druhou.

Věta 2.4.2.1 (Vnoření komutativní pologrupy do grupy)

Komutativní pologrupu $\boldsymbol{G} = (G,\cdot)$, lze vnořit do grupy tehdy a jen tehdy, platí-li v ní pravidlo krácení, tj.

$$\forall x, y, z \in \boldsymbol{G} \qquad x \cdot \mathrm{y} = \mathrm{y} \cdot \mathrm{z} \Rightarrow \mathrm{x} = \mathrm{z}$$

Nyní se nám naskytuje otázka, zda je možné komutativní pologrupu z předchozí věty rozšířit na komutativní grupu, přesněji řečeno, zda lze komutativní grupu vnořit do komutativní grupy i jinak, než postupným přidáváním prvků do pologrupy.

Věta 2.4.2.2:

Jestliže lze komutativní pologrupu $\boldsymbol{G} = (G,\cdot)$, vnořit do grupy H, potom také podílovou (faktorovou) grupu $GxG/\sim$ lze vnořit do grupy H.

Tato věta nám ukazuje, že se v jistém smyslu jedná o nejefektivnější způsob rozšíření. Přesněji, jestliže komutativní pologrupu $\boldsymbol{G}$ lze rozšířit na komutativní grupu H, potom i podílovou grupu $GxG/\sim$ lze vnořit do grupy H. Tedy grupa H podílovou grupu obsahuje. Vše dohromady lze interpretovat tak, že podílová grupa je nejmenší komutativní grupa, která obsahuje naši původní pologrupu.

Na závěr této kapitoly zdůvodníme konkrétní zavedení celých čísel jako dvojic přirozených čísel.

Relace „=“ mezi celými čísly A, B, definovaná v definici 2.1.1, je kongruence.

Důkaz:

Podle věty 2.1.2 je to relace ekvivalence.

$A = B \qquad\qquad C = D$

$[a_1, a_2] = [b_1, b_2] \qquad [c_1, c_2] = [d_1, d_2]$

Složky celých čísel $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2$ jsou přirozená čísla.

Z definice 2.1.1plyne:

$A = B$, tj. $[a_1, a_2] = [b_1, b_2] \Leftrightarrow a_1 + b_2 = b_1 + a_2$

$C = D$, tj. $[c_1, c_2] = [d_1, d_2] \Leftrightarrow c_1 + d_2 = d_1 + c_2$

Sečtením obou rovností získáme

$(a_1 + b_2) + (c_1 + d_2) = (b_1 + a_2) + (d_1 + c_2)$, po úpravě:

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

Z definice 2.1.1 plyne

$[a_1 + c_1, a_2 + c_2] = [b_1 + d_1, b_2 + d_2] \Leftrightarrow A + C = B + D$

Tímto jsme ukázali, že relace „=“ je kompatibilní s operací sčítání. Je-li kompatibilní a je-li ekvivalencí, pak je to podle definice 2.4.1.1 kongruencí. Nyní je jasné, že relace „=“ definovaná mezi dvojicemi přirozených čísel je kongruence, takže $(\mathbb{N}, +) \times (\mathbb{N}, +) /=$ je grupa, kterou lze ztotožnit se $(\mathbb{Z}, +)$, což zapíšeme vztahem $(\mathbb{N}, +) \times (\mathbb{N}, +) /= \cong (\mathbb{Z}, +)$.

Nyní si popíšeme homomorfismus f, pomocí něhož vnoříme komutativní pologrupu $(\mathbb{N}, +)$ do komutativní grupy $(\mathbb{Z}, +)$.

$$f: (\mathbb{N}, +) \longrightarrow (\mathbb{Z}, +) \cong (\mathbb{N}, +) \times (\mathbb{N}, +) /=$$

$$f(a) = [a + a, a]$$

Nyní ověříme, že *f* je vnoření.

Ukažme nejprve, že *f* je homomorfismus, tj.

$f(a + b) = f(a) \oplus f(b)$,

kde je z důvodu přehlednosti použit znak $\oplus$ pro sčítání celých čísel a + pro sčítání přirozených čísel.

$f(a) \oplus f(b) = [a + a, a] \oplus [b + b, b] = [(a + a) + (b + b), a + b] =$

$$= [(a + b) + (a + b), a + b] = f(a + b)$$

Ještě ověříme, že f je prosté zobrazení, tj. jsou-li si rovny obrazy, $f(a) = f(b)$, jsou si rovny i vzory, $a = b$. Jestliže $f(a) = f(b)$, pak $[a + a, a] = [b + b, b]$. V tom případě musí podle definice rovnosti dvou celých čísel platit

$$(a + a) + b = a + (b + b).$$

Ze zákona krácení pro sčítání přirozených čísel plyne, že $a = b$, proto je f injektivní zobrazení, a tedy vnoření.

Užitím axiomu A9 pro přirozená čísla lze součet $a + a$ v definovaném vnoření zapsat jako součin $2.a$, získáme tak zobrazení z $(\mathbb{N},.)$ do $(\mathbb{Z},.)$,

$$f\colon (\mathbb{N},.) \longrightarrow (\mathbb{Z},.) \cong (\mathbb{N},.) \times (\mathbb{N},.)\ /=$$

$$f(a) = [2.a, a],$$

o němž lze dokázat, že je také vnořením. Protože jsou operace sčítání a násobení svázány v $\mathbb{N}$ i $\mathbb{Z}$ distributivním zákonem, je předpisem $f(a) = [a + a, a]$ popsáno vnoření komutativního polookruhu přirozených čísel do komutativního okruhu celých čísel.

KAPITOLA 3

Racionální čísla

Racionální čísla jsou nekonečná množina, která obsahuje všechna celá čísla. Množinu racionálních čísel značíme $\mathbb{Q}$. Toto označení pochází z anglického slova „quotient“, které označuje podíl, česky „kvocient“.

Racionální čísla používáme hlavně pro určení částí celku, které lze v racionálních číslech vyjádřit jako podíly. Jmenovatel označuje celek a čitatel část z celku. Pokud se čitatel rovná jmenovateli, znamená to, že máme celek celý.

Racionální čísla tvoří nekonečnou, ale spočetnou množinu, která je uzavřená vůči operaci sčítání, odčítání, násobení, oproti celým číslům, je uzavřená i vzhledem k operaci dělení. To znamená, že pokud mezi sebou vydělíme dvě racionální čísla, získáme opět racionální číslo.

3.1. Racionální čísla jako dvojice celých čísel

Vyjdeme z množiny celých čísel $\mathbb{Z}$, jejíž prvky budeme označovat velkými písmeny, jak jsme si zavedli v předchozí kapitole. Pro prvky z množiny $\mathbb{Q}$ budeme

používat písmena $\mathcal{A}, \mathcal{B}, \ldots, \mathcal{X}, \mathcal{Y}, \mathcal{Z}$ a pro operace s racionálními čísly budeme využívat znaky zavedené v kapitole 1.1.

Čísla z množiny $\mathbb{Z}$ mají určité vlastnosti, které jsme odvodili v předchozí kapitole a budeme je nadále používat. Z prvků množiny celých čísel budeme tvořit dvojice, obdobně jako když jsme tvořili celá čísla. Jsou-li A_1, A_2 dvě čísla z množiny $\mathbb{Z}$, budeme tuto dvojici označovat $[A_1, A_2] = \mathcal{A}$. Čísla A_1, A_2 v symbolu $[A_1, A_2]$ budeme nazývat složky racionálního čísla.

Definice 3.1.1 (Operace s racionálními čísly)

Uspořádané dvojice z množiny celých čísel $\mathbb{Z}$, jejichž druhá složka je různá od nuly, nazýváme racionálními čísly, je-li mezi nimi definovaná rovnost a početní úkony sčítání a násobení takto:

$$\mathcal{A} = \mathcal{B} \text{ tehdy a jen tehdy, když } A_1.B_2 = A_2.B_1$$

$$\mathcal{A} + \mathcal{B} = [A_1.B_2 + A_2.B_1, A_2.B_2]$$

$$\mathcal{A}.\mathcal{B} = [A_1.B_1, A_2.B_2]$$

Věta 3.1.1 (Vztah „rovná se“)

Každé racionální číslo lze psát v různých tvarech; je-li $[A_1, A_2]$ jeden tvar racionálního čísla, je $[A_1.X, A_2.X]$, kde $X \neq 0$ je celé číslo, jiný tvar téhož racionálního čísla.

Věta 3.1.2 (Vlastnosti vztahu „rovná se“)

Vztah „rovná se“ definovaný mezi racionálními čísly v definici 3.1.1, je relací ekvivalence, tj. pro libovolná tři racionální čísla platí:

$$\text{Reflexivita } \mathcal{A} = \mathcal{A}$$

$$\text{Symetrie } \mathcal{A} = \mathcal{B} \Rightarrow \mathcal{B} = \mathcal{A}$$

$$\text{Tranzitivita } \mathcal{A} = \mathcal{B} \wedge \mathcal{B} = \mathcal{C} \Rightarrow \mathcal{C} = \mathcal{A}$$

Důkaz tranzitivity:

První dvě rovnosti můžeme podle vztahu z definice 3.1.1 psát jako

$$A_1.B_2 = A_2.B_1,\ B_1.C_2 = B_2.C_1.$$

Z tohoto plyne

$$(A_1.B_2).C_2 = (A_2.B_1).C_2, \quad A_2.(B_1.C_2) = A_2.(B_2.C_1)$$

a odtud plyne podle zákona asociativity a tranzitivity relace „=“ v množině celých čísel

$$(A_1.B_2).C_2 = A_2.(B_2.C_1),$$

čili

$$(A_1.C_2).B_2 = (A_2.C_1).B_2,$$

neboť pro celá čísla platí zákony asociativity a komutativity. Poněvadž $B_2 \neq 0$, proto $A_1.C_2 = A_2.C_1$, což můžeme opět podle definice 3.1.1 převést na tvar $\mathcal{A} = \mathcal{C}$.

(Podle [Hru53], str.177)

Z tohoto důkazu také vyplývá, proč jsme ve větě 3.1.1 předpokládali, že druhá složka racionálního čísla je různá od nuly. Kdybychom totiž připustili, že by $B_2 = 0$, viz definice 3.1.1, pak by rovnost $(A_1.C_2).B_2 = (A_2.C_1).B_2$ mohla platit, i v případě $A_1.C_2 \neq A_2.C_1$, tudíž by rovnost dvou racionálních čísel nemusela být tranzitivní.

3.2 Vlastnosti operace sčítání a násobení racionálních čísel

3.2.1 Sčítání racionálních čísel

Abychom mohli vyslovit vlastnosti operace sčítání racionálních čísel, musíme nejprve uvést následující pojmy:

Věta 3.2.1.1

Jsou-li $\mathcal{A}, \mathcal{B}$ dvě libovolná racionální čísla, existuje racionální číslo $\mathcal{X}$ takové, že: $\mathcal{A} + \mathcal{X} = \mathcal{B}$.

Věta 3.2.1.2 (Rozdíl racionálních čísel)

Racionální číslo $\mathcal{X}$, které vyhovuje podmínce $\mathcal{A} + \mathcal{X} = \mathcal{B}$, budeme nazývat rozdíl racionálních čísel $\mathcal{A}, \mathcal{B}$. Píšeme:

$$\mathcal{X} = \mathcal{B} - \mathcal{A} = [B_1.A_2 - B_2.A_1, B_2.A_2]$$

Věta 3.2.1.3 (Nulový prvek)

Nulový prvek v racionálních číslech je prvek tvaru $[0, X] = 0$, kde $X \neq 0$ je celé číslo.

Věta 3.2.1.4 (Opačný prvek)

Opačný prvek k prvku $\mathcal{A} = [A_1, A_2]$ z množiny racionálních čísel je prvek $[-A_1, A_2] = \boldsymbol{\mathcal{A}}$.

Věta 3.2.1.5 (Vlastnosti sčítání racionálních čísel)

Sčítání racionálních čísel, uvedené v definici 3.1.1, se řídí zákonem komutativním a asociativním, tj. pro libovolné prvky množiny racionálních čísel platí:

$$\mathcal{A} + \mathcal{B} = \mathcal{B} + \mathcal{A}$$

$$\mathcal{A} + (\mathcal{B} + \mathcal{C}) = (\mathcal{A} + \mathcal{B}) + \mathcal{C}$$

Dále pro sčítání racionálních čísel platí:

$$\mathcal{A} + \mathcal{Z} = \mathcal{B} + \mathcal{Z} \Rightarrow \mathcal{A} = \mathcal{B}$$

$$\mathcal{A} + \boldsymbol{\mathcal{A}} = 0$$

$$\mathcal{A} + 0 = \mathcal{A} - 0 = \mathcal{A}$$

Věta 3.2.1.6 (Jednoznačnost sčítání)

Součet dvou racionálních čísel je opět racionální číslo, které je oběma sčítanci jednoznačně určeno. Stejní sčítanci v různých tvarech dávají týž součet.

Racionální čísla $(\mathbb{Q}, +)$ tvoří komutativní grupu, neboť sčítání racionálních čísel je komutativní, asociativní, v množině racionálních čísel $\mathbb{Q}$ existuje prvek 0, neutrální prvek vzhledem ke sčítání, k libovolnému racionálnímu číslu existuje číslo opačné, tj. pro každý prvek $\mathbb{Q}$ existuje inverzní prvek.

3.2.2 Násobení racionálních čísel

Věta 3.2.2.1 (Jednotkový prvek)

V množině racionálních čísel existuje jediný jednotkový prvek, je jím číslo ve tvaru $[X, X] = 1$, kde $X \neq 0$ je celé číslo.

Věta 3.2.2.2 (Řešitelnost rovnic v $(\mathbb{Q}, .)$)

Jsou-li $\mathcal{A}, \mathcal{B}$ dvě libovolná racionální čísla, přičemž $A_1 \neq 0$, existuje jediné racionální číslo $\mathcal{X}$ takové, že $\mathcal{A}.\mathcal{X} = \mathcal{B}$.

Definice 3.2.2.1 (Podíl racionálních čísel)

Jsou-li dána racionální čísla $\mathcal{A}, \mathcal{B}$, přičemž $A_1 \neq 0$, pak racionální číslo $\mathcal{X}$, pro něž platí rovnost $\mathcal{A}.\mathcal{X} = \mathcal{B}$, se nazývá podíl čísel $\mathcal{B}, \mathcal{A}$. Píšeme $\mathcal{X} = \mathcal{B}:\mathcal{A}$.

Touto definicí jsme zavedli dělení racionálních čísel, které je proveditelné pro libovolné nenulové racionální číslo.

Definice 3.2.2.2 (Převrácená čísla)

Racionální čísla ve tvaru $[A_1, A_2] = \mathcal{A}, [A_2, A_1] = \mathcal{A}^{-1}$, kde $A_1 \neq 0, A_2 \neq 0$, nazveme převrácená čísla.

Věta 3.2.2.3

Převráceným číslem k převrácenému číslu je původní číslo.

Věta 3.2.2.4 (Celé číslo)

Racionální číslo $\mathcal{A}$, jehož obě složky jsou celá čísla, a jeho druhá složka je různá od nuly, můžeme považovat za podíl racionálních čísel $[A_1.X, X], [A_2.X, X]$, kde $X \neq 0$ je celé číslo.

Věta 3.2.2.5 (Vlastnosti násobení racionálních čísel)

Násobení racionálních čísel uvedené v definici 3.1.1 se řídí komutativním a asociativním zákonem, tj. pro všechna racionální čísla platí:

$$\mathcal{A}.\mathcal{B} = \mathcal{B}.\mathcal{A}$$

$$\mathcal{A}.(\mathcal{B}.\mathcal{C}) = (\mathcal{A}.\mathcal{B}).\mathcal{C}$$

Násobení racionálních čísel je operací s krácením, má neutrální, inverzní i agresivní prvek:

$$\mathcal{A}.\mathcal{Z} = \mathcal{B}.\mathcal{Z} \Rightarrow \mathcal{A} = \mathcal{B}$$

$$\mathcal{A}.1 = \mathcal{A}$$

$$\mathcal{A}.\mathcal{A}^{-1} = 1$$

$$\mathcal{A}.0 = 0$$

Věta 3.2.2.6 (Jednoznačnost násobení)

Součinem dvou racionálních čísel je opět racionální číslo, které je oběma činiteli jednoznačně určeno. Činitelé v různých tvarech dávají týž součin.

Věta 3.2.2.7 (Vlastnosti sčítání a násobení racionálních čísel)

Sčítání a násobení racionálních čísel, definované v definici 3.1.1 se řídí distributivním zákonem, to znamená, že platí: $\mathcal{A}.(\mathcal{B} + \mathcal{C}) = \mathcal{A}.\mathcal{B} + \mathcal{A}.\mathcal{C}$

Důkaz distributivity:

Označíme $\mathcal{A} = [A_1, A_2], \mathcal{B} = [B_1, B_2],\ \mathcal{C} = [C_1, C_2]$, $\oplus$ sčítání racionálních čísel a $\otimes$ jejich násobení, + a . sčítání a násobení celých čísel. Dokazovaná rovnost má poté tvar

$$[A_1, A_2]\otimes([B_1, B_2]\oplus [C_1, C_2]) = [A_1, A_2]\otimes[B_1, B_2]\oplus [A_1, A_2]\otimes[C_1, C_2]$$

$$\begin{aligned}[A_1, A_2]\otimes[B_1, B_2]\oplus [A_1, A_2]\otimes[C_1, C_2] &= [A_1.B_1, A_2.B_2]\oplus[A_1.C_1, A_2.C_2] = \\ &= [A_1.B_1.A_2.C_2 + A_2.B_2.A_1.C_1, A_2.B_2.A_2.C_2] = \\ &= [A_1.B_1.C_2 + B_2.A_1.C_1, B_2.A_2.C_2] = [A_1.(B_1.C_2 + B_2.C_1), A_2.B_2.C_2] \\ &= [A_1, A_2]\otimes[B_1.C_2 + B_2.C_1, B_2.C_2] = [A_1, A_2]\otimes([B_1, B_2]\oplus [C_1, C_2])\end{aligned}$$

Racionální čísla $(\mathbb{Q}, +, \cdot)$ tvoří těleso.

3.3 Uspořádání racionálních čísel

Definice 3.3.1 (Číslo kladné a záporné)

Racionální číslo $\mathcal{A}$ se nazývá kladné, je-li $A_1.A_2 > 0$, a záporné, je-li

$A_1.A_2 < 0$.

Věta 3.3.1

Racionální číslo, které je kladné v jednom tvaru, je kladné i v každém jiném tvaru. Totéž platí i pro racionální čísla záporná.

Například dvojice $[3,-4]$, $[-6.8]$ vyjadřují stejné racionální číslo. Číslo $[3,-4]$ je záporné, neboť $3.(-4) < 0$, také číslo $[-6,8]$ je záporné, což je v souladu s tvrzením.

Věta 3.2.2

Je-li $\mathcal{A}$ libovolné racionální číslo, nastane vždy právě jeden z případů:
$[A_1,A_2] = [0,X]$, $[A_1,A_2]$ je kladné, $-[A_1,A_2]$ je kladné.

Věta 3.3.3

Jsou-li $\mathcal{A},\mathcal{B}$ dvě kladná racionální čísla, jsou kladná i čísla $\mathcal{A}+\mathcal{B}$ a $\mathcal{A}.\mathcal{B}$.

Věta 3.3.4

Jsou-li $\mathcal{A},\mathcal{B}$ racionální čísla a je-li

$\mathcal{A} > \mathcal{B}$, pak $A_1.B_2 > A_2.B_1$ a $A_2.B_2 > 0$, nebo $A_1.B_2 < A_2.B_1$ a $A_2.B_2 < 0$

$\mathcal{A} < \mathcal{B}$, pak $A_1.B_2 < A_2.B_1$ a $A_2.B_2 > 0$, nebo $A_1.B_2 > A_2.B_1$ a $A_2.B_2 < 0$

Tyto vztahy nejsou závislé na tvaru čísel $\mathcal{A},\mathcal{B}$.

Protože racionální čísla jsou uspořádaná, platí v nich vlastnosti:

Je-li $\mathcal{A} < \mathcal{B}$, je $\mathcal{B} > \mathcal{A}$.

Jsou-li $\mathcal{A},\mathcal{B}$ dvě libovolná racionální čísla, platí vždy právě jeden ze vztahů:

$$\mathcal{A} = \mathcal{B}, \mathcal{A} < \mathcal{B}, \mathcal{A} > \mathcal{B}$$

Je-li $\mathcal{A} < \mathcal{B}$ a $\mathcal{B} < \mathcal{C}$, je také $\mathcal{A} < \mathcal{C}$.

Dále také pro racionální čísla platí zákony monotonie. Zákony monotonie vyjadřují, že nerovnost libovolných dvou racionálních čísel se nezmění, přičteme-li k oběma jejím stranám stejné racionální stejné racionální číslo nebo vynásobíme-li obě strany stejným kladným racionálním číslem, tj.

$$\mathcal{A} > \mathcal{B} \Rightarrow \mathcal{A} + \mathcal{C} > \mathcal{B} + \mathcal{C}$$

$$\mathcal{A} > \mathcal{B} \wedge \mathcal{C} > 0 \Rightarrow \mathcal{A}.\mathcal{C} > \mathcal{B}.\mathcal{C}$$

Vynásobením nerovnosti záporným číslem se nerovnost změní následovně:

$$\mathcal{A} > \mathcal{B} \wedge \mathcal{C} < 0 \Rightarrow \mathcal{A}.\mathcal{C} < \mathcal{B}.\mathcal{C}$$

Věta 3.3.5

Jsou-li $\mathcal{A}, \mathcal{B}$ dvě racionální čísla, přičemž číslo $\mathcal{B}$ je kladné, existuje přirozené číslo n tak, že $n.\mathcal{B} > \mathcal{A}$.

Podle těchto vlastností můžeme usoudit, že množina $(\mathbb{Q}, +, \cdot, <)$ je uspořádaným okruhem, a to uspořádaným archimédovsky.

3.4 Vnoření komutativního okruhu do podílového tělesa

Ve druhé kapitole jsme definovali kongruenci pologrupy jako relaci ekvivalence zachovávající pologrupovou operaci. Analogicky lze definovat kongruenci okruhu jako ekvivalenci zachovávající obě binární operace v okruhu.

3.4.1 Faktorizace okruhu

Definice 3.4.1.1

Mějme libovolný okruh $\boldsymbol{O}$ = (O, +, ·). Potom relaci ekvivalence ~ na množině O, nazveme kongruencí okruhu O, jestliže pro libovolné prvky $x_1, x_2, y_1, y_2 \in \boldsymbol{O}$ platí: Pokud $x_1 \sim y_1$ a $x_2 \sim y_2$, potom také $x_1 \cdot x_2 \sim y_1 \cdot y_2$ a $x_1 + x_2 \sim y_1 + y_2$.

Následujícím tvrzením je zajištěno, že na faktorovém okruhu $O/\sim$ lze zavést dvě binární operace tak, že výsledná struktura je opět okruhem.

Věta 3.4.1.1

Nechť $\boldsymbol{O}$ = (O,+,·) je libovolný okruh a ~ je kongruence okruhu. Na množině O/~ lze zavést operace $\oplus$ a $\odot$ tak, že pro libovolné $[x]\sim, [y]\sim \in O/\sim$ platí, že $[x]\sim\oplus[y]\sim = [x+y]\sim$ a $[x]\sim\odot[y]\sim = [x.y]\sim$ a navíc algebraická struktura O/~=(O/~,$\oplus$,$\odot$) je opět okruh.

3.4.2 Okruh a obor integrity

Definice 3.4.2.1

Neprázdnou množinu M nazýváme nekomutativním okruhem, jsou-li v ní definovány dvě operace zvané sčítání a násobení, které mají tyto vlastnosti:

1) Ke každým dvěma prvkům $x_1 \in M, x_2 \in M$, existuje jediný prvek $x_1 + x_2 \in M$, zvaný součet prvků x_1 a x_2 , které budeme nazývat sčítance. Pro tyto prvky také platí komutativní a asociativní zákony pro sčítání.

2) Ke každým dvěma prvkům $x_1 \in M, x_2 \in M$, existuje alespoň jeden takový prvek $y \in M$, že platí $x_1 + y = x_2$. Prvek y budeme nazývat rozdíl prvků x_2, x_1 a budeme ho značit $y = x_2 - x_1$

3) Ke každým dvěma prvkům $x_1 \in M, x_2 \in M$, existuje jediný prvek $x_1.x_2 \in M$, zvaný součin prvků x_1 a x_2 , které budeme nazývat činitelé. Pro tyto prvky také platí distributivní a asociativní zákony pro násobení. Pokud vedle těchto dvou zákonů bude platit ještě komutativní zákon pro násobení, budeme množinu M nazývat komutativním okruhem.

V našem případě budeme hovořit výhradně o komutativních okruzích a budeme pro ně používat souhrnný název okruh.

Z vlastnosti 2) z definice 3.4.2.1 plyne, že v každém okruhu M existuje prvek o, pro který platí $x_1 + o = x_1$, kde $x_1 \in M$.

Věta 3.4.2.1

Budiž M okruh a zvolme libovolný prvek $x_1 \in M$. Je-li $o \in M$, pro nějž platí $x_1 + o = x_1$, pak pro každý jiný prvek $x_2 \in M$ rovněž platí $x_2 + o = x_2$.

Z vlastnosti 2) z definice 2.4.2.1 také plyne, že ke každému prvku $x_1 \in M$ existuje takový prvek $x_1' \in M$, že $x_1 + x_1' = o$, kde o je takový prvek, že $y + o = y$ pro každé $y \in M$.

Věta 3.4.2.2

Jsou-li x_1, x_2 dva libovolné prvky okruhu M, pak existuje jediný prvek $y \in M$, pro který platí $x_1 + y = x_2$.

Důkaz:

Vlastnost 2) z definice3.4.1.1 požaduje existenci alespoň jednoho takového prvku. Nechť v okruhu M existují takové prvky dva, označíme je y_1, y_2, tj. nechť platí $x_1 + y_1 = x_2$, $x_1 + y_2 = x_2$

Pak $x_1 + y_1 = x_1 + y_2$ a vzhledem ke komutativnímu zákonu sčítání také $y_1 + x_1 = y_2 + x_1$. Vezměme prvek $o \in M$ tak, aby $x_1 + o = x_1$, a určeme prvek $x_1' \in M$, pro nějž platí $x_1 + x_1' = o$. Pak vzhledem k vlastnosti 1) z definice 3.4.1.1 je $(y_1 + x_1) + x_1' = (y_2 + x_1) + x_1'$ a podle asociativního zákona pro sčítání $y_1 + (x_1 + x_1') = y_2 + (x_1 + x_1')$, neboli $y_1 + o = y_2 + o$ a odtud podle věty 3.4.1.1 $y_1 = y_2$, takže y_1, y_2 jsou stejné.

(Podle [Hru53], str.169)

Důsledkem věty 3.4.2.2 je, že v každém okruhu existuje jediný prvek o, pro nějž platí $x_1 + o = x_1$ pro každé $x_1 \in M$, a ke každému prvku $x_1 \in M$ existuje jediný prvek $x_1' \in M$ tak, že $x_1 + x_1' = o$.

Definice 3.4.2.2

Prvek $o \in M$, pro nějž platí $x_1 + o = x_1$ pro libovolné $x_1 \in M$, se nazývá nulový prvek okruhu M. A prvek $x_1' \in M$, pro nějž platí $x_1 + x_1' = o$, kde $x_1 \in M$, se nazývá opačný prvek k prvku x_1v okruhu M a značí se $-x_1$.

Věta 3.4.2.3

Odčítat prvek x_1 je totéž jako přičítat prvek $-x_1$.

Věta 3.4.2.4

Je-li o nulový prvek okruhu M, pak pro každý prvek $x_1 \in M$ platí $x_1 . o = o$.

Definice 3.4.2.3

Prvky x_2, x_1 okruhu M, pro něž platí $x_1 \neq o, x_2 \neq o$, ale přesto $x_1.x_2 = o$, se nazývají dělitelé nuly.

Definice 3.4.2.4

Existuje-li v okruhu M takový prvek y, pro nějž platí $x_1.y = x_1$ pro každé $x_1 \in M$, nazýváme prvek y jednotkovým prvkem okruhu M. Má-li okruh M jednotkový prvek y a existuje-li k prvku $x_1 \in M$ prvek $x_1^* \in M$ tak, že $x_1.x_1^* = y$, nazýváme prvek x_1^* inverzním (převráceným) prvkem k prvku x_1 v okruhu M.

Komutativní okruh, který má jednotkový prvek, a nemá dělitele nuly, se nazývá obor integrity.

Definice 3.4.2.5

Okruh M nazýváme uspořádaným, existuje-li v něm část $K \subset M$, jejíž prvky nazýváme kladnými, přičemž jsou splněny tyto požadavky:

1) Pro libovolný prvek $x_1 \in M$ nastane vždy právě jeden z případů: $x_1 = o, x_1$ je kladné, -x_1 je kladné.

2) Jsou-li prvky $x_1 \in M, x_2 \in M$ kladné, pak kladné jsou i prvky $x_1 + x_2$ a $x_1.x_2$.

Je-li -x_1 kladné, nazývá se x_1 záporné.

Věta 3.4.2.5

V uspořádaném okruhu neexistují dělitelé nuly.

Definice 3.4.2.6

Je-li M uspořádaný okruh a jsou-li x_1, x_2 dva jeho prvky, říkáme, že x_1 je větší než x_2, když rozdíl $x_1 - x_2$ je kladný, a že x_1 je menší než x_2, když rozdíl $x_1 - x_2$ je záporný.

Věta 3.4.2.6

Vztahy „větší než“ a „menší než“ mezi prvky uspořádaného okruhu, mají tyto vlastnosti:

1) Je-li $x_1 < x_2$, je $x_2 > x_1$.
2) Zákon trichotomie: Jsou-li x_1, x_2 dva libovolné prvky uspořádaného okruhu, platí vždy jeden ze vztahů: $x_1 = x_2,\ x_1 < x_2, x_1 > x_2$.
3) Tranzitivnost nerovnosti: Je-li $x_1 > x_2$ a $x_2 > x_3$, je také $x_1 > x_3$.

Věta 3.4.2.7

Jsou-li x_1, x_2 takové dva prvky uspořádaného okruhu M, že $x_1 > x_2$, pak

1) $x_1 + x_3 > x_2 + x_3$ pro každé $x_3 \in M$.
2) $x_1.x_3 > x_2.x_3$ pro každé kladné $x_3 \in M$, $x_1.x_3 < x_2.x_3$ pro každé záporné $x_3 \in M$

Definice 3.4.2.7

Je-li x_1 prvkem okruhu M a jestliže každému přirozenému číslu n přiřadíme prvek $n.x_1$ tak, aby platilo:

1) $1.x_1 = x_1$
2) $(n+1).x_1 = n.x_1 + x_1$

pak prvek $n.x_1$ nazýváme součin prvku $x_1 \in M$ a přirozeného čísla n. Tímto je definován součin $n.x_1$ pro každé přirozené číslo n. Číslo n však nemusí být prvkem okruhu M, ale $n.x_1$ vždy náleží okruhu M. Pokud však je n prvkem okruhu M, pak je součin $n.x_1$ totožný se součinem dvou prvků okruhu podle definice 3.4.1.1.

Definice 3.4.2.8

Okruh M se nazývá archimédovsky uspořádaný, je-li uspořádaný, a jestliže mimo to platí tzv. Archimedův axiom: Jsou-li x_1, x_2 dva libovolné prvky okruhu M, přičemž x_1 je kladné, existuje přirozené číslo n tak, že $n.x_1 > x_2$.

Nyní můžeme dokázat platnost věty 3.3.5:

Podle bodu 1 definice 3.4.1.7 je $1.\mathcal{B} = \mathcal{B} = [1.B_1, B_2]$. Teď tedy dokážeme, že $n.\mathcal{B} = [n.B_1, B_2]$. Platí-li tato rovnost pro nějaké přirozené číslo n, pak podle bodu 2 definice 3.4.1.7 platí: $(n+1).\mathcal{B} = n.\mathcal{B} + \mathcal{B} = [n.B_1, B_2] + [B_1, B_2] = [n.B_1.B_2 + B_2.B_1, B_2^2] = [(n+1).B_1, B_2]$. Z tohoto vyplývá, že vztah $n.\mathcal{B} = [n.B_1, B_2]$ platí pro všechna přirozená čísla n.

Protože číslo $\mathcal{B}$ je kladné, proto $B_1.B_2 > 0$. Utvoříme čísla $B_1.A_2,\ B_2.A_1$. Je-li $A_2.B_2 > 0$, mají čísla B_1, B_2, A_2 vesměs stejná znaménka, takže $B_1.A_2$ je kladné. Protože okruh celých čísel je uspořádán archimédovsky, existuje takové přirozené číslo n, že $n.B_1.A_2 > B_2.A_1$. Potom je $[n.B_1, B_2] > [A_1, A_2]$, neboť $B_2.A_2 > 0$. Je-li $B_2.A_2 > 0$, mají čísla B_1, B_2 stejná znaménka, ale číslo A_2 má opačné znaménko, takže číslo $B_1.A_2$ je záporné a $-B_1.A_2$ je kladné. Potom existuje takové přirozené číslo n, že $n.(-B_1.A_2) > -B_2.A_1$, čili $n.B_1.A_2 < B_2.A_1$. Potom je opět $[n.B_1, B_2] > [A_1, A_2]$, neboť $B_2.A_2 < 0$. Ale $[n.B_1, B_2] = n.[B_1, B_2]$, takže v obou případech je $n.[B_1, B_2] > [A_1, A_2]$.

(Podle [Hru53], str.182-183)

Podle tohoto jsme usoudili, že racionální čísla jsou archimédovsky uspořádaný okruh.

3.4.3 Vnoření komutativního okruhu do podílového tělesa

Analogicky ke kapitole 2.4.2 máme větu, která říká, za jakých podmínek můžeme rozšiřovat okruhy na tělesa.

Věta 3.4.3.1

Komutativní okruh $\boldsymbol{O} = (O, +, \cdot)$ lze vnořit do tělesa tehdy a jen tehdy, nejsou-li v něm netriviální dělitelé nuly. Navíc platí, že komutativní okruh lze v tomto případě vnořit do tělesa, které je komutativní.

Nejprve mějme okruh $\boldsymbol{O} = (O, +, \cdot)$ bez netriviálních dělitelů nuly. Označíme $(O \setminus \{0\}, \cdot)$ komutativní pologrupu. Pro konstrukci množiny racionálních čísel použijeme komutativní pologrupu $(\mathbb{Z} \setminus \{0\}, \cdot)$. Z kapitoly dva víme, že tato struktura je komutativní pologrupou s krácením, dokonce je komutativním monoidem.

Podle věty 2.4.2.1 lze takovouto strukturu vnořit do grupy. Podle věty 2.4.2.2 lze vnořit i pologrupu $(O \setminus \{0\} \times O \setminus \{0\},\cdot)$ do grupy. Ke konstrukci grupy

$(O \setminus \{0\} \times O \setminus \{0\},\cdot)/\sim$ potřebujeme mít kongruenci $\sim$. V definici 3.1.1 jsme zavedli relaci „=“, která je relací ekvivalence. Tato relace je zároveň, podle tvrzení, které jsme uvedli v kapitole 2.4.2, kongruencí.

Faktorizací $(\mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\},\cdot)$ podle „=“ dostaneme grupu vzhledem k násobení, kterou bude možné ztotožnit s $(\mathbb{Q} \setminus \{0\},.)$.

Abychom dostali těleso, musíme ještě „ošetřit“ druhou operaci. Sčítání dvojic z množiny $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$zavedené v definici 3.1.1 splňuje axiomy komutativní grupy podle věty 3.2.1.5.

Zkonstruované těleso $(\mathbb{Z} \times \mathbb{Z} \setminus \{0\}/=,+,\cdot)$ nazýváme podílovým tělesem okruhu.

Nyní popíšeme homomorfismus, kterým je vnoříme komutativní okruh celých čísel do tělesa racionálních čísel.

$$f\colon \mathbb{Z} \longrightarrow \mathbb{Q} \cong \mathbb{Z} \times \mathbb{Z} \setminus \{0\}/=$$

$$f(A) = [A.A,\ A],\ A \neq 0$$

$$f(A) = [0,\ X],\ \ A = 0, X \neq 0$$

Ověříme, zda takto popsané zobrazení je vnořením. Pro sčítání racionálních čísel použijeme znak $\oplus$ a znak $\otimes$ pro násobení racionálních čísel, podobně $+$ a $.$ pro příslušné operace v celých číslech. Pokud ukážeme, že platí

$$f(A + B) = f(A) \oplus f(B) \qquad \text{a} \qquad f(A.B) = f(A) \otimes f(B)$$

pro případy $A \neq 0$ i $A = 0$, bude f homomorfismem.

Pro $A \neq 0$ a součet, resp. součin racionálních čísel platí:

$$f(A) \oplus f(B) = [A.A,\ A] \oplus [B.B,\ B] = [A.A.B + A.B.B,\ A.B] =$$

$$= [A + B, 1] = [(A + B)(A + B), A + B] = f(A + B).$$

resp.

$$f(A) \otimes f(B) = [A.A,\ A] \otimes [B.B,\ B] = [A.A.B.B,\ A.B] =$$

$$= [A.B, 1] = [A.B.A.B, A.B] = f(A.B).$$

Pro $A = 0$ a součet, resp. součin racionálních čísel platí:

$$f(0) \oplus f(B) = [0,\ X] \oplus [B.B,\ B] = [0.B + X.B.B,\ X.B] =$$

$$= [X.B.B, X.B] = [B, 1] = [B.B, B] = [(0 + B)(0 + B), 0 + B] = f(0 + B).$$

resp.

$$f(0) \otimes f(B) = [0,\ X] \otimes [B.B,\ B] = [0.B.B,\ X.B] =$$

$$= [0, X.B] = [0, X] = f(0) = f(0.B).$$

Pro důkaz injektivnosti homomorfismu f uvažujme nejprve případ $A \neq 0$, $B \neq 0$.
Z rovnosti $f(A) = f(B)$ v takovém případě plyne

$$[A.A, A] = [B.B, B].$$

Dvě racionální čísla jsou si rovna, když je součin první složky prvního čísla a druhé složky druhého čísla roven součinu druhé složky prvního čísla a první složky druhého čísla, viz definice 3.1.1, tj. když

$$A.A.B = A.B.B.$$

Operace násobení celých čísel je operací s krácením, proto

$$A = B,$$

a tedy f je pro $A \neq 0$, $B \neq 0$ prosté zobrazení. Vezmeme-li $A = 0$, $B = 0$, je z definice zobrazení f zřejmé, že z $f(A) = f(B)$ vyplyne $A = B = 0$. Uvažujme případ $A = 0, B \neq 0$, potom lze rovnost $f(A) = f(B)$ přepsat do tvaru

$$[0, X] = [B.B, B]$$

a dále

$$0.B = X.B.B, \text{ resp. } 0 = X.B.B.$$

Vzhledem k tomu, že v okruhu celých čísel neexistují netriviální dělitelé nuly a $X \neq 0$, musí být $B = 0$, a tedy $B = A = 0$.

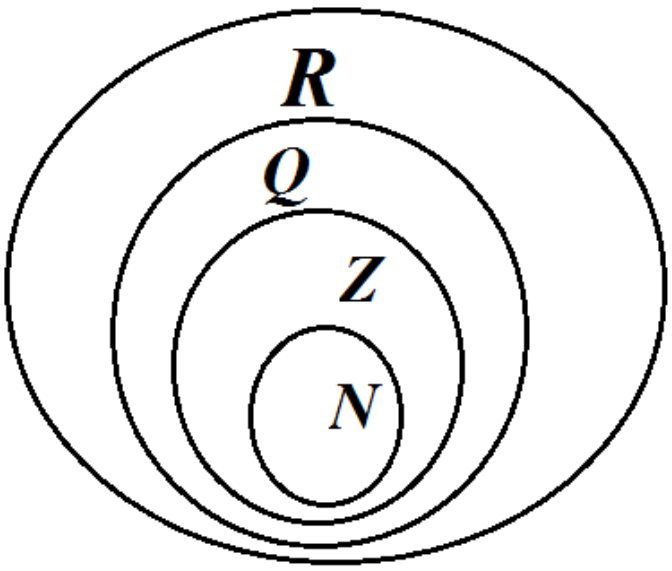
KAPITOLA 4

Reálná čísla

Množinu reálných čísel budeme označovat symbolem $\mathbb{R}$. Tato množina obsahuje všechna přirozená, celá i racionální čísla. Většina funkcí, se kterými v matematice pracujeme, mají právě reálná čísla nebo nějakou jejich souvislou podmnožinu za definiční obor. Reálná čísla jsou nekonečná nespočetná množina, která je uzavřená vzhledem k operacím sčítání, odčítání, násobení i dělení. Reálná čísla tedy v algebraickém smyslu tvoří těleso.

Reálná čísla si můžeme představit jako čísla, která označují vzdálenost mezi jakýmikoli dvěma body na přímce, které budeme říkat číselná osa. Reálné číslo představuje vzdálenost od zvoleného bodu, tím většinou bývá nula. Nula rozděluje číselnou osu na dvě části, kladnou a zápornou, tedy i reálná čísla rozděluje na kladnou a zápornou část. Podle zavedeného systému se na číselné ose dělí reálná čísla podle polohy vzhledem k nule, napravo od nuly kladná a nalevo od nuly záporná. Pro každé reálné číslo je definována i jeho absolutní hodnota, jejímž geometrickým smyslem je vzdálenost obrazu čísla od nuly na číselné ose.

Rozdíl mezi množinou reálných a racionálních čísel nazýváme čísla iracionální. Reálná čísla můžeme také dělit na algebraická, tedy ta, která jsou kořeny mnohočlenů s celočíselnými koeficienty, a transcendentní (zbytek).



4.1 Řezy v množině racionálních čísel

Postup, který jsme do teď užívali, byl následující: Nadefinovali jsme si nějakou množinu, kterou jsme postupně rozšiřovali, aby na ní byla proveditelná nějaká operace. Vycházeli jsme z množiny přirozených čísel, ve které bylo možné provádět odčítání jen za určitých podmínek. Poté jsme množinu $\mathbb{N}$ rozšířili a vytvořili tak okruh celých čísel, kde bylo možné provádět odčítání bez omezení, ale dělení zde bylo možné jen za určitých podmínek. Poté jsme množinu $\mathbb{Z}$ opět rozšířili na těleso racionálních čísel, ve kterém bylo možné provádět dělení vždy, kdykoli byl dělitel různý od nuly. V této kapitole se budeme zabývat dalším rozšířením množiny $\mathbb{Q}$, které již nebude motivováno neomezenou proveditelností operací definovaných na $\mathbb{Q}$.

Hlavním důvodem dalšího rozšiřování množiny racionálních čísel je získání „spojité množiny“. Vyjdeme z množiny racionálních čísel $\mathbb{Q}$, jejíž prvky budeme označovat velkými písmeny, jak jsme si zavedli v předchozí kapitole. Pro prvky z množiny $\mathbb{R}$ budeme používat písmena $a, b, \dots, x, y, z$ a pro operace s reálnými čísly budeme využívat znaky zavedené v kapitole 1.1.

4.1.1 Hustě uspořádaná množina

Množina racionálních čísel, je „nedokonalá“ tím, že není „spojitá“. I přesto lze dle následujícího tvrzení najít mezi libovolnými dvěma racionálními čísly další racionální číslo.

Věta 4.1.1.1

Jsou-li $\frac{A_1}{A_2}, \frac{B_1}{B_2}$ dvě racionální čísla, pro něž platí $\frac{A_1}{A_2} < \frac{B_1}{B_2}$, existuje racionální číslo $\frac{X_1}{X_2}$ tak, že $\frac{A_1}{A_2} < \frac{X_1}{X_2} < \frac{B_1}{B_2}$.

Definice 4.1.1.1 (Hustě uspořádaná množina)

Množinu M nazýváme hustě uspořádanou množinou, má-li aspoň dva prvky, je-li uspořádaná a má-li tu vlastnost, že ke každým dvěma prvkům $\alpha \in M, \beta \in M$, pro něž platí $\alpha \prec \beta$,existuje alespoň jeden takový prvek $\xi \in M$, že $\alpha \prec \xi \prec \beta$.

Podle věty 4.1.1.1 je přirozeně uspořádaná množina racionálních čísel uspořádána hustě, naproti tomu není přirozeně uspořádaná množina celých čísel uspořádána hustě, protože ke každým dvěma prvkům N a $N+1$ z množiny $\mathbb{Z}$ neexistuje žádný prvek X z množiny takový, aby pro něj platilo $N < X < N+1$.

Z definice 4.1.1.1 vyplývá, že mezi každými dvěma prvky hustě uspořádané množiny leží neomezené množství dalších prvků, neboť, jsou-li α, β takové dva prvky hustě uspořádané množiny tak, že $\alpha \prec \beta$, existuje alespoň jeden další prvek ξ, pro který platí $\alpha \prec \xi \prec \beta$, pak musí existovat i další prvek ξ_1, pro který platí $\alpha \prec \xi_1 \prec \beta$. Hustě uspořádaná množina je vždy nekonečná.

Kdybychom se omezili pouze na množinu racionálních čísel, neměli bychom žádné číslo, které by vyhovovalo podmínce $x^2 = 2$. Proto musíme zavést nový číselný obor, kterými zaplníme mezery v množině racionálních čísel.

Vzhledem k tomu, že množina racionálních čísel je nespojitá, budeme v následujících větách a definicích zavádět nové pojmy, související právě s nespojitostí množiny racionálních čísel.

Definice 4.1.1.2 (Řez, horní a dolní skupina)

Množinu $M_1 \subset M$ nazveme řezem uspořádané množiny M, má-li tyto vlastnosti:

1. Není prázdná, ale existuje alespoň jeden prvek množiny M, který do M_1 nepatří.
2. Je-li $\alpha_1 \in M$ libovolný prvek, který patří do M_1, a $\alpha_2 \in M$ libovolný prvek, který do M_1 nepatří, je vždy $\alpha_1 \prec \alpha_2$.
   Množinu M_1 nazýváme dolní skupina.
   Množinu M_2 prvků z M , které do M_1 nepatří, nazýváme horní skupina.

Příklad 4.1.1.1:

Například množina $M_1 = \left\{x \in \mathbb{Q}; x \leq -\frac{1}{2}\right\}$ je řezem množiny racionálních čísel, protože je neprázdná (např. $-\frac{3}{2} \in M_1$) a také $\mathbb{Q} \setminus M_1$ je neprázdná (např. $0 \in \mathbb{Q} \setminus M_1$). Rovněž platí, že $\alpha_1 < \alpha_2$, vezmeme-li $\alpha_1 \in M_1$ a $\alpha_2 \in \mathbb{Q} \setminus M_1$.

Potom můžeme naši množinu M_1 nazývat dolní skupinou a množinu $\mathbb{Q} \setminus M_1$ horní skupinou.

Definice 4.1.1.3 (Skok a mezera)

Řez uspořádané množiny M, jehož dolní skupina M_1 má poslední prvek a jehož horní skupina M_2 má první prvek, se nazývá skokem množiny M. Řez, jehož dolní skupina M_1 nemá poslední prvek a jehož horní skupina M_2 nemá první prvek, se nazývá mezerou množiny M.

Příklad 4.1.1.2

Například řez $M_1 = \{x \in \mathbb{Q}; x^2 \leq 2 \ \vee x < 0\}$ na uspořádané množině racionálních čísel je mezera, neboť $x^2 = 2$ nepatří do dolní skupiny, protože $x^2 = 2$ nenáleží do množiny racionálních čísel a nedá se jednoznačně určit nejbližší číslo, které by do této skupiny patřilo, proto říkáme, že dolní skupina nemá poslední prvek. Pro $M_2 = \mathbb{Q} \setminus M_1$, platí totéž analogicky, neboť se nedá jednoznačně určit číslo takové, aby náleželo racionálním číslům a bylo co nejblíže $x^2 = 2$ a zároveň náleželo do M_2. Řekneme tedy, že skupina M_2 nemá první prvek.

Věta 4.1.1.2 (Vlastnost hustě uspořádané množiny)

Uspořádaná množina je hustě uspořádaná tehdy a jen tehdy, neobsahuje-li skoky.

Podle této věty hustě uspořádaná množina racionálních čísel neobsahuje skoky.

Na základě těchto vět můžeme říci, že množina racionálních čísel je hustě uspořádaná spočetná množina.

Věta 4.1.1.3

Přirozeně uspořádaná množina racionálních čísel obsahuje mezery.

V množině racionálních čísel existují vedle mezer ještě další dva typy řezů. To platí i pro každou jinou hustě uspořádanou množinu. Popišme tyto tři druhy řezů:

1. Dolní skupina M_1 nemá poslední prvek a horní skupina M_2 má první prvek α.
2. Dolní skupina M_1 má poslední prvek α a horní skupina M_2 nemá první prvek.
3. Dolní skupina M_1 nemá poslední prvek a horní skupina M_2 nemá první prvek.

První dva případy se od sebe v podstatě neliší, protože je lhostejné, zda počítáme prvek α do M_1 nebo do M_2. Nebudeme-li k tomuto prvku přihlížet, jsou obě skupiny

v obou případech stejné. Abychom nemuseli zbytečně odlišovat tyto dva případy, učiníme následující úmluvu:

Úmluva: Dolní skupinu M_1 řezu hustě uspořádané množiny budeme vždy tvořit tak, aby neměla poslední prvek.

Nyní máme jen dva druhy řezů hustě uspořádané množiny M, a to řezy, jejichž horní skupina má první prvek α, a řezy, jejichž horní skupina nemá první prvek. Tyto řezy jsme v definici 4.1.1.3 nazvali mezerami.

Definice 4.1.1.4 (Řez racionální a iracionální)

Řez v množině racionálních čísel nazýváme racionálním, jestliže jeho dolní skupina neobsahuje největší číslo, ale horní skupina obsahuje nejmenší číslo. Řez v množině racionálních čísel nazýváme iracionálním, jestliže jeho dolní skupina neobsahuje největší číslo a horní skupina neobsahuje nejmenší číslo.

V další části textu budeme řezy v množině racionálních čísel označovat řeckými písmeny a racionální řez, který je definován racionálním číslem $\mathcal{A}$, které je nejmenším číslem jeho horní skupiny budeme označovat α^*.

Například $\beta = \{x \in \mathbb{Q};\ x^3 < 3\}$ je řez v $\mathbb{Q}$ a $b^* = \left\{x \in \mathbb{Q};\ x < \frac{2}{3}\right\}$ je řez definovaný číslem $\mathcal{B} = \frac{2}{3}$.

Věta 4.1.1.5

Je-li dán řez α v množině racionálních čísel a libovolné kladné racionální číslo $\mathcal{H}$, existuje číslo $\mathcal{A}_1$ v dolní skupině a číslo $\mathcal{A}_2$ v horní skupině řezu α tak, že

$\mathcal{A}_2 - \mathcal{A}_1 = \mathcal{H}$.

4.2 Vlastnosti počítání s řezy v množině racionálních čísel

S řezy můžeme zacházet podobně jako s čísly, a tak pro ně můžeme definovat početní úkony jako pro čísla. V této podkapitole vybudujeme aritmetiku řezů, dospějeme k podobným vlastnostem jako u čísel. Tyto vlastnosti označíme stejnými symboly jako u čísel, ale budeme je označovat hvězdičkou.

4.2.1 Sčítání řezů

Definice 4.2.1.1 (Rovnost řezů)

O řezech α, β říkáme, že jsou si rovny, píšeme $\alpha = \beta$, když každé číslo dolní skupiny řezu α je zároveň také číslem dolní skupiny řezu β a naopak. Píšeme $\alpha = \beta$, není-li tomu tak, píšeme $\alpha \neq \beta$.

Řezy jsou si tedy rovny, když jsou jejich dolní skupiny totožné. Takto definovaná rovnost řezů je relací ekvivalence.

Věta 4.2.1.1

Jsou-li α, β dva řezy a utvoříme-li množinu součtů $a_1 + b_1$, kde a_1 je libovolný prvek dolní skupiny řezu α a b_1 libovolný prvek dolní skupiny řezu β, pak je tato množina řez.

Definice 4.2.1.2 (Jednoznačnost sčítání)

Řez sestrojený ve větě 4.2.1.1 se jmenuje součet řezů α, β a značí se $\alpha + \beta$. Součet řezů α, β je svými sčítanci jednoznačně určen.

Věta 4.2.1.2

Součet dvou racionálních řezů definovaných racionálními čísly $\mathcal{A}, \mathcal{B}$ je racionální řez definovaný číslem $\mathcal{A} + \mathcal{B}$, tj. $a^* + b^* = (a + b)^*$.

Věta 4.2.1.3

Pro sčítání řezů platí komutativní a asociativní zákon, tj. pro libovolné dva, resp. tři řezy platí:

$$\alpha + \beta = \beta + \alpha$$

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$$

Věta 4.2.1.4

Jsou-li α, β dva libovolné řezy, existuje alespoň jeden řez ξ takový, že

$$\alpha + \xi = \beta$$

Důsledek: Množina řezů v tělese racionálních čísel obsahuje prvek nulový, tj. takový řez, že $\alpha + o = \alpha$ a ke každému řezu α v tělese racionálních čísel existuje řez opačný, tj. takový řez $-\alpha$, že $\alpha + (-\alpha) = o$.

Definice 4.2.1.3 (Řez kladný a záporný)

Řez, jehož dolní skupina obsahuje číslo 0, nazýváme kladným. Je-li $-\alpha$ kladný řez, nazýváme řez α záporným.

Věta 4.2.1.5

Je-li α libovolný řez v tělese racionálních čísel, nastane právě jeden z případů $\alpha = o$, α je kladné, $-\alpha$ je kladné.

4.2.2 Násobení řezů

Věta 4.2.2.1 (Součin řezů)

Jsou-li α, β dva kladné řezy a utvoříme-li množinu obsahující všechna záporná racionální čísla, nulu a všechny součiny tvaru $a_1.b_1$, kde a_1 je libovolné kladné číslo dolní skupiny řezu α a b_1 libovolné kladné číslo dolní skupiny řezu β, pak tato množina je řez.

Definice 4.2.2.1(Jednoznačnost násobení)

Jsou-li řezy α, β kladné, pak řez konstruovaný ve větě 4.2.2.1 se jmenuje součin řezů a značí se $\alpha.\beta$. Vedle toho pro každé α a β platí:

$$\alpha.o = o.\beta = o$$

$$\alpha.(-\beta) = (-\alpha).\beta = -(\alpha.\beta)$$

Řez utvořený ve větě 4.2.2.1 je jediný, tedy platí, že je jednoznačně určen.

Věta 4.2.2.2

Součin dvou racionálních řezů definovaných racionálními čísly $\mathcal{A}, \mathcal{B}$ je racionální řez, definovaný součinem $\mathcal{A}.\mathcal{B}$, tj. platí $a^*.b^* = (a.b)^*$.

Věta 4.2.2.3

Pro násobení libovolných dvou či tří řezů platí komutativní a asociativní zákony:

$$\alpha.\beta = \beta.\alpha$$

$$\alpha.(\beta.\gamma) = (\alpha.\beta).\gamma$$

Věta 4.2.2.4

Jsou-li α, β libovolné řezy, přičemž $\alpha \neq o$, existuje alespoň jeden řez ξ tak, že

$$\alpha.\xi = \beta$$

Věta 4.2.2.5

Jsou-li α, β kladné řezy, jsou i řezy $\alpha + \beta$ a $\alpha.\beta$ kladné.

Věta 4.2.2.6

Pro sčítání a násobení řezů platí distributivní zákon:

$$\alpha.(\beta + \gamma) = \alpha.\beta + \alpha.\gamma$$

Množina řezů v tělese racionálních čísel je uspořádaným tělesem, protože o jeho prvcích má smysl říkat, že jsou kladné, nebo záporné a jsou splněny vlastnosti uvedené ve větě 4.2.1.5 a 4.2.2.5.

4.3 Uspořádání řezů

Podle definice 3.4.1.6[2] můžeme stanovit, který řez budeme pokládat za větší a který za menší.

[2] Je-li M uspořádaný okruh a jsou-li x_1, x_2 dva jeho prvky, říkáme, že x_1 je větší než x_2, když rozdíl $x_1 - x_2$ je kladný, a že x_1 je menší než x_2, když rozdíl $x_1 - x_2$ je záporný.

Věta 4.3.1

Jsou-li α, β řezy v tělese racionálních čísel, pak $\alpha > \beta$ tehdy a jen tehdy, když existuje číslo dolní skupiny řezu α, které je číslem horní skupiny řezu β. A $\alpha < \beta$ tehdy a jen tehdy, když existuje horní číslo řezu α, které je číslem dolní skupiny řezu β.

Věta 4.3.2

Jsou-li a^*, b^* dva racionální řezy, pak $a < b$ tehdy a jen tehdy, když $a^* < b^*$.

Věta 4.3.3

Racionální číslo a_1 je číslem dolní skupiny řezu α tehdy a jen tehdy, když $a_1^* < \alpha$. Racionální číslo a_2 je číslem horní skupiny řezu α a jen tehdy, když $a_2^* \geq \alpha$.

Definice 4.3.1 (Reálné, racionální a iracionální číslo)

Místo názvu řez v množině racionálních čísel budeme říkat reálné číslo. Racionální řez se jmenuje racionální číslo a iracionální řez je nazývá iracionální číslo.

Touto definicí jsme nezavedli nic nového, jen jiný název. Tento název jsme mohli zavést už na začátku této kapitoly, ale neučinili jsme tak, proto, abychom nepletli název racionální řez s názvem racionální číslo. Nyní ovšem můžeme tyto pojmy ztotožnit. Proto také můžeme všechny věty a definice vyslovené v této kapitole podle tohoto upravit a získáme tak definice pro reálná čísla.

Z tohoto plyne, že množina reálných čísel, je také uspořádané těleso, a to těleso uspořádané archimedovsky.

Věta 4.3.4

Jsou-li a, b dvě reálná čísla a a kladné, existuje takové přirozené číslo n, že $n.a > b$.

Věta 4.3.5

Množina $\mathbb{Q}$ racionálních čísel je hustá v přirozeně uspořádané množině $\mathbb{R}$ reálných čísel.

Důkaz:

Jsou-li a, b dvě libovolná reálná čísla, pro něž platí $a < b$, pak podle věty 4.3.1 existuje racionální číslo X, které patří do horní skupiny řezu α a současně do dolní skupiny řezu β, tj. podle věty 4.3.3 $\alpha \leq X < \beta$. Protože dolní skupina řezu β nemá poslední prvek, proto v ní existuje racionální číslo $X' > X$. Pro číslo X' tedy platí $\alpha \leq X' < \beta$.

Důsledek:

Přirozeně uspořádaná množina reálných čísel $\mathbb{R}$ je hustě uspořádaná, neboť X' patří mezi reálná čísla.

(Podle [Hru53], str. 221)

4.3.1 Spojité uspořádání

V předchozích podkapitolách jsme zkoumali řezy v přirozeně uspořádané množině racionálních čísel, kde jsme dospěli k pojmu iracionální číslo. Zjistili jsme, že v této množině máme dva druhy řezů, z nichž jeden nám nepřinesl nic nového, a druhý nás vedl k novému druhu čísel, tedy ke zmíněným iracionálním číslům.

Ale v téhle podkapitole budeme zkoumat řezy v přirozeně uspořádané množině reálných čísel $\mathbb{R}$. Reálná čísla je třeba zkonstruovat tak, aby beze zbytku vyplnila číselnou osu. Tím je myšleno, že každá neprázdná omezená množina měla v tomto číselném oboru supremum a infimum.

Věta 4.3.1.1 (Dedekindova věta)

Přirozeně uspořádaná množina reálných čísel $\mathbb{R}$ neobsahuje mezery.

Definice 4.3.1.1 (Spojitá množina)

Hustě uspořádaná množina, která neobsahuje mezery, se nazývá spojitá.

Definice 4.3.1.2 (Množina omezená, omezená shora a omezená zdola)

Množinu M reálných čísel nazýváme omezenou shora, existuje-li takové reálné číslo l, že pro každé $z \in M$ platí $z < \ell$

Množinu M reálných čísel nazýváme omezenou zdola, existuje-li takové reálné číslo n, že pro každé $z \in M$ platí $z > n$.

Je-li množina omezená shora i zdola, se nazývá omezená.

Věta 4.3.1.2 (Vlastnosti suprema a infima)

a) Je-li M neprázdná a shora omezená množina reálných čísel, existuje jediné reálné číslo a mající tyto vlastnosti:
   1) Pro každé $z \in M$ platí $z \leq a$.
   2) Zvolíme-li libovolné reálné číslo $a' < a$, existuje alespoň jedno číslo $z \in M$ tak, že $z > a'$.
b) Je-li M neprázdná a zdola omezená množina reálných čísel, existuje jediné reálné číslo b mající tyto vlastnosti:
   3) Pro každé $z \in M$ platí $z \geq b$.
   4) Zvolíme-li libovolné reálné číslo $b' < b$, existuje alespoň jedno číslo $z \in M$ tak, že $z < b'$.

Definice 4.3.1.3(Supremum, infimum)

Číslo a z věty 4.3.1.2 se nazývá supremum množiny M, číslo b se nazývá infimum množiny M.

Věta 4.3.1.3 (Spočetnost množiny reálných čísel)

Množina všech reálných čísel není spočetná.

Všechny číselné obory jsou konstruovány jako množiny, ty je třeba volit tak, aby jejich vzájemné vztahy odpovídaly představám, které o daném číselném oboru máme. Jak už jsme řekli v úvodu této podkapitoly, reálná čísla je třeba konstruovat tak, aby každá neprázdná a omezená množina měla supremum a infimum, které náleží do množiny reálných čísel.

Definice 4.3.1.4 (Dedekindův řez)

Dedekindův řez je každá dolní množina v přirozeně uspořádané množině, která obsahuje své supremum, tedy pokud toto supremum existuje.

Množina všech Dedekindových řezů na množině racionálních čísel přesně odpovídá výše zmíněným požadavkům, což tedy znamená, že jí lze použít jako izomorfní kopii reálných čísel.

Závěr

Tato práce měla za úkol objasnit, jak se konstruují jednotlivé číselné obory. V první kapitole jsme si zavedli přirozená čísla pomocí Peanových axiomů, vyslovili jsme vlastnosti sčítání a násobení přirozených čísel a také vlastnosti jejich uspořádání.

V kapitole druhé, jsme si zavedli celá čísla jako dvojice čísel přirozených, uvedli vlastnosti operací sčítání a násobení a jejich uspořádání. V této kapitole je také nově definováno číslo nula a číslo opačné a jejich vlastnosti vůči sčítání a násobení. Pro konstrukci tohoto oboru, bylo také nutné objasnit princip vnoření komutativní pologrupy do grupy, neboť toto nám zdůvodní, proč jsme celá čísla zavedli jako dvojice přirozených.

Třetí kapitola je věnována racionálním číslům, která zavádíme jako dvojice celých čísel, ukazujeme zde opět vlastnosti sčítání a násobení a jejich uspořádání. Pro konstrukci racionálních čísel, je nutné ještě uvést princip vnoření komutativního okruhu do tělesa, kterým je objasněno, proč si zavádíme racionální čísla, jako dvojice celých čísel. Oproti celým číslům je zde nově proveditelné dělení a s ním související existence inverzního prvku pro operaci násobení, převráceného čísla.

Ve čtvrté kapitole jsme zkonstruovali reálná čísla metodou Dedekindových řezů. V této kapitole je také vysvětlen pojem iracionální číslo. Množinu iracionálních čísel chápeme jako rozdíl množiny reálných a racionálních čísel. Stejně jako u ostatních kapitol i zde uvádíme vlastnosti sčítání, násobení a uspořádání reálných čísel.

Vzhledem k rozsahu práce, již nebyl prostor ke konstrukci oboru komplexních, resp. hyperkomplexních čísel, která by se konstruovala podobně jako čísla celá a racionální, tedy bychom si je zavedli jako dvojice reálných, resp. Komplexních či určitého typu hyperkomplexních čísel.

Pokud v práci nebylo uvedeno jinak, byly veškeré použité věty a definice převzaty z publikací uvedených v seznamu použité literatury.

Resumé

The thesis deals with the method of construction of numerical domains. The thesis is divided into four chapters. In the first chapter, we occupy ourselves with an implementation of natural numbers with the aid of Pean's axioms, which I implement the basic characteristics of the domain with. In the second chapter we define the integer domain as pairs of natural numbers via method of embedding of Abelian half-group into group. In the third chapter I devote myself to the rational domain and its construction with the help of integer numbers. The issue is an establishment of rational numbers as pairs of integer numbers. In the last chapter we deal with the real domain whose construction is made by the method of Dedekind's cuts. There is also a reference to the real domain as a difference between sets of real and rational numbers.

Seznam použitých pramenů

Tištěné zdroje:

[BCK83] Blažek, Jaroslav aj. *Algebra a teoretická aritmetika. I. Díl.* Praha: SPN, 1983

[Hru53] Hruša, Karel. *Elementární aritmetika.* Praha: Přírodovědecké vydavatelství, 1953.

[Kur68] Kuroš, A.G. *Kapitoly z obecné algebry.* Praha: Academia, 1968

[Jat10] Jatiová, Kateřina. *Postupná rozšiřování významu pojmu číslo ve školské matematice*. Diplomová práce. Plzeň: 2010

[Mat09] Matějovská, Eva. *Historické souvislosti rozšiřování číselného oboru ve školské matematice.* Diplomová práce. Plzeň: 2009

Internetové zdroje:

[Bot11] Botur, Michal. *Úvod do aritmetiky* [online]. 2011. Dostupné z http://www.kag.upol.cz/ucitprir/texty%5CAritmetika_botur.pdf

[Ema11] Emanovský, Petr. *Úvod do studia matematiky* [online]. 2011.Dostupné z http://www.kag.upol.cz/ucitprir/texty%5Cuvod_do_studia_mat_eman.pdf

[1] Tesková, Libuše. *Teoretická aritmetika.* [online]. Dostupné z http://home.zcu.cz/~teskova/WWW-KMA/ARI.pdf

[2] www.matweb.cz

[3] cs.wikipedia.org

[4] en.wikipedia.org