INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Profesní příprava učitelů přírodovědných oborů pro uplatnění v konkurenčním prostředí

CZ.1.07/2.2.00/15.0310

ÚVOD DO ARITMETIKY

Michal Botur

2011

Obsah

1 Algebraické základy **3**
- 1.1 Binární relace . . . 3
- 1.2 Zobrazení a operace . . . 7
- 1.3 Algebry s jednou a dvěma binárními operacemi . . . 8
- 1.4 Faktorizace pologrupy a okruhu . . . 10
- 1.5 Věta o vnoření komutativní pologrupy do grupy . . . 11
- 1.6 Vnoření komutativního okruhu do tělesa . . . 16
- 1.7 Uspořádání na okruzích . . . 21
- 1.8 Absolutní hodnota . . . 26

2 Zavedení přirozených čísel pomocí Peanových axiomů **29**
- 2.1 Peanovy axiomy . . . 30
- 2.2 Uspořádání na množině $\mathbb{N}$ . . . 35
- 2.3 Transfinitní indukce a dobře uspořádané množiny . . . 37

3 Konstrukce oboru integrity celých čísel **39**
- 3.1 Uspořádání celých čísel . . . 42
- 3.2 Vnoření celých čísel do uspořádaných okruhů . . . 43

4 Konstrukce tělesa racionálních čísel **45**

5 Konstrukce reálných čísel metodou Dedekindových řezů **49**
- 5.1 Řezy na lineárně uspořádaných množinách . . . 50
- 5.2 Dedekindovy řezy jakožto model reálných čísel . . . 51
- 5.3 Sčítání reálných čísel . . . 52
- 5.4 Násobení kladných reálných čísel . . . 55
- 5.5 Těleso reálných čísel a jeho uspořádání . . . 59
- 5.6 Dedekindova věta, věta o supremu a věta o infimu . . . 61

6 Reálná čísla konstruovaná metodou Cauchyovských posloupností **65**
- 6.1 Fundamentální posloupnosti, základní vlastnosti . . . 65
- 6.2 Aritmetika tělesa fundamentálních posloupností . . . 69
- 6.3 Uspořádání tělesa $\mathbf{F}_{\mathbb{T}}/\sim$ . . . 72
- 6.4 Vlastnosti tělesa $\overline{\mathbb{T}}$ . . . 74

6.5 Těleso reálných čísel 76

7 Komplexní čísla **79**

8 Hyperkomplexní čísla **85**

9 Mocniny **89**
9.1 Mocniny kladných reálných čísel 91

10 Poziční číselné soustavy **97**

11 Základní kritéria dělitelnosti celých čísel **101**

Předmluva

Tento text vznikl jako zápis přednášek pro 3. ročník učitelských kombinací matematiky. Postupně se rozrostl o několik dalších kapitol a částí. Nyní, jak doufám, máte v rukou učebnici, která obsahuje vše podstatné pro pochopení základních konstrukcí číselných oborů. Přestože očekávám, že čtenář již má určitou zkušenost s vyšší matematikou, není k zvládnutí látky potřebné žádné předchozí studium matematických teorií. Jedinou podmínkou pro pochopení textu je zběžná znalost pojmů z teorie množin (jako je množina, podmnožina, průnik, sjednocení atd.) a znalost běžné notace užívané v teorii množin.

První kapitola zavádí základní algebraický aparát, který je potřebný ke konstrukci číselných oborů. Hlavními výsledky je potom zavedení podílové grupy, podílového tělesa a uspořádaných okruhů. Druhá kapitola může být studována nezávisle na první. Věnujeme se v ní Peanově axiomatice přirozených čísel a zavádíme v ní číselný obor $(\mathbb{N}, +, \cdot)$. Ve třetí a čtvrté kapitole využijeme předchozích výsledků k zavedení celých a racionálních čísel. Následující dvě kapitoly prezentují dva z možných způsobů rozšíření racionálních čísel na čísla reálná (jedná se o metodu Dedekindových řezů a metodu fundamentálních posloupností). V posledních částech se věnujeme úvodu do problematiky komplexních čísel, zmíníme se o hyperkomplexních číslech a závěrem připomeneme vlastnosti mocnin, číselných soustav a kritéria dělitelnosti.

Za pomoc při práci a cenné připomínky chci poděkovat prof. Mgr. Radomíru Halašovi, Ph.D., prof. RNDr. Ivanu Chajdovi, DrSc. a doc. RNDr. Janu Kührovi, Ph.D. Za pomoc a péči o text děkuji Zuzaně Brovjákové. Tato skripta byla napsána v rámci projektu a financovaná projektem ESF „Profesní příprava učitelů přírodovědných oborů pro uplatnění v konkurenčním prostředí“ CZ.1.07/2.2.00/15.0310.

Kapitola 1

Algebraické základy

1.1 Binární relace

Teorie množin je základním aparátem k matematickému modelování. Předpokládáme, že čtenář zná množinové operace (průnik, sjednocení apod.). Připomeňme ještě, že pro libovolné množiny A, B rozumíme jejich kartézským součinem množinu $A \times B = \{\langle a, b\rangle \mid a \in A, b \in B\}$, kde $\langle a, b\rangle$ je uspořádaná dvojice prvků a a b. Kartézskou mocninou A^n rozumíme kartézský součin: $\overbrace{A \times A \times \cdots \times A}^{n\times}$.

Kartézské součiny a mocniny používáme k definici a popisu relací (vztahů). Uvedeme si následující příklad modelovaného vztahu. Představme si množinu všech lidí L, kteří kdy žili. Potom zavedeme relaci „být sourozencem“ tak, že jeden člověk je sourozencem druhého člověka, jestliže mají oba lidé stejného alespoň jednoho rodiče. Tento sourozenecký vztah lze potom určit následující množinou uspořádaných dvojic:

$$\{\langle a, b\rangle \mid a \text{ je sourozencem } b\} \subseteq L^2.$$

Předchozí příklad ukazuje, že vztah mezi prvky množiny A a prvky množiny B lze modelovat pomocí některé podmnožiny $A \times B$. Navíc můžeme uvažovat i opačně, každá podmnožina množiny $A \times B$ představuje možný vztah mezi prvky množiny A a prvky množiny B (jistě neplatí, že každý možný vztah je smysluplný, na druhou stranu neumíme předem vyloučit, že některá konkrétní podmnožina kartézského součinu nemůže být v nějakém významu užitečným vztahem). Předchozí úvahy motivují následující definici.

Definice 1 *Mějme množiny A a B. Potom libovolnou množinu $R \subseteq A \times B$ nazýváme binární relaci mezi množinami A a B. Libovolnou množinu $R \subseteq A^2$ nazýváme binární relací na množině A.*

Slovo binární naznačuje, že modelujeme vztahy mezi dvěma množinami. Definici lze snadno rozšířit tak, že množinu $R \subseteq A_1 \times A_2 \times \cdots \times A_n$ nazveme n-nární relací mezi množinami $A_1, \ldots, A_n$ a analogicky $R \subseteq A^n$ nazveme n-nární relací na množině A. V této učebnici zužitkujeme pouze teorii binárních relací, proto si vystačíme s tímto omezeným pojetím relace.

Uvedeme si příklady některých známých binárních relací:

(i) Relace být rovnoběžný „$\parallel$“ na množině všech přímek v rovině.

(ii) Relace být větší nebo roven „$\leq$“ na množině reálných čísel.

(iii) Relace být kolmý „$\perp$“ na množině rovin v prostoru.

(iv) Relace „$|$“ na množině přirozených čísel $\mathbb{N}$, kde $a|b$ čteme jako „číslo a dělí číslo b“ (tedy existuje $n \in \mathbb{N}$ takové, že $a \cdot n = b$).

Zaměříme se ještě chvíli na značení binárních relací. Jak jsme uvedli v definici, binární relace je množina, proto ji můžeme značit velkým písmenem (např. R, R_1, S apod.). Obvykleji se ovšem setkáváme s užíváním relačních symbolů (například $<$, $\leq$, $\sim$, $\perp$, $\prec$, $\ll$, $\cong$, $\neq$ apod.). Užívání relačních symbolů značně zjednodušuje notaci, proto u binární relace R značíme pomocí aRb skutečnost, že $\langle a, b\rangle \in R$ (tedy a je ve vztahu R s b).

Na druhou stranu, jestliže budeme binární relaci značit pomocí relačního symbolu, nesmíme zapomínat, že se jedná stále o množinu. Například relace $<$ je rovna množině

$$\{\langle a, b\rangle \in \mathbb{N}^2 \mid \text{existuje } n \in \mathbb{N} \text{ takové, že } a + n = b\}.$$

I množinu můžeme značit relačním symbolem.

V následujícím textu se budeme setkávat s několika druhy relací. Mezi velmi významné relace patří relace uspořádání a relace ekvivalence. K jejich zavedení budeme potřebovat následující pojmy:

Definice 2 *Řekneme, že relace R na množině A je:*

(i) Reflexivní, jestliže pro libovolné $a \in A$ platí aRa (tedy $\langle a, a\rangle \in R$).

(ii) Ireflexivní, jestliže pro libovolné $a \in A$ neplatí aRa (tedy $\langle a, a\rangle \notin R$).

(iii) Symetrická, jestliže platí, že z aRb plyne bRa pro všechna $a, b \in A$.

(iv) Antisymetrická, jestliže z aRb a bRa plyne $a = b$ pro libovolná $a, b \in A$.

(v) Asymetrická, jestliže z aRb plyne, že neplatí bRa (tedy z $\langle a, b\rangle \in R$ plyne $\langle b, a\rangle \notin R$) pro všechna $a, b \in A$.

(vi) Tranzitivní, jestliže z aRb a bRc plyne aRc.

Prvním významným typem binárních relací je uspořádání.

Definice 3 *Binární relaci $\leq$ na množině A nazveme uspořádáním na množině A, jestliže $\leq$ je reflexivní, tranzitivní a antisymetrická relace. Dvojici $(A, \leq)$ potom nazýváme uspořádanou množinou.*

Relace uspořádání modeluje situaci, kdy můžeme považovat některé prvky za větší než jiné. V našem intuitivním vnímání má tomuto uspořádání nejblíže klasická relace $\leq$ na reálných číslech. Naše definice ovšem připouští to, že některé dva prvky mohou být nesrovnatelné. Přestože se toto může na první pohled zdát nepřirozené, ukážeme si jednoduchý příklad uspořádání s nesrovnatelnými prvky.

Vezměme tříprvkovou množinu $\{1, 2, 3\}$ a všechny její podmnožiny. Tento systém množin[1] označme S. Potom si snadno všimneme, že relace $\subseteq$ je relací uspořádání na množině S, přičemž množiny $\{1, 2\}$ a $\{2, 3\}$ jsou nesrovnatelné (ani jedna není podmnožinou druhé).

Všechna uspořádání v teorii číselných oborů jsou uspořádání bez nesrovnatelných prvků. Máme-li uspořádanou množinu $(A, \leq)$, potom řekneme, že $\leq$ je lineárně uspořádaná množina, jestliže pro libovolné $x, y \in A$ platí, že $x \leq y$ nebo $y \leq x$.

Analogicky někdy definujeme ostré uspořádání $<$ na množině A jako binární relaci na A, která je ireflexivní, tranzitivní a asymetrická. Je snadné domyslet, že mezi uspořádáními a ostrými uspořádáními je vzájemně jednoznačná korespondence definovaná následujícím vztahem:

$$x \leq y \text{ tehdy a jen tehdy, jestliže } x < y \text{ nebo } x = y$$

nebo analogicky

$$x < y \text{ tehdy a jen tehdy, jestliže } x \leq y \text{ a současně } x \neq y.$$

Ostré uspořádání $<$ na množině A nazveme trichotomické, jestliže pro libovolné prvky $x, y \in A$ platí právě jedno z tvrzení $x < y$, $x = y$, nebo $y < x$. Čtenář si může snadno ověřit, že ostré uspořádání $<$ je trichotomické právě tehdy, když $\leq$ je lineární uspořádání.

Kromě uspořádání si nyní ještě připomeňme jeden významný typ relací, kterým je relace ekvivalence. Jak již napovídá jazykový základ slova ekvivalence, relace nám dává objekty do vztahu, jsou-li v jistém smyslu stejné (stejně hodnotné) nebo mají-li něco stejného. V tomto textu budeme pro konkrétní relaci ekvivalence používat symbol $\sim$ (budeme-li mít v daném okamžiku zavedeno více ekvivalencí, budeme je odlišovat indexem; tj. $\sim_1$, $\sim_2$ apod.). Jsou-li tedy dva prvky x, y ekvivalentní podle ekvivalence $\sim$, značíme toto $x \sim y$.

Definice 4 *Binární relaci $\sim$ na množině A nazýváme relace ekvivalence, jestliže je tato relace reflexivní, symetrická a tranzitivní.*

S pojmem relace ekvivalence úzce souvisí další pojem takzvaného rozkladu množiny na třídy. Rozkladem množiny na třídy rozumíme rozdělení (roztrhání) této množiny na menší množiny. Přirozeně očekáváme, že každý prvek z původní množiny bude náležet právě jedné množině rozkladu. Definujme tedy formálně.

Definice 5 *Systém neprázdných množin $M_i \subseteq M$ takových, že $i \in I$ (přesněji $\{M_i \subseteq M \mid i \in I\}$) nazveme rozkladem množiny M na třídy, jestliže platí, že $\bigcup_{i \in I} M_i = M$, a navíc pro $i, j \in I$ takové, že $i \neq j$ platí $M_i \cap M_j = \emptyset$.*

[1] Tedy $S = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Následující věta ukáže souvislost mezi relací ekvivalence a rozkladem množiny na třídy. Předpokládejme, že M je množina a na ní máme definovanou ekvivalenci $\sim$. Potom označme $[x]_\sim$ množinu všech prvků, které jsou s prvkem x ekvivalentní. Tedy $[x]_\sim = \{y \in M \mid x \sim y\}$ a tuto množinu nazýváme třídu rozkladu relace $\sim$ reprezentovanou prvkem x. Potom systém všech takovýchto množin označíme $M/\sim$. Jak nám ukáže následující věta, takto vytvořený systém množin tvoří rozklad.

Celou situaci si demonstrujme na následujícím příkladu. Vezměme například množinu všech aut, potom řekneme, že auta jsou „stejnobarevná“, jestliže mají stejnou barvu. Jak se snadno vidí „stejnobarevnost“ je relace (vztah) na množině všech automobilů, a navíc se jedná o relaci ekvivalence (snadno se ověří reflexivita, symetrie i tranzitivita této relace). Na základě této relace můžeme auta **roztřídit** (tedy vytvořit rozklad na třídy) a to tak, že v každé vzniklé množině budou právě všechna auta stejné barvy. Rozkladem na třídy je tedy systém takovýchto skupin (množin) aut. Je vidět, že takovým způsobem postupovat můžeme a zřejmě vznikne korektní rozklad. Naopak pokud máme nějakou množinu rozloženou na třídy (tedy prvky množiny nějakým způsobem roztříděné), můžeme vytvořit relaci ekvivalence tak, že dva prvky jsou ekvivalentní, právě když leží ve stejné třídě. Snadno se ověří reflexivita, symetrie i tranzitivita. Celou zde popsanou myšlenku popisuje následující věta.

Věta 1 *(i) Mějme množinu M a relaci ekvivalence $\sim$ na množině M. Potom platí, že systém $M/\sim$ je rozklad množiny M na třídy.*

(ii) Mějme množinu M a rozklad množiny M na třídy $\{M_i \subseteq M \mid i \in I\}$. Potom relace $\sim$ definovaná na množině M tak, že $x \sim y$ tehdy a jen tehdy jestliže existuje $i \in I$ takové, že $x, y \in M_i$ je relace ekvivalence.

(iii) Korespondence popsaná v bodech (i) a (ii) této věty je vzájemně jednoznačná. Tedy vytvoříme-li z ekvivalence rozklad podle bodu (i) a poté z rozkladu ekvivalenci podle bodu (ii), dostaneme původní relaci ekvivalence[2]*.*

Důkaz: ad (i) Musíme dokázat, že systém $M/\sim$ je rozklad množiny na třídy. Nejprve platí, že pro libovolné $x \in M$ je $[x]_\sim \subseteq M$. Tedy $\bigcup_{x\in M}[x]_\sim \subseteq M$. Opačně jestliže $x \in M$, potom z reflexivity plyne $x \sim x$, a tedy platí $x \in [x]_\sim$. Proto také platí $x \in \bigcup_{x\in M}[x]_\sim$. Dohromady dostáváme $\bigcup_{x\in M}[x]_\sim \subseteq M$, a v důsledku také $\bigcup_{x\in M}[x]_\sim = M$. Zbývá dokázat, že dvě různé množiny rozkladu mají prázdný průnik.

Dokážeme, že pokud mají dvě třídy ekvivalence neprázdný průnik, potom se rovnají. Nechť $x, y \in M$ jsou takové, že existuje $a \in [x]_\sim \cap [y]_\sim$, potom platí, že $a \in [x]_\sim$ a $a \in [y]_\sim$. Z definice tříd ekvivalence plyne, že $x \sim a$ a $y \sim a$. Ze symetrie a tranzitivity proto máme $x \sim y$ (resp. $y \sim x$). Nyní dokážeme rovnost množin $[x]_\sim$ a $[y]_\sim$.

Nechť $z \in [x]_\sim$, potom platí, že $x \sim z$. Protože také $y \sim x$, z tranzitivity plyne $y \sim z$. Proto $z \in [y]_\sim$. Dohromady potom dostáváme $[x]_\sim \subseteq [y]_\sim$. Opačně jestliže $z \in [y]_\sim$, potom $y \sim z$. Užitím tranzitivity a symetrie získáváme $x \sim z$, a v důsledku také $z \in [x]_\sim$. Máme dokázanou opačnou inkluzi $[y]_\sim \subseteq [x]_\sim$. Dohromady také rovnost $[x]_\sim = [y]_\sim$.

[2] Analogicky můžeme tvrdit, že jestliže z rozkladu vytvoříme ekvivalenci podle bodu ii) a poté z této ekvivalence vytvoříme rozklad podle i), získáme původní rozklad.

ad (ii) Mějme rozklad množiny M na třídy $\{M_i \subseteq M \mid i \in I\}$. Připomeňme, že pro libovolné $x \in M$ existuje jediné $i \in I$ takové, že $x \in M_i$. Zavedeme relaci $\sim$ takovou, že $x \sim y$ tehdy a jen tehdy, když existuje $i \in I$ takové, že $x, y \in M_i$. Dokážeme, že takto vytvořená relace je ekvivalence. Již jsme zmínili, že pro libovolné $x \in M$ existuje jediné $i \in I$ tak, že $x \in M_i$. Z tohoto plyne reflexivita relace $\sim$. Pokud prvky $x, y \in M$ náleží do stejné třídy M_i, potom také $y, x \in M$ má stejnou vlastnost. Proto je relace $\sim$ symetrická. Předpokládejme nakonec, že $x \sim y$ a $y \sim z$ pro některé prvky $x, y, z \in M$. Podle definice $\sim$ platí, že existují $i, j \in I$ takové, že $x, y \in M_i$ a $y, z \in M_j$. Protože ale prvek y může náležet jediné třídě rozkladu, platí, že $M_i = M_j$, a proto $x, y, z \in M_j$. Dohromady dostáváme $x \sim z$, což dokončuje důkaz tranzitivity.

ad (iii) Mějme relaci ekvivalence $\sim$ na množině M. Zavedeme ekvivalenci $\sim_*$ tak, že $a \sim_* b$, jestliže $a, b \in [x]_\sim$. Nyní $a \sim_* b$ implikuje, že $a, b \in [x]_\sim$, a tedy také $a \sim x$ a $x \sim b$. Proto z tranzitivity a symetrie $\sim$ dostáváme, že $a \sim b$.

Naopak předpokládejme, že $a \sim b$. Potom $a, b \in [a]_\sim$, a tedy konečně $a \sim_* b$. Dokázali jsme, že $a \sim b$ nastává tehdy a jen tehdy, jestliže $a \sim_* b$, a tedy obě relace jsou stejné $\square$

Popsaná konstrukce rozkládání množiny na třídy podle nějaké ekvivalence se nazývá faktorizace množiny na třídy. Vzniklé množině $M/\sim$ říkáme faktorová množina. Připomeňme ještě, že pro libovolnou ekvivalenci $\sim$ platí, že $x \sim y$ tehdy a jen tehdy, když $[x]_\sim = [y]_\sim$, jak jsme ostatně dokázali ve Větě 1. Konečně ještě uveďme, že prvek x nazýváme reprezentantem třídy $[x]_\sim$. Každá třída je proto určena (reprezentována) kterýmkoliv svým prvkem.

1.2 Zobrazení a operace

Zobrazením rozumíme libovolné přiřazení prvků z jedné množiny do množiny druhé. Zobrazení zavádíme jako speciální případ binárních relací.

Definice 6 *Binární relaci $f \subseteq A \times B$ nazveme zobrazením, jestliže pro libovolné $x \in A$ existuje jediné $y \in B$ takové, že $\langle x, y\rangle \in f$ (v případě zobrazení tuto skutečnost častěji značíme pomocí zápisu $f(x) = y$). Skutečnost, že f je zobrazení prvků z množiny A do množiny B, zapisujeme pomocí $f : A \longrightarrow B$. Dále množinu A nazýváme množinou vzorů a B nazýváme množinou obrazů.*

Zobrazení f nazýváme *injektivní,* jestliže různé obrazy z množiny A mají různé vzory v B (formálně z $f(x) = f(y)$ plyne $x = y$). Zobrazení je *surjektivní*, jestliže každý prvek z množiny B má alespoň jeden obraz (tj. pro libovolné $y \in B$ existuje $x \in A$ takové, že $f(x) = y$). Zobrazení, které je injektivní i surjektivní současně, nazýváme *bijekcí.*

Speciálním případem zobrazení jsou operace na množině.

Definice 7 *Zobrazení $f : A^n \longrightarrow A$ nazýváme n-nární operací na množině A.*

Příkladem jsou například binární operace $+$ a $\cdot$ na množině reálných čísel $\mathbb{R}$. V teorii množin se můžeme setkat s operacemi sjednocení $\cup$, průniku $\cap$ nebo množinového rozdílu $\setminus$.

1.3 Algebry s jednou a dvěma binárními operacemi

V této kapitole se budeme věnovat některým algebraickým teoriím, jež jsou nezbytné pro konstrukci číselných oborů. Připomeňme si nejprve základní pojmy. Mějme množinu G a na ní libovolnou binární operaci $*$ (tedy zobrazení, které dvojici $\langle x, y\rangle \in M^2$ přiřadí prvek $x*y \in M$). Potom algebraickou strukturu $\mathbf{G} = (G, *)$ nazýváme *grupoid*. *Pologrupou* rozumíme libovolný grupoid, který splňuje tzv. asociativní zákon (tj. $x*(y*z) = (x*y)*z$). Prvek e v pologrupě $\mathbf{G}$ nazveme *neutrálním*, jestliže pro libovolný prvek $x \in G$ platí, že $x * e = e * x = x$. Pologrupě s jednotkovým prvkem říkáme *monoid*. Předpokládejme nakonec, že $\mathbf{G} = (G, *)$ je monoid, potom prvek $x' \in G$ je *inverzní* k prvku $x \in G$, pokud platí $x * x' = x' * x = e$. Monoid G takový, že ke každému prvku $x \in G$ existuje inverzní prvek $x' \in G$, se nazývá *grupa*. Navíc operaci $*$ nazveme *komutativní*, jestliže platí $x * y = y * x$ pro všechny prvky $x, y \in G$.

Je třeba upozornit, že v teorii grup se můžeme setkat s několika různými způsoby značení. Kromě zcela obecného značení, jež jsme používali v předchozím odstavci, užíváme takzvanou aditivní symboliku, kdy operaci značíme stejně jako klasické sčítání $+$ (přestože nemusí jít o klasický součet), neutrální prvek značíme 0 (nazýváme jej nulový prvek) a inverzní prvkem k prvku x značíme jako $-x$ (a nazýváme jej alternativně jako opačný prvek). Někdy analogicky užíváme takzvanou multiplikativní symboliku, která vychází ze značení klasického násobení. Operace je tedy značena jako $\cdot$, neutrální prvek nazýváme jednotkovým prvkem a značíme jej 1 a konečně inverzní prvek k prvku x je značen x^{-1}. Uvědomme si, že tvrzení dokazována v teorii grup nejsou v žádném případě na užité symbolice závislá a všechna tvrzení můžeme volně přepisovat z libovolné symboliky do jiné. V následujícím Lematu uvedeme jako příklad obě symboliky, přičemž v dalším textu budeme předpokládat, že jednotlivé přepisy zvládne čtenář sám.

Lemma 1 *(i) V každé pologrupě* $\mathbf{G} = (G, \cdot)$ *(resp.* $\mathbf{G} = (G, +)$*)existuje nejvýše jeden neutrální prvek* 1 *(resp.* 0*).*

(ii) V každém monoidu $\mathbf{G} = (G, \cdot)$ *(resp.* $\mathbf{G} = (G, +)$*) existuje ke každému prvku* $x \in G$ *nejvýše jeden inverzní (resp. opačný) prvek* x^{-1} *(resp.* $-x$*). Důsledkem tohoto je, že* $(x^{-1})^{-1} = x$ *(resp.* $-(-x) = x$*).*

(iii) Jestliže $\mathbf{G} = (G, \cdot)$ *(resp.* $\mathbf{G} = (G, +)$*) je grupa a prvky* $x^{-1}, y^{-1} \in G$ *(resp.* $-x, -y \in G$*) jsou inverzní (resp. opačné) prvky postupně k prvkům* $x, y \in G$*, potom prvek* $y^{-1} \cdot x^{-1}$ *(resp.* $(-y) + (-x)$*) je inverzní k prvku* $x \cdot y$ *(resp.* $x + y$*). Platí tedy* $y^{-1} \cdot x^{-1} = (x \cdot y)^{-1}$ *(resp.* $(-y) + (-x) = -(x + y)$*).*

Důkaz: ad (i) Předpokládejme, že existují dva neutrální prvky, které označíme $1_a, 1_b \in G$. Potom přímo podle definice neutrálního prvku platí, že $1_a = 1_a \cdot 1_b = 1_b$.
ad (ii) Předpokládejme, že k prvku $x \in G$ existují dva inverzní prvky $x_a^{-1}, x_b^{-1} \in G$. Potom z vlastnosti inverzního a neutrálního prvku můžeme počítat:

$$x_a^{-1} = x_a^{-1} \cdot 1 = x_a^{-1} \cdot (x \cdot x_b^{-1}) = (x_a^{-1} \cdot x) \cdot x_b^{-1} = 1 \cdot x_b^{-1} = x_b^{-1}.$$

Druhou část tvrzení dostaneme ze skutečnosti, že oba prvky x a $(x^{-1})^{-1}$ jsou inverzní k prvku x^{-1}. Musí se proto rovnat.

ad (iii) Platí, že $(x\cdot y)\cdot(y^{-1}\cdot x^{-1}) = x\cdot 1\cdot x^{-1} = 1$. Analogicky také platí $(y^{-1}\cdot x^{-1})\cdot(x\cdot y) = y\cdot 1\cdot y^{-1} = 1$. Tedy $y^{-1}\cdot x^{-1}$ je inverzní k $x\cdot y$ stejně jako prvek $(x\cdot y)^{-1}$. Protože jsme v předchozím bodě dokázali, že takovýto inverzní prvek je jediný, musí nastat rovnost $y^{-1}\cdot x^{-1} = (x\cdot y)^{-1}$. □

Definujme si nyní některé algebry se dvěma binárními operacemi. Tyto operace obvykle značíme stejně jako klasický součet a součin, což ale obecně neznamená, že se o klasický součet a součin jedná.

Řekneme, že algebraická struktura $\mathbf{O} = (O, +, \cdot)$ je *okruh*, jestliže platí, že struktura $(O, +)$ je komutativní grupa, struktura $(O, \cdot)$ je pologrupa a platí takzvané distributivní zákony: $x\cdot(y+z) = x\cdot y + x\cdot z$ a $(y+z)\cdot x = y\cdot x + z\cdot x$. Řekneme, že okruh je *unitární*, jestliže v něm existuje jednotkový prvek (tedy neutrální prvek vzhledem k operaci $\cdot$). Okruh nazveme *komutativní,* jestliže je operace $\cdot$ komutativní.

Komutativní unitární okruh je *oborem integrity,* jestliže součinem dvou nenulových prvků je opět nenulový prvek (jestliže $x\cdot y = 0$, potom $x = 0$ nebo $y = 0$; obvykle pak říkáme, že v okruhu nejsou netriviální dělitelé nuly).

Konečně jestliže okruh $\mathbf{O} = (O, +, \cdot)$ splňuje podmínku, že struktura $(O\setminus\{0\}, \cdot)$ je grupa (jinak řečeno ve struktuře existují inverzní prvky k nenulovým prvkům), potom jej nazýváme *těleso*[3].

Lemma 2 *V každém okruhu* $\mathbf{O} = (O, +, \cdot)$ *platí pro libovolné* $x \in O$, *že* $x\cdot 0 = 0\cdot x = 0$. *Navíc pro každé* $x, y \in O$ *platí, že* $x\cdot(-y) = (-x)\cdot y = -(x\cdot y)$ *(a tedy také* $(-x)\cdot(-y) = x\cdot y$*).*

Důkaz: Pro $x \in O$ platí, že $x\cdot 0 + x\cdot x = x\cdot(x+0) = x\cdot x$. Přičteme-li nyní k této rovnosti prvek $-(x\cdot x)$, dostáváme, že $x\cdot 0 = x\cdot 0 + x\cdot x + (-(x\cdot x)) = x\cdot x + (-(x\cdot x)) = 0$. Zcela analogicky pro $0\cdot x = 0$.

Nechť máme prvky $x, y \in O$. Potom platí, že $x\cdot y + x\cdot(-y) = x\cdot(y+(-y)) = x\cdot 0 = 0$. Toto ovšem přímo podle definice a jednoznačnosti existence opačného prvku z Lemmatu 1 dává, že $x\cdot(-y) = -(x\cdot y)$. Analogicky dokážeme také $(-x)\cdot y = -(x\cdot y)$. Z dokázaných částí věty a opět z Lemmatu 1 dostáváme $(-x)\cdot(-y) = -(x\cdot(-y)) = -(-(x\cdot y)) = x\cdot y$. □

Dokázané tvrzení nám umožňuje zjednodušit symboliku a bez újmy na korektnosti budeme zápisem $-x\cdot y$ rozumět kterýkoliv z navzájem rovných prvků $x\cdot(-y)$, $(-x)\cdot y$ a $-(x\cdot y)$. Proto nadále budeme zápisem $x-y$ rozumět výraz $x+(-y)$. Nyní je již snadným cvičením dokázat, že platí $x\cdot(y-z) = x\cdot y - x\cdot z$ a také $(y-z)\cdot x = y\cdot x - z\cdot x$.

Lemma 3 *V tělese neexistují netriviální dělitelé nuly (proto každé komutativní těleso je oborem integrity).*

[3]Připomeňme, že v literatuře se ještě setkáváme s pojmem *pole*, což je komutativní těleso (tedy těleso s komutativní operací $\cdot$)

Důkaz: Nechť platí, že $\mathbf{O} = (O, +, \cdot)$ je těleso a pro některé prvky $x, y \in O$ platí, že $x \cdot y = 0$. Potom pokud $x \neq 0$, existuje z definice tělesa $x^{-1} \in O$, a tedy $y = 1 \cdot y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0$. Proto z $x \neq 0$ plyne, že $y = 0$, což dokazuje tvrzení. □

1.4 Faktorizace pologrupy a okruhu

Konstrukci faktorizace užíváme nejen u množin, ale u celých algebraických struktur (v této kapitole se budeme věnovat speciálně grupám a okruhům). Uveďme následující příklad. Vezměme celá čísla $\mathbb{Z}$ spolu s operacemi sčítání a násobení. Zavedeme ekvivalenci takovou, že dvě čísla jsou ekvivalentní, jestliže dávají stejný zbytek při dělení číslem 2. Platí, že navzájem ekvivalentní jsou právě všechna sudá čísla a taktéž všechna lichá čísla. Vzniklá faktorová množina má dva prvky, a to množinu všech sudých a množinu všech lichých čísel. Snadno si všimneme, že můžeme z klasického sčítání a násobení odvodit operace sčítání a násobení na faktorové množině tak, že např. sudá + sudá = sudá, sudá + lichá = lichá a lichá + lichá = sudá. Podobně zavedeme násobení.

Abychom mohli prezentovanou myšlenku realizovat, musí námi vytvořená ekvivalence splňovat něco více než jen to, že je pouhá ekvivalence. K tomuto zavádíme následující definici.

Definice 8 *Mějme libovolnou pologrupu* $\mathbf{G} = (G, \cdot)$. *Potom relaci ekvivalence* $\sim$ *na množině* G *nazveme kongruencí grupy* $\mathbf{G}$, *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* $\sim$ *je kompatibilní s operací* $+$ *nebo alternativně, že* $\sim$ *zachovává operaci* $+$*).*

Mějme libovolný okruh $\mathbf{O} = (O, +, \cdot)$. *Potom relaci ekvivalence* $\sim$ *na množině* O *nazveme kongruencí okruhu* $\mathbf{O}$, *jestliže pro libovolné prvky* $x_1, x_2, y_1, y_2 \in O$ *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* $x_1 + x_2 \sim y_1 + y_2$ *(říkáme, že relace* $\sim$ *je kompatibilní s operacemi* $+$ *a* $\cdot$ *nebo alternativně, že* $\sim$ *zachovává operace* $+$ *a* $\cdot$*).*

Předchozí myšlenky mají vyústění v následující větě.

Věta 2 *(i) Mějme libovolnou pologrupu* $\mathbf{G} = (G, \cdot)$ *a na ní kongruenci* $\sim$. *Potom lze na množině* $G/\sim$ *zavést operaci* $\cdot$ *tak, že pro libovolné* $[x]_\sim, [y]_\sim \in G/\sim$ *platí, že* $[x]_\sim \cdot [y]_\sim = [x \cdot y]_\sim$, *a navíc algebraická struktura* $\mathbf{G}/\sim = (G/\sim, \cdot)$ *je opět pologrupa.*

(ii) Mějme libovolný okruh $\mathbf{O} = (O, +, \cdot)$ *a na něm kongruenci* $\sim$. *Potom lze na množině* $O/\sim$ *zavést operace* $+$ *a* $\cdot$ *tak, že pro libovolné* $[x]_\sim, [y]_\sim \in O/\sim$ *platí, že* $[x]_\sim + [y]_\sim = [x + y]_\sim$ *a* $[x]_\sim \cdot [y]_\sim = [x \cdot y]_\sim$. *Navíc algebraická struktura* $\mathbf{O}/\sim = (O/\sim, +, \cdot)$ *je opět okruh.*

Důkaz: ad (i) K ověření korektnosti definice operace stačí ukázat, že výsledek operace součinu nezávisí na volbě reprezentanta. Z rovností $[x_1]_\sim = [y_1]_\sim$ a $[x_2]_\sim = [y_2]_\sim$ plyne $x_1 \sim y_1$ a $x_2 \sim y_2$. Protože $\sim$ je kongruence, dostáváme $x_1 \cdot x_2 \sim y_1 \cdot y_2$. Toto ovšem dává

opět $[x_1 \cdot x_2]_\sim = [y_1 \cdot y_2]_\sim$. Tedy operace $\cdot$ je definovaná korektně. Asociativitu dokazuje následující výpočet:

$$\begin{aligned}
[x]_\sim \cdot ([y]_\sim \cdot [z]_\sim) &= [x]_\sim \cdot [y \cdot z]_\sim = \\
&= [x \cdot (y \cdot z)]_\sim = \\
&= [(x \cdot y) \cdot z]_\sim = \\
&= [x \cdot y]_\sim \cdot [z]_\sim = \\
&= ([x]_\sim \cdot [y]_\sim) \cdot [z]_\sim.
\end{aligned}$$

Dokázali jsme, že $\mathbf{G}/\!\sim = (G/\!\sim, \cdot)$ je opět pologrupa.

ad (ii) Mějme okruh $\mathbf{O} = (O, +, \cdot)$ a na něm kongruenci $\sim$. Podle definice kongruence na okruhu je $\sim$ kongruencí na obou pologrupách $(O, +)$ a $(O, \cdot)$. Vzhledem k dokázané části věty jsou operace $+$ a $\cdot$ opět korektně definovány na množině $O/\!\sim$, a navíc obě struktury $(O/\!\sim, +)$ i $(O/\!\sim, \cdot)$ jsou pologrupy. Dokažme nejprve, že $(O/\!\sim, +)$ je grupa. Zřejmě platí, že $[x]_\sim + [0]_\sim = [x + 0]_\sim = [x]_\sim = [0 + x]_\sim = [0]_\sim + [x]_\sim$ pro libovolné $[x]_\sim \in O/\!\sim$. Tedy prvek $[0]_\sim$ je neutrálním. Podobně platí, že $[x]_\sim + [-x]_\sim = [x + (-x)]_\sim = [0]_\sim = [(-x) + x]_\sim = [-x]_\sim + [x]_\sim$. Proto $[-x]_\sim$ je opačný prvek k prvku $[x]_\sim$ (formálně bychom zapsali $-[x]_\sim = [-x]_\sim$). Snadno také ověříme distributivní zákony. Například pro libovolné $[x]_\sim, [y]_\sim, [z]_\sim \in O/\!\sim$ platí

$$\begin{aligned}
[x]_\sim \cdot ([y]_\sim + [z]_\sim) &= [x]_\sim \cdot [y + z]_\sim = \\
&= [x \cdot (y + z)]_\sim = [x \cdot y + x \cdot z]_\sim = \\
&= [x \cdot y]_\sim + [x \cdot z]_\sim = \\
&= [x]_\sim \cdot [y]_\sim + [x]_\sim \cdot [z]_\sim.
\end{aligned}$$

Analogicky se dokáže i druhá distributivita. □

V druhé části důkazu jsme mimo jiné dokázali také to, že faktorizací grupy dostaneme znova grupu. Tato úvaha je ve značné šíři prostudována teorií univerzální algebry. Konstrukce faktorizací je snadno zobecnitelná na jiné struktury a je často užívaným matematickým aparátem (kromě samotné algebry hraje významnou roli například v topologii, geometrii, logice apod.). Protože další studium faktorizace není pro naše téma nezbytné, nebudeme jej dále rozvíjet, přesto nelze než doporučit čtenáři důkladné pochopení této v dalším textu hojně užívané konstrukce.

1.5 Věta o vnoření komutativní pologrupy do grupy

Opět si nejprve připomeneme některé základní pojmy. Jestliže máme dvě pologrupy $\mathbf{G} = (G, *)$ a $\mathbf{H} = (H, \circ)$, potom zobrazení $f : G \longrightarrow H$, 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 jej *vnořením.*

Ve skutečnosti pojem vnoření jedné pologrupy do druhé silně koresponduje s postupem rozšíření jedné pologrupy na druhou. Například v následující větě budeme zkoumat

za jakých podmínek lze komutativní pologrupu rozšířit na grupu (tedy kdy můžeme do pologrupy přidat další prvky s odpovídajícími výsledky operace tak, abychom získali grupu). Postupovat budeme tak, že nejprve zkonstruujeme grupu a potom do ní původní pologrupu vnoříme.

Věta 3 (o vnoření komutativní pologrupy do grupy) *Komutativní pologrupu* $\mathbf{G} = (G, \cdot)$ *lze vnořit do grupy tehdy a jen tehdy, platí-li v ní pravidlo krácení. Tj.*

$$x \cdot y = x \cdot z \quad \Longrightarrow \quad y = z. \tag{PK}$$

Důkaz: *Dokážeme, že pokud lze pologrupu vnořit do grupy, platí pravidlo krácení.* Nechť existuje vnoření $f : \mathbf{G} \longrightarrow \mathbf{H}$ z pologrupy $\mathbf{G} = (G, \cdot)$ do grupy $\mathbf{H} = (H, \cdot)$. Nechť pro některé $x, y, z \in G$ platí rovnost $x \cdot y = x \cdot z$. Potom, protože f je homomorfismus, můžeme počítat: $f(x) \cdot f(y) = f(x \cdot y) = f(x \cdot z) = f(x) \cdot f(z)$. Protože $\mathbf{H}$ je grupa a $f(x) \in H$, existuje inverzní prvek $(f(x))^{-1} \in H$. Proto také platí

$$\begin{aligned} f(y) \;=\; & 1 \cdot f(y) = \\ & (f(x))^{-1} \cdot f(x) \cdot f(y) = \\ & (f(x))^{-1} \cdot f(x) \cdot f(z) = \\ & 1 \cdot f(z) = \\ & f(z). \end{aligned}$$

Injektivita zobrazení f nakonec z rovnosti $f(y) = f(x)$ dokazuje rovnost $x = y$. Tímto je ověřeno pravidlo krácení[4].

Dokážeme, že pologrupu s pravidlem krácení lze izomorfně vnořit do grupy. Jak jsme již zmínili, možnost vnoření pologrupy do grupy je ekvivalentní s možností rozšíření pologrupy na grupu (přidáním nových prvků). Celá konstrukce našeho důkazu je inspirována vynálezem zlomků. Zlomky mají dvě složky (čitatel a jmenovatel). Proto i my budeme pracovat s dvojicemi. Mějme tedy pologrupu $\mathbf{G} = (G, \cdot)$, v které platí pravidlo krácení. Označme nyní klasickou kartézskou mocninu $G^2 = \{\langle x, y\rangle \mid x, y \in G\}$. Potom na množině G^2 můžeme zavést operaci $\langle x_1, y_1\rangle \cdot \langle x_2, y_2\rangle = \langle x_1 \cdot x_2, y_1 \cdot y_2\rangle$ pro libovolné dvojice $\langle x_1, y_1\rangle, \langle x_2, y_2\rangle \in G^2$. Všimněme si, že pokud by nám jednotlivé dvojice představovaly zlomky, potom i součin těchto dvojic je stejný jako součin zlomků. Jak vidíme z asociativity součinu na $\mathbf{G}$, dokážeme také rovnost

$$\begin{aligned} \langle x_1, y_1\rangle \cdot (\langle x_2, y_2\rangle \cdot \langle x_3, y_3\rangle) \;&=\; \langle x_1, y_1\rangle \cdot \langle x_2 \cdot x_3, y_2 \cdot y_3\rangle = \\ &=\; \langle x_1 \cdot (x_2 \cdot x_3), y_1 \cdot (y_2 \cdot y_3)\rangle = \\ &=\; \langle (x_1 \cdot x_2) \cdot x_3, (y_1 \cdot y_2) \cdot y_3\rangle = \\ &=\; \langle x_1 \cdot x_2, y_1 \cdot y_2\rangle \cdot \langle x_3, y_3\rangle = \\ &=\; (\langle x_1, y_1\rangle \cdot \langle x_2, y_2\rangle) \cdot \langle x_3, y_3\rangle. \end{aligned}$$

[4]Trochu jednodušeji se dá argumentovat také takto: v každé grupě platí pravidlo krácení (krátíme násobením inverzním prvkem), proto pokud je pologrupa vnořitelná do grupy, je její součástí, a tedy musí pravidlo krácení splňovat také.

Proto také algebra $\mathbf{G}^2 = (G^2, \cdot)$ je pologrupa.

Víme, že u zlomků mohou různé dvojice vyjadřovat stejné hodnoty (např. $\frac{1}{2}$ a $\frac{2}{4}$). Je třeba zavést postup, jak rozpoznat dvojice představující stejnou hodnotu. Jinak řečeno je třeba nalézt vhodnou relaci ekvivalence (kongruenci) na pologrupě $\mathbf{G}^2 = (G^2, \cdot)$. Nejprve zavedeme binární relaci $\sim$ na množině G^2 tak, že pro libovolné dvojice $\langle x_1, y_1\rangle, \langle x_2, y_2\rangle \in G^2$ platí, že

$$\langle x_1, y_1\rangle \sim \langle x_2, y_2\rangle \text{ tehdy a jen tehdy, jestliže } \quad x_1 \cdot y_2 = x_2 \cdot y_1. \qquad (EQ)$$

Připomeňme, že pologrupa $\mathbf{G}$ je komutativní z čehož ihned plyne, že také pologrupa $\mathbf{G}^2$ je komutativní. V dalších výpočtech budeme této vlastnosti užívat bez upozorňování. Dokážeme, že relace $\sim$ je kongruence na pologrupě $\mathbf{G}^2$.

- *reflexivita;* Jestliže $\langle x, y\rangle \in \mathbf{G}^2$, potom přímo z rovnosti $x \cdot y = x \cdot y$ a podmínky (EQ) plyne, že $\langle x, y\rangle \sim \langle x, y\rangle$. Relace $\sim$ je tedy reflexivní.

- *symetrie;* Předpokládejme, že $\langle x_1, y_1\rangle \sim \langle x_2, y_2\rangle$ pro některé prvky $\langle x_1, y_1\rangle, \langle x_2, y_2\rangle \in \mathbf{G}^2$. Potom z podmínky (EQ) dostáváme rovnost $x_1 \cdot y_2 = x_2 \cdot y_1$, ale tedy také $x_2 \cdot y_1 = x_1 \cdot y_2$. Podmínkou (EQ) rovnou dostáváme zpět $\langle x_2, y_2\rangle \sim \langle x_1, y_1\rangle$, což dokazuje symetrii relace $\sim$.

- *tranzitivita;* Předpokládejme, že platí $\langle x_1, y_1\rangle \sim \langle x_2, y_2\rangle$ a také $\langle x_2, y_2\rangle \sim \langle x_3, y_3\rangle$ pro některé dvojice $\langle x_1, y_1\rangle, \langle x_2, y_2\rangle, \langle x_3, y_3\rangle \in \mathbf{G}^2$. Použitím podmínky (EQ) dostáváme rovnosti $x_1 \cdot y_2 = x_2 \cdot y_1$ a $x_2 \cdot y_3 = x_3 \cdot y_2$. Jejich vynásobením získáme vztah $x_1 \cdot y_2 \cdot x_2 \cdot y_3 = x_2 \cdot y_1 \cdot x_3 \cdot y_2$. Z komutativity a pravidla krácení v poslední rovnosti obdržíme rovnost $x_1 \cdot y_3 = x_3 \cdot y_1$. Nyní z podmínky (EQ) rovnou získáme $\langle x_1, y_1\rangle \sim \langle x_3, y_3\rangle$, což dokazuje tranzitivitu.

- *kompatibilita vzhledem k operaci $\cdot$;* Předpokládejme, že platí $\langle x_1, y_1\rangle \sim \langle x_2, y_2\rangle$ a také $\langle x_3, y_3\rangle \sim \langle x_4, y_4\rangle$ pro dvojice $\langle x_1, y_1\rangle, \langle x_2, y_2\rangle, \langle x_3, y_3\rangle, \langle x_4, y_4\rangle \in \mathbf{G}^2$. Z podmínky (EQ) dostáváme $x_1 \cdot y_2 = x_2 \cdot y_1$ a $x_3 \cdot y_4 = x_4 \cdot y_3$. Vynásobením těchto rovností získáme rovnost $x_1 \cdot y_2 \cdot x_3 \cdot y_4 = x_2 \cdot y_1 \cdot x_4 \cdot y_3$, což můžeme také přepsat do tvaru $(x_1 \cdot x_3) \cdot (y_2 \cdot y_4) = (x_2 \cdot x_4) \cdot (y_1 \cdot y_3)$. Z podmínky (EQ) dostáváme $\langle x_1 \cdot x_3, y_1 \cdot y_3\rangle \sim \langle x_2 \cdot x_4, y_2 \cdot y_4\rangle$. Podle definice součinu platí $\langle x_1, y_1\rangle \cdot \langle x_3, y_3\rangle = \langle x_1 \cdot x_3, y_1 \cdot y_3\rangle$ a také $\langle x_2, y_2\rangle \cdot \langle x_4, y_4\rangle = \langle x_2 \cdot x_4, y_2 \cdot y_4\rangle$. Což konečně dává $\langle x_1, y_1\rangle \cdot \langle x_3, y_3\rangle \sim \langle x_2, y_2\rangle \cdot \langle x_4, y_4\rangle$ a dokazuje tvrzení.

Protože relace $\sim$ je kongruencí na pologrupě $\mathbf{G}^2$, můžeme podle Věty 2 zavést faktorovou pologrupu $\mathbf{G}^2/\!\sim$, jejíž prvky jsou právě třídy ekvivalence $[\langle x, y\rangle]_\sim = \{\langle x', y'\rangle \in G^2 \mid \langle x, y\rangle \sim \langle x', y'\rangle\}$. Domluvme se, že budeme nadále užívat značení $\frac{x}{y} = [\langle x, y\rangle]_\sim$ pro třídy množiny $\mathbf{G}^2/\!\sim$. Tato notace nám zjednoduší výpočty. Například pro $\frac{x_1}{y_1}, \frac{x_2}{y_2} \in \mathbf{G}^2/\!\sim$ platí, že

$$\frac{x_1}{y_1} \cdot \frac{x_2}{y_2} = [\langle x_1, y_1\rangle]_\sim \cdot [\langle x_2, y_2\rangle]_\sim = [\langle x_1, y_1\rangle \cdot \langle x_2, y_2\rangle]_\sim = [\langle x_1 \cdot x_2, y_1 \cdot y_2\rangle]_\sim = \frac{x_1 \cdot x_2}{y_1 \cdot y_2}.$$

Taktéž můžeme ukázat, že platí:

$$\frac{x_1}{y_1} = \frac{x_2}{y_2} \iff [\langle x_1, y_1\rangle]_\sim = [\langle x_2, y_2\rangle]_\sim \iff \langle x_1, y_1\rangle \sim \langle x_2, y_2\rangle \iff x_1{\cdot}y_2 = x_2{\cdot}y_1.$$

Jak vidíme, naše notace inspirována zlomky plně koresponduje s dokázanými skutečnostmi. Nyní zbývá dokázat, že zkonstruovaná struktura $\mathbf{G}^2/\!\sim$ je grupa.

- *Ukážeme, že $\frac{x}{x} = \frac{a}{b}$, právě když $a = b$.* Jestliže $a = b$, potom přímo z $a \cdot x = a \cdot x$ plyne $\frac{x}{x} = \frac{a}{a} = \frac{a}{b}$. Opačně, nechť $\frac{x}{x} = \frac{a}{b}$, potom platí $x \cdot b = x \cdot a$ a z pravidla krácení v pologrupě $\mathbf{G}$ dostáváme $a = b$. Tímto jsme dokázali, že právě všechny prvky ve tvaru $\frac{x}{x}$ jsou si navzájem rovny.

- *Dokážeme, že $\frac{x}{x}$ je neutrálním prvkem.* Jestliže $\frac{a}{b} \in \mathbf{G}^2/\!\sim$, potom můžeme počítat $\frac{a}{b} \cdot \frac{x}{x} = \frac{a\cdot x}{b\cdot x}$. Ale (EQ) dokazuje, že z rovnosti $a \cdot b \cdot x = b \cdot a \cdot x$ plyne $\frac{a}{b} = \frac{a\cdot x}{b\cdot x}$. Proto konečně $\frac{a}{b} = \frac{a}{b} \cdot \frac{x}{x}$, a tedy $\frac{x}{x}$ je neutrálním prvkem.

- *Ukážeme, že $\frac{x}{y}$ je inverzním prvkem k prvku $\frac{y}{x}$.* Snadno platí, že $\frac{x}{y} \cdot \frac{y}{x} = \frac{x\cdot y}{y\cdot x} = \frac{x\cdot y}{x\cdot y}$. Z dokázaného, ale víme, že $\frac{x\cdot y}{x\cdot y}$ je neutrální prvek.

Podařilo se nám z původní pologrupy $\mathbf{G}$ zkonstruovat grupu zlomků $\mathbf{G}^2/\!\sim$. Nyní ukážeme, že tato grupa je rozšířením původní pologrupy, tedy že existuje vnoření z pologrupy $\mathbf{G}$ do grupy $\mathbf{G}^2/\!\sim$. Zavedeme proto zobrazení $f : G \to G^2/\sim$ takové, že pro každé $x \in X$ platí $f(x) = \frac{x\cdot x}{x}$.

Nejprve ukážeme, že zobrazení je injektivní. Nechť $f(x) = f(y)$, potom tedy $\frac{x\cdot x}{x} = \frac{y\cdot y}{y}$ a z rovnosti zlomků dostáváme $x\cdot x\cdot y = y\cdot y\cdot x$. Komutativita a pravidlo krácení dokazuje, že také $x = y$.

Konečně dokážeme, že zobrazení je homomorfismem. Jestliže $x, y \in G$, potom platí

$$f(x) \cdot f(y) = \frac{x \cdot x}{x} \cdot \frac{y \cdot y}{y} = \frac{x \cdot x \cdot y \cdot y}{x \cdot y} = \frac{x \cdot y \cdot x \cdot y}{x \cdot y} = f(x \cdot y).$$

□

Grupu $\mathbf{G}^2/\!\sim$ z předchozí věty nazýváme podílovou grupou pologrupy $\mathbf{G}$. Připomeňme, že užíváme-li v grupě $\mathbf{G}$ multiplikativní symboliku (stejnou jako při klasickém násobení), je přirozenou analogií užívat v podílové pologrupě symboliku odpovídající zlomkům. Potom pro libovolné $\frac{x_1}{y_1}, \frac{x_2}{y_2} \in G$ platí, že:

$$\frac{x_1}{y_1} \cdot \frac{x_2}{y_2} = \frac{x_1 \cdot x_2}{y_1 \cdot y_2}, \tag{1}$$

a navíc také

$$\frac{x_1}{y_1} = \frac{x_2}{y_2} \text{ tehdy a jen tehdy, platí-li v pologrupě } \mathbf{G} \text{ rovnost } x_1 \cdot y_2 = x_2 \cdot y_1. \tag{2}$$

Užíváme-li ovšem v grupě $\mathbf{G}$ aditivní symboliku, potom by značení prvků v podílové grupě zlomky ztratilo jakoukoliv názornost. V případě multiplikativní symboliky dvojice $[\langle x, y\rangle]_\sim \in \mathbf{G}^2/\!\sim$ symbolizovala „podíl“ prvků, ovšem v případě aditivní symboliky nám tatáž třída symbolizuje „rozdíl“ prvků. Proto dvojici $[\langle x, y\rangle]_\sim$ budeme v případě aditivní symboliky značit $x - y$ (pozor, jedná se stále o dvojici prvků, které oddělujeme pomlčkou tak, aby nám asociovala rozdíl, trochu atypicky je v tomto případě pomlčka relační symbol a neoznačuje operaci).

Shrneme-li vše dohromady, potom, jestliže $\mathbf{G} = (G, +)$ je komutativní pologrupa s pravidlem krácení, můžeme zkonstruovat grupu $\mathbf{G}^2/\!\sim\, = \{x - y \mid x, y \in G\}$, kde operace sčítání je definována tak, že:

$$(x_1 - y_1) + (x_2 - y_2) = (x_1 + x_2) - (y_1 + y_2), \tag{1_+}$$

a navíc také

$$x_1 - y_1 = x_2 - y_2 \text{ tehdy a jen tehdy,}$$
$$\text{platí-li v pologrupě } \mathbf{G} \text{ rovnost } x_1 + y_2 = x_2 + y_1. \tag{2_+}$$

Užíváme-li aditivní symboliku, jsou neutrálním prvkem třída všech navzájem si rovných dvojic $x - x$ a opačným prvkem k prvku $x - y$ je dvojice $y - x$.

V tomto okamžiku se naskytuje otázka, zda-li je možno komutativní grupu z předchozí věty rozšířit na komutativní grupu (přesněji řečeno vnořit do komutativní grupy) i jiným způsobem. Následující věta nám ukazuje, že v jistém smyslu se jedná o nejefektivnější způsob rozšíření. Přesněji, jestliže komutativní pologrupu $\mathbf{G}$ lze rozšířit na komutativní grupu $\mathbf{H}$, potom i podílovou pologrupu $\mathbf{G}^2/\!\sim$ z předchozí věty lze vnořit do grupy $\mathbf{H}$, tedy grupa $\mathbf{H}$ podílovou grupu obsahuje. Vše dohromady můžeme také interpretovat tak, že podílová grupa je nejmenší komutativní grupa, která obsahuje naší původní pologrupu.

Věta 4 *Jestliže lze komutativní pologrupu* $\mathbf{G} = (G, \cdot)$ *vnořit do grupy* $\mathbf{H}$*, potom také podílovou grupu* $\mathbf{G}^2/\!\sim$ *lze vnořit do grupy* $\mathbf{H}$*.*

Důkaz: Předpokládejme, že máme vnoření (injektivní homomorfismus) h z komutativní pologrupy $\mathbf{G}$ do grupy $\mathbf{H}$. Podle předchozí věty musí platit v pologrupě $\mathbf{G}$ pravidlo krácení. Protože pro prvek $x \in G$ platí, že $f(x) \in H$ existuje v grupě $\mathbf{H}$ prvek $(f(x))^{-1}$ inverzní k $f(x)$. Nyní definujeme zobrazení $f : \mathbf{G}^2/\!\sim \longrightarrow H$ tak, že $f(\frac{x}{y}) = h(x) \cdot (h(y))^{-1}$.

Dokážeme, že zobrazení f je definováno korektně. Uvědomme si, že obecně nepředpokládáme, že grupa $\mathbf{H}$ je komutativní (i když, jak dokážeme, grupa $\mathbf{H}$ obsahuje komutativní podgrupu, která je izomorfní s podílovou grupou $\mathbf{G}^2/\!\sim$). Musíme ukázat, že obraz prvku $\frac{x}{y} \in \mathbf{G}^2/\!\sim$ nezávisí na jeho reprezentaci. Tedy jestliže $\frac{x_1}{y_1}, \frac{x_2}{y_2} \in \mathbf{G}^2/\!\sim$ jsou takové, že $\frac{x_1}{y_1} = \frac{x_2}{y_2}$, potom podle (1) platí, že $x_1 \cdot y_2 = x_2 \cdot y_1$. Z tohoto přímo dostáváme, že $h(x_1) \cdot h(y_2) = h(x_1 \cdot y_2) = h(x_2 \cdot y_1) = h(x_2) \cdot h(y_1)$. Dále z komutativity pologrupy $\mathbf{G}$ plyne, že

$$\begin{aligned}(h(y_1))^{-1} \cdot (h(y_2))^{-1} &= (h(y_2) \cdot h(y_1))^{-1} = \\ &= (h(y_2 \cdot y_1))^{-1} =\end{aligned}$$

$$\begin{aligned} &= (h(y_1 \cdot y_2))^{-1} = \\ &= (h(y_1) \cdot h(y_2))^{-1} = \\ &= (h(y_2))^{-1} \cdot (h(y_1))^{-1}. \end{aligned}$$

Obě dvě rovnosti dohromady ukazují, že

$$\begin{aligned} f\left(\frac{x_1}{y_1}\right) &= h(x_1) \cdot (h(y_1))^{-1} = \\ &= h(x_1) \cdot h(y_2) \cdot (h(y_2))^{-1} \cdot (h(y_1))^{-1} = \\ &= h(x_2) \cdot h(y_1) \cdot (h(y_1))^{-1} \cdot (h(y_2))^{-1} = \\ &= h(x_2) \cdot (h(y_2))^{-1} = \\ &= f\left(\frac{x_2}{y_2}\right). \end{aligned}$$

Tímto je korektnost definice zobrazení f dokázaná.

Dokážeme, že zobrazení f je homomorfismus. Předpokládejme, že $\frac{x_1}{y_1}, \frac{x_2}{y_2} \in \mathbf{G}^2/\!\sim$. Analogicky jako v předchozím případě lze dokázat[5], že $(h(y_1))^{-1} \cdot h(x_2) = h(x_2) \cdot (h(y_1))^{-1}$. Potom vzhledem k Lemmatu 1(iii) platí

$$\begin{aligned} f\left(\frac{x_1}{y_1}\right) \cdot f\left(\frac{x_2}{y_2}\right) &= h(x_1) \cdot (h(y_1))^{-1} \cdot h(x_2) \cdot (h(y_2))^{-1} = \\ &= (h(x_1) \cdot h(x_2)) \cdot (h(y_1) \cdot h(y_2))^{-1} = \\ &= h(x_1 \cdot x_2) \cdot (h(y_1 \cdot y_2))^{-1} = \\ &= f\left(\frac{x_1 \cdot x_2}{y_1 \cdot y_2}\right). \end{aligned}$$

.

Dokážeme, že zobrazení f je injektivní. Předpokládejme, že pro prvky $\frac{x_1}{y_1}, \frac{x_2}{y_2} \in \mathbf{G}^2/\!\sim$ platí rovnost $f(\frac{x_1}{y_1}) = f(\frac{x_2}{y_2})$. Platí také $h(x_1) \cdot (h(y_1))^{-1} = h(x_2) \cdot (h(y_2))^{-1}$ a také po vynásobení rovnosti hodnotou $h(y_1) \cdot h(y_2)$ dostáváme $h(x_1) \cdot h(y_2) = h(x_2) \cdot h(y_1)$. Protože h je homomorfismus, platí $h(x_1 \cdot y_2) = h(x_2 \cdot y_1)$. Navíc zobrazení h je injektivní (vnoření). Proto $x_1 \cdot y_2 = x_2 \cdot y_1$ přímo dokazuje rovnost $\frac{x_1}{y_1} = \frac{x_2}{y_2}$. □

1.6 Vnoření komutativního okruhu do tělesa

Analogicky k předchozí kapitole existuje věta, která nám ukazuje za jakých podmínek a jakým způsobem lze rozšiřovat okruhy (struktury bez dělení) na tělesa. Tento postup je ve skutečnosti zobecněním myšlenky zlomků.

Věta 5 *Komutativní okruh $\mathbf{O} = (O, +, \cdot)$ lze vnořit do tělesa tehdy a jen tehdy, nejsou-li v něm netriviální dělitelé nuly (tedy součinem nenulových prvků je opět nenulový prvek). Navíc platí, že komutativní okruh lze v tomto případě vnořit do tělesa, které je komutativní.*

[5] Platí, že $(h(y_1))^{-1} \cdot h(x_2) \cdot h(y_1) = (h(y_1))^{-1} \cdot h(x_2 \cdot y_1) = (h(y_1))^{-1} \cdot h(y_1 \cdot x_2) = (h(y_1))^{-1} \cdot h(y_1) \cdot h(x_2) = h(x_2)$.

Důkaz: *Dokážeme, že lze-li komutativní okruh vnořit do tělesa, potom v něm nejsou netriviální dělitelé nuly.* Mějme vnoření f okruhu $\mathbf{O}$ do tělesa $\mathbf{T}$. Připomeňme, že v tělesech nejsou netriviální dělitelé nuly (viz Lemma 2). Navíc platí, že $f(0) = 0$. Proto jestliže pro některé prvky $x, y \in O$ platí, že $x \cdot y = 0$, potom také $f(x) \cdot f(y) = f(x \cdot y) = f(0) = 0$. Protože $f(x), f(y) \in T$ a v tělese nejsou netriviální dělitelé nuly, musí platit buď $f(x) = 0$ také nebo $f(y) = 0$. Jestliže $f(x) = 0 = f(0)$, potom z injektivity zobrazení f dostáváme $x = 0$. Analogicky, z $f(y) = 0 = f(0)$ plyne $y = 0$. Dokázali jsme, že v každém případě platí jedna z rovností $x = 0$ nebo $y = 0$. V okruhu proto nejsou netriviální dělitelé nuly.

Dokážeme, že okruh bez netriviálních dělitelů nuly lze vnořit do tělesa. Mějme okruh $\mathbf{O} = (O, +, \cdot)$ bez netriviálních dělitelů nuly. Nejprve dokážeme, že struktura $(O \setminus \{0\}, \cdot)$ je komutativní pologrupa s pravidlem krácení.

- Protože nemáme netriviální dělitele nuly, součin dvou nenulových prvků je opět nenulový. Proto pro $x, y \in O \setminus \{0\}$ platí také $x \cdot y \in O \setminus \{0\}$, a proto množina je uzavřena na operaci $\cdot$. Protože struktura $(O, \cdot)$ je komutativní pologrupa, tím spíše také $(O \setminus \{0\}, \cdot)$ je komutativní a asociativní (tedy pologrupa).

- Nechť pro některé prvky $x, y, z \in O \setminus \{0\}$ platí $x \cdot z = y \cdot z$. Potom můžeme počítat v okruhu $x \cdot z - y \cdot z = 0$, a tedy $(x - y) \cdot z = 0$. Protože v okruhu neexistují netriviální dělitelé nuly a protože víme, že $z \in O \setminus \{0\}$ $(z \neq 0)$, musí platit $x - y = 0$. Dohromady dostáváme $x = y$.

Připomeňme, že podle Věty 3 můžeme na množině $(O \setminus \{0\})^2$ zavést relaci ekvivalence (přesněji kongruenci) $\sim$ předpisem

$$\langle x_1, y_1 \rangle \sim \langle x_2, y_2 \rangle \text{ tehdy a jen tehdy, jestliže } x_1 \cdot y_2 = x_2 \cdot y_1. \qquad (EQ)$$

Podle Věty 3 můžeme takto vytvořit grupu zlomků $(O \setminus \{0\})^2/\sim \; = \{\frac{x}{y} \mid x, y \in O; x, y \neq 0\}$. Abychom konstrukci tělesa dokončili, musíme v něm vytvořit nulový prvek (zlomek) a na zlomcích zavést sčítání. Přirozenou myšlenkou je rozšířit stávající zlomky o zlomky s nulovým čitatelem. Zavedeme proto množinu $O \times (O \setminus \{0\}) = \{\langle x, y \rangle \mid x \in O, y \in O; y \neq 0\}$. Snadno platí, že $O \times (O \setminus \{0\}) = (O \setminus \{0\})^2 \cup \{\langle 0, x \rangle \mid x \in O; x \neq 0\}$. Tedy množina $O \times (O \setminus \{0\})$ vznikla z množiny $(O \setminus \{0\})^2$ přidáním dvojic ve tvaru $\langle 0, x \rangle$, kde x je nenulový prvek. Ukážeme, že relace $\sim$ zavedená na množině $O \times (O \setminus \{0\})$ podle předpisu (EQ) je opět relace ekvivalence a prvky ve tvaru $\langle 0, x \rangle$ jsou všechny navzájem ekvivalentní.

- Jestliže platí pro některé $\langle a, b \rangle, \langle 0, x \rangle \in O \times (O \setminus \{0\})$ tvrzení $\langle a, b \rangle \sim \langle 0, x \rangle$, potom podle (EQ) také $a \cdot x = b \cdot 0 = 0$. Víme, že v okruhu $\mathbf{O}$ neexistují netriviální dělitele nuly proto platí, že $a = 0$ nebo $x = 0$. Jenomže $\langle 0, x \rangle \in O \times (O \setminus \{0\})$, a tedy $x \neq 0$. Proto $a = 0$.

- Opačně jestliže máme dvě dvojice $\langle 0, x \rangle, \langle 0, y \rangle \in O \times (O \setminus \{0\})$, potom z rovnosti $0 \cdot y = 0 = 0 \cdot x$ získáme rovnou $\langle 0, x \rangle \sim \langle 0, y \rangle$.

Dokázali jsme tedy, že $\langle a,b\rangle \sim \langle 0,x\rangle$ platí tehdy a jen tehdy, jestliže $a=0$. Protože $\sim$ je ekvivalence na $(O\setminus\{0\})^2$, a navíc každé dva prvky z $\{\langle 0,x\rangle \mid x\in O; x\neq 0\}$ jsou navzájem ekvivalentní podle $\sim$, je relace $\sim$ ekvivalence na množině $O\times(O\setminus\{0\})$. Navíc z uvedeného plyne, že množina $O\times(O\setminus\{0\})/\!\sim$ vznikne z množiny $(O\setminus\{0\})^2/\!\sim$ přidáním jediného prvku (třídy) $\frac{0}{x}=\{\langle 0,x\rangle \mid x\in O; x\neq 0\}$.

Ověříme, že také operace násobení je definována na množině $O\times(O\setminus\{0\})/\!\sim$ korektně. Pro prvky z množiny $(O\setminus\{0\})^2/\!\sim$ je násobení definováno korektně již podle Věty 3. Zbývá dokázat korektnost násobení prvkem $\frac{0}{x}$. Zřejmě ale pro libovolné $\frac{a}{b},\frac{0}{x}\in O\times(O\setminus\{0\})/\!\sim$ platí $\frac{a}{b}\cdot\frac{0}{x}=\frac{a\cdot 0}{x\cdot b}=\frac{0}{x\cdot b}$. Protože ve výsledku jsou si všechny prvky ve tvaru $\frac{0}{x}$ navzájem rovny, při definování součinu prvkem $\frac{0}{x}$ nezáleží na výběru reprezentanta. Součin je tedy definován korektně.

Nyní zbývá definovat operaci součtu na množině $O\times(O\setminus\{0\})/\!\sim$. Pro libovolné prvky $\frac{x_1}{y_1},\frac{x_2}{y_2}\in O\times(O\setminus\{0\})/\!\sim$ definujeme

$$\frac{x_1}{y_1}+\frac{x_2}{y_2}:=\frac{x_1\cdot y_2+x_2\cdot y_1}{y_1\cdot y_2}.$$

Je třeba ověřit následující:

- *Operace součtu je definována korektně.* Ukážeme, že výsledek součtu zlomků nezávisí na výběru reprezentantů. Nechť $\frac{x_1}{y_1},\frac{x_2}{y_2},\frac{x_1'}{y_1'},\frac{x_2'}{y_2'}\in O\times(O\setminus\{0\})/\!\sim$ tak, že $\frac{x_1}{y_1}=\frac{x_1'}{y_1'}$ a $\frac{x_2}{y_2}=\frac{x_2'}{y_2'}$. Platí tedy také rovnosti $x_1\cdot y_1'=x_1'\cdot y_1$ a $x_2\cdot y_2'=x_2'\cdot y_2$. Jejich užitím lze počítat:

$$\begin{aligned}(x_1\cdot y_2+x_2\cdot y_1)\cdot y_1'\cdot y_2' &= x_1\cdot y_2\cdot y_1'\cdot y_2'+x_2\cdot y_1\cdot y_1'\cdot y_2'\\ &= x_1'\cdot y_2'\cdot y_1\cdot y_2+x_2'\cdot y_1'\cdot y_1\cdot y_2\\ &= (x_1'\cdot y_2'+x_2'\cdot y_1')\cdot y_1\cdot y_2.\end{aligned}$$

  Celkem tedy platí:

$$\frac{x_1}{y_1}+\frac{x_2}{y_2}=\frac{x_1\cdot y_2+x_2\cdot y_1}{y_1\cdot y_2}=\frac{x_1'\cdot y_2'+x_2'\cdot y_1'}{y_1'\cdot y_2'}=\frac{x_1'}{y_1'}+\frac{x_2'}{y_2'}.$$

- *Operace součtu je asociativní.* Toto představuje pouze technické cvičení počítání se zlomky. Tedy pro libovolné $\frac{x_1}{y_1},\frac{x_2}{y_2},\frac{x_3}{y_3}\in O\times(O\setminus\{0\})/\!\sim$ platí, že

$$\begin{aligned}\left(\frac{x_1}{y_1}+\frac{x_2}{y_2}\right)+\frac{x_3}{y_3} &= \frac{x_1\cdot y_2+x_2\cdot y_1}{y_1\cdot y_2}+\frac{x_3}{y_3}\\ &= \frac{(x_1\cdot y_2+x_2\cdot y_1)\cdot y_3+x_3\cdot y_1\cdot y_2}{y_1\cdot y_2\cdot y_3}\\ &= \frac{x_1\cdot y_2\cdot y_3+x_2\cdot y_1\cdot y_3+x_3\cdot y_1\cdot y_2}{y_1\cdot y_2\cdot y_3}\\ &= \frac{x_1\cdot y_2\cdot y_3+(x_2\cdot y_3+x_3\cdot y_2)\cdot y_1}{y_1\cdot y_2\cdot y_3}\end{aligned}$$

$$\begin{aligned} &= \frac{x_1}{y_1} + \frac{x_2 \cdot y_3 + x_3 \cdot y_2}{y_2 \cdot y_3} \\ &= \frac{x_1}{y_1} + \left(\frac{x_2}{y_2} + \frac{x_3}{y_3} \right). \end{aligned}$$

- *Ukážeme, že zlomek* $\frac{0}{x}$ *tvoří nulový prvek.* Jestliže $\frac{x_1}{y_1} \in O \times (O \setminus \{0\})/\!\sim$, potom $\frac{0}{x} + \frac{x_1}{y_1} = \frac{0 \cdot y_1 + x_1 \cdot x}{y_1 \cdot x} = \frac{x_1 \cdot x}{y_1 \cdot x}$. Z definice rovnosti zlomků přímo plyne, že $\frac{x_1 \cdot x}{y_1 \cdot x} = \frac{x_1}{y_1}$.
- *Ukážeme, že ke zlomku* $\frac{x}{y}$ *je* $\frac{-x}{y}$ *opačný zlomek.* Nechť $\frac{x}{y} \in O \times (O \setminus \{0\})/\!\sim$, potom $\frac{x}{y} + \frac{-x}{y} = \frac{x \cdot y + (-x) \cdot y}{y \cdot y} = \frac{0}{y \cdot y}$. Jak máme dokázáno, $\frac{0}{y \cdot y}$ je nulovým prvkem.

K tomu abychom dokázali, že $(O \times (O \setminus \{0\})/\!\sim, \cdot, +)$ je těleso, zbývá ověřit distributivitu násobení vzhledem ke sčítání. Připomeňme ještě, že komutativitu sčítání i násobení lze triviálně ověřit. Navíc jednotkovým prvkem jsou zlomky ve tvaru $\frac{x}{x}$. Mějme libovolné prvky $\frac{x_1}{y_1}, \frac{x_2}{y_2}, \frac{x_3}{y_3} \in O \times (O \setminus \{0\})/\!\sim$. Potom počítejme

$$\begin{aligned} \left(\frac{x_1}{y_1} + \frac{x_2}{y_2} \right) \cdot \frac{x_3}{y_3} &= \frac{x_1 \cdot y_2 + x_2 \cdot y_1}{y_1 \cdot y_2} \cdot \frac{x_3}{y_3} \cdot \frac{y_3}{y_3} \\ &= \frac{(x_1 \cdot y_2 + x_2 \cdot y_1) \cdot x_3 \cdot y_3}{y_1 \cdot y_2 \cdot y_3^2} \\ &= \frac{x_1 \cdot y_2 \cdot x_3 \cdot y_3 + x_2 \cdot y_1 \cdot x_3 \cdot y_3}{y_1 \cdot y_2 \cdot y_3^2} \\ &= \frac{x_1 \cdot x_3}{y_1 \cdot y_3} + \frac{x_2 \cdot x_3}{y_2 \cdot y_3} \\ &= \frac{x_1}{y_1} \cdot \frac{x_3}{y_3} + \frac{x_2}{y_2} \cdot \frac{x_3}{y_3}. \end{aligned}$$

Zkonstruované těleso $(O \times (O \setminus \{0\})/\!\sim, \cdot, +)$ nazýváme podílovým tělesem okruhu $\mathbf{O}$ a obvykle jej značíme $\mathbb{Q}(\mathbf{O})$. K dokázání zbytku věty zbývá najít vnoření $f : \mathbf{O} \longrightarrow \mathbb{Q}(\mathbf{O})$. To definujeme následovně:

$$f(x) := \begin{cases} \frac{x \cdot x}{x} & \text{jestliže} \quad x \neq 0 \\ \\ \frac{0}{a} & \text{Jestliže} \quad x = 0, \quad a \neq 0. \end{cases}$$

Vzhledem k důkazu Věty 3 lze snadno vidět, že zobrazení je injektivní. Navíc zobrazení zachovává násobení pro nenulové zlomky. Ověřit tutéž vlastnost pro nulový zlomek je triviální. Tedy zbývá dokázat zachovávání sčítání. Nechť $x, y \in \mathbf{O}$. Nejprve z definice rovnosti zlomků snadno vidíme, že platí $\frac{(x+y) \cdot x \cdot y}{x \cdot y} = \frac{(x+y) \cdot (x+y)}{x+y}$. Nyní již rovnou:

$$f(x)+f(y)=\frac{x\cdot x}{x}+\frac{y\cdot y}{y}=\frac{x\cdot x\cdot y+x\cdot y\cdot y}{x\cdot y}=\frac{(x+y)\cdot x\cdot y}{x\cdot y}=$$
$$=\frac{(x+y)\cdot(x+y)}{x+y}=f(x+y).$$

□

Analogicky jako u komutativních grup můžeme ukázat, že podílové těleso je v jistém smyslu nejmenším tělesem obsahující původní okruh.

Věta 6 *Jestliže lze komutativní okruh bez netriviálních dělitelů nuly* $\mathbf{O}=(O,+,\cdot)$ *vnořit do tělesa* $\mathbf{T}$*, potom také podílové těleso* $\mathbb{Q}(\mathbf{O})$ *lze vnořit do tělesa* $\mathbf{T}$*.*

Důkaz. Analogicky k důkazu Věty 4 předpokládejme, že máme vnoření $h:\mathbf{O}\longrightarrow\mathbf{T}$. Připomeňme, že u každého vnoření je splněno[6], že $h(x)=0$ tehdy a jen tehdy, jestliže $x=0$. Definujeme zobrazení $f:\mathbb{Q}(\mathbf{O})\longrightarrow\mathbf{T}$ tak, že pro $\frac{x}{y}\in\mathbb{Q}(\mathbf{O})$ platí $f(\frac{x}{y})=h(x)\cdot(h(y))^{-1}$. Uvědomme si, že pro $\frac{x}{y}\in\mathbb{Q}(\mathbf{O})$ platí $y\neq 0$, a tedy $h(y)\neq 0$. Z toho plyne existence prvku[7] $(h(y))^{-1}$.

- *Dokážeme, že zobrazení f je definováno korektně.* Z důkazu Věty 4 plyne, že f je korektně definováno na množině $(O\setminus\{0\})^2/\!\sim$. Zbývá tedy ověřit korektnost definice pro nulový zlomek. Platí, že $f(\frac{0}{a})=h(0)\cdot(h(a))^{-1}=0\cdot(h(a))^{-1}=0$, což jsme měli dokázat.

- *Dokážeme, že zobrazení f zachovává násobení.* V důkazu Věty 4 je ukázáno, že zobrazení f zachovává násobení v grupě $((O\setminus\{0\})^2/\!\sim,\cdot)$. Zbývá tedy ověřit násobení nulou. Pro $\frac{x}{y},\frac{0}{a}\in\mathbb{Q}(\mathbf{O})$ platí

$$f\left(\frac{x}{y}\cdot\frac{0}{a}\right)=f\left(\frac{0}{y\cdot a}\right)=h(0)\cdot(h(a\cdot b))^{-1}=0=f\left(\frac{x}{y}\right)\cdot 0=f\left(\frac{x}{y}\right)\cdot f\left(\frac{0}{a}\right).$$

- Dokážeme, že zobrazení f zachovává sčítání. Mějme prvky prvky $\frac{x_1}{y_1},\frac{x_2}{y_2}\in\mathbb{Q}(\mathbf{O})$. Připomeňme, že z komutativity okruhu $(O,+,\cdot)$ plyne rovnost $(h(y_1))^{-1}\cdot(h(y_2))^{-1}=(h(y_2))^{-1}\cdot(h(y_1))^{-1}$ (viz Věta 4).

$$\begin{aligned}f\left(\frac{x_1}{y_1}+\frac{x_2}{y_2}\right) &= f\left(\frac{x_1\cdot y_2+x_2\cdot y_1}{y_1\cdot y_2}\right)\\ &= h(x_1\cdot y_2+x_2\cdot y_1)\cdot(h(y_1\cdot y_2))^{-1}\\ &= h(x_1\cdot y_2+x_2\cdot y_1)\cdot(h(y_1))^{-1}\cdot(h(y_2))^{-1}\end{aligned}$$

[6]Jestliže $x=0$, potom již máme dokázáno, že $f(0)=0$. Jestliže opačně platí, že $f(x)=0$, potom také $f(x)=f(0)$ a z injektivity plyne $x=0$.

[7]V tělese existují inverzní prvky právě ke všem nenulovým prvkům.

$$\begin{aligned} &= (h(x_1)\cdot h(y_2) + h(x_2)\cdot h(y_1))\cdot (h(y_1))^{-1}\cdot (h(y_2))^{-1} \\ &= h(x_1)\cdot h(y_2)\cdot (h(y_1))^{-1}\cdot (h(y_2))^{-1} + h(x_2)\cdot h(y_1)\cdot (h(y_1))^{-1}\cdot (h(y_2))^{-1} \\ &= h(x_1)\cdot (h(y_1))^{-1} + h(x_2)\cdot (h(y_2))^{-1} \\ &= f\left(\frac{x_1}{y_1}\right) + f\left(\frac{x_2}{y_2}\right). \end{aligned}$$

□

1.7 Uspořádání na okruzích

V následující kapitole se budeme věnovat problematice uspořádání okruhů. Připomeňme, že obecně v algebře rozumíme uspořádáním relaci $\leq$, která je reflexivní, antisymetrická a tranzitivní. Tato tradiční definice nevyžaduje, aby každé dva prvky byly srovnatelné (tedy může nastat případ, kdy platí současně $x \not\leq y$ a $y \not\leq x$; nejtypičtějším příkladem je relace množinové inkluze $\subseteq$, která „uspořádává“ množiny, přičemž existují nesrovnatelné množiny).

Protože naším hlavním cílem je konstrukce číselných množin (lépe řečeno oboru integrity celých čísel a následně tělesa racionálních a reálných čísel), bude námi vytvořená teorie motivována uspořádáním právě na těchto číselných strukturách. V prvé řadě budeme hledat uspořádání, které je lineární (tedy platí, že každé dva prvky budeme moci srovnat). Další požadované vlastnosti, které klademe na hledané uspořádaní, jsou *monotónnost sčítaní* (tedy jestliže $x \leq y$, potom také $x + z \leq y + z$) a *monotónnost násobení* kladným prvkem (tedy jestliže $x \leq y$ a $z \geq 0$, potom $x \cdot z \leq y \cdot z$).

Připomeňme, že se v praxi setkáváme ještě s pojmem ostrého uspořádání $<$, ve kterém vlastnost antisymetrie z klasického uspořádání nahrazuje asymetrie. Je ovšem zřejmé, že relace $\leq$ a $<$ můžeme vzájemně odvozovat a to pouze tím, že k ostrému uspořádání přidáme rovnost, resp. od klasického uspořádání rovnost „odebereme“. V našem případě nejprve nalezneme uspořádaní ostré a teprve následně z něj odvodíme klasické uspořádání.

Zaměřme se nejprve na hlavní myšlenku naší konstrukce. Můžeme si uvědomit, že uspořádaní lze definovat tak, že $x < y$, jestliže existuje *kladný prvek* z takový, že $x + z = y$. Problém ovšem spočívá v tom, jak určit kladné prvky. Budeme proto postupovat tak, že si nejprve určíme (lépe řečeno definujeme) množinu kladných prvků a následně pomocí této množiny uspořádání nalezneme.

Definice 9 *Mějme okruh* $\mathbf{O} = (O, +, \cdot)$*, potom množinu* $K \subseteq O$ *nazveme kladnou částí, jestliže platí:*

(i) Pro libovolné prvky $x, y \in K$ *platí, že* $x + y, x \cdot y \in K$*.*

(ii) Pro libovolný prvek $x \in O$ *platí právě jedno z tvrzení:* $x \in K$*,* $-x \in K$*, nebo* $x = 0$*.*

Jestliže K *je kladná část v okruhu* $\mathbf{O}$*, potom dvojici* $(\mathbf{O}, K)$ *nazveme uspořádaný okruh podle kladné části* K*. Existuje-li jediná kladná část v okruhu, potom jej nazýváme pouze uspořádaným okruhem.*

Jak již bylo naznačeno, v některých okruzích kladná část existovat nemusí (a tedy uspořádaní s hledanými vlastnostmi nemusí existovat), stejně tak existují okruhy s více kladnými částmi (tedy existuje více způsobů jak okruh uspořádat). V případě číselných struktur (vyjma komplexních čísel) potom ukážeme, že takové uspořádání existuje jediné. Následující věta popíše vztah uspořádání a kladných částí. Připomeňme ještě, že podle Definice 9 nulový prvek 0 nenáleží kladné části.

Věta 7 *Mějme uspořádaný okruh* $(\mathbf{O}, K)$ *a zaveďme relaci* $>$ *(kterou nazýváme ostré uspořádání indukované kladnou částí* K*) na množině* O *tak, že pro* $x, y \in O$ *platí* $x > y$ *tehdy a jen tehdy, když* $x - y \in K$*. Potom platí, že:*

i) Relace $>$ *je ireflexivní, asymetrická a tranzitivní.*

ii) Relace $>$ *je trichotomická (tj. pro libovolné prvky* $x, y \in O$ *platí právě jedno z tvrzení* $x > y$*,* $y > x$*, nebo* $x = y$*).*

iii) Pro libovolné prvky $x, y, z \in O$ *platí, že z nerovnosti* $x > y$ *plyne nerovnost* $x + z > y + z$*.*

iv) Pro libovolné prvky $x, y \in O$ *a* $z \in K$ *platí, že z nerovnosti* $x > y$ *plyne nerovnost* $x \cdot z > y \cdot z$*.*

Důkaz: ad i) Ireflexivita plyne rovnou z tvrzení $x - x = 0 \notin K$. Dokážeme tranzitivitu. Jestliže $x > y$ a $y > z$ pro některé $x, y, z \in O$, potom platí, že $x - y, y - z \in K$. Z uzavřenosti kladné části na sčítáni plyne $(x - y) + (y - z) = x - z \in K$. To přímo dokazuje, že $x > z$. Asymetrii relace dokážeme sporem. Pokud $x > y$ a $y > x$, potom z tranzitivity rovnou plyne $z > z$, což odporuje dokázané ireflexivitě.

ad ii) Mějme prvky $x, y \in O$. Potom z definice kladné části vidíme, že platí právě jeden z výroků $x - y \in K$, $-(x - y) \in K$ (což je totéž jako $y - x \in K$) nebo $x - y = 0$. Tyto výroky jsou postupně ekvivalentní s výroky $x > y$, $y > x$ a $x = y$.

ad iii) Nechť $x > y$, potom platí, že $x - y \in K$. Platí ale také $(x+z)-(y+z) = x-y \in K$. Proto $x + z > y + z$.

ad iv) Jestliže $x > y$ a $y \in K$, potom platí, že $x - y \in K$. Z uzavřenosti kladné části na násobení dostáváme $x \cdot z - y \cdot z = (x - y) \cdot z \in K$. Z tohoto plyne $x \cdot z > y \cdot z$ □

V minulé větě jsme ukázali, jak lze pomocí kladné části zavést uspořádaní daných vlastností. Přirozeně existuje opačný postup, kdy z uspořádaní splňující podmínky věty najít kladnou část. Existuje vzájemně jednoznačná korespondence mezi kladnými částmi a uspořádáními s vlastnostmi i)-iv) z předchozí věty.

Věta 8 *Jestliže máme okruh* $\mathbf{O} = (O, +, \cdot)$ *a binární relaci* $>$ *splňující podmínky i)-iv) z předchozí věty, potom množina* $K = \{x \in O \mid x > 0\}$ *je kladnou částí a uspořádání indukované touto kladnou částí je právě uspořádání* $>$*.*

Důkaz: Nechť $x, y \in K$. Potom platí, že $x, y > 0$ a z vlastnosti iii) lze odvodit, že $x + y > 0 + y = y > 0$. Tedy $x + y \in K$. Analogicky podle předpokladu ii) a iv) platí $x+y > y$, a proto také $x \cdot y + y \cdot y = (x+y) \cdot y > y \cdot y$. Použijeme-li na poslední nerovnost podmínku iii) a přičteme k oběma stranám nerovnosti prvek $-y \cdot y$, dostáváme $x \cdot y > 0$.

Jestliže $x \in O$, potom platí právě jedno ze tří tvrzení (což plyne z trichotomie uspořádáni) $x > 0$, $0 > x$, nebo $x = 0$. Jestliže $x > 0$, potom $x \in K$. Pokud $0 > x$, potom z vlastnosti iii) plyne $0 = x - x > 0 - x = -x$ a proto $-x \in K$. Analogicky lze ověřit, že žádné z těchto dvou výroků nemohou nastat současně. Platí proto vlastnost trichotomie množiny K z definice.

Označme $>_K$ uspořádání indukované kladnou části K (tedy $x >_K y$ tehdy a jen tehdy, jestliže $x - y \in K$). Nyní dokážeme, že toto uspořádáni je totožné s uspořádáním $>$. Nechť $x > y$, potom podle vlastnosti iv) platí $x - y > y - y = 0$, a tedy $x - y \in K$. Z tohoto podle definice plyne $x >_K y$. Předpokládejme, že $x >_K y$. Potom platí, že $x - y \in K$, a tedy také, že $x - y > 0$. Opět z vlastnosti iv) dostáváme $x = (x - y) + y > 0 + y = y$ a tedy $x > y$. Protože jsme dokázali, že platí $x > y$ tehdy a jen tehdy, jestliže $x >_K y$, jsou obě uspořádáni totožná. □

S ohledem na předchozí větu připomeneme často užívanou terminologii. O okruhu řekneme, že jej lze uspořádat, jestliže lze zavést uspořádáni splňující podmínky i)-iv) Věty 7. Platí proto, že okruh lze uspořádat tehdy a jen tehdy, jestliže má kladnou část.

Věta 9 *(i) V uspořádaném okruhu $(\mathbf{O}, K)$ platí pro libovolný nenulový prvek $x \in O$, že $x^2 \in K$ (speciálně tedy $1 \in K$).*

(ii) Mějme uspořádaný okruh $(\mathbf{O}, K)$. Jestliže prvek $x \in K$ je takový, že existuje inverzní prvek x^{-1}, potom také $x^{-1} \in K$.

(iii) Každý okruh, jenž lze uspořádat, nemá netriviální dělitele nuly.

(iv) Každý okruh, jenž lze uspořádat, má nekonečně mnoho prvků.

Důkaz: ad (i) Mějme libovolný prvek $x \in O$. Potom za předpokladu $x \neq 0$, plyne z trichotomie, že $x \in K$ nebo $-x \in K$. Z uzavřenosti kladné části na součin přímo plyne, že $x^2 \in K$ nebo $(-x)^2 \in K$. Platí ale $(-x)^2 = (-x) \cdot (-x) = x \cdot x = x^2$. Proto $x^2 \in K$.

ad (ii) Jelikož $x \in K$ a podle předchozí části také $(x^{-1})^2 \in K$, platí, že $x^{-1} = (x^{-1})^2 \cdot x \in K$.

ad (iii) Předpokládejme sporem, že pro některé nenulové $a, b \in O$ platí $a \cdot b = 0$. Z trichotomie kladné části plyne, že buďto $a \in K$ nebo $-a \in K$. Stejně tak buďto $b \in K$ nebo $-b \in K$. Potom z uzavřenosti kladné části na součiny plyne, že jeden ze čtyř výrazů $a \cdot b$, $(-a) \cdot b$, $a \cdot (-b)$ nebo $(-a) \cdot (-b)$ náleží kladné části. Ovšem pokud $a \cdot b = 0$, potom také $0 = a \cdot b = (-a) \cdot b = a \cdot (-b) = (-a) \cdot (-b)$. Proto $0 \in K$, což je spor.

ad (iv) Aby nedošlo ke kolizi ve značení, budeme v tomto důkazu značit jednotkový prvek v okruhu místo 1 písmenem e. Označme podle následující notace pro libovolné $n \in \mathbb{N}$ výraz $1 \times x = x$ a $(n+1) \times x = n \times x + x$. Platí tedy, že $n \times x = \overbrace{x + x + \ldots + x}^{n\times}$. Označme nyní množinu $E = \{n \times e \mid n \in \mathbb{N}\}$. Platí, že $1 \times e = e \in K$ a také, pokud $n \times e \in K$, potom z uzavřenosti kladné části na součty plyne, že $(n+1) \times e = n \times e + e \in K$. Matematickou

indukcí jsme dokázali, že $E \subseteq K$, a tedy pro libovolné $n \in \mathbb{N}$ platí, že $n \times e \neq 0$. Nyní ukážeme, že pro libovolná různá čísla $m, n \in \mathbb{N}$ platí, že $n \times e \neq m \times e$.

Předpokládejme sporem, že $n \times e = m \times e$ pro různá čísla $m, n \in \mathbb{N}$. Bez újmy na obecnosti předpokládejme, že $m < n$. Potom platí, že $n - m \in \mathbb{N}$ a také platí, že $0 = (n \times e) - (m \times e) = \overbrace{e + e + \ldots + e}^{n\times} - (\overbrace{e + e + \ldots + e}^{m\times}) = \overbrace{e + e + \ldots + e}^{n\times} - \overbrace{e - e - \ldots - e}^{m\times} = \overbrace{e + e + \ldots + e}^{(n-m)\times} = (n - m) \times e$. Toto je ale spor s tím, že $(n - m) \times e \neq 0$. □

Důsledkem je mimo jiné to, že každý komutativní uspořádaný okruh je oborem integrity. K poslednímu tvrzení, jež ve skutečnosti zobecňuje poslední část předchozí věty, potřebujeme zavést následující pojmy. *Charakteristikou* prvku $x \in O$ v okruhu $\mathbf{O} = (O, \cdot, +)$ rozumíme nejmenší přirozené číslo $n \in \mathbb{N}$ takové, že $n \times x = 0$. Pokud takovéto číslo neexistuje, potom řekneme, že prvek má nekonečnou charakteristiku[8]. Charakteristiku prvku značíme obvykle Char x (v našem případě platí Char $x = n$).

Analogicky definujeme *charakteristiku okruhu* (značíme Char $\mathbf{O}$) jako nejmenší číslo $n \in \mathbb{N}$ takové, že pro libovolné $x \in O$ platí $n \times x = 0$. Lze tedy psát, že Char $\mathbf{O} = max\ \{\text{Char } x \mid x \in O\}$. Ukážeme, že charakteristika jednotkového prvku (značme jej nadále e) je rovna charakteristice okruhu. Přímo z definice plyne, že Char $e \leq$ Char $\mathbf{O}$. Nechť Char $e = n$, potom pro libovolné $x \in O$ platí $n \times x = \overbrace{x + x + \ldots + x}^{n\times} = \overbrace{e \cdot x + e \cdot x + \ldots + e \cdot x}^{n\times} = (\overbrace{e + e + \ldots + e}^{n\times}) \cdot x = (n \times e) \cdot x = 0 \cdot x = 0$. Proto také Char $e = n \geq$ Char x pro všechna $x \in O$. Toto dohromady dává, že Char $e =$ Char $\mathbf{O}$. Připomeňme, že v posledním bodu předchozí věty jsme dokázali, že v každém uspořádaném okruhu má jednotkový prvek nekonečnou charakteristiku. Toto lze ještě rozšířit v dalším tvrzení.

Věta 10 *Jestliže $(\mathbf{O}, K)$ je uspořádaný okruh, potom každý nenulový prvek okruhu má nekonečnou charakteristiku.*

Důkaz. Předpokládejme, že $x \in O$ je takový, že Char $x = n$. Potom platí, že $0 = n \times x = n \times (e \cdot x) = (n \times e) \cdot x$. Protože v uspořádaných okruzích neexistují netriviální dělitelé nuly, a navíc víme, že $n \times e \neq 0$, platí $x = 0$. □

V poslední části vyřeší problém uspořádaní podílového tělesa $\mathbb{Q}(\mathbf{O})$ komutativního uspořádaného okruhu $(O, +, \cdot)$ bez netriviálních dělitelů nuly.

Věta 11 *Mějme uspořádaný okruh $(O_1, +, \cdot)$ s kladnou částí $P_1 \subseteq O_1$ a uspořádaný okruh $(O_2, +, \cdot)$ s kladnou částí $P_2 \subseteq O_2$. Nechť $f : P_1 \longrightarrow P_2$ je vnoření[9] kladné části P_1 do kladné části P_2, potom existuje jediné vnoření $g : O_1 \longrightarrow O_2$, které je rozšířením zobrazení f (tedy platí pro všechna $x \in P_1$, že $f(x) = g(x)$).*

[8] V literatuře se setkáváme s tím, že místo nekonečné charakteristiky se definuje tzv. nulová charakteristika.

[9] Injektivní zobrazení splňující pro všechny $x, y \in P_1$, že $f(x+y) = f(x)+f(y)$ a $f(x \cdot y) = f(x) \cdot f(y)$.

Důkaz: Definujme zobrazení $g : O_1 \longrightarrow O_2$ tak, že

$$g(x) = \begin{cases} f(x), \text{ jestliže } x \in P_1; \\ -f(-x), \text{ jestliže } -x \in P_1; \\ 0, \text{ jestliže } x = 0; \end{cases}$$

Rozborem na jednotlivé případy dokážeme, že zobrazení je homomorfismus. Jestliže $x, y \in P_1$, potom také $x \cdot y, x+y \in P_1$ a platí $g(x+y) = f(x+y) = f(x)+f(y) = g(x)+g(y)$ a analogicky ověříme pro násobení.

Jestliže $x = 0$, potom $g(0 + y) = g(y) = 0 + g(y) = g(0) + g(y)$, podobně $g(0 \cdot y) = g(0) = 0 = 0 \cdot g(y) = g(0) \cdot g(y)$. Analogicky dokážeme variantu, kdy $y = 0$.

Pokud $-x, -y \in P_1$, potom platí, že $-(x + y) = -x - y \in P_1$ a můžeme počítat $g(x+y) = -f(-x-y) = -f(-x)-f(-y)) = g(x)+g(y)$. Platí také, že $x \cdot y = (-x) \cdot (-y) \in P_1$, proto $g(x \cdot y) = f(x \cdot y) = f((-x) \cdot (-y)) = f(-x) \cdot f(-y) = (-f(-x)) \cdot (-f(-y)) = g(x) \cdot g(y)$.

Poslední variantou je $-x \in P_1$, $y \in P_1$. Rozlišme nyní tři možné případy:

- $x+y \in P_1$, potom lze počítat $-f(-x)+f(y)-f(x+y) = f(y)-(f(-x)+f(x+y)) = f(y) - f(-x + x + y) = f(y) - f(y) = 0$. Proto platí $f(x + y) = -f(-x) + f(y)$, což lze přepsat do tvaru $g(x + y) = f(x + y) = -f(-x) + f(y) = g(x) + g(y)$.
- $-(x + y) \in P_1$, potom $-f(-x) + f(y) + f(-(x + y)) = -f(-x) + f(y - (x + y)) = -f(-x) + f(-x) = 0$. Proto také platí, že $-f(-(x + y)) = -f(-x) + f(y)$, a tedy také $g(x + y) = -f(-(x + y)) = -f(-x) + f(y) = g(x) + g(y)$.
- $x + y = 0$, potom $-x = y$, a tedy $g(x + y) = g(0) = 0 = -f(y) + f(y) = -f(-x) + f(y) = g(x) + g(y)$.

Zbývá dokázat, že v tomto případě homomorfismus zachovává také součiny. Platí, že $-x \cdot y = (-x) \cdot y \in P_1$, a proto také $g(x \cdot y) = -f(-x \cdot y) = -f((-x) \cdot y) = -f(-x) \cdot f(y) = g(x) \cdot g(y)$. □

Vyslovíme jedno jednoduché a užitečné tvrzení.

Lemma 4 *Jestliže $(O, +, \cdot)$ je okruh a $P_1, P_2 \subseteq O$ jsou kladné části takové, že $P_1 \subseteq P_2$, potom také $P_1 = P_2$.*

Důkaz. Předpokládejme sporem, že $P_1 \subset P_2$. Potom platí, že $P_2 \setminus P_1 \neq \emptyset$, a tedy existuje $x \in P_2 \setminus P_1$. Platí, že $x \in P_2$, a tedy také $x \neq 0$ (kladná část neobsahuje nulu). Protože navíc $x \notin P_1$ (a $x \neq 0$), z trichotomie dostáváme, že $-x \in P_1$. Jelikož $P_1 \subset P_2$, platí také $-x \in P_2$, což je spor s trichotomií (nemůže platit, že $x, -x \in P_2$).

□

Věta 12 *Jestliže $(O, +, \cdot)$ je komutativní okruh bez netriviálních dělitelů nuly a jestliže $P \subset O$ je některá jeho kladná část, potom existuje jediná kladná část R v podílovém tělese $\mathbb{Q}(\mathbf{O})$ taková, že $f(P) \subseteq R$ (kde f je vnoření okruhu $(O, +, \cdot)$ do tělesa $\mathbb{Q}(\mathbf{O})$ definované ve důkazu Věty 5). Touto kladnou částí R je množina $\{\frac{x}{y} \mid x \cdot y \in P\}$.*

Důkaz. Předpokládejme, že $\frac{x_1}{y_1} = \frac{x_2}{y_2}$ je takový zlomek, že $x_1 \cdot y_1 \in P$ (platí tedy $x_1 \neq 0$, a v důsledku také $x_2 \neq 0$). Navíc lze dedukovat, že oba prvky x_1, y_1 jsou buďto současně oba kladné nebo oba záporné (byl-li by jeden z prvků kladný a druhý záporný, potom by platilo $-x_1 \cdot y_1 \in P$, což je spor s trichotomií). Protože $x_1 \cdot y_2 = x_2 \cdot y_1$ musí platit současně $x_2, y_2 \in P$ nebo $-x_2, -y_2 \in P$[10]. V každém případě ale platí, že $(-x_2)\cdot(-y_2) = x_2 \cdot y_2 \in P$. Z tohoto plyne, že lze korektně definovat množinu $R = \{\frac{x}{y} \mid x \cdot y \in P\}$. Dokážeme nyní, že tato množina je kladná část v $\mathbb{Q}(O)$.

Nejprve jestliže $\frac{x_1}{y_1}, \frac{x_2}{y_2} \in R$, potom $x_1 \cdot y_1, x_2 \cdot y_2 \in P$. Protože také $y_1^2, y_2^2 \in P$ (viz Věta 9(i)) platí, že $(x_1 \cdot y_2 + x_2 \cdot y_1) \cdot y_1 \cdot y_2 = x_1 \cdot y_1 \cdot y_2^2 + x_2 \cdot y_2 \cdot y_1^2 \in P$. Z tohoto ovšem plyne, že $\frac{x_1}{y_1} + \frac{x_2}{y_2} = \frac{x_1 \cdot y_2 + x_2 \cdot y_1}{y_1 \cdot y_2} \in R$.

Analogicky také $x_1 \cdot x_2 \cdot y_1 \cdot y_2 \in P$ dokazuje, že $\frac{x_1}{y_1} \cdot \frac{x_2}{y_2} = \frac{x_1 \cdot x_2}{y_1 \cdot y_2} \in R$. Proto je množina R uzavřena na součty i součiny.

Jestliže máme zlomek $\frac{x}{y} \in \mathbb{Q}(O)$, potom protože $x \cdot y \in O$, platí právě jedno z tvrzení $x \cdot y \in P$, $-x \cdot y \in P$ nebo $x \cdot y = 0$. Tyto tři výroky jsou ale po řadě ekvivalentní s tím, že $\frac{x}{y} \in P$, $-(\frac{x}{y}) = \frac{-x}{y} \in P$ nebo $\frac{x}{y} = 0$ (protože z $\frac{x}{y} \in \mathbb{Q}(O)$ plyne, že $y \neq 0$, jelikož navíc v $(O, +, \cdot)$ nejsou netriviální dělitelé nuly – jinak by okruh nešel rozšířit na těleso – dostáváme z $x \cdot y = 0$ tvrzení $x = 0$). Toto dokazuje trichotomii množiny R.

V poslední části dokážeme, že R je jediná kladná část, která obsahuje kladnou část P (přesněji řečeno obsahuje zlomky $\frac{x^2}{x}$, kde $x \in P$). Nejprve, jestliže $x \in P$, potom také $x^3 \in P$, což dokazuje, že $\frac{x^2}{x} \in R$.

Předpokládejme nyní, že existuje kladná část R' obsahující P. Dokážeme, že $R \subseteq R'$. Nechť $\frac{x}{y} \in R$ jsou takové, že $x, y \in P$ (toto můžeme předpokládat, protože platí $\frac{x}{y} = \frac{-x}{-y}$). Potom $\frac{x^2}{x}, \frac{y^2}{y} \in R'$. Jak dokazuje Věta 9(ii), musí také $\frac{y}{y^2} \in R'$ a z uzavřenosti kladné části na součin konečně dostáváme, že $\frac{x}{y} = \frac{x^2}{x} \cdot \frac{y}{y^2} \in R'$. Máme dokázáno, že $R \subseteq R'$ a podle Lemma 4 také $R = R'$. □

1.8 Absolutní hodnota

V uspořádaném okruhu $\mathbf{O}$ s kladnou částí K můžeme přirozeným způsobem definovat absolutní hodnotu jako zobrazení $x \mapsto |x|$ definované tak, že

$$|x| := \begin{cases} x, & \text{jestliže platí } x \in K \text{ nebo } x = 0 \\ -x & \text{v ostatních případech} \end{cases}$$

Věta 13 *V uspořádaném okruhu* $\mathbf{O}$ *platí pro libovolné* $x, y \in \mathbf{O}$ *následující tvrzení:*

i) $|x| = 0$ *právě, když* $x = 0$,

ii) $|x| \cdot |y| = |x \cdot y|$,

[10] Snadno lze ověřit, že v opačném případě by platilo $x_1 \cdot y_2 = -x_2 \cdot y_1 = -x_1 \cdot y_2$, z čehož lze dedukovat $x_1 \cdot y_2 = 0$. Protože $x_1 \neq 0$ a $y_2 \neq 0$ (jmenovatel nemůže být roven nule) a protože v uspořádaném okruhu neexistují netriviální dělitelé nuly, dostáváme spor.

iii) $|x+y| \leq |x| + |y|$,

iv) $|x| - |y| \leq |x-y|$.

Důkaz: ad i) Jestliže $x \neq 0$, potom $|x| \in K$, a tedy $|x| \neq 0$. Dokázali jsme, že $|x| = 0$ implikuje $x = 0$. Opačné tvrzení plyne přímo z definice.

ad ii) Jestliže $x = 0$, potom $|0 \cdot y| = |0| = 0 = 0 \cdot |y| = |0| \cdot |y|$. Analogicky pro $y = 0$. Jestliže $x, y \in K$, potom také $x \cdot y \in K$, a proto $|x \cdot y| = x \cdot y = |x| \cdot |y|$. Pokud $-x, -y \in K$, potom $(-x) \cdot (-y) = x \cdot y \in K$. Proto platí, že $|x \cdot y| = x \cdot y = (-x) \cdot (-y) = |x| \cdot |y|$.

Předpokládejme konečně, že $-x, y \in K$, potom $-x \cdot y \in K$, a proto platí, že $|x \cdot y| = -(x \cdot y) = (-x) \cdot y = |x| \cdot |y|$. Analogicky v případě, že $x, -y \in K$. Z trichotomie kladné části plyne, že jsme takto prozkoumali všechny možné případy.

ad iii) Pokud $x, y \in K$, potom také $x + y \in K$ a platí $|x + y| = x + y = |x| + |y|$. Jestliže $x = 0$, potom snadno $|0 + y| = |y| = 0 + |y| = |0| + |y|$. Pokud $-x, -y \in K$, potom $-(x + y) = -x - y \in K$ a platí také $|x + y| = -(x + y) = -x - y = |x| + |y|$.

Konečně předpokládejme, že $x, -y \in K$, potom platí $-x < 0 < x$ a také $y < 0 < -y$). Z dokázaných nerovností jistě plyne, že $|x| + |y| = x - y > x + y, -x - y$. Protože platí $|x+y| = x+y$ nebo $|x+y| = -x-y$, dostáváme dohromady $|x+y| < |x|+|y|$. Analogicky provedeme důkaz v případě, kdy platí $-x, y \in K$.

ad iv) Díky dokázané předchozí části můžeme počítat $|x| = |x - y + y| \leq |x - y| + |y|$. Z monotonnosti sčítání ihned plyne $|x| - |y| \leq |x - y|$. □

Kapitola 2

Zavedení přirozených čísel pomocí Peanových axiomů

Přirozená čísla jsou nejdůležitější abstrakcí, kterou lidstvo vynalezlo. Věnujme čas tomu, abychom pochopili její podstatu. Co to vlastně je číslo? Často číslo chybně ztotožňujeme s jeho zápisem (s nějakým symbolem nebo řadou symbolů). Způsobů, jak zapsat číslo, je vynalezeno mnoho, ale na číslech jako takových se nic nezměnilo. Aritmetika je nezávislá na způsobu zápisu čísel (v opačném případě bychom museli mít jinou teorii aritmetiky pro římské číslice a jinou teorii pro arabský zápis).

Přirozená čísla vznikla „oddělením“ informace o počtu „předmětů“ v nějaké skupině od těchto předmětů. Samotné číslo je proto právě informace o množství (přičemž již neupřesňujeme, o množství **čeho** se jedná). Operace sčítání a násobení potom představují „sjednocování skupin předmětů“ a „násobného zvětšování skupin předmětů“.

V dalších úvahách nahradíme pojmy „skupina“ a „předmět“ za pojmy „množina“ a „prvek“, které jsou jejich matematickým synonymem. Aby vlastnost „počet prvků“ v množině dával smysl, musíme být schopni rozpoznat, kdy dvě množiny mají stejný počet prvků. Tento problém dokázali lidé řešit ještě před vynálezem čísel. Antropologové se u primitivních národů, živících se rybolovem, setkali se zajímavou metodou. Jestliže rybář potřeboval zjistit, kolik ryb chytil, rozložil ryby, ke každé položil jeden klacík a potom všechny tyto klacíky představovaly množství ryb, které chytil.

Všimněme si, že touto důmyslnou metodou mohou rybáři nejen spočítat svůj úlovek, ale především pomocí klacíku je možné provádět i základní aritmetiku (sčítání, odčítání a při troše invence i násobení a především dělení úlovku).

Naprosto stejného postupu užíváme i my. Řekneme, že dvě množiny mají stejnou mohutnost, jestliže existuje vzájemně jednoznačné přiřazení prvků z jedné množiny k prvkům množiny druhé (každý prvek z první množiny má přiřazen právě jeden prvek z druhé množiny a naopak). Vezmeme-li třídu[1] všech konečných[2] množin, potom relace „mít stejnou mohutnost“ je relací ekvivalence. Její faktorové třídy nám mohou představovat jednotlivá čísla (číslo n je potom třída všech n-prvkových množin). Opačně každá n-prvková

[1] Třídou rozumíme v matematice zobecnění množiny (každá množina je třída, ale naopak třída nemusí být množinou). Potřeba vytvoření nového pojmu vznikla s poznatkem toho, že neexistuje množina všech množin – musela by obsahovat sebe samu.

[2] Teorie množin nemá větší problémy s definováním konečné množiny. Možnou definicí je, že konečná množina je právě taková množina M, kdy pro každou její ostrou podmnožinu $N \subset M$ neexistuje bijekce mezi M a N.

množina reprezentuje číslo n.

Popsaná konstrukce je jenom jedna z mnoha. V dalším textu se zaměříme na „filozoficky“ zcela jiné pojetí aritmetiky.

2.1 Peanovy axiomy

Peanovy axiomy zavádějí přirozená čísla pomocí pojmu následovník a pomocí principu matematické indukce. Prvních pět axiomů určují množinu přirozených čísel a další čtyři axiomy definují aritmetiku (sčítání a násobení).

Axiomy lze formulovat následovně:

(P1) Existuje prvek 1 takový, že $1 \in \mathbb{N}$.

(P2) Jestliže prvek $x \in \mathbb{N}$, potom také prvek $x' \in \mathbb{N}$ (prvek x' nazýváme následovníkem prvku x a intuitivně nám symbolizuje číslo o jedno větší než číslo x).

(P3) Platí, že $x' \neq 1$ (tedy 1 není následovníkem žádného prvku).

(P4) Jestliže $x' = y'$, potom také platí $x = y$.

(P5) Jestliže máme libovolnou množinu $R \subseteq \mathbb{N}$ takovou, že $1 \in R$, a navíc pro každé $x \in R$ také $x' \in R$, potom platí, že $R = \mathbb{N}$.

Vysvětleme si myšlenku axiómů. První dva axiomy zavádějí v principu jazyk teorie. Říkají, že máme číslo 1 a každé číslo má svého následovníka. Třetí a čtvrtý axiom nám zaručují, že se posloupnost následovníků nemůže žádným způsobem uzavřít do cyklu.

První čtyři axiomy nám říkají, že přirozená čísla tvoří jednička a její následovníci (jsou vždy nové – neopakují se). Posledním axiomem řekneme navíc to, že přirozená čísla tvoří **právě** jednička a její následovníci. Ukážeme si příklad modelu, který splňuje první čtyři Peanovy axiomy a poslední nesplňuje.

Nechť $N = \{a, b, 1, 2, 3, \ldots\}$ a nechť $a' = b$, $b' = a$, $1' = 2$, $2' = 3$ atd. Snadno ověříme, že takto vytvořená množina splňuje axiomy (P1)-(P4), přičemž poslední axiom (P5) není splněn (vezmeme-li množinu $K = \{1, 2, \ldots\} \subset N$, potom $1 \in K$, jestliže $x \in K$, potom také $x' \in K$, a navíc $K \neq N$).

Následujících čtyř axiomů užíváme k definici sčítání a násobení:

(A1) $x + 1 = x'$,

(A2) $x + y' = (x + y)'$,

(B1) $x \cdot 1 = x$,

(B2) $x \cdot y' = x \cdot y + x$.

Nyní již můžeme vyslovit očekávané základní věty platící pro sčítání a násobení přirozených čísel.

Věta 14 *Mějme libovolná přirozená čísla $x, y, z \in \mathbb{N}$. Potom platí, že*

(Ai) *součet $x + y$ je jednoznačně definován,*

(Aii) $x + y = y + x$,

(Aiii) $(x + y) + z = x + (y + z)$,

(Aiv) *jestliže $x + z = y + z$, potom také $x = y$.*

Důkaz: ad (Ai) Mějme libovolné přirozené číslo $a \in \mathbb{N}$. Potom označme následující množinu

$$R_a = \{x \in \mathbb{N} \mid a + x \text{ je korektně a jednoznačně definováno}\}.$$

K důkazu věty stačí ověřit, že množina R_a je rovna množině všech přirozených čísel. V Peanově aritmetice používáme k tomuto důkazu axiomu (P5).

Platí, že $x + 1 \overset{(A1)}{=} x'$, a tedy součet $x + 1$ je korektně a jednoznačně definován. Proto $1 \in R_a$.

Předpokládejme, že $x \in R_a$. Tedy součet $a+x$ je definován, a tak výraz $(a+x)'$ máme jednoznačně určen. Podle axiomu (A2) platí, že $a+x' = (a+x)'$, a tedy také součet $a+x'$ je jednoznačně definován. Proto také $x' \in R_a$.

Dokázali jsme, že $1 \in R_a$, a jestliže platí, že $x \in R_a$, potom také $x' \in R_a$. Z axiomu (P5) tedy plyne rovnost množin $R_a = \mathbb{N}$. Protože číslo a jsme volili zcela libovolně, je tímto věta dokázána.

ad (Aiii) Pro libovolná přirozená čísla $a, b \in \mathbb{N}$ označme následující množinu

$$R_{a,b} = \{x \in \mathbb{N} \mid (a + b) + x = a + (b + x)\}.$$

Podobně jako v předchozí části užijeme pátý Peanův axiom.

Platí, že $(a + b) + 1 \overset{(A1)}{=} (a + b)' \overset{(A2)}{=} a + b' \overset{(A1)}{=} a + (b + 1)$. Což ovšem znamená, že $1 \in R_{a,b}$.

Předpokládejme nyní, že $x \in R_{a,b}$. Platí, že $(a + b) + x = a + (b + x)$. Nyní můžeme počítat

$$\begin{aligned}(a + b) + x' \overset{(A2)}{=} &((a + b) + x)' = \\ &(a + (b + x))' \overset{(A2)}{=} \\ &a + (b + x)' \overset{(A2)}{=} \\ &a + (b + x').\end{aligned}$$

Dokázali jsme také $x' \in R_{a,b}$, a proto z pátého Peanova axiomu dostáváme, že $R_{a,b} = \mathbb{N}$.

ad (Aii) Nejprve dokážeme komutativitu čísla 1 s libovolným přirozeným číslem. Označme proto množinu

$$R = \{x \in \mathbb{N} \mid 1 + x = x + 1\}.$$

Je zřejmé, že $1 \in \mathbb{N}$ (protože $1 + 1 = 1 + 1$). Předpokládejme nyní, že $x \in \mathbb{N}$, platí tedy $1 + x = x + 1$. Protože asociativitu již máme dokázanou, můžeme počítat $x' + 1 = (x + 1) + 1 = (1 + x) + 1 = 1 + (x + 1) = 1 + x'$. Dostáváme, že $x' \in R$, a podle pátého Peanova axiomu platí rovnost $R = \mathbb{N}$. Máme proto obecně dokázáno, že $1 + x = x + 1$.

Nyní přejdeme k důkazu obecné komutativity. Označme si pro libovolné přirozené číslo $a \in \mathbb{N}$ množinu

$$R_a = \{x \in \mathbb{N} \mid a + x = x + a\}.$$

Protože jsme dokázali, že 1 komutuje s každým prvkem, platí, že $1 \in R_a$.

Nechť nyní $x \in R_a$ (tedy platí, že $x + a = a + x$; podmínku v tomto kroku důkazu obvykle nazýváme indukční předpoklad). Vzhledem k asociativitě a komutativitě 1 s každým prvkem lze počítat:

$$\begin{aligned} x' + a &= (x + 1) + a = \\ &= x + (1 + a) = \\ &= x + (a + 1) = \\ &= (x + a) + 1 = \\ &= (a + x) + 1 = \\ &= a + (x + 1) \\ &= a + x'. \end{aligned}$$

Proto také platí, že $x' \in R_a$, a užitím pátého Peanova axiomu dostáváme množinovou rovnost $R_a = \mathbb{N}$.

ad (Aiv) Označme pro libovolná přirozená čísla $a, b \in \mathbb{N}$ množinu

$$R_{a,b} = \{x \in \mathbb{N} \mid \text{ z rovnosti } a + x = b + x \text{ plyne rovnost } a = b\}.$$

Předpokládejme, že $a + 1 = b + 1$. Toto lze podle axiomu (A1) přepsat do tvaru $a' = b'$. Užitím Peanova axiomu (P4) dostáváme, že $a = b$, tedy $1 \in R_{a,b}$.

Předpokládejme nyní, že $x \in R_{a,b}$. Platí proto, že z rovnosti $a + x = b + x$ plyne rovnost $a = b$ (což je naším indukčním předpokladem). Budeme se snažit dokázat, že za tohoto předpokladu plyne z rovnosti $a + x' = b + x'$ opět rovnost $a = b$. Nechť navíc platí $a + x' = b + x'$. Užitím axiomu (A2) dostáváme rovnost $(a + x)' = a + x' = b + x' = (b + x)'$. Užitím axiomu (P4) získáme rovnost $a + x = b + x$. Z indukčního předpokladu ale vidíme, že z $a + x = b + x$ plyne rovnou $a = b$. Dohromady jsme dokázali: pokud $x \in R_{a,b}$, potom plyne z rovnosti $a + x' = b + x'$ také rovnost $a = b$, a tedy $x' \in R_{a,b}$.

Z dokázaných vlastností a z pátého Peanova axiomu plyne, že $R_{a,b} = \mathbb{N}$. □

Věta 15 *Mějme libovolná přirozená čísla $x, y, z \in \mathbb{N}$. Potom platí, že*

(Mi) součin $x \cdot y$ je jednoznačně definován,

(Mii) $x \cdot y = y \cdot x$,

(Miii) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

(Miv) jestliže platí, že $x \cdot z = y \cdot z$*, potom také* $x = y$.

Věta 16 *Mějme libovolná přirozená čísla* $x, y, z \in \mathbb{N}$*. Potom platí, že*

(Di) $x \cdot (y + z) = x \cdot y + x \cdot z$,

(Dii) $(y + z) \cdot x = y \cdot x + z \cdot x$.

Důkaz: ad (Mi) Mějme libovolné přirozené číslo $a \in \mathbb{N}$. Označme množinu

$$R_a = \{x \in \mathbb{N} \mid a \cdot x \text{ je korektně a jednoznačně definováno}\}.$$

Platí, že $a \cdot 1 \overset{(M1)}{=} a$, a tedy součin $a \cdot 1$ je korektně a jednoznačně definován. Proto $1 \in R_a$.

Předpokládejme, že $x \in R_a$. Součin $a \cdot x$ je definován a také výraz $a \cdot x + a$ máme jednoznačně určen (vzhledem k tomu, že v (Ai) jsme ukázali jednoznačnost definice každého součtu). Podle axiomu (M2) ale platí, že $a \cdot x' = a \cdot x + a$, a proto také součet $a + x'$ je jednoznačně definován, a v důsledku platí $x' \in R_a$.

Podle pátého Peanova axiomu je důsledkem rovnost množin $R_a = \mathbb{N}$, což dokazuje větu.

ad (Di) Pro dokázání levé distributivity definujeme pro libovolná přirozená čísla $a, b \in \mathbb{N}$ následující množinu

$$R_{a,b} = \{x \in \mathbb{N} \mid a \cdot (b + x) = a \cdot b + a \cdot x\}.$$

Z axiomů (A1), (M1) a (M2) dostáváme $a \cdot (b+1) \overset{(A1)}{=} a \cdot b' \overset{(M2)}{=} a \cdot b + a \overset{(M1)}{=} a \cdot b + a \cdot 1$. Proto platí, že $1 \in R_{a,b}$.

Předpokládejme $x \in R_{a,b}$. Potom platí, že $a \cdot (b + x) = a \cdot b + a \cdot x$ (což je náš indukční předpoklad *i.p.*). Protože komutativitu a asociativitu operace sčítání máme již dokázanou, nebudeme jednotlivé sčítance nadále oddělovat závorkami. Tyto vlastnosti budeme nadále užívat bez zvláštního upozorňování. Platí rovnost $a \cdot (b + x') \overset{(A2)}{=} a \cdot (b + x)' \overset{(M2)}{=} a \cdot (b + x) + a \overset{i.p.}{=} a \cdot b + a \cdot x + a \overset{(M2)}{=} a \cdot b + a \cdot x'$. Z předchozího přímo plyne, že také $x' \in R_{a,b}$ a tedy jsou splněny všechny podmínky pro aplikaci pátého peanova axiomu. Dokázali jsme, že $\mathbb{N} = R_{a,b}$.

ad (Miii) Opět označme pro libovolná čísla $a, b \in \mathbb{N}$ množinu

$$R_{a,b} = \{x \in \mathbb{N} \mid a \cdot (b \cdot x) = (a \cdot b) \cdot x\}.$$

Snadno vidíme, že platí $a \cdot (b \cdot 1) \overset{(M1)}{=} a \cdot b \overset{(M1)}{=} (a \cdot b) \cdot 1$. Tedy $1 \in R_{a,b}$.

Nechť máme indukční předpoklad *i.p.* takový, že $x \in R_{a,b}$, tedy platí $a \cdot (b \cdot x) = (a \cdot b) \cdot x$. Potom lze počítat

$$\begin{aligned} a \cdot (b \cdot x') &\overset{(M2)}{=} a \cdot (b \cdot x + b) \overset{(Di)}{=} \\ & a \cdot (b \cdot x) + a \cdot b \overset{i.p}{=} \\ & (a \cdot b) \cdot x + a \cdot b \overset{(M2)}{=} \\ & (a \cdot b) \cdot x'. \end{aligned}$$

Opět vidíme, že platí $x' \in R_{a,b}$, a proto z pátého Peanova axiomu dostáváme $R_{a,b} = \mathbb{N}$.

Dokážeme pomocné tvrzení $x' \cdot y = x \cdot y + y$ Označme následující množinu

$$R_a = \{x \in \mathbb{N} \mid a' \cdot x = a \cdot x + x\}$$

pro pevně zvolené číslo $a \in \mathbb{N}$. Potom lze počítat $a' \cdot 1 \overset{(M1)}{=} a' \overset{(A1)}{=} a + 1 \overset{(M1)}{=} a \cdot 1 + 1$. Z tohoto dostáváme $1 \in R_a$.

Předpokládejme nyní, že $x \in R_a$, potom je naším indukčním předpokladem *i.p.* tvrzení, že $a' \cdot x = a \cdot x + x$. Počítejme proto nyní

$$\begin{aligned} a' \cdot x' &\overset{(A1)}{=} a' \cdot (x + 1) \overset{(Di)}{=} \\ & a' \cdot x + a' \cdot 1 \overset{i.p}{=} \\ & a \cdot x + x + a + 1 \overset{(M2)}{=} \\ & a \cdot x' + x'. \end{aligned}$$

Vidíme, že $x' \in R_a$, a máme splněny podmínky pro aplikaci pátého Peanova axiomu. Tedy $R_a = \mathbb{N}$ dokazuje větu.

Dokážeme pomocné tvrzení $1 \cdot x = x$. Analogicky k předchozím případům definujeme množinu

$$R = \{x \in \mathbb{N} \mid 1 \cdot x = x\}.$$

Z axiomu (M1) dostáváme $1 \cdot 1 = 1$, a tedy také $1 \in R$. Předpokládejme, že $x \in R$ (tedy $1 \cdot x = x$). Potom platí, že $1 \cdot x' \overset{(M2)}{=} 1 \cdot x + 1 \overset{i.p}{=} x + 1 \overset{(A1)}{=} x'$. Tedy $x' \in R$, a navíc jsou splněny podmínky pro aplikaci pátého Peanova axiomu. Proto $R = \mathbb{N}$.

ad (Mii) Opět označme pro libovolné přirozené číslo $a \in \mathbb{N}$ množinu

$$R_a = \{x \in \mathbb{N} \mid a \cdot x = x \cdot a\}.$$

Z již dokázaného pomocného tvrzení víme, že $1 \cdot x = x \overset{(M1)}{=} x \cdot 1$. Proto $1 \in R_a$. Předpokládejme nyní, že $x \in R_a$, tedy indukčním předpokladem *i.p.* je tvrzení $x \cdot a = a \cdot x$. Vzhledem k dokázanému pomocnému tvrzení lze počítat $x' \cdot a = x \cdot a + x \overset{i.p.}{=} a \cdot x + x \overset{(M2)}{=} a \cdot x'$. Proto platí, že $x' \in R_a$, a tedy podle pátého Peanova axiomu platí $R_a = \mathbb{N}$.

ad (Dii) Pravá distributivita ihned plyne z dokázané komutativity násobení a z levé distributivity.

ad (Miv) K důkazu tohoto tvrzení jsou potřeba výsledky z následující kapitoly. Důkaz tedy předvedeme na patřičném místě. □

V dalších kapitolách budeme užívat následující jednoduché tvrzení.

Lemma 5 *Každé číslo $x \in \mathbb{N}$ takové, že $x \neq 1$ je následovníkem některého přirozeného čísla (tedy platí $y' = x$ pro některé $y \in \mathbb{N}$).*

Důkaz: K dokázání věty stačí ukázat, že množina $R = \{x \in \mathbb{N} \mid x = 1 \text{ nebo } x = y' \text{ pro některé } y \in \mathbb{N}\}$ je rovna množině přirozených čísel. Skutečnost, že $1 \in \mathbb{N}$, je explicitně vyjádřena v definici množiny R. Je navíc zřejmé, že jestliže $x \in R$, potom x' je ve tvaru následovníku, tedy $x' \in R$. Tímto podle pátého Peanova axiomu platí $R = \mathbb{N}$. □

2.2 Uspořádání na množině $\mathbb{N}$

Cílem této kapitoly je zavést obecně známé uspořádání na množině přirozených čísel a ukázat některé základní vlastnosti tohoto uspořádání. Připomeňme, že rozlišujeme takzvané „ostré“ uspořádání $<$ a „neostré“ uspořádání $\leq$.

Definice 10 *Mějme přirozená čísla $x, y \in \mathbb{N}$. Potom řekneme, že číslo x je (ostře) menší než číslo y (značíme $x < y$), jestliže existuje takové $n \in \mathbb{N}$, že platí $x + n = y$. Řekneme, že číslo x je menší nebo rovno číslu y (značíme $x \leq y$), jestliže $x < y$ nebo $x = y$.*

Věta 17 *Relace ostrého uspořádání $<$ na množině přirozených čísel $\mathbb{N}$ je ireflexivní, tranzitivní a asymetrické.*

Relace standardního uspořádání $\leq$ na množině přirozených čísel je reflexivní, tranzitivní a antisymetrické.

Důkaz: Začneme dokazování části věty o ostrém uspořádání. Předpokládejme nejprve sporem, že $x < x$. Potom existuje takové $n \in \mathbb{N}$, že $x + n = x$. Přičtením jednotky k rovnosti dostáváme $x + n + 1 = x + 1$, a tedy také $x + n' = x + 1$. Z pravidla krácení pro sčítání dostáváme $n' = 1$, což je spor s axiomem (P3).

Nyní dokážeme tranzitivitu ostrého uspořádání. Nechť $x < y$ a $y < z$,. Potom existují čísla $m, n \in \mathbb{N}$ taková, že $x + m = y$ a $y + n = z$. Dosazením první rovnosti do druhé a užitím asociativity sčítání dostáváme $x + (m + n) = (x + m) + n = y + n = z$, a protože $m + n \in \mathbb{N}$, máme dokázáno, že $x < z$.

Asymetrii dokážeme opět sporem. Jestliže platí $x < y$ a $y < x$, potom z tranzitivity uspořádání máme $x < x$, což je spor s ireflexivitou.

Vlastnosti neostrého uspořádání již přirozeně plynou z dokázaného. Triviálně $x \leq x$ (protože $x = x$), tranzitivitu standardního uspořádání snadno dostaneme z dokázané tranzitivity ostrého uspořádání. Stejně jako antisymetrie přímo plyne z dokázané asymetrie.

□

Uvědomme si navíc, že z Lemma 5 plyne pro libovolné $x \in \mathbb{N}$, že pokud $x \neq 1$, potom existuje $y \in \mathbb{N}$ takové, že $x = y'$, a tedy také $x = 1 + y$, což dává $1 < x$. Z ireflexivity ostrého uspořádání naopak vidíme, že $1 < x$ implikuje to, že $x \neq 1$. Tedy tvrzení $x \neq 1$ a $1 < x$ jsou ekvivalentní. Z tohoto mimo jiné plyne skutečnost, že 1 je nejmenší prvek přirozeného uspořádání (tedy vždy platí $1 \leq x$).

Věta 18 *Relace „ostrého“ i „přirozeného“ uspořádání jsou monotónní vzhledem ke sčítání i násobení. Tedy pro libovolná čísla $x, y, z \in \mathbb{N}$ z nerovnosti $x < y$ (resp. $x \leq y$) plynou obě nerovnosti $x + z < y + z$ a $x \cdot z < y \cdot z$ (resp. obě nerovnosti $x + z \leq y + z$ a $x \cdot z \leq y \cdot z$).*

Důkaz. Předpokládejme, že $x < y$. Potom existuje $n \in \mathbb{N}$ takové, že $x + n = y$. Z tohoto snadno vidíme, že $x + z + n = y + z$, a tedy z definice uspořádání rovnou dostáváme $x + z < y + z$. Analogicky užitím distributivity vidíme, že $x \cdot z + n \cdot z = (x + n) \cdot z = y \cdot z$, a protože $n \cdot z \in \mathbb{N}$, platí tak $x \cdot z < y \cdot z$. Kompatibility přirozeného uspořádání plynou ihned z kompatibilit ostrého uspořádání. □

Věta 19 *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 $x < y$, $y < x$, nebo $x = y$).*

Důkaz. Z ireflexivity a asymetrie ostrého uspořádání rovnou vidíme, že nemohou nastat dvě opačné nerovnosti nebo ostrá nerovnost s rovností současně. Stačí tedy dokázat, že vždy nastane alespoň jedna z možností trichotomie. Vezměme si libovolné pevné číslo $a \in \mathbb{N}$ a označme množinu $R_a = \{x \in \mathbb{N} \mid x < a \text{ nebo } a < x \text{ nebo } a = x\}$. Jak jsme již ukázali, pokud $a \neq 1$, potom $1 < a$, a tedy $1 \in R_a$. Stejně tak pokud $a = 1$, potom přímo z definice množiny R_a plyne, že $1 \in R_a$.

Nyní předpokládejme, že $x \in R_a$. Indukčním předpokladem je tvrzení $x < a$ nebo $a < x$ nebo $a = x$. Nadále budeme postupovat rozborem jednotlivých případů. Snadno vidíme, že $x < x'$ (protože $x + 1 = x'$). Proto pokud platí $a < x$ nebo $a = x$, dostáváme rovnou z tranzitivity $a < x'$. V těchto případech také $x' \in R_a$.

Pokud platí $x < a$, potom podle definice ostrého uspořádání existuje číslo $n \in \mathbb{N}$ takové, že $x + n = a$. Jestliže $n = 1$, potom dostáváme, že $x' = x + 1 = a$, a tedy $x' \in R_a$. Jestliže $n \neq 1$, potom podle Lemma 5 existuje $m \in \mathbb{N}$ takové, že $m' = n$. Potom ovšem $a = x + n = x + m' = x + m + 1 = x' + m$, a tedy opět $x' \in R_a$.

Rozborem na jednotlivé případy jsme došli k závěru, že za předpokladu $x \in R_a$ vždy platí $x' \in R_a$. Podle pátého Peanova axiomu také platí, že $R_a = \mathbb{N}$, což dokazuje větu. □

Důsledek 1 *Přirozené uspořádání $\leq$ na množině $\mathbb{N}$ je lineární (tedy pro libovolná čísla $x, y \in \mathbb{N}$ platí alespoň jedno z tvrzení $x \leq y$ nebo $y \leq x$).*

Nyní máme dostatek prostředků k dokázání tvrzení (Miv) (tedy pravidla krácení pro násobení). Předpokládejme, že platí $x \cdot z = y \cdot z$. Z trichotomie plyne, že musí nastat právě jedna z možností $x < y$, $y < x$ nebo $x = y$. Dokázaná kompatibilita ostrého uspořádání nám ukazuje, že pokud $x < y$, potom $x \cdot z < y \cdot z$ (což je spor), a stejně tak, pokud $y < x$, potom $y \cdot z < x \cdot z$ (opět spor). Z dokázaného tedy plyne, že zbývá jedině $x = y$.

2.3 Transfinitní indukce a dobře uspořádané množiny

Princip matematické indukce, který v Peanově aritmetice přímo představuje axiom (P5), lze v jistých případech zobecnit na takzvanou transfinitní indukci. Matematická indukce je ve svém principu ideální způsob, jak dokázat tvrzení, ovšem pouze pro konečné množství prvků.

Uvedeme si příklad. Matematickou indukcí dokážeme, že existuje součet libovolného konečného množství čísel. Jedno číslo jistě sečíst lze (jeho součtem je ono samo). Navíc jestliže můžeme sečíst n čísel, k výslednému součtu můžeme vždy jedno číslo přičíst (protože dvě čísla sečíst můžeme). Tedy můžeme sečíst $n+1$ čísel. Z principu matematické indukce plyne, že lze sečíst libovolný konečný počet čísel. Je důležité si uvědomit, že si výsledek matematické indukce nemůžeme interpretovat tak, že lze sečíst libovolné (i nekonečné) množství čísel. Součty nekonečného množství čísel lze uspokojivě najít pouze u některých číselných řad, jak ostatně víme z matematické analýzy.

Elegance dokazování matematickou indukcí vedla matematiky k nalezení obecnějšího postupu dokazování, který se matematické indukci podobá a v případě přirozených čísel s matematickou indukcí splývá. Připomeňme, že uspořádáním na množině rozumíme binární relaci na množině, které je reflexivní, tranzitivní a antisymetrické. Množinu spolu s relací uspořádání nazveme uspořádanou množinou.

Definice 11 *Řekneme, že uspořádaná množina $(M, \leq)$ je dobře uspořádanou množinou, jestliže každá její neprázdná podmnožina $R \subseteq M$ má nejmenší prvek (t.j. existuje $1_R \in R$ takové, že $1_R \leq x$ pro každé $x \in R$).*

Uvědomme si základní vlastnosti dobře uspořádaných množin. V prvé řadě pro každou podmnožinu $\{x, y\} \subseteq M$ v dobře uspořádané množině $(M, \leq)$ existuje nejmenší prvek v $\{x, y\}$. Z tohoto přímo dostáváme, že $x \leq y$ nebo $y \leq x$, a tedy každá dobře uspořádaná množina je nutně uspořádaná lineárně.

Ovšem pojem dobře uspořádané množiny je daleko silnější než pojem lineárně uspořádané množiny. Vezměme si například množinu kladných racionálních čísel $(\mathbb{Q}^+, \leq)$ spolu se standardním uspořádáním (vystačíme si prozatím s naší intuitivní středoškolskou představou), potom její podmnožina $\{\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots, \frac{1}{2^i}, \ldots\}$ nejmenší prvek nemá.

Věta 20 *Uspořádaná množina $(\mathbb{N}, \leq)$ je dobře uspořádaná (Rozumíme množina přirozených čísel $\mathbb{N}$ spolu se standardním uspořádáním $\leq$).*

Důkaz: Předpokládejme, že máme neprázdnou podmnožinu přirozených čísel $X \subseteq \mathbb{N}$. Označme si potom množinu

$$L(X) = \{x \in \mathbb{N} \mid \text{pro každé } y \in X \text{ platí, že } x < y\}.$$

Mohou nastat dva případy. Jestliže $1 \notin L(X)$, potom přímo z definice množiny existuje $x \in X$ takové, že $1 \not< x$. Jak ale víme, toto je ekvivalentní s tím, že $x = 1$. Proto platí, že $1 \in X$, a tedy 1 je nejmenším prvkem množiny X.

Předpokládejme nyní, že $1 \in L(X)$. Musí potom platit, že existuje $x \in L(X)$ takové, že $x' \notin L(X)$ (kdyby takovéto x neexistovalo, potom by byly splněny podmínky k aplikaci pátého Peanova axiomu, a tedy by platilo $L(X) = \mathbb{N}$; to ovšem implikuje spor $X = \emptyset$). Ze způsobu zavedení množiny $L(X)$ vidíme, že existuje $y \in X$ takové, že $x' \not< y$ (protože $x' \notin L(X)$), ale také $x < y$ (platí $x \in L(X)$). Snadno platí, že $x < y$ implikuje $x' \leq y$ [3]. Toto dohromady dává, že $x' = y$, a tedy $x' \in X$. Protože ale $x < y$ pro všechna $y \in X$, platí, že $x' \leq y$ pro všechna $y \in X$. Tímto je dokázáno, že x' je nejmenší prvek množiny X. □

Příkladů dobře uspořádaných množin je ale přesto více. Především každá lineárně uspořádaná konečná množina je dobře uspořádanou množinou. Uvažujme, že označíme množinu $\mathbb{N}^* = \{1^*, 2^*, 3^*, \ldots\} = \{n^* \mid n \in \mathbb{N}\}$. Potom můžeme zavést uspořádaní na $\mathbb{N} \cup \mathbb{N}^*$ tak, že $1 < 2 < 3 < \ldots < 1^* < 2^* < 3^* < \ldots$. Lze snadno ověřit, že takto vytvořena množina je také dobře uspořádanou množinou. Příkladů uspořádaných množin je skutečně mnoho (teorie dobře uspořádaných množin je ve skutečnosti teorií ordinálních čísel v teorii množin), proto následující věta poskytuje zajímavé rozšíření aparátu matematické indukce. Ve větě zavedený princip se nazývá princip transfinitní indukce.

Věta 21 *Nechť $(M, \leq)$ je dobře uspořádaná množina. Označíme-li pro libovolný prvek $t \in M$ úsekem množinu $M_t = \{x \in M \mid x < t\}$, potom pro každá množina $S \subseteq M$, která splňuje tvrzení*

$$Z \text{ inkluze } M_t \subseteq S \text{ plyne } t \in S \qquad (TI)$$

je rovna celé množině M.

Důkaz. Předpokládejme, že množina $S \subseteq M$ splňuje podmínku (TI), a navíc platí, že $S \neq M$. Potom platí, že $M \setminus S$ je neprázdná, množina a tudíž má nejmenší prvek $s \in M \setminus S$. Proto každé $x < s$ náleží množině S (protože nenáleží množině $M \setminus S$), a tedy platí, že $M_s \subseteq S$. Z tvrzení (TI) dostáváme $s \in S$, což je spor (protože $s \in S \cup M \setminus S = \emptyset$). □

[3] Jestliže $x < y$, potom existuje $n \in \mathbb{N}$ takové, že $x + n = y$. Jestliže $n = 1$, potom $x' = x + 1 = y$. Jestliže $n \neq 1$, potom existuje $m \in \mathbb{N}$ takové, že $m' = n$. Toto ovšem implikuje rovnost $y = x + n = x + m' = x + m + 1 = x' + m$, a tedy z definice $x' < y$. Proto v obou případech platí $x' \leq y$.

Kapitola 3

Konstrukce oboru integrity celých čísel

Jestliže máme definovanou strukturu přirozených čísel $(\mathbb{N}, +, \cdot)$, můžeme zkonstruovat čísla celá. Motivací k následující skutečnosti je rozšíření pologrupy $(\mathbb{N}, +)$ na grupu, a to navíc tak, aby i pologrupa $(\mathbb{N}, \cdot)$ byla rozšířena přirozeným způsobem.

Postup rozšíření komutativní pologrupy s pravidlem krácení na grupu byl popsán ve Větě 3, a jak bylo navíc dokázáno, $(\mathbb{N}, +)$ je pologrupou s pravidlem krácení. Umíme tedy zkonstruovat grupu $\mathbb{N}^2/\sim$. Domluvme se nejprve, že strukturu $\mathbb{N}^2/\sim$ budeme značit obvyklejším a jednodušším $\mathbb{Z}$. Připomeňme základní vlastnosti této grupy. Prvky množiny $\mathbb{N}^2/\sim$ jsou třídy, které (v souladu s úmluvou o aditivní symbolice) značíme $x - y$, kde $x, y \in \mathbb{N}$. Připomínáme, že označením $x-y$ rozumíme dvojici (přesněji řečeno třídu dvojic), a tedy znak „$-$“ **nesymbolizuje** přímo operaci odečítání, přestože s tímto významem plně koresponduje.

Dále v souladu s konstrukcí víme, že i různé dvojice prvků (v našem případě přirozených čísel) mohou označovat stejnou hodnotu (mohou být ekvivalentní podle zavedené relace $\sim$). Platí tedy:

$$x_1 - y_1 = x_2 - y_2 \text{ tehdy a jen tehdy, platí-li } x_1 + y_2 = x_2 + y_1.$$

Operaci sčítání potom definujeme následovně:

$$(x_1 - y_1) + (x_2 - y_2) = (x_1 + x_2) - (y_1 + y_2).$$

Takto vzniklá struktura je grupa, kde nulovým prvkem jsou všechny (navzájem si rovné) dvojice $x - x$ a k prvku $x - y$ je opačným prvkem $y - x$.

Konečně připomeňme, že přirozená čísla $\mathbb{N}$ lze vnořit do $\mathbb{Z}$ zobrazením $f : \mathbb{N} \longrightarrow \mathbb{Z}$ tak, že číslu $x \in \mathbb{N}$ přiřadíme prvek $2x - x \in \mathbb{Z}$.

Následující věta nám ukáže, jakým způsobem lze zavést na množině $\mathbb{Z}$ operaci součinu tak, aby výše uvedená korespondence f zachovávala také součiny (tj. zavedeme součin tak, aby platilo $f(x \cdot y) = f(x) \cdot f(y)$).

Věta 22 *Operace $\cdot$ na množině $\mathbb{Z}$ definovaná tak, že:*

$$(x_1 - y_1) \cdot (x_2 - y_2) = (x_1 \cdot x_2 + y_1 \cdot y_2) - (x_1 \cdot y_2 + x_2 \cdot y_1)$$

je definována korektně, a navíc platí, že $(\mathbb{Z}, \cdot)$ je komutativní pologrupa a zobrazení $f : \mathbb{N} \longrightarrow \mathbb{Z}$ definované výše zachovává násobení. Jednotkovým prvkem v této pologrupě je $2 - 1$.

Důkaz: Abychom dokázali korektnost definice operace $\cdot$, musíme ukázat, že různé reprezentace stejného prvku dávají po vynásobení opět reprezentace téhož prvku. Předpokládejme proto, že platí $x_1 - y_1 = x_1' - y_1'$ a $x_2 - y_2 = x_2' - y_2'$. Podle definice rovnosti prvku v $\mathbb{Z}$ dostáváme následující rovnosti (tentokrát čísel v $\mathbb{N}$):

$$x_1 + y_1' = x_1' + y_1, \tag{A}$$

$$x_2 + y_2' = x_2' + y_2. \tag{B}$$

Vynásobíme-li postupně rovnost (A) prvkem x_2, rovnost (A) prvkem y_2, rovnost (B) prvkem x_1' a rovnost (B) prvkem y_1', obdržíme rovnosti:

$$x_1 \cdot x_2 + y_1' \cdot x_2 = x_1' \cdot x_2 + y_1 \cdot x_2, \tag{C}$$

$$x_1' \cdot y_2 + y_1 \cdot y_2 = x_1 \cdot y_2 + y_1' \cdot y_2, \tag{D}$$

$$x_1' \cdot x_2 + x_1' \cdot y_2' = x_1' \cdot x_2' + x_1' \cdot y_2, \tag{E}$$

$$y_1' \cdot x_2' + y_1' \cdot y_2 = y_1' \cdot x_2 + y_1' \cdot y_2'. \tag{F}$$

Nyní získané rovnosti (C), (D), (E) a (F) sečteme

$$\begin{aligned} x_1 \cdot x_2 + y_1' \cdot x_2 + x_1' \cdot y_2 + y_1 \cdot y_2 + x_1' \cdot x_2 + x_1' \cdot y_2' + y_1' \cdot x_2' + y_1' \cdot y_2 = \\ x_1' \cdot x_2 + y_1 \cdot x_2 + x_1 \cdot y_2 + y_1' \cdot y_2 + x_1' \cdot x_2' + x_1' \cdot y_2 + y_1' \cdot x_2 + y_1' \cdot y_2'. \end{aligned}$$

Nyní můžeme užít pravidla krácení (které platí pro sčítání v $\mathbb{N}$) a pomocí něj „odečíst“ prvky, které se opakují na levé a pravé straně rovnosti (tj. prvky $y_1' \cdot x_2$, $x_1' \cdot y_2$, $x_1' \cdot x_2$ a $y_1' \cdot y_2$). Takto dostaneme rovnost:

$$x_1 \cdot x_2 + y_1 \cdot y_2 + x_1' \cdot y_2' + y_1' \cdot x_2' = y_1 \cdot x_2 + x_1 \cdot y_2 + x_1' \cdot x_2' + y_1' \cdot y_2'.$$

Podle definice rovnosti prvku v $\mathbb{Z}$ nyní dostáváme:

$$(x_1 \cdot x_2 + y_1 \cdot y_2) - (y_1 \cdot x_2 + x_1 \cdot y_2) = (x_1' \cdot x_2' + y_1' \cdot y_2') - (x_1' \cdot y_2' + y_1' \cdot x_2').$$

Užitím definice součinu můžeme poslední rovnost přepsat do tvaru:

$$(x_1 - y_1) \cdot (x_2 - y_2) = (x_1' - y_1') \cdot (x_2' - y_2'),$$

což jsme měli dokázat.

Máme tedy dokázáno, že operace součinu je definována korektně. V další části věty dokážeme, že $(\mathbb{Z}, \cdot)$ je komutativní pologrupa. Komutativitu dokážeme následujícím výpočtem

$$\begin{aligned} (x_1 - y_1) \cdot (x_2 - y_2) &= (x_1 \cdot x_2 + y_1 \cdot y_2) - (x_1 \cdot y_2 + x_2 \cdot y_1) = \\ &= (x_2 \cdot y_1 + y_2 \cdot y_1) - (x_2 \cdot y_1 - x_1 \cdot y_2) = \\ &= (x_2 - y_2) \cdot (x_1 - y_1). \end{aligned}$$

Asociativitu ověříme podobným, pouze technicky mírně náročnějším výpočtem:

$$\begin{aligned}
& [(x_1 - y_1) \cdot (x_2 - y_2)] \cdot (x_2 - y_3) = \\
= \; & [(x_1 \cdot x_2 + y_1 \cdot y_2) - (x_1 \cdot y_2 + x_2 \cdot y_1)] \cdot (x_3 - y_3) = \\
= \; & (x_1 \cdot x_2 \cdot x_3 + y_1 \cdot y_2 \cdot x_3 + x_1 \cdot y_2 \cdot y_3 + x_2 \cdot y_1 \cdot y_3) - \\
& (x_1 \cdot y_2 \cdot x_3 + x_2 \cdot y_1 \cdot x_3 + x_1 \cdot x_2 \cdot y_3 + y_1 \cdot y_2 \cdot y_3) = \\
= \; & (x_1 - y_1) \cdot [(x_2 \cdot x_3 + y_2 \cdot y_3) - (x_2 \cdot y_3 + x_3 \cdot y_2)] = \\
= \; & (x_1 - y_1) \cdot [(x_2 - y_2) \cdot (x_2 - y_3)].
\end{aligned}$$

Dokázali jsme, že struktura $(\mathbb{Z}, \cdot)$ je komutativní pologrupa. Vidíme, že také platí $(x - y) \cdot (2 - 1) = (2x + y) - (2y - x)$. Jenomže také $(2x + y) - (2y - x) = x - y$ (protože $2x + y + y = 2y + x + x$), proto je $2 - 1$ jednotkový prvek. Zbývá dokázat, že zobrazení $f : \mathbb{Z} \longrightarrow \mathbb{N}$ zachovává násobení. Proto počítejme:

$$f(x) \cdot f(y) = (2 \cdot x - x) \cdot (2 \cdot y - y) = (5 \cdot x \cdot y - 4 \cdot x \cdot y) = (2 \cdot x \cdot y - x \cdot y) = f(x \cdot y).$$

□

Dokázanou větu můžeme ještě následovně rozšířit.

Věta 23 *Struktura $(\mathbb{Z}, +, \cdot)$ je komutativní okruh, přičemž zobrazení $f : \mathbb{N} \longrightarrow \mathbb{Z}$ je vnořením.*

Důkaz: Máme dokázáno, že $(\mathbb{Z}, +)$ je grupa, a stejně tak, že $(\mathbb{Z}, \cdot)$ je komutativní pologrupa. Zobrazení f je navíc homomorfismus, který zachovává součet i součin, a tedy f je vnořením. K tomu, abychom dokázali větu, zbývá ověřit, že $(\mathbb{Z}, +, \cdot)$ je okruh. Stačí dokázat distributivitu (vzhledem ke komutativitě operace $\cdot$ stačí ověřit jenom jednu distributivitu). Proto počítejme:

$$\begin{aligned}
& [(x_1 - y_1) \cdot [(x_2 - y_2) + (x_2 - y_3)] = \\
= \; & (x_1 - y_1) \cdot [(x_2 + x_3) - (y_2 + y_3)] = \\
= \; & (x_1 \cdot (x_2 + x_3) + y_1 \cdot (y_2 + y_3)) - (x_1 \cdot (y_2 + y_3) + y_1 \cdot (x_2 + x_3)) = \\
= \; & (x_1 \cdot x_2 + x_1 \cdot x_3 + y_1 \cdot y_2 + y_1 \cdot y_3)) - (x_1 \cdot y_2 + x_1 \cdot y_3 + y_1 \cdot x_2 + y_1 \cdot x_3) = \\
= \; & ((x_1 \cdot x_2 + y_1 \cdot y_2) - (x_1 \cdot y_2 + x_2 \cdot y_1)) + ((x_1 \cdot x_3 + y_1 \cdot y_3) - (x_1 \cdot y_3 + x_3 \cdot y_1)) = \\
= \; & (x_1 - y_1) \cdot (x_2 - y_2) + (x_1 - y_1) \cdot (x_3 - y_3).
\end{aligned}$$

□

Protože máme ukázáno, že struktura $(\mathbb{N}, +, \cdot)$ je vnořitelná do $(\mathbb{Z}, +, \cdot)$, nemá smysl rozlišovat mezi celými čísly $\mathbb{N}$ a množinou obrazů $f(\mathbb{N})$ v tomto vnoření. Domluvme se, že nyní budeme tyto dvě množiny ztotožňovat. Celým číslem budeme rozumět i obraz $f(x) = 2x - x$ prvku $x \in \mathbb{N}$. Tímto ztotožněním dosáhneme toho, že množina přirozených čísel je podmnožinou množiny celých čísel ($\mathbb{N} \subseteq \mathbb{Z}$), přestože z formálního hlediska by tato inkluze platit nemohla.

3.1 Uspořádání celých čísel

Cílem kapitoly je využít poznatku o uspořádaných okruzích, které jsme v předešlých částech získali, ke studiu okruhu celých čísel.

Věta 24 *Okruh celých čísel má jedinou kladnou část a tou je množina* $\mathbb{N}$.

Důkaz: Nejprve dokážeme, že $\mathbb{N}$ je kladnou částí. Množina přirozených čísel je uzavřena na sčítání i násobení, zbývá proto ověřit trichotomii. Mějme celé číslo $x - y \in \mathbb{Z}$. Potom $x, y \in \mathbb{N}$ a z trichotomie ostrého uspořádáni plyne, že může nastat právě jedná z variant $x < y$, $y < x$ nebo $x = y$. Studujme jednotlivé případy.

Jestliže $x > y$, potom existuje $m \in \mathbb{N}$ takové, že $y + m = x$. Proto platí, že $x - y = (y + m) - y$. Všimněme si, že nyní nastává rovnost $(y + m) - y = 2m - m$ (protože $y + m + m = 2m + y$). Jak ale víme, prvky ve tvaru $2m - m$ jsou přirozená čísla, proto $x - y \in \mathbb{N}$.

Jestliže $x < y$, potom k číslu $x-y$ je opačným číslem $y-x$ a z argumentů v předchozím odstavci plyne, že $y - x \in \mathbb{N}$.

Jestliže $x = y$, potom $x - y = x - x$, což je nula (nulový prvek).

Dohromady máme dokázáno, že nastane vždy alespoň jeden z případů $x - y \in \mathbb{N}$, $y - x \in \mathbb{N}$ nebo $x - x = 0$, kde 0 symbolizuje nulový prvek v $(\mathbb{Z}, +)$. K dokončení důkazu trichotomie potřebujeme ukázat, že nemohou nastat žádné dvě z možností současně. Postupovat budeme tak, že ukážeme obrácené implikace k předchozímu tvrzení.

Jestliže $x - y \in \mathbb{N}$, potom existuje $n \in \mathbb{N}$ takové, že $x - y = 2n - n$. Tedy platí rovnost $x + n = y + 2n = y + n + n$. Z pravidla krácení pro sčítání na celých číslech dostáváme $y + n = x$, a tedy $x > y$.

Analogicky, jestliže $y - x \in \mathbb{N}$, potom $x < y$.

Pokud $x - y = 0$, potom musí platit, že $x = y$, protože nulové prvky jsou právě dvojice ve tvaru $x - x$.

Dokázali jsme, že $x > y$ je ekvivalentní s $x - y \in \mathbb{N}$, $x < y$ je ekvivalentní s $y - x \in \mathbb{N}$ a také $x - y = 0$ je ekvivalentní s $x = y$. Toto spolu s trichotomií ostrého uspořádání na $\mathbb{N}$ dává také trichotomii množiny $\mathbb{N}$ v $\mathbb{Z}$. Proto je $\mathbb{N}$ kladnou částí v $\mathbb{Z}$.

V druhé části věty ukážeme, že jiná kladná část v $\mathbb{Z}$ neexistuje. Předpokládejme, že K je kladná část v $\mathbb{Z}$. Zkoumejme množinu $K \cap \mathbb{N}$ (zřejmě $K \cap \mathbb{N}$ je podmnožinou množiny $\mathbb{N}$). Potom podle Vety 9 i) platí $1 \in K$ (resp. $2 - 1 \in K$), a tedy $1 \in K \cap \mathbb{N}$. Navíc pokud $n \in K \cap \mathbb{N}$, z uzavřenosti kladné části na součty platí, že $n + 1 \in K \cap \mathbb{N}$. Podle principu matematické indukce (pátého Peanova axiomu) musí platit $K \cap \mathbb{N} = \mathbb{N}$, proto $\mathbb{N} \subseteq K$.

Nyní stačí užít Lemma 4 (jelikož $\mathbb{N}$ a K jsou kladné části splňující $\mathbb{N} \subseteq K$, potom $\mathbb{N} = K$). □

Předcházející věta má zajímavý důsledek. Jelikož $\mathbb{N}$ je (jedinou) kladnou části v $\mathbb{Z}$, z trichotomie kladné části vidíme, že každý prvek $n \in \mathbb{Z}$ je buďto přímo přirozeným číslem, nebo $-n$ je přirozené číslo nebo $n = 0$. Celá čísla $\mathbb{Z}$ proto obsahují pouze přirozená čísla $\mathbb{N}$, opačné prvky k přirozeným číslům (prvky ve tvaru $-n$, kde $n \in \mathbb{N}$) a nulu. Nyní můžeme

zavést standardní značení celých čísel (přesněji $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$) s vědomím, že takové značení je v souladu s předchozí teorií.

V kapitole věnované uspořádaným okruhům jsme dokázali, že uspořádaný okruh neobsahuje netriviální dělitele nuly (viz Věta 9 iii)). Uvědomíme-li si navíc, že okruh celých čísel je komutativní a obsahuje jednotku, dostáváme následující větu:

Věta 25 *Struktura $(\mathbb{Z}, +, \cdot)$ je obor integrity.*

3.2 Vnoření celých čísel do uspořádaných okruhů

Cílem této kapitoly je ukázat, že obor integrity celých čísel je v jistém smyslu nejmenším uspořádaným okruhem. Dokažme nejprve pomocnou větu.

Věta 26 *Jestliže $(O, +, \cdot)$ je uspořádaný okruh s jednotkovým prvkem $e \in O$, potom existuje jediné vnoření oboru integrity $(\mathbb{Z}, +, \cdot)$ do okruhu $(O, +, \cdot)$.*

Důkaz: Dokážeme, že zobrazení $f : \mathbb{N} \longrightarrow O$ takové, že $f(n) = n \times e$ (pro libovolné $n \in \mathbb{N}$) je vnoření. Platí, že $f(m + n) = (m + n) \times e = m \times e + n \times e = f(m) + f(n)$. Analogicky $f(m \cdot n) = (m \cdot n) \times e = (m \cdot n) \times (e \cdot e) = (m \times e) \cdot (n \times e) = f(m) \cdot f(n)$. Protože f je vnoření kladné části $\mathbb{N}$ do kladné části okruhu O, podle Věty 11 je toto vnoření rozšiřitelné na vnoření $g : \mathbb{Z} \longrightarrow O$. □

Máme dokázáno, že obor integrity celých čísel je v jistém smyslu „nejmenší“ ze všech uspořádaných okruhů. Máme-li nějaký uspořádaný okruh, jistě obsahuje podokruh, který je až na značení prvků totožný s celými čísly. Dokážeme si, že celá čísla lze navíc charakterizovat jako právě uspořádané okruhy s dobře uspořádanou kladnou částí.

Nejprve si uvědomme, že obor integrity $\mathbb{Z}$ má dobře uspořádanou kladnou část (což je množina $\mathbb{N}$), a tedy okruhy s dobře uspořádanou kladnou částí existují. Navíc můžeme vyslovit větu:

Věta 27 *Každý uspořádaný okruh s dobře uspořádanou kladnou částí je izomorfní s oborem integrity celých čísel.*

Důkaz: Mějme okruh $(O, +, \cdot)$ s dobře uspořádanou kladnou částí P. Označme si $e \in O$ jednotkový prvek v tomto okruhu a $o \in O$ nulový prvek. Nejprve dokážeme, že e je nejmenší prvek kladné části. Pokud je kladná část dobře uspořádaná, musí mít nejmenší prvek, označme jej $x \in P$. Předpokládejme sporem, že $x < e$. Proto platí, že $o < x < e$. Víme, že uspořádaní je monotónní vzhledem k násobení kladným prvkem, a proto $o = o \cdot x < x^2 < e \cdot x = x$. Z tohoto plyne, že $x^2 \in P$, a navíc $x^2 < x$, což je ve sporu s tím, že x je nejmenší prvek kladné části. Proto nejmenší prvek kladné části nemůže být menší než jednotkový prvek.

Nyní vezměme v potaz vnoření f přirozených čísel do kladné části P, potom $f(\mathbb{N}) = \{n \times e \,|\, n \in \mathbb{N}\} \subseteq P$. Pokud vnoření nemá být izomorfismem, nesmí být surjektivní, a proto platí $P \setminus f(\mathbb{N}) \neq \emptyset$. Protože kladná část je dobře uspořádána, existuje nejmenší

prvek množiny $P \setminus f(\mathbb{N})$ a ten si označme x. Zřejmě $e = f(1) \in f(\mathbb{N})$, a proto $e < x$ (víme, že e je nejmenší prvek kladné části a rovnost můžeme vyloučit, protože $x \notin f(\mathbb{N})$). Z monotónnosti kladné části vzhledem ke sčítání platí $o < x - e < x$. Z tohoto ihned plyne, že $x - e \in P$, a navíc $x - e \notin P \setminus f(\mathbb{N})$ (protože $x - e < x$ a x je nejmenším prvkem této množiny). Z těchto skutečností dostáváme, že $x - e \in f(\mathbb{N})$, a protože také $e \in f(\mathbb{N})$ musí platit, že $x = (x - e) + e \in f(\mathbb{N})$. Toto je spor s tím, že $x \in P \setminus f(\mathbb{N})$. □

Poslední věta nabízí alternativní definici celých čísel jakožto uspořádaného okruhu s dobře uspořádanou kladnou části.

Kapitola 4

Konstrukce tělesa racionálních čísel

Samotná konstrukce tělesa racionálních čísel je téměř celá popsána v předcházejících částech textu. Známe obor integrity $(\mathbb{Z}, +, \cdot)$, a víme jak z oboru integrity vytvořit podílové těleso $\mathbb{Q}(\mathbb{Z})$ (postup je popsán ve Větě 5). V tomto okamžiku můžeme definovat racionální čísla jakožto podílové těleso okruhu $\mathbb{Z}$. Množinu racionálních čísel značíme obvyklým $\mathbb{Q}$ místo složitějšího $\mathbb{Q}(\mathbb{Z})$. Dále z teorie uspořádaných okruhů plyne, že množina racionálních čísel má jedinou kladnou část a tou je množina $\{\frac{x}{y} \mid x \cdot y \in \mathbb{N}\}$ (plyne z Věty 12 a z toho, že $\mathbb{N}$ je jedinou kladnou částí v okruhu $\mathbb{Z}$). Tuto kladnou část obvykle značíme $\mathbb{Q}^+$.

Z tohoto pohledu můžeme považovat konstrukci tělesa racionálních čísel za hotovou. Dokážeme si analogicky jako v předcházející kapitole, že těleso racionálních čísel je nejmenší uspořádané těleso.

Věta 28 *Těleso racionálních čísel* $(\mathbb{Q}, +, \cdot)$ *je vnořitelné do každého uspořádaného tělesa.*

Důkaz: Nechť $(T, +, \cdot)$ je uspořádané těleso. Podle Věty 26 existuje vnoření oboru integrity $(\mathbb{Z}, +, \cdot)$ do tělesa T. Ovšem Věta 6 rovnou ukazuje, že v tomto případě existuje také vnoření tělesa $\mathbb{Q}(\mathbb{Z})$ do tělesa T. Protože $\mathbb{Q}(\mathbb{Z})$ jsou právě racionální čísla $\mathbb{Q}$, je důkaz hotov. □

Konstrukce i základní charakterizace racionálních čísel je tímto v podstatě hotova. Významnou roli v naší teorii nyní budou hrát nové vlastnosti, které má uspořádaná množina racionálních čísel oproti uspořádané množině celých čísel. Už z naší středoškolské intuitivní představy můžeme vydedukovat podstatný rozdíl. Jestliže vezmeme uspořádanou množinu $(\mathbb{Z}, \leq)$, potom pro libovolné $n \in \mathbb{Z}$ platí, že $n-1 < n < n+1$, přičemž neexistuje $m \in \mathbb{Z}$ takové, že by platilo $n - 1 < m < n$ (resp. $n < m < n + 1$). V tomto případě říkáme, že číslo n kryje číslo $n-1$ a že číslo n je pokrýváno číslem $n+1$ (Obvykle tuto skutečnost značíme $n - 1 \prec n \prec n + 1$).

Oproti tomu v množině racionálních čísel platí, že pokud $x, y \in \mathbb{Q}$ jsou taková čísla, že $x < y$, potom vždy existuje $z \in \mathbb{Q}$ takové, že $x < z < y$ (například aritmetický průměr čísel x a y). To znamená, že neexistují taková racionální čísla $x, y \in \mathbb{Q}$, že $x \prec y$.

Uspořádaní typu $(\mathbb{Z}, \leq)$ (tedy uspořádaní, kdy každý prvek kryje některý prvek a je pokrýván některým prvkem) nazýváme diskrétní. Naopak uspořádání $(\mathbb{Q}, \leq)$ nazýváme husté (prvky se nekryjí).

Vhodným pozorováním dokážeme o uspořádání racionálních čísel říci ještě více. Nejprve je ovšem potřeba si osvětlit pojem *archimedovskost*. Vlastnost, kterou tradičně v al-

gebře pojmenováváme po tomto významném antickém mysliteli, má skutečně historické kořeny v úvahách Archiméda, ovšem v oblasti geometrie.

Přestože současná klasická geometrie plně koresponduje s geometrií, kterou vynalezli a silně rozvinuli antičtí učenci, existuje jeden podstatný rozdíl v našem a antickém vnímání prostoru. Velmi abstraktní pojem nekonečna přináší mnoho úskalí při logické argumentaci a především při filosofické obhajobě. Bez nekonečna ale nemůžeme rozumným způsobem zavést přímky. Protože přímka je nereálný a při skutečném pozorování světa nerealizovatelný pojmem, Řekové s ním nepracovali (zřejmě jej ani „nevynalezli“). Rovná čára byla místo toho modelována úsečkami (spojnicemi dvou bodů). V tomto případě je třeba se vyrovnat s omezenou délkou úsečky (například různoběžné úsečky nemusí mít průsečík apod.). Řešení se našlo v podobě Archimédova axiomu, který říkal, že jestliže máme dvě libovolné úsečky, potom existuje $n \in \mathbb{N}$ takové, že n-násobným prodloužením kratší ze dvou úseček dostaneme úsečku delší, než je druhá. Jinak řečeno, opakovaným skládáním libovolné úsečky za sebe můžeme překonat libovolnou vzdálenost.

Tento axiom je do dnešní doby v hojné míře používán v mnoha teoriích. Svou zásadní roli hraje také v uspořádaných tělesech. Máme-li libovolné uspořádané těleso $(\mathbb{T}, T^+)$, potom podle Věty 28 lze uspořádané těleso $(\mathbb{Q}, \mathbb{Q}^+)$ jediným způsobem vnořit do $(\mathbb{T}, T^+)$. Proto můžeme bez újmy na obecnosti předpokládat, že $\mathbb{Q} \subseteq \mathbb{T}$, přičemž $\mathbb{Q}^+ \subseteq T^+$. Nyní již dává smysl analogická úvaha k archimedovskosti.

Vezměme si interval $\langle 0, 1\rangle$ v tělese $\mathbb{T}$. Řekneme, že toto těleso je archimedovské, jestliže konečným skládáním tohoto intervalu za sebe můžeme překonat libovolnou (kladnou) hodnotu tělesa T. Jednodušeji řečeno, těleso $\mathbb{T}$ je archimedovské, jestliže pro libovolné $x \in \mathbb{T}$ existuje $n \in \mathbb{N}$ takové, že $x < n$. Příkladem archimedovských těles jsou samozřejmě racionální čísla, a jak si v další kapitole dokážeme, také čísla reálná.

Pro čtenáře bude v tomto okamžiku jednodušší, bude-li si představovat v následujících důkazech pod pojmem archimedovské těleso $\mathbb{T}$ konkrétní těleso reálných čísel (tak jak je s tímto tělesem intuitivně seznámen). Těleso $\mathbb{R}$ je archimedovské a přímo obsahuje racionální čísla.

Věta 29 *Jestliže $\mathbb{T}$ je archimedovské těleso, potom pro libovolné prvky $x, y \in \mathbb{T}$ takové, že $x < y$, existuje $z \in \mathbb{Q}$ splňující $x < z < y$.*

Důkaz: Nejprve označme T^+ kladnou část uspořádaného tělesa $\mathbb{T}$. Mějme $x, y \in \mathbb{T}$ takové, že $x < y$. V prvé řadě potřebujeme najít racionální číslo, které je menší než $y - x$. Protože těleso $\mathbb{T}$ je archimedovské, existuje $n \in \mathbb{N}$ takové, že $\frac{1}{y-x} < n$. Protože $y - x, n \in T^+$, plyne z této nerovnosti, že $\frac{1}{n} < y - x$.

Opět z archimedovskosti tělesa $\mathbb{T}$ plyne existence čísel $s, t \in \mathbb{N}$ takových, že $n \cdot x < s$ a $-n \cdot x < t$. Dohromady proto dostáváme, že $-t < n \cdot x < s$, a protože $n \in \mathbb{T}^+$, platí také $\frac{-t}{n} < x < \frac{s}{n}$ (přičemž $\frac{-t}{n}, \frac{s}{n} \in \mathbb{Q}$).

Protože množina $\left\{\frac{-t}{n}, \frac{-t+1}{n}, \cdots, \frac{s}{n}\right\}$ je konečná, musí v ní existovat číslo $\frac{p}{n}$ takové, že $\frac{p}{n} \leq x$ a současně $x < \frac{p+1}{n}$. Snadno už z předchozích nerovností vidíme, že

$$\frac{p+1}{n} = \frac{p}{n} + \frac{1}{n} < x + (y - x) = y.$$

Proto $\frac{p+1}{n} \in \mathbb{Q}$ je hledané číslo. □

Věta 29 se častěji formuluje ve tvaru: Těleso racionálních čísel $\mathbb{Q}$ je husté[1] v každém uspořádaném archimedovském tělese. Poslední věta bude hrát důležitou roli při konstruování reálných čísel.

[1]Přesná definice pojmu „být hustý v“ kopíruje Větu 29. Pro uspořádaná tělesa $\mathbf{T_1} \subseteq \mathbf{T_2}$ platí, že $\mathbf{T_1}$ je husté v $\mathbf{T_2}$, jestliže pro libovolné $x, y \in \mathbf{T_2}$ takové, že platí $x < y$, existuje $z \in \mathbf{T_1}$, takové, že $x < z < y$.

Kapitola 5

Konstrukce reálných čísel metodou Dedekindových řezů

V okamžiku, kdy známe těleso racionálních čísel a ovládáme aritmetiku zlomků, není na první pohled zřejmé, proč a jak rozšiřovat toto těleso dále. Někdy se nepřesně jako důvod k rozšiřování uvádí skutečnost, že mnoho známých a podstatných hodnot nelze psát ve tvaru zlomku (brzy si připomeneme důkaz této skutečnosti pro $\sqrt{2}$, ale iracionální jsou také konstanty π nebo Eulerovo číslo e). Byla-li by tato skutečnost opravdu hlavním motivem k dalším konstrukcím, pravděpodobně bychom mohli pokračovat přidáváním některých prvků. Tento postup se ale ukáže být při delším uvažování jako nedostatečný.

Pokud vytvoříme například těleso takové, že k racionálním číslům přidáme všemožné odmocniny a obvyklou konstrukcí z takovéto množiny vytvoříme těleso, potom ve vzniklém tělese budou všechna čísla algebraická (tzn. každé číslo tohoto tělesa bude kořenem některého polynomu nad $\mathbb{Z}$). Jak již dnes víme, například čísla π a e jsou transcendentní (nejsou algebraická), proto by v nově vniklém tělese opět nebyla.

Dá se říci, že hlavní motivací k rozšiřování číselných struktur dosud bylo zajištění korektního fungování některé operace (nejprve odečítání a poté dělení nenulovým číslem). Pro případ reálných čísel tuto motivaci opustíme.

Hlavním tahounem v rozvoji reálných čísel se nakonec ukázala být matematická analýza. K rozvoji mnohých teorií matematické analýzy je nezbytná platnost některých vět (například věty o supremu a infimu: každá neprázdná, shora omezená množina má supremum a duálně). Je důležité, aby naše číselná osa byla spojitá (kontinuální), neměla mezery, jinak by nastaly mnohé problémy například s limitami (posloupnost prvků by mohla konvergovat právě směrem do mezery). Jak si nakonec ukážeme, tyto defekty těleso racionálních čísel má a naše nově zkonstruované těleso již mít nebude.

Je proto možné si představovat, že reálná čísla „zaplňují“ mezery v číselné ose, které nepokrývají racionální čísla. Konečně se můžeme dostat k následující větě, která dokazuje, že tyto mezery v číselné ose skutečně existují.

Věta 30 *V tělese $\mathbb{Q}$ neexistuje číslo $x \in \mathbb{Q}$ takové, že $x^2 = 2$.*

Důkaz: Předpokládejme sporem, že existuje racionální číslo $\frac{p}{q} \in \mathbb{Q}$ takové, že $(\frac{p}{q})^2 = 2$. Můžeme předpokládat, že zlomek je v základním tvaru[1]. Platí proto, že $p^2 = 2 \cdot q^2$, Z tohoto

[1]Protože existence a definice základního tvaru zlomku je závislá na výsledcích teorie dělitelnosti v $\mathbb{Z}$,

vidíme, že p^2 je sudé číslo, a proto také p je sudé číslo (druhá mocnina lichého čísla je vždy číslo liché). Proto můžeme zapsat $p = 2n$ pro některé $n \in \mathbb{N}$.

Dosadíme-li do předchozí rovnosti, dostaneme $4 \cdot n^2 = 2 \cdot q^2$, a tedy také $2 \cdot n^2 = q^2$. Analogicky jako v minulém případě vidíme, že číslo q musí být sudé. To je ale ve sporu s tím, že $\frac{p}{q}$ je v základním tvaru. □

5.1 Řezy na lineárně uspořádaných množinách

Hlavním aparátem v konstrukci reálných čísel budou takzvané řezy na lineárních množinách. Podívejme se v této části na zavedení řezů obecně. Mějme libovolnou lineárně uspořádanou množinu $(L, \leq)$ (pro naše potřeby si můžeme představit kteroukoliv dosud zkoumanou číselnou množinu). Potom *řezem* na lineárně uspořádané množině L rozumíme jakékoliv rozdělení (rozseknutí) množiny L na dvě části (horní a dolní část). Definujme formálně. Dvojici množin $H \subseteq L$ (představující horní část řezu) a $D \subseteq L$ (představující dolní část řezu) nazveme řezem, platí-li:

(1) Obě množiny H i D jsou neprázdné.

(2) Platí, že $H \cap D = \emptyset$ a současně $H \cup D = L$.

(3) Jestliže $x \in H$, a navíc $y \in L$ je takový prvek, že $x \leq y$, potom také $y \in H$. Analogicky, jestliže $x \in D$ a $y \in L$ je takový prvek, že $y \leq x$, potom také $y \in D$.

V teorii řezů hraje podstatnou roli, zda-li dolní část řezu D má největší prvek nebo zdali horní část řezu H má prvek nejmenší. Obecně může nastat kterýkoliv z následujících případů.

Řez 1. druhu: Jestliže dolní část řezu D má největší prvek a horní část H má nejmenší prvek, potom řez nazýváme řezem 1. druhu. Příkladem může být řez $D = \{1, 2, 3\}$, $H = \{4, 5, 6, \cdots\}$ na uspořádané množině $(\mathbb{N}, \leq)$.

Je vhodné si uvědomit, že na uspořádané množině $(\mathbb{Q}, \leq)$ tento druh řezu neexistuje, protože jestliže $d \in D$ je největší prvek dolní části a $h \in H$ je nejmenší prvek horní části, potom existuje $x \in \mathbb{Q}$ takové, že $d < x < h$. Navíc $x \notin D$ (jinak by prvek d nebyl největší v D) a současně $x \notin H$ (protože prvek h by nebyl nejmenší v H). Dohromady $x \notin D \cup H$, což je ve sporu s podmínkou (2).

Řez 2. druhu Jestliže dolní část D má největší prvek a horní část H nemá nejmenší prvek, potom řez nazýváme řezem 2. druhu. Příkladem může být řez na uspořádané množině $(\mathbb{Q}, \leq)$ definovaný tak, že $D = \{x \in \mathbb{Q} \,|\, x \leq 2\}$, $H = \{x \in \mathbb{Q} \,|\, x > 2\}$.

Řez 3. druhu Jestliže dolní část D nemá největší prvek a horní část H má nejmenší prvek, potom řez nazýváme řezem 3. druhu. Příkladem může být řez na uspořádané množině $(\mathbb{Q}, \leq)$ definovaný tak, že $D = \{x \in \mathbb{Q} \,|\, x < 2\}$, $H = \{x \in \mathbb{Q} \,|\, x \geq 2\}$.

---

která není předmětem těchto skript, můžeme použít „antickou fintu“. Nemusíme předpokládat, že zlomek je v základním tvar, ale ve tvaru, kde jmenovatel q je minimální přirozené číslo. Protože $\mathbb{N}$ je dobře uspořádaná množina, je jistě tento předpoklad korektní.

Řez 4. druhu Jestliže dolní část D nemá největší prvek a horní část H nemá nejmenší prvek, potom řez nazýváme řezem 4. druhu. Jak si brzy ukážeme, právě tento druh řezů je v této kapitole stěžejním. Zatímco si uvedeme příklad řezu 4. druhu na racionálních číslech, na reálných číslech tento řez neexistuje (tento fakt, který je obsahem Dedekindovy věty, je ve skutečnosti hlavním výsledkem celé kapitoly).

Vezměme nyní uspořádanou množinu racionálních čísel $(\mathbb{Q}, \leq)$ a uvažujme množiny $D = \{x \in \mathbb{Q} \,|\, x < \sqrt{2}\}$, $H = \{x \in \mathbb{Q} \,|\, x > \sqrt{2}\}$.[2] Dokázali jsme, že $\sqrt{2} \notin \mathbb{Q}$, proto dvojice D, H tvoří řez na $(\mathbb{Q}, \leq)$. Přičemž ani dolní část nemá největší prvek a ani horní část nemá prvek nejmenší. Jedná se tedy o řez 4. druhu.

Řezy 4. druhu se někdy nazývají *mezery*.

5.2 Dedekindovy řezy jakožto model reálných čísel

Dosavadní představa řezů je již dostačující pro definici Dedekindových řezů na racionálních číslech. V následující části budeme pracovat s řezy na uspořádané množině racionálních čísel $(\mathbb{Q}, \leq)$. Uvědomme si, že je nadbytečné pracovat s dvojicemi množin, protože dolní část je množinovým doplňkem horní části. Proto v první řadě zjednodušíme naši definici tak, že budeme pracovat pouze s horní části řezu.

Každý řez nám bude představovat právě jedno reálné číslo. Hodnotu řezu si na číselné ose můžeme představit jako místo, kde je „rozdělena“ horní část řezu od dolní části. V případě řezu 2. a 3. druhu je oním předělem právě největší prvek dolní části (resp. nejmenší prvek horní části). V případě řezu 4. druhu je předěl v „mezeře“ a řez nám bude představovat iracionální číslo.

Před finální definicí Dedekindova řezu musíme ještě vyřešit situaci, kdy jedno číslo může být vyjádřeno dvěma způsoby (řezem 2. druhu a řezem 3. druhu). Jednoduše vyloučíme řezy 3. druhu z našich úvah, čímž problém odpadne. Dohromady dostaneme následující definici.

Definice 12 *Množinu $M \subset \mathbb{Q}$ nazveme Dedekindovým řezem, platí-li:*

(1) $M \neq \emptyset$, $M \neq \mathbb{Q}$,

(2) jestliže $x \in M$, a navíc $y \in \mathbb{Q}$ je takové, že $x \leq y$, potom také $y \in M$,

(3) množina M nemá nejmenší prvek (přesněji, jestliže $x \in M$, potom existuje $y \in M$ takové, že $y < x$).

Množinu všech Dedekindových řezů značíme $\mathbb{R}$ a nazýváme ji množinou reálných čísel. Jestliže M je Dedekindův řez, potom označme $M' := \mathbb{Q} \setminus M$.

Řezy, jejichž dolní část má největší prvek, budou představovat právě racionální čísla. Následující věta zjednoduší úvahy o racionálních řezech.

[2] Protože číslo $\sqrt{2}$ ještě nemáme definováno, bylo by korektnější definovat $D = \{x \in \mathbb{Q} \,|\, x \leq 0 \text{ nebo } x^2 \leq 2\}$ a $H = \{x \in \mathbb{Q} \,|\, x \geq 0 \text{ a současně } x^2 > 2\}$.

Věta 31 *Jestliže $a \in \mathbb{Q}$, potom množina $a^* = \{x \in \mathbb{Q} \,|\, a < x\}$ je Dedekindův řez (tedy $a^* \in \mathbb{R}$). Navíc platí, že zobrazení $^* : \mathbb{Q} \longrightarrow \mathbb{R}$ je injektivní.*

Důkaz: Nejprve dokážeme, že množina a^* je Dedekindův řez. Jistě platí, že $a \notin a^*$ (protože $a \not< a$), a tedy $a^* \neq \mathbb{Q}$. Stejně tak $a < a + 1$, kde $a + 1 \in \mathbb{Q}$, proto $a + 1 \in a^*$. Proto platí také, že $a^* \neq \emptyset$.

Předpokládejme nyní, že $x \in a^*$ (tedy $a < x$), a současně nechť $y \in \mathbb{Q}$ je číslo splňující $x \leq y$. Potom platí, že $a < x \leq y$, a proto $y \in a^*$.

Dokážeme nyní, že a^* nemá nejmenší prvek. Předpokládejme, že $x \in a^*$. Potom platí $a < x$, a protože podle Věty 29 jsou racionální čísla uspořádaná hustě, existuje $y \in \mathbb{Q}$ takové, že $a < y < x$. Proto také platí $y \in a^*$, a v důsledku x není nejmenší prvek. Protože jsme $x \in a^*$ volili zcela obecně, máme dokázáno, že v a^* neexistuje nejmenší prvek.

Vše dohromady nakonec dokazuje, že a^* je Dedekindův řez, a proto $a^* \in \mathbb{R}$. Nyní ukážeme, že přiřazení *, které racionálnímu číslu přiřazuje Dedekindův řez, je injektivní. Jestliže $a, b \in, \mathbb{Q}$ jsou takové prvky, že $a \neq b$. Bez újmy na obecnosti můžeme předpokládat $a < b$. Z tohoto ovšem rovnou plyne, že $b \in a^*$ a současně $b \notin b^*$ ($b \not< b$). Dohromady, $a^* \neq b^*$ čímž je injektivita dokázána. □

Jak již bylo definováno, množina všech Dedekindových řezů nám vytvoří model reálných čísel, přičemž zobrazení * bude vnořením tělesa racionálních čísel do tělesa čísel reálných. Je proto korektní uvažovat, že právě Dedekindovy řezy ve tvaru a^* jsou racionální čísla. Stejně tak si můžeme snadno ověřit, že se jedná právě o řezy 2. druhu (tedy právě takové řezy, ve kterých má dolní část řezu největší prvek).

V tomto okamžiku máme korektně definovanou množinu reálných čísel. Dalším krokem je zavedení početních operací (aritmetiky) na $\mathbb{R}$.

5.3 Sčítání reálných čísel

Následující věta, kterou postupně dokážeme, ukazuje jakým způsobem sčítáme Dedekindovy řezy (tedy reálná čísla).

Věta 32 *Mějme Dedekindovy řezy $A, B \in \mathbb{R}$. Definujme množinu $A + B$ tak, že*

$$A + B = \{a + b \,|\, a \in A, b \in B\}.$$

Potom platí, že $A+B \in \mathbb{R}$ (tedy operace $+$ je na $\mathbb{R}$ korektně definovaná). Struktura $(\mathbb{R}, +)$ je komutativní grupa, kde neutrálním prvkem je řez 0^* a opačným řezem k řezu $A \in \mathbb{R}$ je řez

$$-A = \{x \in \mathbb{Q} \,|\, \text{existuje } a \in A' \text{ takové, že } -a < x\}.$$

Navíc platí, že zobrazení $^* : \mathbb{Q} \longrightarrow \mathbb{R}$ je izomorfní vnoření $(\mathbb{Q}, +)$ do $(\mathbb{R}, +)$ (tj. $(a+b)^* = a^* + b^*$).

Důkaz: Důkaz celé věty budeme pro větší přehlednost provádět po částech.

Tvrzení. *Jestliže $A, B \in \mathbb{R}$, potom také $A + B \in \mathbb{R}$.*

Protože $A, B \in \mathbb{R}$ a také $A, B \neq \emptyset$, existují prvky $a \in A$ a $b \in B$, a proto $a+b \in A+B$. Dostáváme $A + B \neq \emptyset$. Analogicky existují prvky $x \notin A$ a $y \notin B$. Pro libovolné $a \in A$ a $b \in B$ platí, že $x < a$ a $y < b$. Z monotonnosti sčítání dostáváme, že $x + y < a + b$ pro všechna $a \in A$ a $b \in B$, což dokazuje, že $x + y < z$ pro všechna $z \in A + B$. Proto také $x + y \notin A + B$ a $A + B \neq \mathbb{Q}$.

Předpokládejme, že $x \in A + B$, a navíc $x \leq y$. Z definice množiny $A + B$ plyne, že existují prvky $a \in A$ a $b \in B$ takové, že $a + b = x$. Proto platí, že $a + b < y$, a tedy také $a < y - b$. Protože A je Dedekindův řez, máme nyní dokázáno, že $y - b \in A$. Dohromady vidíme, že $y = (y - b) + b \in A + B$.

Nakonec musíme dokázat, že množina $A+B$ nemá nejmenší prvek. Jestliže $x \in A+B$, potom existují prvky $a \in A$ a $b \in B$ takové, že $x = a + b$. Protože navíc A je Dedekindův řez, a nemá proto nejmenší prvek, existuje prvek $a' \in A$ takový, že $a' < a$. Z monotonnosti relace $<$ plyne, že $a'+b < a+b = x$. Protože $a'+b \in A+B$, nemůže být prvek x nejmenším prvkem množiny $A + B$.

Všechny předchozí argumenty dohromady ukazují, že množina $A+B$ tvoří Dedekindův řez, a tedy $A + B \in \mathbb{R}$. □

Tvrzení. $(\mathbb{R}, +)$ *je komutativní pologrupa s neutrálním prvkem* 0^*.

Důkaz: Mějme libovolné řezy $A, B \in \mathbb{R}$. Zřejmě platí

$$A + B = \{a + b \,|\, a \in A, b \in B\} = \{b + a \,|\, b \in B, a \in A\} = B + A.$$

Analogicky lze dokázat, že pro všechny řezy $A, B, C \in \mathbb{R}$ platí, že

$$A + (B + C) = \{a + b + c \,|\, a \in A, b \in B, c \in C\} = (A + B) + C.$$

Zbývá ověřit, že 0^* je neutrální prvek. Mějme libovolný Dedekindův řez $A \in \mathbb{R}$.

Nechť $x \in A + 0^*$. Potom existují $a \in A$ a $b \in 0^*$ takové, že $x = a + b$. Protože $b \in 0^*$, platí také $0 < b$, a tedy $a < a + b$. Protože A je Dedekindův řez, platí, že $x = a + b \in A$. Dokázali jsme, že $A + 0^* \subseteq A$.

Opačně, nechť $x \in A$. Protože A je Dedekindův řez a nemá tedy nejmenší prvek, existuje $y \in A$ takové, že $y < x$. Platí $0 < x - y$, a tedy také $x - y \in 0^*$. Nyní již snadno vidíme, že $x = y + (x - y) \in A + 0^*$. Proto také $A \subseteq A + 0^*$.

Dohromady platí, že $A + 0^* = A$, a proto 0^* je neutrálním prvkem. □

Následující tvrzení je pouze pomocné, ovšem brzy jej zužitkujeme.

Tvrzení. Mějme libovolné $x \in \mathbb{Q}^+$ a libovolný Dedekindův řez $A \in \mathbb{R}$, potom

existují prvky $a \in A'$ a $b \in A$ takové, že $b - a < x$.

Důkaz: Platí $0 < x$. Z hustoty uspořádaní $\mathbb{Q}$ plyne existence čísla $y \in \mathbb{Q}$ takového, že $0 < y < x$. Protože A je Dedekindův řez, existuje $q \in A'$ a $p \in A$. Z archimedovskosti tělesa racionálních čísel plyne existence čísla $n \in \mathbb{N}$ takového, že $n > \frac{p-q}{y}$. Protože $0 < y$ a relace $<$ je monotonní vzhledem k násobení kladným číslem, můžeme z předchozí nerovnosti vyvodit, že $q + n \cdot y > p$. Platí proto $q + n \cdot y \in A$ a také $q + 0 \cdot y = q \in A'$. Proto existuje $i \in \{0, \cdots, n\}$ takové, že $q + i \cdot y \in A'$, a navíc $q + (i+1) \cdot y \in A$. Označme $a = q + i \cdot y$ a $b = q + (i+1) \cdot y$. Nyní vidíme, že $b - a = (q + (i+1) \cdot y) - (q + i \cdot y) = y < x$.□

Tvrzení. Množina $-A$ je Dedekindův řez

Důkaz: Protože existuje $a \in A'$, a navíc platí $-a < 1 - a$, dostáváme $1 - a \in -A$, a v důsledku také $-A \neq \emptyset$. Předpokládejme sporem, že $-A = \mathbb{Q}$. Potom pro libovolné $x \in \mathbb{Q}$ platí $-x \in -A$. Proto existuje $y \in A'$ takové, že $-y < -x$, a tedy také $x < y$. Protože $y \in A'$ musí také platit $x \in A'$. Tímto jsme dokázali, že $A' = \mathbb{Q}$, a tedy $A = \emptyset$, což je spor. Dohromady $-A \neq \mathbb{Q}$.

Předpokládejme, že $x \in -A$, a nechť $y \in \mathbb{Q}$ je takový prvek, že $x < y$. Jelikož $x \in -A$, existuje $a \in A'$ splňující nerovnost $-a < x$. Potom platí $-a < y$, a proto $y \in -A$.

Zbývá dokázat, že $-A$ nemá nejmenší prvek. Vezměme libovolný prvek $x \in -A$. Podle definice existuje $a \in A'$ takové, že $-a < x$. Protože racionální čísla jsou uspořádaná hustě, musí existovat $y \in \mathbb{Q}$ takové, že $-a < y < x$. Vidíme, že potom $y \in -A$, a tedy prvek x nemůže být nejmenším prvkem množiny $-A$. Protože prvek x byl z množiny $-A$ zvolen libovolně, nemá množina $-A$ nejmenší prvek. □

Tvrzení. Platí, že $-A + A = 0^*$

Důkaz: Nechť $x \in 0^*$. Potom zřejmě $x \in \mathbb{Q}^+$ a podle již dokázaného tvrzení musí existovat $a \in A'$ a $b \in A$ takové, že $b - a < x$. Z tohoto vidíme, že $-a < x - b$, a proto $x - b \in -A$. Dohromady vidíme, že také $x = (x - b) + b \in -A + A$. Proto platí množinová inkluze $0^* \subseteq -A + A$.

Nechť opačně platí $x \in -A + A$. Potom existují $a \in -A$ a $b \in A$ taková, že $x = a + b$. Jelikož navíc $a \in -A$, musí existovat $m \in A'$ takové, že $-m < a$. Ovšem z toho že platí současně $m \in A'$ a $b \in A$, plyne, že $m < b$. Z monotonnosti sčítání ihned obdržíme $0 = m - m < m + a < b + a = x$. Z poslední nerovnosti plyne $x \in 0^*$, a tedy $-A + A \subseteq 0^*$.□

Tvrzení. Pro libovolná čísla $x, y \in \mathbb{Q}$ platí $(x + y)^* = x^* + y^*$.

Důkaz: Předpokládejme, že $a \in (x + y)^*$. Potom platí, že $x + y < a$ a z hustoty uspořádání racionálních čísel plyne existence čísla $a' \in \mathbb{Q}$ takového, že $x + y < a' < a$. Nyní vidíme, že $x < a' - y$, a proto $a' - y \in x^*$. Protože současně platí $0 < a - a'$, získáváme nerovnost $y < y + a - a'$, a tedy také $y + a - a' \in y^*$. Dohromady vidíme, že $a = (a' - y) + (y + a - a') \in x^* + y^*$ a proto $(x + y)^* \subseteq x^* + y^*$.

Nechť opačně $a \in x^* + y^*$. Potom existují prvky $m \in x^*$ a $n \in y^*$ takové, že $a = m+n$. Platí, že $x < m$ a současně $y < n$. Proto také $x + y < m + n = a$, a tedy $a \in (x + y)^*$. Dohromady jsme dostali $x^* + y^* \subseteq (x + y)^*$. □

Tímto máme hlavní větu o sčítání reálných čísel plně dokázanou.

5.4 Násobení kladných reálných čísel

Při definování součinu reálných čísel narážíme na větší komplikace než při sčítání. Nejprve zavedeme kladné řezy a definujeme násobení na těchto kladných řezech.

V souladu s naším intuitivním vnímáním racionálních čísel (tedy Dedekindových řezů) zavedeme následující pojmy: Řez $A \in \mathbb{R}$ nazveme *záporný,* jestliže platí, že $0 \in A$. Řez A je *nulový,* právě když $A = 0^*$. *Kladné* řezy jsou všechny nezáporné a nenulové řezy. Množinu všech kladných řezů značíme $\mathbb{R}^+$. Dokažme si následující tvrzení.

Lemma 6 *Mějme Dedekindův řez $A \in \mathbb{R}$. Potom následující tvrzení jsou ekvivalentní:*

i) A je kladný řez

ii) $A \subset \mathbb{Q}^+$

iii) existuje číslo $x \in \mathbb{Q}^+$ takové, že $x \notin A$.

Důkaz: *i) ⇒ ii)* Nechť A je kladný řez. Jestliže pro některé $a \in \mathbb{Q}^- \cup \{0\}$ platí, že $a \in A$, potom protože $a \leq 0$, platí $0 \in A$, a tedy A je záporný řez (což je spor). Dokázali jsme, že $A \subseteq \mathbb{Q}^+$.

Předpokládejme nyní sporem, že $A = \mathbb{Q}^+$. Protože $\mathbb{Q}^+ = 0^*$, plyne z předchozího, že A je nulový řez (což je spor). Tedy dohromady jsme dokázali, že $A \subset \mathbb{Q}^+$.

ii) ⇒ iii) Plyne triviálně.

iii) ⇒ i) Nechť existuje číslo $x \in \mathbb{Q}^+$ takové, že $x \notin A$, potom $0 \notin A$ (jinak z $0 < x$ plyne $x \in A$, což je spor). Tedy A není záporný řez. Jelikož navíc $A \neq \mathbb{Q}^+ = 0^*$, musí být A kladný řez. □

Definice 13 *Pro kladné řezy $A, B \in \mathbb{R}^+$ zaveďme:*

$$A \cdot B = \{a \cdot b \,|\, a \in A, b \in B\}.$$

Připomeňme, že relace ostrého uspořádání $<$ na racionálních číslech $\mathbb{Q}$ je monotónní vzhledem k násobení **kladným** číslem.

Lemma 7 *Jestliže $A, B \in \mathbb{R}^+$, potom také $A \cdot B \in \mathbb{R}^+$. Tedy operace $\cdot$ je na množině kladných Dedekindových řezů korektně definovaná operace.*

Důkaz: Analogicky jako v předchozích tvrzeních dokážeme, že $A \cdot B$ je Dedekindův řez. Jestliže $A, B \in \mathbb{R}^+$, potom existují prvky $a \in A$ a $b \in B$. Platí proto $a \cdot b \in A \cdot B$ a dohromady $A \cdot B \neq \emptyset$.

Podle předchozího lemmatu také existují $x, y \in \mathbb{Q}^+$ takové, že $x \notin A$ a $y \notin B$. Proto pro všechny prvky $a \in A$ a všechny $b \in B$ platí $x < a$ a $y < b$. Protože čísla x, y, a a b jsou kladná čísla, z monotonnosti násobení kladným číslem plyne, že $x \cdot y < a \cdot b$, a tedy platí $x \cdot y \notin A \cdot B$. Navíc si uvědomme, že $x \cdot y \in \mathbb{Q}^+$. Tedy existuje kladné číslo, které nenáleží $A \cdot B$.

Předpokládejme nyní, že $x \in A \cdot B$, a navíc $x < y$. Z definice množiny $A \cdot B$ plyne existence čísel $a \in A$ a $b \in B$ takových, že $x = a \cdot b$. Platí tedy $a \cdot b = x < y$. Protože platí $a \in \mathbb{Q}^+$, dostáváme také $a^{-1} \in \mathbb{Q}^+$, a v důsledku $b = a^{-1} \cdot a \cdot b < a^{-1} \cdot y$. Jelikož B je Dedekindův řez, musí platit $a^{-1} \cdot y \in B$ a konečně $y = a \cdot a^{-1} \cdot y \in A \cdot B$.

Předpokládejme nyní, že $x \in A \cdot B$. Existují tedy čísla $a \in A$ a $b \in B$ taková, že $x = a \cdot b$. Protože A je Dedekindův řez existuje $a' \in A$ takové, že $a' < a$. Protože $b \in \mathbb{Q}^+$ platí také $a' \cdot b < a \cdot b = x$. Jelikož také $a' \cdot b \in A \cdot B$, nemůže být prvek x nejmenší v množině $A \cdot B$.

Dohromady jsme dokázali, že množina $A \cdot B$ je Dedekindův řez, který neobsahuje některé kladné číslo. Z předchozího lemmatu proto vidíme, že $A \cdot B \in \mathbb{R}^+$. □

Lemma 8 *Struktura $(\mathbb{R}^+, \cdot)$ je pologrupa s neutrálním prvkem 1^* (tedy monoid).*

Důkaz: Mějme libovolné Dedekindovy řezy $A, B \in \mathbb{R}^+$, potom platí, že

$$A \cdot B = \{a \cdot b \,|\, a \in A, b \in B\} = \{b \cdot a \,|\, b \in B, a \in A\} = B \cdot A.$$

Analogicky můžeme dokázat pro libovolné řezy $A, B, C \in \mathbb{R}^+$, že platí:

$$A \cdot (B \cdot C) = \{a \cdot b \cdot c \,|\, a \in A, b \in B, c \in C\} = (A \cdot B) \cdot C.$$

Předpokládejme nyní, že $A \in \mathbb{R}^+$. Jestliže $x \in A \cdot 1^*$, potom existují prvky $a \in A$ a $b \in 1^*$ takové, že $x = a \cdot b$. Protože $b \in 1^*$ implikuje $1 < b$, a protože $a \in \mathbb{Q}^+$, platí, že $a = a \cdot 1 < a \cdot b = x$. Jelikož A je Dedekindův řez a $a \in A$ dostáváme $x \in A$. Proto platí $A \cdot 1^* \subseteq A$.

Obráceně, nechť $x \in A$. Protože A je Dedekindův řez, existuje $y \in A$ takové, že $y < x$. Navíc $y^{-1} \in \mathbb{Q}^+$ implikuje, že $1 = y \cdot y^{-1} < x \cdot y^{-1}$, a tedy také $x \cdot y^{-1} \in 1^*$. Nyní už snadno vidíme, že $x = y \cdot (x \cdot y^{-1}) \in A \cdot 1^*$. Platí proto $A \subseteq A \cdot 1^*$.

Z obou dokázaných množinových inkluzí plyne $A \cdot 1^* = A$. Proto Dedekindův řez 1^* je neutrálním prvkem vzhledem k operaci násobení. □

Definice 14 *Pro libovolný kladný Dedekindův řez $A \in \mathbb{R}^+$ definujme:*

$$A^{-1} = \{x \in \mathbb{Q} \,|\, \textit{existuje } a \in \mathbb{Q}^+ \cap A' \textit{ takové, že } a^{-1} < x\}.$$

Lemma 9 *$A^{-1} \in \mathbb{R}^+$ pro libovolný kladný Dedekindův řez $A \in \mathbb{R}^+$.*

Důkaz: Vezměme libovolný Dedekindův řez $A \in \mathbb{R}^+$. Podle Lemmatu 6 existuje $x \in \mathbb{Q}^+$ takové, že $x \notin A$. Z tohoto ihned plyne, že $x \in \mathbb{Q}^+ \cap A'$, a protože navíc $x^{-1} < x^{-1} + 1$, dostáváme ihned $x^{-1} + 1 \in A^{-1}$. Proto $A^{-1} \neq \emptyset$.

Nejprve si uvědomme, že pokud $x \in \mathbb{Q}^+ \cap A'$, potom platí, že $x^{-1} \in \mathbb{Q}^+$, a tedy čísla větší než x^{-1} jsou opět kladná. Proto platí, že $A^{-1} \subseteq \mathbb{Q}^+$. Předpokládejme sporem, že $A^{-1} = \mathbb{Q}^+$. Potom pro libovolné $x \in \mathbb{Q}^+$, protože také $x^{-1} \in \mathbb{Q}^+ = A^{-1}$, existuje $a \in \mathbb{Q}^+ \cap A'$ takové, že $a^{-1} < x^{-1}$. Protože $a, x \in \mathbb{Q}^+$, můžeme dále počítat $x = 1 \cdot x = a^{-1} \cdot a \cdot x < x^{-1} \cdot a \cdot x = a$. A tedy $x < a$. Jelikož $a \in A'$, musí také platit, že $x \in A'$. Dokázali jsme tedy, že $\mathbb{Q}^+ \subseteq A'$, což je spor s tím, že $A \neq \emptyset$. Proto máme dokázáno, že $A^{-1} \subset \mathbb{Q}^+$.

Předpokládejme, že $x \in A^{-1}$ a $y \in \mathbb{Q}$ je takové, že $x \leq y$. Potom existuje $a \in \mathbb{Q}^+ \cap A'$ takové, že $a^{-1} < x$. V důsledku také platí $a^{-1} < y$, a tedy $y \in A^{-1}$.

Vezměme prvek $x \in A^{-1}$. Potom existuje $a \in \mathbb{Q}^+$ takové, že $a^{-1} < x$. Protože množina racionálních čísel je uspořádána hustě, musí existovat $y \in \mathbb{Q}^+$ takové, že $a^{-1} < y < x$. Podle definice množiny A^{-1} platí $y \in A^{-1}$, a proto x není nejmenší prvek. Jelikož prvek x byl zvolen zcela libovolně, nemá množina A^{-1} nejmenší prvek.

Vše dohromady dokazuje, že $A^{-1} \in \mathbb{R}^+$. □

Jak je vidět, směřování všech důkazů vět o násobení reálných čísel jsou prostými analogiemi důkazů vět o sčítání. I nadále budeme postupovat obdobně, ovšem v tomto okamžiku je potřeba dokázat jakousi analogii archimedovskosti pro násobení, a to tvrzení, že jestliže $q \in \mathbb{Q}$ takové, že $1 < q$, potom pro každé $x \in \mathbb{Q}$ existuje $n \in \mathbb{N}$ splňující $q^n > x$. Dokažme nejprve pomocné lemma.

Lemma 10 *Jestliže $q \in \mathbb{Q}^+$ a $n \in \mathbb{N}$, potom platí nerovnost:*

$$q^n \geq n \cdot q - n + 1.$$

Důkaz: Větu dokážeme matematickou indukcí. Pro $n = 1$ zřejmě platí $q^1 = q = 1 \cdot q + 1 - 1$.

Nechť platí $q^n \geq n \cdot q - n + 1$. Uvědomme si, že $q^2 - 2q + 1 = (q-1)^2 \geq 0$, a proto dostáváme $q^2 \geq 2q - 1$. Nyní z indukčního předpokladu a ze skutečnosti, že $q > 0$ dostáváme $q^{n+1} \geq n \cdot q^2 - n \cdot q + q \geq (2q-1) \cdot n - n \cdot q + q = (n+1) \cdot q - (n+1) - 1$.□

Věta 33 *Jestliže $q \in \mathbb{Q}$ je takové, že $q > 1$, potom pro libovolné $x \in \mathbb{Q}$ existuje $n \in \mathbb{N}$ takové, že $q^n > x$.*

Důkaz: Jelikož $q - 1 > 0$, existuje zlomek $\frac{x-q}{q-1}$, a navíc díky archimedovskosti existuje $n \in \mathbb{N}$ takové, že $n > \frac{x-q}{q-1}$. Protože $q - 1 > 0$, plyne z nerovnosti také $q + n \cdot (q-1) > x$. Navíc z nerovnosti dokázané v předchozím lemmatu dostáváme, že $q + n \cdot (q-1) = (n+1) \cdot q - (n+1) + 1 \leq q^{n+1}$. Dohromady $g^{n+1} > x$. □

Dále můžeme pokračovat ve studiu násobení kladných Dedekindových řezů.

Lemma 11 *Jestliže $A \in \mathbb{R}^+$ a $x \in \mathbb{Q}$ je takové, že $x > 1$. Potom existuje $a \in \mathbb{Q}^+ \cap A'$ a $b \in A$ takové, že $\frac{b}{a} < x$.*

Důkaz: Protože těleso racionálních čísel je uspořádáno hustě, existuje $q \in \mathbb{Q}$ takové, že $1 < q < x$. Protože $A \in \mathbb{R}^+$ musí existovat prvky $o \in \mathbb{Q}^+ \cap A'$ a $p \in A$. Platí $0 < o < p$, a proto $p \cdot o^{-1} \in \mathbb{Q}^+$. Nyní podle předchozího lemmatu musí existovat $n \in \mathbb{N}$ takové, že $q^n > p \cdot o^{-1}$. Protože současně platí $o^{-1} \in \mathbb{Q}^+$, dostáváme nerovnost $o \cdot q^n > p$, a tedy také $o \cdot q^n \in A$. Protože $q > 1$ dává monotonnost násobení kladným číslem následující nerovnost:

$$o \cdot q^0 < o \cdot q^1 < \cdots < o \cdot q^n.$$

Vzhledem k tomu, že $o \cdot q^0 = o \in A' \cap \mathbb{Q}^+$, musí existovat $m \in \{0, 1, \cdots, n\}$ takové, že $o \cdot q^m \in A' \cap \mathbb{Q}+$ a současně $o \cdot q^{m+1} \in A$. Označíme-li nyní $a = o \cdot q^m$ a $b = o \cdot q^{m+1}$, dostáváme přímo

$$\frac{b}{a} = \frac{o \cdot q^{m+1}}{o \cdot q^m} = q < x.$$

□

Lemma 12 *Pro libovolný kladný Dedekindův řez $A \in \mathbb{R}^+$ platí, že $1^* = A \cdot A^{-1}$.*

Důkaz: Jestliže $x \in 1^*$, potom $1 < x$ a podle předchozí věty existují $a \in A' \cap \mathbb{Q}^+$ a $b \in A$ takové, že $b \cdot a^{-1} < x$. Protože $b^{-1} \in \mathbb{Q}^+$ platí také $a^{-1} < x \cdot b^{-1}$, což ukazuje, že $x \cdot b^{-1} \in A^{-1}$. Nyní již je vidět, že $x = b \cdot x \cdot b^{-1} \in A \cdot A^{-1}$. Proto $1^* \subseteq A \cdot A^{-1}$.

Opačně, nechť $x \in A \cdot A^{-1}$. Potom existují $m \in A$ a $n \in A^{-1}$ taková, že $x = m \cdot n$. Z definice množiny A^{-1} plyne existence prvku $a \in A' \cap \mathbb{Q}^+$ takového, že $a^{-1} < n$. Jelikož $a \in A'$, musí také platit $a < m$. Protože všechna racionální čísla a, a^{-1},m a n jsou kladná, dostáváme $1 < a \cdot a^{-1} < m \cdot n = x$. Proto $x \in 1^*$ a současně $A \cdot A^{-1} \subseteq 1^*$.

Dohromady jsme ukázali, že $1^* = A \cdot A^{-1}$, a tedy reálná čísla (Dedekindovy řezy) A, A^{-1} jsou navzájem inverzní vzhledem k násobení. □

Lemma 13 *Jestliže $x, y \in \mathbb{Q}^+$, potom platí, že $(x \cdot y)^* = x^* \cdot y^*$.*

Důkaz: Jestliže $a \in (x \cdot y)^*$, potom z hustoty uspořádání racionálních čísel plyne existence $b \in \mathbb{Q}$ takového, že $x \cdot y < b < a$. Protože $x, y > 0$, platí také, že $x < b \cdot y^{-1}$ a tedy $b \cdot y^{-1} \in x^*$. Také platí, že $1 < b^{-1} \cdot a$, a proto $y < y \cdot b^{-1} \cdot a$. Proto také $y \cdot b^{-1} \cdot a \in y^*$. Nyní už je ale vidět, že $a = (b \cdot y^{-1}) \cdot (y \cdot b^{-1} \cdot a) \in x^* \cdot y^*$, a proto $(x \cdot y)^* \subseteq x^* \cdot y^*$.

Opačně, jestliže $a \in x^* \cdot y^*$, potom existují prvky $m \in x^*$ a $n \in y^*$ takové, že $a = m \cdot n$. Proto $x < m$ a $y < n$. Všechna racionální čísla m, n, x a y jsou kladná a můžeme dedukovat $x \cdot y < m \cdot n = a$. Z tohoto důvodu ihned dostáváme $a \in (x \cdot y)^*$. Dohromady $x^* \cdot y^* \subseteq (x \cdot y)^*$. □

Dosavadní výsledky můžeme shrnout v následující větě:

Věta 34 *Operace součinu $\cdot$, která kladným Dedekindovým řezům $A, B \in \mathbb{R}^+$ přiřadí*

$$A \cdot B = \{a \cdot b \,|\, a \in A, b \in B\},$$

je korektně definovaná operace na $\mathbb{R}^+$. Struktura $(\mathbb{R}^+, \cdot)$ je potom komutativní grupa s jednotkovým prvkem 1^*, kde k řezu $A \in \mathbb{R}^+$ je inverzním řezem

$$A^{-1} = \{x \in \mathbb{Q} \,|\, \text{existuje } a \in A' \cap \mathbb{Q}^+ \text{ takový, že } a^{-1} < x\}.$$

Navíc zobrazení $* : \mathbb{Q}^+ \longrightarrow \mathbb{R}^+$ je izomorfní vnoření $(\mathbb{Q}^+, \cdot)$ do $(\mathbb{R}^+, \cdot)$.

5.5 Těleso reálných čísel a jeho uspořádání

V této části zkompletujeme naše dosavadní výsledky do konstrukce reálných čísel.

Lemma 14 *Množina $\mathbb{R}^+$ je uzavřena na sčítání. Tj. jestliže $A, B \in \mathbb{R}^+$, potom také $A + B \in \mathbb{R}^+$.*

Důkaz: Nechť $A, B \in \mathbb{R}^+$, potom podle Lemmatu 6 existují prvky $x, y \in \mathbb{Q}^+$ takové, že $x \notin A$ a $y \notin B$. Platí proto pro libovolné prvky $a \in A$ a $b \in B$, že $x < a$ a $y < b$. Z tohoto dostáváme $x + y < a + b$. Proto $x + y < z$ pro libovolné $z \in A + B$ a dohromady $x + y \notin A + B$. Jenomže zřejmě $x + y \in \mathbb{Q}^+$. Protože existuje kladné racionální číslo takové, které nenáleží řezu $A + B$, platí podle Lemmatu 6 $A + B \in \mathbb{R}^+$. □

Lemma 15 *Jestliže $A, B, C \in \mathbb{R}^+$, potom platí, že $A \cdot (B + C) = A \cdot B + A \cdot C$.*

Důkaz: Vezměme libovolné řezy $A, B, C \in \mathbb{R}^+$. Nechť $x \in A \cdot (B + C)$, potom existují prvky $a \in A$ a $y \in B + C$ takové, že $x = a \cdot y$. Analogicky, jestliže $y \in B + C$, musí existovat $b \in B$ a $c \in C$ takové, že $y = b + c$. Nyní již vidíme, že $a \cdot b \in A \cdot B$, $a \cdot c \in A \cdot C$ a konečně $a \cdot b + a \cdot c \in A \cdot B + A \cdot C$. Nyní můžeme počítat $a \cdot b + a \cdot c = a \cdot (b + c) = a \cdot y = x$. Dohromady jsme dokázali, že platí $x \in A \cdot B + A \cdot C$. Proto $A \cdot (B + C) \subseteq A \cdot B + A \cdot C$.

Opačně, nechť $x \in A \cdot B + A \cdot C$. Potom existují prvky $m \in A \cdot B$ a $n \in A \cdot C$ takové, že $x = m + n$. Protože $m \in A \cdot B$, existují prvky $a_1 \in A$ a $b \in B$ takové, že platí $m = a_1 \cdot b$. Stejně tak z $n \in A \cdot C$ plyne existence prvků $a_2 \in A$ a $c \in C$ takových, že $n = a_2 \cdot c$. Nyní označme $a = \min\{a_1, a_2\}$. Připomeňme, že všechna racionální čísla a_1, a_2, b a c jsou kladná. Platí také $a \in A$. Proto snadno $a \cdot (b + c) \in A \cdot (B + C)$. Můžeme, ale počítat $a \cdot (b + c) = a \cdot b + a \cdot c \leq a_1 \cdot b + a_2 \cdot c = m + n = x$. Protože $A \cdot (B + C)$ je Dedekindův řez, plyne z dokázané nerovnosti, že $x \in A \cdot (B + C)$. Dohromady jsme dokázali, že $A \cdot B + A \cdot C \subseteq A \cdot (B + C)$. □

Lemma 16 *Nechť $A \in \mathbb{R}$ je Dedekindův řez. Potom platí, že $A \in \mathbb{R}^+$ tehdy a jen tehdy, když $-A \in \mathbb{R}^-$*

Důkaz: Jestliže $A \in \mathbb{R}^+$, potom podle Lemmatu 6 existuje $a \in A' \cap \mathbb{Q}^+$. Proto $-a < 0$, a v důsledku $0 \in -A$. Podle definice proto platí $-A \in \mathbb{R}^-$.

Opačně, jestliže $-A \in \mathbb{R}^-$, potom $0 \in -A$ a podle definice řezu $-A$ existuje $a \in A'$ takové, že $-a < 0$. Platí tedy, že $a \in \mathbb{Q}^+$. Dokázali jsme, že existuje kladné racionální číslo $a \in \mathbb{Q}^+$ takové, že $a \notin A$. podle Lemmatu 6 platí $A \in \mathbb{R}^+$. □.

Definice 15 *Mějme řezy $A, B \in \mathbb{R}$, potom odvozujeme součin $A \cdot B$ ze součinu kladných řezů následovně:*

$$A \cdot B = \begin{cases} A \cdot B & \text{jestliže } A \in \mathbb{R}^+, B \in \mathbb{R}^+, \\ -((-A) \cdot B) & \text{jestliže } A \in \mathbb{R}^-, B \in \mathbb{R}^+, \\ -(A \cdot (-B)) & \text{jestliže } A \in \mathbb{R}^+, B \in \mathbb{R}^-, \\ (-A) \cdot (-B) & \text{jestliže } A \in \mathbb{R}^-, B \in \mathbb{R}^-, \\ 0^* & \text{jestliže } A = 0^* \text{ nebo } B = 0^*. \end{cases}$$

Věta 35 *Algebraická struktura $(\mathbb{R}, +, \cdot)$ je komutativní těleso takové, že zobrazení $^* : \mathbb{Q} \longrightarrow \mathbb{R}$ je izomorfní vnoření. Těleso $\mathbb{R}$ nazýváme tělesem reálných čísel a v tomto kontextu nazýváme Dedekindovy řezy reálnými čísly.*

Důkaz: Nejprve Věta 32 tvrdí, že $(\mathbb{R}, +)$ je komutativní grupa. Zkoumejme proto strukturu $(\mathbb{R} \setminus \{0\}, \cdot)$. Nejprve z komutativity operace $\cdot$ na množině $\mathbb{R}^+$ a definice obecného součinu na $\mathbb{R}$ bezprostředně plyne komutativita operace $\cdot$ na $\mathbb{R}$. Uvědomíme-li si, že z Lemmatu 16 a Definice 15 bezprostředně plyne $-(A \cdot B) = (-A) \cdot B = A \cdot (-B)$ pro všechny Dedekindovy řezy $A, B \in \mathbb{R}$, můžeme obecnou asociativitu dokazovat skrze asociativitu součinu na kladných (a v triviálním důsledku nezáporných) Dedekindových řezech. Například jestliže $B \in \mathbb{R}^-$ a $A, C \in \mathbb{R}^+$, potom $A \cdot B, B \cdot C \in \mathbb{R}^-$, a lze proto počítat $(A \cdot B) \cdot C = -(A \cdot (-B)) \cdot C = -((A \cdot (-B)) \cdot C) = -(A \cdot ((-B) \cdot C) = A \cdot (-((-B) \cdot C)) = A \cdot (B \cdot C)$. Analogicky lze snadno ověřit i ostatní případy asociativity součinu.

Zbývá dokázat distributivita. Distributivitu pro kladné (a snadno potom také nulové) Dedekindovy řezy byla dokázána v Lemmatu 15. Abychom mohli použít podobnou konstrukcí jako v případě asociativity musíme ještě ověřit následující případ. Nechť $A, B \in \mathbb{R}^+$ a současně $C \in \mathbb{R}^-$ tak, že $B - C \in \mathbb{R}^+$, potom s ohledem na dokázané tvrzení $A \cdot B = A \cdot (B + C + (-C)) = A \cdot (B + C) + A \cdot (-C)$. Z tohoto ihned plyne, že $A \cdot (B + C) = A \cdot B + A \cdot C$. Ostatní případy již lze přímo odvodit z dokázaného. □

Věta 36 *Těleso reálných čísel $(\mathbb{R}, +, \cdot)$ lze uspořádat podle kladné části $\mathbb{R}^+$, přičemž pro libovolná reálná čísla (Dedekindovy řezy) $A, B \in \mathbb{R}$ platí, že $A < B$ tehdy a jen tehdy, jestliže $B \subset A$ (kde $<$ je uspořádání indukované kladnou části $\mathbb{R}^+$).*

Důkaz: V předchozím textu bylo dokázáno, že jestliže $A, B \in \mathbb{R}^+$, potom také $A \cdot B, A + B \in \mathbb{R}^+$. Z Lemmatu 16 navíc plyne trichotomie množiny $\mathbb{R}^+$ (tj. pro každé reálné číslo $A \in \mathbb{R}$ platí právě jedno z následujících tvrzení $A \in \mathbb{R}^+$, $-A \in \mathbb{R}^+$, nebo $A = 0^*$). Tedy množina $\mathbb{R}^+$ je kladná část, která indukuje uspořádání takové, že $A < B$ tehdy a jen tehdy, když $B - A \in \mathbb{R}^+$.

Dokažme druhou část věty. Nechť $A, B \in \mathbb{R}$ jsou takové, že $A \subset B$. Vezměme prvek $m \in B \setminus A$. Protože B je Dedekindův řez, nemá nejmenší prvek. Musí tedy existovat $n \in B$ takové, že $n < m$. Proto také dohromady $m, n \in B \setminus A$. Nechť nyní existuje $x \in A - B$. Podle definice existují prvky $a \in A$ a $b \in -B$ takové, že $x = a+b$. Opět z definice množiny $-B$ existuje $b' \in B'$ takové, že $-b' < b$.

Nejprve protože $m \notin A$, platí, že $m < a$. Také podobně, jelikož $b' \notin B$, platí, že $b' < n$, a tedy $-n < -b' < b$. Z monotonnosti sčítání dostáváme, že $m - n < a + b = x$. Protože prvek x jsme volili zcela obecně z řezu $A - B$, musí platit, že $m - n \notin A - B$. Víme také, že $n < m$, a proto $m - n \in \mathbb{Q}^+$. Podle Lemmatu 6 již platí, že $A - B \in \mathbb{R}^+$ (resp. $B < A$).

Předpokládejme nyní opačně, že $B < A$. Potom $A - B \in \mathbb{R}^+$, a tedy existuje $m \in \mathbb{Q}^+$ takové, že $m \notin A - B$. Nechť $x \in A$ je takový, že $x \notin B$, potom $-x < -x + m$, což dokazuje, že $m - x \in -B$. V důsledku nyní $m = x + (m - x) \in A - B$, což je spor. □

Věta 37 *Těleso $\mathbb{R}$ je uspořádáno archimedovsky.*

Důkaz: Vezměme libovolný Dedekindův řez $A \in \mathbb{R}$. Jistě existuje číslo $x \in A \subset \mathbb{Q}$, a protože těleso $\mathbb{Q}$ je archimedovské, můžeme najít $n \in \mathbb{N}$ takové, že $x < n$. Z definice Dedekindova řezu ihned plyne, že $n \in A$, a tedy také $n^* \subset A$. Předchozí věta přímo dokazuje, že $A < n^*$. □

5.6 Dedekindova věta, věta o supremu a věta o infimu

Poměrně komplikovanou konstrukcí se nám podařilo najít těleso, které rozšiřuje těleso racionálních čísel $\mathbb{Q}$ o nové prvky. Jak máme dokázáno, vzniklé těleso lze uspořádat, a to dokonce archimedovsky. Nyní zbývá dokázat, že vzniklá struktura přináší nové kvality. Následující Dedekindova věta završuje teorii tím, že dokáže spojitost tělesa reálných čísel.

Věta 38 (Dedekindova) *V tělese reálných čísel nejsou mezery (tj. řezy 4. druhu).*

Důkaz: Vezměme řez $A \subset \mathbb{R}$. Budeme předpokládat, že množina A nemá nejmenší prvek a dokážeme, že v tomto případě má množina A' prvek největší. Nejprve označme množinu

$$\beta = \{x \in \mathbb{Q} \,|\, x^* \in A\},$$

o které dokážeme, že je Dedekindovým řezem (a tedy také reálným číslem).

Domluvme se, že pro přehlednost budeme v tomto důkaze značit malými písmeny racionální čísla a obecně reálná čísla písmeny řecké abecedy. Množina β, jak ukážeme, je Dedekindovým řezem na $\mathbb{Q}$, a proto také reálným číslem. Přestože po vyslovení této věty užijeme vnoření * ke ztotožnění racionálních čísel x s odpovídajícími Dedekindovými řezy x^*, čímž dosáhneme inkluze $\mathbb{Q} \subseteq \mathbb{R}$ (podobně jako v předchozích případech konstrukce číselných oborů), budeme v důkazu této věty rozlišovat mezi racionálním číslem $x \in \mathbb{Q}$ a jemu odpovídajícím reálným číslem $x^* \in \mathbb{R}$.

Dokážeme, že platí $\beta \neq \emptyset, \mathbb{Q}$. Nejprve $A \neq \emptyset$, a tedy existuje $\alpha \in A$. Protože reálná čísla jsou uspořádána archimedovsky, existuje $n \in \mathbb{N} \subset \mathbb{Q}$ takové, že $\alpha < n^*$. Proto platí, že $n^* \in A$ z čehož plyne $n \in \beta$, a tedy $\beta \neq \emptyset$. Analogicky jelikož $A \neq \mathbb{R}$, existuje $\alpha \in \mathbb{R}$ takové, že $\alpha \notin A$. Z archimedovskosti plyne existence takového $n \in \mathbb{N} \subseteq Q$, že $n^* < \alpha$. Proto také $n^* \notin A$ a $n^* \notin \beta$.

Předpokládejme, že $x \in \beta$, a navíc $y \in \mathbb{Q}$ je takové číslo, že $x < y$. Platí tedy, že $x^* \in A$ a současně $x^* < y^*$. Protože A je řez, musí také platit $y^* \in A$, a tedy $y \in \beta$.

Nyní dokážeme, že β nemá nejmenší prvek. Jestliže $x \in \beta$, potom $x^* \in A$. Jelikož podle předpokladu A nemá nejmenší prvek, musí existovat $\alpha \in A$ takové, že $\alpha < x^*$. Protože těleso $\mathbb{R}$ je archimedovským rozšířením tělesa $\mathbb{Q}$, existuje podle Věty 29 takové racionální číslo $y \in \mathbb{Q}$, že $\alpha < y^* < x^*$. Z uvedených skutečností ovšem plyne, že $y \in \beta$ a současně $y < x$. Proto (obecně zvolené číslo) $x \in \beta$ není nejmenším prvkem množiny β.

Z dokázaných částí plyne, že β je Dedekindův řez, a proto také $\beta \in \mathbb{R}$. Nejprve dokážeme, že $\beta \notin A$ a v poslední části potom ukážeme, že β je maximální prvek v A'.

Jestliže sporem $\beta \in A$, potom protože A nemá nejmenší prvek, existuje $\alpha \in A$ takové, že $\alpha < \beta$. Věta 29 dokazuje existenci $x \in \mathbb{Q}$ takového, že $\alpha < x^* < \beta$ (jelikož $\mathbb{R}$ je archimedovské). Protože $x^* \in A$, musí platit také $x \in \beta$, a v důsledku také $x^* \subseteq \beta$. Podle Věty 36 z tohoto plyne, že $\beta < x^*$ (což je spor).

Analogicky dokážeme, že β je největším prvkem dolní části A'. Protože $\beta \notin A$ musí platit, že $\beta \in A'$. Předpokládejme sporem, že existuje $\alpha \in A'$ takové, že $\beta < \alpha$. Opět z archimedovskosti a z Věty 29 plyne existence $x \in \mathbb{Q}$ takového, že $\beta < x^* < \alpha$. Z nerovnosti $(x^* < \alpha)$ ihned plyne, že $x^* \in A'$, a tedy $x \notin \beta$. Proto $\beta \subseteq x^*$ a podle Věty 29 platí $x^* \leq \beta$ což je spor. Dokázali jsme, že pro každé $\alpha \in A'$ platí $\alpha \leq \beta$, a tedy β je maximálním prvkem množiny A'. □

Důsledkem Dedekindovy věty jsou důležité věty o supremu a infimu, které můžeme vyslovit. Je třeba zdůraznit, že věty platí až v tělese reálných čísel. Bez existence těchto vět (nebo ekvivalentních konstrukcí) by nebylo možné definovat základní pojmy matematické analýzy v plném rozsahu (jedná se především o existenci limit, a v důsledku potom o existenci derivací a integrálů).

Věta 39 (o supremu) *Každá neprázdná, shora omezená množina $M \subset \mathbb{R}$ má supremum.*

Věta 40 (o infimu) *Každá neprázdná, zdola omezená množina $M \subset \mathbb{R}$ má infimum.*

Důkaz: Dokážeme větu o infimu, přičemž důkaz věty o supremu je jednoduchou duální analogií. Mějme neprázdnou, zdola omezenou množinu $M \subset \mathbb{R}$ a označme potom následující množiny:

$$A = \{x \in \mathbb{R} \,|\, \text{existuje } m \in M \text{ platí, že } m < x\},$$

$$A' = \{x \in \mathbb{R} \,|\, \text{pro každé } m \in M \text{ platí, že } m \geq x\}.$$

Přímo z definice množin A a A' plyne, že $A \cap A' = \emptyset$ a současně $A \cup A' = \mathbb{R}$. Navíc protože množina M je neprázdná, existuje $m \in M$, a tedy $m < m + 1$ dokazuje, že

$m+1 \in A$ (a tedy A je neprázdná množina). Protože navíc množina M je zdola omezená, musí být také množina A' neprázdná.

Nyní již snadno ověříme, že dvojice množin A, A' tvoří řez na $\mathbb{R}$. Jestliže $x \in A$ a $y \in \mathbb{R}$ je takové, že $x < y$, potom podle definice množiny A existuje $m \in M$ takové, že $m < x$, a tedy také $m < y$. Proto $y \in A$.

Analogickou úvahou jako v mnoha předchozích případech lze dokázat, že A nemá nejmenší prvek. Mějme libovolný prvek $x \in A$. Podle definice existuje $m \in M$ takové, že $m < x$. Jelikož množina $\mathbb{R}$ je archimedovská, musí být podle Věty 29 uspořádaná hustě a tedy existuje $y \in \mathbb{R}$ takové, že $m < y < x$. Platí tedy, že $y \in A$, a proto x není nejmenší v A. Jelikož jsme prvek x volili zcela obecně, dokázali jsme, že A nemá nejmenší prvek.

Nyní podle Dedekindovy věty neexistují řezy 4. druhu, a tedy množina A' musí mít největší prvek. Protože množina A' je množinou všech dolních závor, musí být tento největší prvek největší dolní závorou, a tedy infimem. □

Kapitola 6

Reálná čísla konstruovaná metodou Cauchyovských posloupností

6.1 Fundamentální posloupnosti, základní vlastnosti

V této kapitole se seznámíme s alternativním způsobem konstrukce reálných čísel, způsobem, který objevil matematik Georg Cantor (1845-1918). Teorie pracuje s pojmem limity posloupnosti, který je v teorii nejdůležitějším. V první řadě zavedeme takzvané fundamentální (někdy také Cauchyovské) posloupnosti. Jedná se o takové posloupnosti, v kterých se jednotlivé prvky posloupnosti pohybují ve stále se zkracujícím intervalu, přičemž onen interval se zkracuje „limitně“ k nule. Intuitivně vnímáme, že tato posloupnost by měla konvergovat k nějakému bodu (k limitě této posloupnosti).

Příkladem může být těleso racionálních čísel $\mathbb{Q}$ a posloupnost čísel $1;\ 1,4;1,41;\ 1,414;\ \ldots$, která vzniká tak, že každý další člen vznikne z předchozího přidáním další číslice v dekadickém rozvoji čísla $\sqrt{2}$ ($=1,414213562373095\ldots$). Jednotlivé členy posloupnosti jsou zřejmě racionální čísla (mají ukončený dekadický rozvoj), ovšem limitou je číslo iracionální ($\sqrt{2}$).

Hlavní myšlenkou je vzít všechny takové posloupnosti a roztřídit je podle toho k jakému „místu“ na číselné ose se blíží. Každá taková třída bude představovat číslo reálné. Výhodou uvedeného postupu je jeho zobecnitelnost pro všechna uspořádána komutativní tělesa a především úzká souvislost s pojmy matematické analýzy. Užitím dané konstrukce reálných čísel může ukázat, že například různé definice spojitosti funkce jsou navzájem ekvivalentní apod.

Nadále v kapitole budeme předpokládat, že $\mathbb{T} = (T, +, \cdot)$ je komutativní uspořádané těleso podle kladné části T^+. Posloupnost $a_1, a_2, a_3, \ldots$ budeme značit $(a_i)_{i\in\mathbb{N}}$ nebo častěji jednoduše (a_i). Budeme-li nadále mluvit o posloupnosti, budeme automaticky tímto rozumět posloupnost prvků z $\mathbb{T}$. Uvědomme si, že podle Věty 28 platí, že těleso racionálních čísel $\mathbb{Q}$ je do tělesa $\mathbb{T}$ vnořitelné. Budeme proto předpokládat, že $\mathbb{Q} \subseteq \mathbb{T}$ (přesněji ztotožníme obraz popsaného vnoření $\mathbb{Q} \longrightarrow \mathbb{T}$ přímo s racionálními čísly $\mathbb{Q}$). Tímto ztotožněním dosáhneme, že všechna racionální čísla jsou prvky tělesa $\mathbb{T}$, a proto pro libovolné $x \in \mathbb{T}$ existují hodnoty jako $2x$, $\frac{x}{2}$ ($= \frac{1}{2} \cdot x$), $\frac{x}{3}$ apod.

Definice 16 *Posloupnost (a_i) nazveme fundamentální, jestliže pro každé $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ takové, že pro každé $m, n \in \mathbb{N}$ takové, že $m, n \geq n_0$ platí $|a_m - a_n| < \varepsilon$.*

Definice 17 *Řekneme, že prvek $a \in \mathbb{T}$ je limitou posloupnosti (a_i), jestliže pro každé $\varepsilon > 0$ existuje $n_0 \in \mathbb{N}$ takové, že pro každé $n \geq n_0$ platí $|a - a_n| < \varepsilon$. V takovémto případě značíme $a = \lim a_i$, posloupnost (a_i) nazýváme konvergentní (konverguje ke své limitě a). V případě, že posloupnost limitu nemá, nazýváme ji divergentní posloupnost.*

Věta 41 *Každá konvergentní posloupnost je fundamentální.*

Důkaz: Předpokládejme, že máme posloupnost (a_i) takovou, že $a = \lim a_i$. Vezměme libovolné $\varepsilon > 0$. Z definice limity posloupnosti existuje pro $\frac{\varepsilon}{2}(> 0)$ přirozené číslo $n_0 \in \mathbb{N}$ takové, že pro všechna $n \geq n_0$ platí $|a - a_n| < \frac{\varepsilon}{2}$. Z vlastností absolutních hodnot ale dostáváme, že pro $m, n \in \mathbb{N}$ takové, že $m, n \geq n_0$ platí $\varepsilon = \frac{\varepsilon}{2} + \frac{\varepsilon}{2} > |a - a_m| + |a - a_n| = |a_m - a| + |a - a_n| \geq |a_m - a + a - a_n| = |a_m - a_n|$. □

Je důležité si uvědomit, že obrácená implikace obecně neplatí. Tedy v některých uspořádaných tělesech existují fundamentální posloupnosti, které limitu (v tomto tělese) nemají. Příkladem jsou posloupnosti vycházející z dekadického rozvoje (příklad takovéto posloupnosti je uveden na začátku kapitoly pro hodnotu $\sqrt{2}$). Velice zajímavý a důležitý příklad fundamentální posloupnosti na množině racionálních čísel je posloupnost $\left(1 + \sum_{i=1}^{n} \frac{1}{i!}\right)_{n \in \mathbb{N}}$. Je zřejmé, že členy posloupnosti jsou racionální čísla (konečné součty racionálních čísel) a vzhledem k rychlosti růstu faktoriálu se dá dokázat, že posloupnost je fundamentální. Navíc platí, že

$$e = 1 + \sum_{i=1}^{\infty} \frac{1}{i!} = \lim_{n \to \infty} \left(1 + \sum_{i=1}^{n} \frac{1}{i!}\right).$$

Jak víme, číslo e je iracionální. Důkaz výše zmíněných tvrzení může čtenář najít v [BlI, Zed2].

Připomeňme, že těleso splňuje takzvanou Cauchyho podmínku konvergence řad, jestliže každá jeho fundamentální posloupnost má limitu. Naším cílem bude najít konstrukci, která dokáže rozšířit libovolné uspořádané komutativní těleso na těleso splňující Cauchyho podmínku. V případě, že naším tělesem bude těleso racionálních čísel $\mathbb{Q}$, potom jeho „zúplněním“ dostaneme právě těleso reálných čísel $\mathbb{R}$.

Je třeba si navíc uvědomit, že každý prvek vzniklého tělesa je limitou nějaké posloupnosti (minimálně konstantní posloupnosti, kde všechny členy jsou stejné). Zatímco v teorii Dedekindových řezů nám reálná čísla zastupují právě Dedekindovy řezy, v Cantorově teorii nám bude reálně číslo reprezentovat fundamentální posloupnost, přičemž každá posloupnost reprezentuje právě svou limitu. Přesněji řečeno, pokud má fundamentální posloupnost v tělese limitu, reprezentuje posloupnost právě tuto hodnotu, jestliže naopak posloupnost limitu nemá, bude tato posloupnost reprezentovat nový prvek, který můžeme intuitivně umístit právě do pozice chybějící limity.

V uvedené konstrukci musíme překonat některá úskalí. Především, různé fundamentální posloupnosti mohou mít stejnou limitu. Například $1 = \lim 1 = \lim 1 + \frac{1}{n}$, a tedy fundamentální posloupnosti (1) a $\left(1 + \frac{1}{n}\right)$ reprezentují obě stejnou hodnotu 1. Dalším příkladem posloupností, které mají stejnou limitu, v tomto případě ovšem neexistující

v tělese racionálních čísel, jsou následující posloupnosti. Posloupnost (a_i) definujeme z dekadického rozvoje Eulerova čísle $e(= 2,718281828459045\ldots)$. Tedy $a_1 = 2$, $a_2 = 2,7$, $a_3 = 2,71$ atd. Potom platí, že

$$\lim_{n\to\infty} a_i = e = \lim_{n\to\infty} \left(1 + \sum_{i=1}^{n} \frac{1}{i!}\right).$$

Proto posloupnosti (a_i) a $\left(1 + \sum_{i=1}^{n} \frac{1}{i!}\right)_{n\in\mathbb{N}}$ budou v naší nové struktuře reprezentovat obě stejnou hodnotu (v tomto případě touto hodnotou bude Eulerovo číslo e).

Posledním problémem bude najít správné kritérium, které rozhodne, kdy dvě posloupnosti reprezentují stejnou hodnotu. Jinými slovy, hledáme ekvivalenci takovou, která nám roztřídí posloupnosti podle své limity (ať už existující v daném tělese nebo zatím jenom myšlené limity). Definice této ekvivalence je následující: řekneme, že dvě fundamentální posloupnosti (a_i) a (b_i) jsou ekvivalentní, jestliže existuje limita posloupnosti $(a_i - b_i)$ a tato je rovna nule. To, že zavedená relace je relace ekvivalence, dokážeme v následujícím textu.

Touto myšlenkou konstrukce nekončí. Dále musíme zavést sčítání a násobení vzniklých hodnot a dokázat, že vzniklá struktura je uspořádané těleso. Nakonec ukážeme, že těleso $\mathbb{T}$ lze do vzniklého tělesa vnořit, přičemž vzniklé těleso splňuje Cauchyho podmínku. Poměrně komplikovaná konstrukce nám potom přinese několik užitečných vět, kterými lze reálná čísla charakterizovat.

Nyní se vraťme ke zkoumání fundamentálních posloupností a realizací naší teorie.

Věta 42 *Každá fundamentální posloupnost (a_i) je omezená (tj. existují hodnoty $A, B \in \mathbb{T}$ takové, že $A \leq a_i \leq B$ pro všechna $i \in \mathbb{N}$).*

Důkaz: Protože posloupnost (a_i) je fundamentální, existuje $n_0 \in \mathbb{N}$ takové, že pro každé $m, n \in \mathbb{N}$ takové, že $m, n \geq n_0$ platí $|a_m - a_n| < 1$. Můžeme proto tvrdit, že pro každé $n \in \mathbb{N}$ takové, že $n \geq n_0$ platí, že $|a_{n_0} - a_n| < 1$ a také $a_{n_0} - 1 \leq a_n \leq a_{n_0} + 1$. Označme proto

$$A = \min\{a_1, a_2, \cdots, a_{n_0-1}, a_{n_0} - 1, a_{n_0} + 1\},$$
$$B = \max\{a_1, a_2, \cdots, a_{n_0-1}, a_{n_0} - 1, a_{n_0} + 1\}.$$

Protože uvedené množiny jsou konečné, uvedená maxima a minima existují. Nyní již je snadné ověřit, že pokud $n \in \mathbb{N}$ je takové, že $n < n_0$, potom $a_n \in \{a_1, a_2, \cdots, a_{n_0-1}, a_{n_0} - 1, a_{n_0} + 1\}$, a proto $A \leq a_n \leq B$. Pokud $n \geq n_0$, potom $A \leq a_{n_0} - 1 \leq a_n \leq a_{n_0} + 1 \leq B$. □

Věta 43 *Jestliže jsou posloupnosti (a_i) a (b_i) fundamentální, potom také posloupnosti $(a_i + b_i)$ a $(a_i \cdot b_i)$ jsou fundamentální.*

Důkaz: Nejprve dokážeme část věty pro součet posloupností. Vezměme libovolné $\varepsilon > 0$. Protože posloupnosti (a_i) a (b_i) jsou fundamentální existují $m_0, n_0 \in \mathbb{N}$ takové, že pro každé $m, n, o, p \in \mathbb{N}$ splňující $m, n \geq m_0$ a $o, p \geq n_0$ platí, že $|a_m - a_n|, |b_o - b_p| < \frac{\varepsilon}{2}$.

Z předchozího tvrzení plyne, že pro všechna $m, n \in \mathbb{N}$ splňující $m, n \geq \max\{m_0, n_0\}$ platí $\varepsilon = \frac{\varepsilon}{2} + \frac{\varepsilon}{2} > |a_m - a_n| + |b_m - b_n| \geq |a_m - a_n + b_m - b_n| = |(a_m + b_m) - (a_n + b_n)|$. Tedy pro každé $\varepsilon > 0$ existuje k_0 $(= \max\{n_0, m_0\})$ takové, že pro libovolné $m, n \in \mathbb{N}$ splňující $m, n \geq k_0$ platí $|(a_m - b_n) - (a_n + b_n)| < \varepsilon$.

Mějme fundamentální posloupnosti (a_i) a (b_i). Protože fundamentální posloupnosti jsou omezené, existují hodnoty $A, B \in \mathbb{T}$ takové, že $|a_i| < A$, $|b_i| < B$ pro všechna $i \in \mathbb{N}$. Mějme nyní libovolné $\varepsilon > 0$. Potom existují $m_0, n_0 \in \mathbb{N}$ takové, že všechna $m, n, o, p \in \mathbb{N}$ splňující $m, n \geq m_0$ a $o, p \geq n_0$ platí

$$|a_m - a_n| < \frac{\varepsilon}{2B},$$

$$|b_p - b_o| < \frac{\varepsilon}{2A}.$$

Nyní pro libovolné $m, n \geq \max\{m_0, n_0\}$ platí, že

$$|a_m \cdot b_m - a_n \cdot b_n| = |a_m \cdot b_m + a_m \cdot b_n - a_m \cdot b_n - a_n \cdot b_n| \leq |a_m \cdot b_n - a_n \cdot b_n| +$$

$$+|a_m \cdot b_m - a_m \cdot b_n| = |b_n| \cdot |a_m - a_n| + |a_m| \cdot |b_m - b_n| < B \cdot \frac{\varepsilon}{2B} + A \cdot \frac{\varepsilon}{2A} = \varepsilon.$$

Tedy pro libovolné $\varepsilon > 0$ existuje k_0 $(= \max\{m_0, n_0\})$ takové, že pro všechna $m, n \in \mathbb{N}$ splňující $m, n \geq k_0$ platí $|a_m \cdot b_m - a_n \cdot b_n| < \varepsilon$. □

Jistou analogii k dokázanému tvrzení můžeme najít také v následující větě.

Věta 44 *Jestliže (a_i) a (b_i) jsou konvergentní posloupnosti, potom také $(a_i + b_i)$ a $(a_i \cdot b_i)$ jsou konvergentní posloupnosti, a navíc platí, že*

$$\lim(a_i + b_i) = (\lim a_i) + (\lim b_i),$$

$$\lim(a_i \cdot b_i) = (\lim a_i) \cdot (\lim b_i).$$

Důkaz: Předpokládejme, že $\lim a_i = a$ a $\lim b_i = b$. Vezměme navíc libovolné $\varepsilon > 0$. Potom podle definice limity existují čísla $m_0, n_0 \in \mathbb{N}$ taková, že pro libovolné čísla $m, n \in \mathbb{N}$ splňující $m_0 \leq m$ a $n_0 \leq n$ platí $|a - a_n| < \frac{\varepsilon}{2}$ a $|b - b_n| < \frac{\varepsilon}{2}$. Označíme-li $k_0 = \max\{m_0, n_0\}$, potom pro libovolné $n \in \mathbb{N}$ takové, že $k_0 \leq n$ platí $|(a+b) - (a_n + b_n)| \leq |a - a_n| + |b - b_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$. Toto dokazuje, že $\lim(a_i + b_i) = a + b = \lim a_i + \lim b_i$.

Nyní dokážeme část věty o součinu limit. Jelikož posloupnosti (a_i) a (b_i) mají limitu, jsou také fundamentální, a tedy i omezené (viz. Věty 41 a 42). Existuje proto $A, B \in T^+$ takové, že $|a| < A$ a $|b_i| < B$ pro každé $i \in \mathbb{N}$. Nyní vezměme libovolné $\varepsilon > 0$. Z kladnosti hodnot A a B plyne, že také $\frac{\varepsilon}{2A} > 0$ a $\frac{\varepsilon}{2B} > 0$, a proto definice limity dokazuje existenci čísel $m_0, n_0 \in \mathbb{N}$ takových, že pro všechna $m, n \in \mathbb{N}$ splňující $m_0 < m$ a $n_0 < n$ platí

$$|a - a_m| < \frac{\varepsilon}{2B},$$

$$|b - b_n| < \frac{\varepsilon}{2A}.$$

Označíme analogicky jako v předchozích případech $k_0 = \max\{m_0, n_0\}$. Nyní platí pro všechna $n \in \mathbb{N}$ taková, že $k_0 \leq n$, že

$$|a_n \cdot b_n - a \cdot b| = |a_n \cdot b_n + a \cdot b_n - a \cdot b_n - a \cdot b| \leq |a_n \cdot b_n - a \cdot b_n| + |a \cdot b_n - a \cdot b|$$

$$= |b_n| \cdot |a_n - a| + |a| \cdot |b_n - b| < B \cdot \frac{\varepsilon}{2B} + A \cdot \frac{\varepsilon}{2A} = \varepsilon.$$

Z dokázaného plyne, že $\lim(a_i \cdot b_i) = a \cdot b = (\lim a_i) \cdot (\lim b_i)$. □

Důsledek 2 *Jestliže (a_i) je konvergentní posloupnost, potom také $(-a_i)$ a je konvergentní posloupnosti a navíc platí, že*

$$\lim(-a_i) = -\lim a_i.$$

Důkaz: Vezmeme-li posloupnost (-1), potom snadno platí, že $\lim -1 = -1$ a podle předchozí věty také $\lim(-a_i) = \lim(-1 \cdot a_i) = (\lim -1) \cdot (\lim a_i) = -\lim a_i$. □

6.2 Aritmetika tělesa fundamentálních posloupností

Nyní máme dokázány základní tvrzení k tomu, abychom mohli přejít ke stěžejní části naší konstrukce. Označme nejprve $\mathbf{F}_\mathbb{T}$ množinu všech fundamentálních posloupností. Z Věty 43 plyne, že na množině $\mathbf{F}_\mathbb{T}$ můžeme definovat součet a součin posloupností $(a_i), (b_i) \in \mathbf{F}_\mathbb{T}$ tak, že $(a_i) + (b_i) = (a_i + b_i)$ a $(a_i) \cdot (b_i) = (a_i \cdot b_i)$. Platí přitom následující tvrzení:

Věta 45 *Struktura $(\mathbf{F}_\mathbb{T}, +, \cdot)$ tvoří komutativní okruh s nulovou posloupnosti (0) (posloupnost, ve které $a_i = 0$ pro všechna $i \in \mathbb{N}$), opačný prvek k posloupnosti $(a_i) \in \mathbf{F}_\mathbb{T}$ je posloupnost $(-a_i)$ a jednotkou (1) (posloupnost ve které platí $a_i = 1$ pro všechna $i \in \mathbb{N}$).*

Důkaz: Jestliže $(a_i), (b_i), (c_i) \in \mathbf{F}_\mathbb{T}$, potom, protože $\mathbb{T}$ je komutativní těleso a z definice součtu a součinu posloupnosti můžeme dokázat:

i) $(a_i) + (b_i) = (a_i + b_i) = (b_i + a_i) = (b_i) + (a_i)$,

ii) $(a_i) + ((b_i) + (c_i)) = (a_i + b_i + c_i) = ((a_i) + (b_i)) + (c_i)$,

iii) $(a_i) + (0) = (a_i + 0) = (a_i)$,

iv) $(a_i) + (-a_i) = (a_i - a_i) = (0)$,

v) $(a_i) \cdot (b_i) = (a_i \cdot b_i) = (b_i \cdot a_i) = (b_i) \cdot (a_i)$,

vi) $(a_i) \cdot ((b_i) \cdot (c_i)) = (a_i \cdot b_i \cdot c_i) = ((a_i) \cdot (b_i)) \cdot (c_i)$,

vii) $(a_i) \cdot (1) = (a_i \cdot 1) = (a_i)$,

vii) $(a_i) \cdot ((b_i) + (b_i)) = (a_i \cdot (b_i + c_i)) = (a_i \cdot b_i + a_i \cdot c_i) = (a_i) \cdot (b_i) + (a_i) \cdot (c_i)$.

Dokázané rovnosti dohromady dokazují větu. □

Okruh z předchozí věty se stane základem námi konstruovaného tělesa. Jak jsme již zmiňovali v předchozích částech, posloupnosti budou reprezentovat hodnoty, které odpovídají jejím (někdy neexistujícím) limitám. Proto je třeba roztřídit posloupnosti podle svých limit. K tomuto použijeme přirozeně aparát faktorizace.

Definice 18 *Na množině* $\mathbf{F}_\mathbb{T}$ *definujme relaci* $\sim$ *tak, že pro* $(a_i), (b_i) \in \mathbf{F}_\mathbb{T}$ *platí, že* $(a_i) \sim (b_i)$ *tehdy a jen tehdy, jestliže posloupnost* $(a_i - b_i)$ *je konvergentní, a navíc* $\lim(a_i - b_i) = 0$.

Věta 46 *Relace* $\sim$ *je kongruence na okruhu* $\mathbf{F}_\mathbb{T}$*, přičemž platí, že faktorový okruh* $(\mathbf{F}_\mathbb{T}/\sim, +, \cdot)$ *je komutativní těleso.*

Důkaz: Nejprve dokážeme, že relace $\sim$ je relace ekvivalence. Protože pro všechna $(a_i) \in \mathbf{F}_\mathbb{T}$ platí, že $\lim(a_i - a_i) = \lim 0 = 0$ platí $(a_i) \sim (a_i)$ a relace je reflexivní.

Jestliže platí $(a_i) \sim (b_i)$, potom podle definice platí také $\lim(a_i - b_i) = 0$, a tedy také z Důsledku 2 plyne, že $\lim(b_i - a_i) = \lim(-(a_i - b_i)) = -\lim(a_i - b_i) = -0 = 0$. Proto $(b_i) \sim (a_i)$ a relace je symetrická.

Předpokládejme, že $(a_i) \sim (b_i)$ a také $(b_i) \sim (c_i)$. Podle definice dostáváme $\lim(a_i - b_i) = \lim(b_i - c_i) = 0$. Díky Větě 44 můžeme počítat $\lim(a_i - c_i) = \lim(a_i - b_i + b_i - c_i) = \lim(a_i - b_i) + \lim(b_i - c_i) = 0 + 0 = 0$. Důsledkem je $(a_i) \sim (c_i)$, a proto je relace $\sim$ také tranzitivní.

V předcházející části jsme dokázali, že relace $\sim$ je relace ekvivalence, nyní ukážeme, že se jedná navíc o kongruenci. Vezměme posloupnosti $(a_i), (a'_i), (b_i), (b'_i) \in \mathbf{F}_\mathbb{T}$ a předpokládejme, že $(a_i) \sim (a'_i)$ a $(b_i) \sim (b'_i)$. Z definice ekvivalence $\sim$ plyne, že $\lim(a_i - a'_i) = \lim(b_i - b'_i) = 0$. Z Věty 44 proto dostáváme $\lim((a_i + b_i) - (a'_i + b'_i)) = \lim(a_i - a'_i) + \lim(b_i - b'_i) = 0 + 0 = 0$, a tedy také platí, že $(a_i + b_i) \sim (a'_i + b'_i)$. Vzhledem k tomu, že z definice součtu posloupnosti dostáváme $(a_i) + (b_i) = (a_i + b_i)$ (a analogicky $(a'_i) + (b'_i) = (a'_i + b'_i)$), dokázali jsme $(a_i) + (b_i) \sim (a'_i) + (b'_i)$.

Protože posloupnosti (a_i) a (b'_i) jsou fundamentální, existují hodnoty $A, B \in \mathbb{T}$ takové, že pro všechna $n \in \mathbb{N}$ platí $|a_i| < A$ a $|b'_i| < B$ (viz Věta 42, která říká, že fundamentální posloupnost musí být i omezená shora i zdola). Zvolme nyní libovolné $0 < \varepsilon$. Protože $\lim(a_i - a'_i) = \lim(b_i - b'_i) = 0$ platí, že

- existuje $n_0 \in \mathbb{N}$ takové, že pro všechna $n \in \mathbb{N}$ splňující $n_0 \leq n$ platí

$$|a_n - a'_n| < \frac{\varepsilon}{2B},$$

- existuje $m_0 \in \mathbb{N}$ takové, že pro všechna $n \in \mathbb{N}$ splňující $m_0 \leq n$ platí

$$|b_n - b'_n| < \frac{\varepsilon}{2A}.$$

Potom pro libovolné $n \in \mathbb{N}$ takové, že $\max\{n_0, m_0\} \leq n$ platí, že

$$\begin{aligned} |a_n \cdot b_n - a'_n \cdot b'_n| &= |a_n \cdot b_n - a_n \cdot b'_n + a_n \cdot b'_n - a'_n \cdot b'_n| \leq \\ &\leq |a_n \cdot b_n - a_n \cdot b'_n| + |a_n \cdot b'_n - a'_n \cdot b'_n| = \\ &= |a_n| \cdot |b_n - b'_n| + |b'_n| \cdot |a_n - a'_n| < \\ &< A \cdot \frac{\varepsilon}{2A} + B \cdot \frac{\varepsilon}{2B} = \\ &= \varepsilon. \end{aligned}$$

Dokázali jsme, že pro libovolné $0 < \varepsilon$ existuje $\max\{n_0, m_0\} \in \mathbb{N}$ takové, že pro všechna $n \in \mathbb{N}$ splňující $\max\{n_0, m_0\} \leq n$ platí

$$|a_n \cdot b_n - a'_n \cdot b'_n| < \varepsilon.$$

Proto $\lim(a_i \cdot b_i - a'_i \cdot b'_i) = 0$, a tedy také $a_i \cdot b_i \sim a'_i \cdot b'_i$. Tímto jsme dokázali, že relace $\sim$ je kongruencí na okruhu $\mathbf{F}_{\mathbb{T}}$.

Jelikož algebra $(\mathbf{F}_{\mathbb{T}}, +, \cdot)$ je komutativní okruh, také faktorová algebra $(\mathbf{F}_{\mathbb{T}}/\sim, +, \cdot)$ musí být komutativním okruhem. Abychom dokázali, že faktorová algebra je těleso, musíme dokázat, že ke každé nenulové posloupnosti existuje také její inverzní posloupnost. Nejprve zjednodušíme značení faktorových tříd $[(a_i)]_\sim$ na $[a_i]$ (zápisem $[a_i]$ tedy rozumíme množinu všech tříd ekvivalentních s posloupnosti (a_i)).

Vezměme libovolnou nenulovou třídu $[a_i]$. Jelikož je třída nenulová platí, že $(a_i) \not\sim (0)$, a tedy $\lim a_i = \lim(a_i - 0) \neq 0$. Sporem dokážeme, že existuje $0 < \eta$ a $n_0 \in \mathbb{N}$ takové, že pro všechna $n \in \mathbb{N}$ takové, že $n_0 \leq n$ platí $|a_n| \geq \eta$. Jestliže sporem pro každé $0 < \varepsilon$ a libovolné $n_0 \in N$ existuje $n \in \mathbb{N}$ takové, že $n_0 \leq n$, a navíc $|a_n| < \varepsilon$, potom uvažujme libovolné $0 < \varepsilon$. Protože posloupnost (a_i) je fundamentální, existuje $n_0 \in \mathbb{N}$ takové, že pro všechna $p, q \in \mathbb{N}$ taková, že $n_0 \leq p, q$ platí, že $|a_p - a_q| < \frac{\varepsilon}{2}$. Podle předpokladu také existuje $n \in \mathbb{N}, n_0 \leq n$ takové, že $|a_n| < \frac{\varepsilon}{2}$.

Dohromady, pro každé $p \in \mathbb{N}$ takové, že $n_0 \leq p$ platí, že $|a_p - 0| = |a_p - a_n + a_n| \leq |a_p - a_n| + |a_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$. Dokázali jsme, že pro libovolné $0 < \varepsilon$ existuje $n_0 \in \mathbb{N}$ takové, že pro všechna $p \in \mathbb{N}, n_0 \leq p$ platí $|a_p - 0| < \varepsilon$. Toto podle definice limity dokazuje, že $\lim a_i = 0$ což je spor.

Máme dokázáno, že pro nenulovou posloupnost (a_i) existuje $0 < \eta$ a $n_0 \in \mathbb{N}$ takové, že pro všechna $n \in \mathbb{N}$ splňující $n_0 \leq n$ platí, že $\eta \leq |a_n|$. Definujme proto posloupnost (b_i) následovně:

$$b_i = \begin{cases} \eta & \text{jestliže } i < n_0 \\ a_i & \text{jestliže } n_0 \leq i. \end{cases}$$

Snadno nyní vidíme, že posloupnost (b_i) je také fundamentální a posloupnost $(a_i - b_i)$ má každý i-tý člen $(n_0 \leq i)$ roven 0. Proto platí, že $\lim(a_i - b_i) = 0$, a proto $(a_i) \sim (b_i)$, a tedy $[a_i] = [b_i]$.

Nyní již zbývá ověřit, že také posloupnost (b_i^{-1}) je fundamentální. Především si uvědomme, že platí $0 < \eta \leq |b_n|$ pro libovolné $n \in \mathbb{N}$, proto $b_n \neq 0$ a b_n^{-1} existuje. Protože posloupnost (b_i) je fundamentální existuje pro každé $1 < \varepsilon$ číslo $n_0 \in \mathbb{N}$ takové, že pro všechna $p, q \in \mathbb{N}$ splňující $n_0 \leq p, q$ platí, že $|b_p - b_q| < \eta^2 \varepsilon$.

Nyní ovšem můžeme $p, q \in \mathbb{N}$ splňující $n_0 \leq p, q$ počítat: $|b_p^{-1} - b_q^{-1}| \cdot \eta^2 \leq |b_p^{-1} - b_q^{-1}| \cdot |b_p| \cdot |b_q| = |(b_p^{-1} - b_q^{-1}) \cdot b_p \cdot b_q| = |b_q - b_p| < \eta^2\varepsilon$. Z tohoto ovšem odvodíme $|b_p^{-1} - b_q^{-1}| < \varepsilon$, což dokazuje fundamentálnost posloupnosti (b_i^{-1}). Nyní už snadno vidíme, že $[a_i] \cdot [b_i^{-1}] = [b_i] \cdot [b_i^{-1}] = [(b_i) \cdot (b_i^{-1})] = [b_i \cdot b_i^{-1}] = [1]$, což dokazuje, že $\mathbf{F}_{\mathbb{T}}/\!\sim$ je těleso. Zdůrazněme, že existují inverze $[a_i]^{-1} = [b_i^{-1}]$. □

6.3 Uspořádání tělesa $\mathbf{F}_{\mathbb{T}}/\!\sim$

Domluvme se, že nadále budeme těleso $\mathbf{F}_{\mathbb{T}}/\!\sim$ z předchozí věty značit jednodušeji $\overline{\mathbb{T}}$. Můžeme si všimnout, že existuje izomorfní vnoření $f : \mathbb{T} \longrightarrow \overline{\mathbb{T}}$ takové, že pro libovolné $x \in \mathbb{T}$ platí, že $f(x) = [x]$ (tj. posloupnost, která má všechny své členy a_i rovny x).

Nyní ukážeme, že těleso $\overline{\mathbb{T}}$ dokážeme uspořádat (neboli nalezneme jeho kladnou část). Nejprve definujme kladnou fundamentální posloupnost jako takovou fundamentální posloupnost (a_i), pro kterou existuje $0 < \varepsilon$ a $n_0 \in \mathbb{N}$, že $\varepsilon < a_n$ pro všechna $n \in \mathbb{N}$ splňující $n_0 \leq n$.

Jestliže (a_i) je taková posloupnost, že (a_i) není kladná a ani $(-a_i)$ není kladná, potom pro libovolné $0 < \varepsilon$ a libovolné přirozené číslo $n \in \mathbb{N}$ existují čísla $r, s \in \mathbb{N}$ taková, že platí $n_0 \leq r, s$, a navíc $\frac{\varepsilon}{2} \not< a_r, -a_s$.

Protože posloupnost (a_i) je fundamentální, a proto existuje $n_0 \in \mathbb{N}$ takové, že pro všechna $p, q \in \mathbb{N}$ splňující $n_0 \leq p, q$ platí $|a_p - a_q| < \frac{\varepsilon}{2}$. Vezměme nyní libovolné $p \in \mathbb{N}$ takové, že $n_0 \leq p$. Podle předchozího odstavce existují čísla $r, s \in \mathbb{N}$ taková, že $n_0 < r, s$, a navíc $\frac{\varepsilon}{2} \not< a_r, -a_s$ (tedy $\frac{\varepsilon}{2} \geq a_r, -a_s$). Nyní můžeme počítat:

$$a_p = (a_p - a_r) + a_r \leq |a_p - a_r| + a_r < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Analogicky ovšem

$$-a_p = (a_s - a_p) - a_s \leq |a_s - a_p| - a_s < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Z předchozích dvou rovností ihned plyne, že $|a_p| < \varepsilon$. Dohromady jsme dokázali, že pro libovolné $0 < \varepsilon$ existuje $n_0 \in \mathbb{N}$ takové, že pro všechna $p \in \mathbb{N}$ splňující $n_0 \leq p$ platí $|a_p - 0| = |a_p| < \varepsilon$. Toto dohromady dokazuje, že $\lim a_i = 0$.

Jestliže tedy (a_i) není kladná posloupnost a také $(-a_i)$ není kladná, potom $\lim a_i = 0$, a tedy $[a_i] = 0$.

Nyní dokážeme, že námi prezentovanou definici kladné posloupnosti lze korektně rozšířit i na celé třídy posloupností. Uvažujme proto libovolnou třídu posloupností $[a_i]$ takovou, že (a_i) je kladná posloupnost. Nechť $(b_i) \in [a_i]$ (tj. $(a_i) \sim (b_i)$, a tedy také $\lim(a_i - b_i) = 0$). Existuje proto $0 < \varepsilon$ a $n_0 \in \mathbb{N}$ takové, že $\varepsilon < a_p$ pro všechna $p \in \mathbb{N}$ splňující $n_0 \leq p$. Navíc existuje $m_0 \in \mathbb{N}$ takové, že $|a_s - b_s| < \frac{\varepsilon}{2}$ pro všechna $s \in \mathbb{N}$ splňující $m_0 \leq s$.

Dohromady pro každé $p \in \mathbb{N}$ takové, že $\max\{m_0, s_0\} \leq p$, platí, že $b_p = a_p - (a_p - b_p) \geq a_p - |a_p - b_p| > \varepsilon - \frac{\varepsilon}{2} = \frac{\varepsilon}{2}$. Toto ovšem dokazuje, že také posloupnost (b_i) je kladná. Dokázali jsme, že jestliže máme kladnou posloupnost, potom také všechny posloupnosti

s ní ekvivalentní jsou kladné. Můžeme proto takto definovat kladnou třídu posloupností. Množinu všech kladných tříd posloupností označme $\overline{\mathbb{T}}^+$.

Přesněji, třída posloupností (podle ekvivalence $\sim$) je kladná, jestliže je libovolný její reprezentant kladný (což je ekvivalentní s tím, že všichni reprezentanti této třídy jsou kladné posloupnosti).

Spojíme-li dokázaná tvrzení, můžeme dedukovat: Jestliže $[a_i]$ není kladná třída, a navíc ani $-[a_i] = [-a_i]$ není kladná třída, potom $\lim a_i = 0$ a tedy $[a_i] = [0]$. Proto množina $\overline{\mathbb{T}}^+$ splňuje trichotomii.

Konečně ověříme, že množina $\overline{\mathbb{T}}^+$ je uzavřena na součty a součiny. Jestliže $[a_i], [b_i] \in \overline{\mathbb{T}}^+$, potom existují $0 < \varepsilon_1, \varepsilon_2$ a $m_0, n_0 \in \mathbb{N}$ taková, že pro všechna $m, n \in \mathbb{N}$ splňující $m_0 < m$ a $n_0 < n$ platí, že $\varepsilon_1 < a_m$ a $\varepsilon_2 < b_n$. Proto také $\varepsilon_1 + \varepsilon_2 < a_p + b_p$ pro všechna $p \in \mathbb{N}$ splňující $\max\{m_0, n_0\} \leq p$ a také $\varepsilon_1 \cdot \varepsilon_2 < a_p \cdot b_p$ pro všechna $p \in \mathbb{N}$ splňující $\max\{m_0, n_0\} \leq p$. Tedy $[a_i + b_i], [a_i \cdot b_i] \in \overline{\mathbb{T}}^+$.

Zkoumejme ještě výše zavedené vnoření $f : \mathbb{T} \longrightarrow \overline{\mathbb{T}}^+$ z pohledu uspořádání. Jestliže $x \in \mathbb{T}^+$, potom platí, že $0 < \frac{x}{2} < x$, a tedy také $f(x) = [x] \in \overline{\mathbb{T}}^+$.

Předcházející úvahy můžeme shrnout do následující věty:

Věta 47 *Fundamentální posloupnost $(a_i) \in \mathrm{F}_{\mathbb{T}}$ nazveme kladnou, jestliže existuje $0 < \varepsilon$ a $n_0 \in \mathbb{N}$ takové, že pro všechna $n \in \mathbb{N}$ splňující $n_0 \leq n$ platí, že $\varepsilon < a_n$. Potom platí:*

i) Jestliže $[a_i] \in \overline{\mathbb{T}}$, potom (a_i) je kladná posloupnost právě, když všechny posloupnosti náležející do třídy $[a_i]$ jsou kladné. V tomto případě budeme třídu $[a_i]$ nazývat kladnou třídou a množinu všech kladných tříd budeme značit $\overline{\mathbb{T}}^+$.

ii) Množina všech kladných tříd $\overline{\mathbb{T}}^+$ tvoří kladnou část tělesa $\overline{\mathbb{T}}$ (ve smyslu Definice 9). V následujícím textu budeme uspořádáním na tělese $\overline{\mathbb{T}}$ automaticky rozumět uspořádaní podle kladné části $\overline{\mathbb{T}}^+$.

iii) Vnoření $f : \mathbb{T} \longrightarrow \overline{\mathbb{T}}$ je izotonní, tedy $f(\mathbb{T}^+) \subseteq \overline{\mathbb{T}}^+$ a také pro všechna $x, y \in \mathbb{T}$ platí, že jestliže $x < y$, potom také $f(x) < f(y)$.

Diskutujme nyní některé vlastnosti uspořádaného tělesa $\overline{\mathbb{T}}$. Jestliže $[a_i] \in \overline{\mathbb{T}}$, potom protože je posloupnost (a_i) fundamentální v $\mathbb{T}$, existuje $x \in \mathbb{T}$ takové, že $a_i < x$ pro všechna $i \in \mathbb{N}$ (viz Věta 42). Naším cílem je nyní dokázat, že $[a_i] \leq [x]$. Jinými slovy chceme ukázat, že pro libovolné $[a_i] \in \overline{\mathbb{T}}$ existuje $x \in \mathbb{T}$ takové, že $[a_i] \leq [x]$.

Jistě platí, že $0 < x - a_i = |x - a_i|$. Jestliže platí $[a_i] \not< [x]$, a tedy posloupnost $[x - a_i] = [x] - [a_i]$ není kladná, potom pro libovolné $0 < \varepsilon$ a libovolné $n_0 \in \mathbb{N}$ existuje $n \in \mathbb{N}$ takové, že $n_0 \leq n$, a navíc $x - a_n < \varepsilon$.

Nyní vezměme libovolné $0 < \varepsilon$. Z fundamentálnosti posloupnosti (a_i) ihned plyne, existence $n_0 \in \mathbb{N}$ takového, že pro všechna $p, q \in \mathbb{N}$ splňující $n_0 \leq p, q$ platí $|a_q - a_p| < \frac{\varepsilon}{2}$. Z předchozího odstavce plyne, že existuje $n \in \mathbb{N}$ takové, že $n_0 \leq n$, a navíc $x - a_n < \frac{\varepsilon}{2}$. Dohromady tedy platí, že pro libovolné $p \in \mathbb{N}$ takové, že $n_0 \leq p$ platí také $|x - a_p| \leq |x - a_n| + |a_n - a_p| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$. Z dokázaného tedy plyne, že $\lim(x - a_p) = 0$, a tedy $[a_i] = [x]$.

Podobně, pokud $0 < [a_i]$, potom existuje $x \in \mathbb{T}$ takové, že $0 < [a_i]^{-1} < [x]$, a tedy také $0 < [x^{-1}] < [a_i]$.

Shrneme-li předchozí odstavce, dokázali jsme, že pro libovolný kladný prvek $[a_i]$ tělesa $\overline{\mathbb{T}}$ existují kladné prvky v tělese $x, y \in \mathbb{T}$ takové, že $0 < [x] < [a_i] < [y]$. Tuto skutečnost budeme nadále často využívat. Všimněme si ještě toho, že z uvedené vlastnosti ihned plyne, že pokud těleso $\mathbb{T}$ je archimedovské, potom také těleso $\overline{\mathbb{T}}$ je archimedovské.

6.4 Vlastnosti tělesa $\overline{\mathbb{T}}$

Následující věta ukazuje, že každá posloupnost z $\mathbb{T}$ má v $\overline{\mathbb{T}}$ limitu. Navíc vnoření f limity zachovává.

Věta 48 *Mějme fundamentální posloupnost $(a_i) \in \mathbf{F}_{\mathbb{T}}$. Potom platí, že:*

i) Posloupnost $(f(a_i))$ má v $\overline{\mathbb{T}}$ limitu, kterou je třída $[a_i]$, tj. $\lim f(a_i) = [a_i]$.

ii) Jestliže existuje $a = \lim a_i$, potom $f(a) = \lim f(a_i)$.

Důkaz: V souladu s předchozí konstrukcí budeme značit prvky tělesa $\overline{\mathbb{T}}$ jakožto třídy posloupností (např $[a_i]$, $[\varepsilon_i]$ apod.), zatímco prvky tělesa $\mathbb{T}$ budeme značit samotnými znaky (např. a, ε apod.). Připomeňme, že zobrazení $f : \mathbb{T} \longrightarrow \overline{\mathbb{T}}$ je definováno pomocí $f(a) = [a]$, kde $[a]$ značí třídu obsahující konstantní posloupnost (a) (posloupnost, kde všechny členy a_i jsou rovny a).

ad. i) Nadále zjednodušme notaci, kdy označíme třídu $A = [a_i]$ a také $A_p = f(a_p) = [a_p]$ (třída určena konstantní posloupností, kdy každý její člen je roven hodnotě a_p). Máme tak pro libovolné $n \in \mathbb{N}$ definovanou posloupnost A_n.

Vezměme libovolné $0 < [\varepsilon_i]$, potom existuje $\varepsilon \in \mathbb{T}$ takové, že $0 < [\varepsilon] < [\varepsilon_i]$. Jelikož (a_i) je fundamentální posloupnost, existuje $n_0 \in \mathbb{N}$ takové, že pro všechna $p, q \in \mathbb{N}$ splňující $n_0 \leq p, q$ platí $|a_p - a_q| < \varepsilon$.

Nyní dokážeme, že pro libovolné $p \in \mathbb{N}$ splňující $n_0 \leq p$ platí $|A - A_p| \leq [\varepsilon]$. Pro pevně zvolené $p \in \mathbb{N}$ takové, že $n_0 < p$ označme posloupnost $(b_i) = |A - A_p|$ (tedy $b_i = |a_i - a_p|$). Potom pro všechna $i \in \mathbb{N}$ splňující $n_0 \leq i$ platí, že $b_i = |a_i - a_p| < \varepsilon$, a v důsledku také $b_i - \varepsilon < 0$. Posloupnost $(b_i - \varepsilon)$ tedy nemůže být kladná (nemůže existovat $0 < \eta$ a $m_0 \in \mathbb{N}$ takové, že pro všechna $m \in \mathbb{N}$ splňující $m_0 \leq m$ platí $0 < \eta < b_i - \varepsilon$, protože by pro $o = \max\{m_0, n_0\}$ muselo platit $b_o - \varepsilon < 0 < b_o - \varepsilon$).

Dokázali jsme proto, že pro všechna $p \in \mathbb{N}$ takové, že $n_0 \leq p$ platí $[b_i - \varepsilon] \leq 0$, a tedy také $|A - A_p| = [b_i] \leq [\varepsilon] < [\varepsilon_i]$. Což konečně ukazuje, že $\lim f(a_i) = \lim A_i = A = [a_i]$.

ad. ii) Nyní předpokládejme, že $(a_i) \in \mathbf{F}_{\mathbb{T}}$ je taková, že existuje $a = \lim a_i$. Podle předchozí části věty potom platí, že $\lim f(a_i) = [a_i]$. Navíc platí také $\lim(a - a_i) = \lim a - \lim a_i = a - a = 0$, a tedy $[a] = [a_i]$. Dohromady, $\lim f(a_i) = [a_i] = [a] = f(a)$. □

Dokázali jsme, že těleso $\overline{\mathbb{T}}$ je rozšířením tělesa $\mathbb{T}$, které navíc zachovává existující limity v $\mathbb{T}$. Poslední a také nejdůležitější část teorie nám říká, že těleso $\overline{\mathbb{T}}$ splňuje Cauchyho podmínku konvergence řad (každá fundamentální posloupnost z $\overline{\mathbb{T}}$ má v $\overline{\mathbb{T}}$ svoji limitu). Tímto se ukáže, že další rozšiřování v předchozím významu není možné (tedy $\overline{\mathbb{T}} = \overline{\overline{\mathbb{T}}}$).

Věta 49 *Těleso $\overline{\mathbb{T}}$ splňuje Cauchyho podmínku konvergence řad (každá fundamentální posloupnost prvků z tělesa $\overline{\mathbb{T}}$ má v tělese $\overline{\mathbb{T}}$ limitu). Navíc $\overline{\mathbb{T}}$ je nejmenší uspořádané těleso splňující Cauchyho podmínku konvergence řad a obsahující těleso $\mathbb{T}$.*

Důkaz: Mějme posloupnost prvků $(\alpha_i) \in \mathbf{F}_{\overline{\mathbb{T}}}$. Proto každý prvek posloupnosti α_i je ve skutečnosti třídou $[a_{ij}]$, kde $(a_{ij})_{j\in\mathbb{N}}$ je fundamentální posloupnost v $\mathbb{T}$. V případě, že je posloupnost (α_i) od některého členu α_i konstantní, potom je zřejmě její limitou tato konstanta. Pokud posloupnost konstantní není, lze bez újmy na obecnosti předpokládat, že každé dva po sobě jdoucí prvky jsou různé (po sobě opakující se členy můžeme vynechat, přičemž se nezmění existence limity ani hodnota limity). Označme nyní $[\varepsilon_i] = |\alpha_i - \alpha_{i+1}|$. Platí tedy $0 < |\varepsilon_i|$. Navíc z fundamentálnosti posloupnosti (α_i) plyne, že pro každé $0 < \varepsilon$ existuje $n_0 \in \mathbb{N}$ takové, že pro všechna $p, q \in \mathbb{N}$ splňující $n_0 \leq n$ platí $|\alpha_p - \alpha_q| < \varepsilon$. A tedy také pro každé $n \in \mathbb{N}$ splňující $n_0 \leq n$ platí $|\varepsilon_n - 0| = |\alpha_n - \alpha_{n+1}| < \varepsilon$. Proto platí $0 = \lim \varepsilon_i$.

Jak bylo dokázáno ve Větě 48 i)

$$\lim_{j\to\infty} a_{ij} = [a_{ij}] = \alpha_i,$$

a proto pro každé $i \in \mathbb{N}$ (a odpovídající $0 < \varepsilon_i$) existuje $n_0 \in \mathbb{N}$ takové, že pro všechna $n \in \mathbb{N}$ splňující $n_0 \leq n$ platí $|a_{in} - \alpha_i| < \varepsilon_i$. Označme potom takovéto $b_i = a_{in}$ jako aproximující prvek posloupnosti α_i (a pro tento platí $|b_i - \alpha_i| < \varepsilon_i$).

Konečně budeme chtít dokázat, že $\lim \alpha_i = [b_i]$. Vezměme proto libovolné $0 < \varepsilon$. Protože (α_i) je fundamentální a protože $\lim \varepsilon_i = 0$, existují hodnoty $n_1, n_2 \in \mathbb{N}$ takové, že

$$|\alpha_p - \alpha_q| < \frac{\varepsilon}{3} \text{ pro všechna } n_1 \leq p, q$$

$$0 < \varepsilon_p < \frac{\varepsilon}{3} \text{ pro všechna } n_2 \leq p.$$

Označme proto $n_0 = \max\{n_1, n_2\}$. Nyní pro všechna $p, q \in \mathbb{N}$ splňující $n_0 \leq p, q$ platí

$$|b_p - \alpha_p|, |\alpha_p - \alpha_q|, |\alpha_q - b_q| < \frac{\varepsilon}{3},$$

a proto

$$|b_p - b_q| \leq |b_p - \alpha_p| + |\alpha_p - \alpha_q| + |\alpha_q - b_q| < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon.$$

Dokázali jsme proto, že posloupnost (b_i) je fundamentální, proto $[b_i] \in \overline{T}$. Protože ale $0 \leq |b_i - \alpha_i| < \varepsilon_i$ pro všechna $i \in \mathbb{N}$, platí také $0 \leq \lim |b_i - \alpha_i| \leq \lim \varepsilon_i = 0$. Proto $\lim(b_i - \alpha_i) = 0$ a konečně $\lim \alpha_i = \lim(\alpha_i - b_i + b_i) = \lim(\alpha_i - b_i) + \lim b_i = \lim b_i = [b_i]$.

Zbývá dokázat, že těleso je skutečně minimální a splňující Cauchyho podmínku a obsahující $\mathbb{T}$. Ovšem skutečnost $\lim a_i = [a_i]$ ukazuje, že každý prvek z $\overline{\mathbb{T}}$ je limitou některé posloupnosti z $\mathbb{T}$. Tedy těleso je minimální. □

Touto větou byla dokončena konstrukce tělesa splňující Cauchyho podmínku konvergence. Jak se ukázalo, každé komutativní uspořádané těleso může být vnořeno do tělesa splňující Cauchyho podmínku konvergence.

6.5 Těleso reálných čísel

Nyní dokončíme myšlenku kapitoly. Jelikož víme, že $\mathbb{Q}$ je uspořádané těleso podle kladné části $\mathbb{Q}^+$, můžeme toto těleso jednoznačně vnořit do tělesa $\overline{\mathbb{Q}}$, které splňuje Cauchyho podmínku konvergence. Toto těleso nazveme tělesem reálných čísel a budeme jej nadále značit $\mathbb{R}$.

Je třeba si uvědomit, že v libovolném archimedovsky uspořádaném tělese $\mathbb{T}$ existuje nad každou hodnotou přirozené číslo $n \in \mathbb{N}$. Triviálně lze matematickou indukcí ověřit také to, že pro všechna $n \in \mathbb{N}$ platí $n < 2^n$. Dohromady proto můžeme ke každé hodnotě tělesa $\mathbb{T}$ najít přirozené číslo 2^n, které je větší.

Snadno můžeme ověřit, že $0 < 2^{-n}$. Navíc jestliže $0 < \varepsilon$, potom existuje $n \in \mathbb{N}$ takové, že $\varepsilon^{-1} < 2^n$, a z monotonnosti násobení kladnou hodnotou dostáváme $2^{-n} = 2^{-n} \cdot \varepsilon^{-1} \cdot \varepsilon < 2^{-n} \cdot 2^n \cdot \varepsilon = \varepsilon$. Předchozí úvahy dokázaly následující lemma.

Lemma 17 *V každém archimedovsky uspořádaném tělese platí* $\lim 2^{-n} = 0$.

Věta 50 (O supremu) *Jestliže $\mathbb{T}$ je archimedovsky uspořádané těleso, potom má každá neprázdná, shora omezená podmnožina $A \subset \overline{\mathbb{T}}$ v tělese $\overline{\mathbb{T}}$ supremum.*

Důkaz: Mějme archimedovské těleso $\mathbb{T}$ a neprázdnou, shora omezenou množinu $A \subseteq \mathbb{T}$. Z Věty 28 víme, že těleso racionálních čísel $\mathbb{Q}$ může být vnořeno do každého uspořádaného tělesa (tedy i do tělesa $\mathbb{T}$). Protože $\mathbb{T}$ je archimedovské těleso a A je shora omezená množina, existuje horní závora $n \in \mathbb{N}$ množiny A, tj. pro libovolné $x \in A$ platí $x \leq n$ (horní závora existuje, protože je množina A omezená a současně nad touto závorou musí existovat přirozené číslo, což plyne z archimedovskosti).

Existuje také celé číslo $m \in \mathbb{Z}$ takové, že z není horní závorou množiny A (toto číslo zkonstruujeme tak, že vezmeme libovolné $x \in A$ a pomocí archimedovskosti najdeme $k \in \mathbb{N}$ splňující $-x < k$; $-k$ je potom hledané celé číslo m).

Dokázali jsme, že existují $m, n \in \mathbb{Z}$ takové, že m není horní závorou a n je horní závorou A. Nyní pro libovolné $i \in \mathbb{N}$ definujme množinu:

$$M_i = \left\{ \frac{h}{2^i} \mid h \in \mathbb{Z} \text{ a současně } m \leq \frac{h}{2^i} \leq n \right\}.$$

Snadno můžeme ověřit, že $m, n \in M_i$ (pro každé $i \in \mathbb{N}$), protože $m = \frac{2^i m}{2^i}$ a $n = \frac{2^i n}{2^i}$. Současně také vidíme, že všechny množiny M_i jsou konečné. Proto lze korektně definovat posloupnost (a_i) takovou, že a_i je nejmenší prvek z M_i, jenž je současně horní závorou množiny A (takovýto prvek existuje, proto že $n \in M_i$ je horní závora a M_i je konečná).

Dokážeme, že posloupnost (a_i) je fundamentální. Jistě platí následující řetězec inkluzí $M_1 \subset M_2 \subset \cdots \subset M_i \subset \cdots$ (protože $\frac{h}{2^i} = \frac{2h}{2^{i+1}}$). Z tohoto nutně plyne, že $a_1 \geq a_2 \geq \cdots \geq a_i \geq \cdots$, jinak řečeno, posloupnost (a_i) je nerostoucí.

Mějme nyní libovolné $0 < \varepsilon$. Z Lemmatu 17 plyne existence $n_0 \in \mathbb{N}$ takového, že $0 < \frac{1}{2^{n_0}} \leq \varepsilon$. Ze způsobu zavedení posloupnosti (a_i) plyne, že $a_i - \frac{1}{2^i} \in M_i$, a také proto $a_i - \frac{1}{2^{n_0}}$ není horní závora množiny A. Proto pro všechna $p, q \in \mathbb{N}$ splňující $n_0 \leq p, q$

platí $a_{n_0} - \frac{1}{2^{n_0}} < a_p \leq a_{n_0}$ a současně $a_{n_0} - \frac{1}{2^{n_0}} < a_q \leq a_{n_0}$. Z těchto nerovností ihned dostáváme $|a_p - a_q| < \frac{1}{2^{n_0}} \leq \varepsilon$. Dokázali jsme proto, že posloupnost (a_i) je fundamentální. Věta 49 říká, že těleso $\overline{\mathbb{T}}$ splňuje Cauchyho podmínku konvergence řad, a proto existuje $a = \lim a_i$.

Nyní dokážeme, že $a = \sup A$. Jestliže existuje horní závora $x \in \overline{\mathbb{T}}$ taková, že $x < a$, potom existuje $n \in \mathbb{N}$ takové, že $0 < \frac{1}{2^n} < a - x$. Posloupnost (a_i) je klesající, platí proto $a \leq a_n$ a také $0 < \frac{1}{2^n} < a - x \leq a_n - x$. Z této nerovnosti ihned dostáváme $x \leq a_n - \frac{1}{2^n}$. Proto také prvek $a_n - \frac{1}{2^n}$ je dolní závorou, což je spor (protože $a_n - \frac{1}{2^n} \in M_n$ a současně a_n je nejmenší dolní závora z množiny M_n). □

Věta 51 *Každé archimedovsky uspořádané těleso $\mathbb{T}$ lze vnořit do tělesa reálných čísel, přičemž $\overline{\mathbb{T}} = \mathbb{R}$.*

Důkaz: Vezměme libovolné archimedovsky uspořádané těleso $\mathbb{T}$. Podle Věty 28 platí $\mathbb{Q} \subseteq \mathbb{T}$. V důkazu Věty 50 jsme zkonstruovali pro libovolnou neprázdnou, shora omezenou množinu $A \subset \overline{\mathbb{T}}$ posloupnost $(a_i) \in \mathbf{F}_{\mathbb{Q}}$ takovou, že $\sup A = \lim a_i$. Vezmeme-li libovolný prvek $x \in \overline{\mathbb{T}}$, potom tedy existuje fundamentální posloupnost racionálních čísel (a_i) taková, že $x = \sup\{x\} = \lim a_i = [a_i] \in \mathbb{R}$ (toto platí vzhledem k Větě 50). Proto $\mathbb{T} \subseteq \overline{\mathbb{T}} \subseteq \mathbb{R}$.

Protože $\mathbb{Q} \subseteq \mathbb{T}$, platí také inkluze $\mathbb{R} = \overline{\mathbb{Q}} \subseteq \overline{\mathbb{T}}$. □

Jestliže těleso $\mathbb{T}$ není archimedovské, potom existuje horní závora množiny $\mathbb{Q} \subset \mathbb{T}$. Dokážeme, že neexistuje $s = \sup \mathbb{Q}$. Pokud by takové supremum existovalo, potom vzhledem k rovnosti $2\mathbb{Q} = \mathbb{Q}$, platí $s < 2s = 2 \cdot \sup \mathbb{Q} = \sup 2\mathbb{Q} = \sup \mathbb{Q} = s$ (což je spor). Dokázali jsme i následující tvrzení:

Věta 52 *Věta o supremu platí jenom v archimedovských tělesech.*

Teorii můžeme uzavřít následující větou, která charakterizuje těleso reálných čísel jako univerzální strukturu.

Věta 53 *Každé těleso, v němž platí věta o supremu, je izomorfní s reálnými čísly.*

Důkaz: Jestliže v tělese platí věta u supremu, je podle Věty 52 archimedovské a podle Věty 51 jej lze izomorfně vnořit do reálných čísel ($\mathbb{T} \subseteq \mathbb{R}$). Dokážeme, že žádné podtěleso reálných čísel nesplňuje větu o supremu. Jestliže $x \in \mathbb{R}$, potom z důkazu Věty 50 máme nerostoucí posloupnost racionálních čísel (a_i) splňující $\lim a_i = -x$. Potom také platí $x = \lim -a_i$, kde $(-a_i)$ je neklesající posloupnost racionálních čísel. Jistě platí, že $\sup\{-a_i \mid i \in \mathbb{Q}\} = \lim -a_i = x$. Dokázali jsem, že každý prvek $x \in \mathbb{R}$ je supremem prvků z $\mathbb{Q}$. Protože každé uspořádané těleso $\mathbb{T}$ obsahuje těleso $\mathbb{Q}$, musí z předpokladu existence suprem platit $\mathbb{R} \subseteq \mathbb{T}$. □

Předcházející věta nám mimo jiné dokazuje, že obě prezentovaná pojetí reálných čísel (konstruovaná pomocí Dedekindových řezů nebo pomocí fundamentálních posloupností) jsou navzájem ekvivalentní. Vzniklé struktury jsou izomorfní, a liší se proto pouze v označení prvků.

Kapitola 7

Komplexní čísla

V předchozích kapitolách se nám podařilo zavést základní číselné obory. Motivace k tomuto zavádění se zdá být jasná. Přirozená čísla nám představují informaci o množství jednotlivých prvků (předmětů, věcí, apod.). Vznikla abstrakcí informace o „počtu“ věcí v nějaké skupině od konkrétních předmětů. Zjednodušeně řečeno, lidé si uvědomili, že je jedno, zda-li počítáme ryby nebo ananasy. Úvaha jako taková je stejná, proto informaci o počtu oddělili od konkrétních předmětů a informaci o počtu abstrahovali do čísla.

Racionální čísla byla vytvořena k měření délek, ploch apod. Užíváme je tehdy, kdykoliv je potřeba dělit celek na díly. Pro praktický život je naprosto dostatečné kalkulovat množství v racionálních hodnotách, lépe řečeno, jinak to ani pořádně nejde (je dosti sporné předpokládat, že je někdo schopen pracovat s přesnou hodnotou reálného čísla, např. čísla π, obvykle v životě pracujeme s racionálním číslem, které je s jakousi dostatečnou přesností blízké dané hodnotě; například číslo π určené na několik desetinných míst).

Reálná čísla jsou proto již dosti abstraktním modelem, který je užitečný matematikům k rozvoji jiných teorií a není aplikovatelný přímo. Nejpřesnější je asi názor, že se v reálných číslech podařilo najít matematický model dokonalé „spojité“ přímky. Díky tomuto lze rozvíjet celou teorii limitního a diferenciálního počtu. Objevem reálných čísel mohli začít matematici bez dalších starostí začít pracovat s limitami, supremy a s jinými prostředky vyžadujícími spojitost. Na první pohled toto vypadá jako neužitečný detail, který jsme mohli přijmout jaksi samozřejmě. Je velmi důležité si uvědomit, že pravý opak je pravdou. Historie matematiky je plna omylů, které vycházejí z přirozené intuitivní představy (Zenónovy paradoxy apod.). Známe mnoho příkladů intuitivně přijatelných předpokladů vedoucích k značně paradoxním důsledkům[1]. Dokončená konstrukce reálných čísel dokazuje, že předpoklad spojitého tělesa je korektní a bezesporný. Konstrukce reálných čísel proto v důsledku vedla k rozvoji mnoha matematických teorií (teorie míry, teorie pravděpodobnosti apod.)

Zbývá se zamyslet nad motivací existence záporných čísel. Jestliže budeme přemýšlet libovolně dlouho, nic objektivně odpovídajícího záporným hodnotám nenajdeme. S celými čísly nás seznámili učitelé již brzy na základní škole ve věku, kdy jsme byli schopni představu přijmout bez podivu. Dlouhodobým užíváním záporných čísel se nám představa natolik zautomatizovala, že jsme si nevšimli toho, že záporná čísla nic nepředstavují. Ne-

[1] Dodnes se vedou značné diskuze o přijatelnosti axiomu výběru, který se zdá být přirozený, ale některé jeho netriviální důsledky je někdy značně těžké přijmout (například Tarského-Banachova věta o „hrášku a sluníčku“, která říká, že libovolnou kouli můžeme rozdělit na konečně mnoho částí, z kterých lze poskládat dvě stejné koule, jako byla původní)

existuje skupina předmětů se zápornou velikostí. Představme si zápornou skupinu mínus tří koní, která potká tři koně skutečné. Podle aritmetiky by v okamžiku všichni beze stopy zmizeli.

Ani představa dluhu nic nového nepřináší. Jestliže si zajdeme do banky půjčit nějakou sumu peněz, nevznikne někde v hloubi budovy v trezoru skupina antibankovek (dluh se nezhmotňuje). Dluh nemá reálnou podobu. Jedná se o pocit, který je tím intenzivnější, čím blíže je nám exekutor, ale stále jde jen o pocit. Zamyslíme-li se nad smyslem pojmu dluh, ve skutečnosti zjistíme, že je stejně abstraktní jako záporná čísla. Dluh je stále představa ve společném vědomí lidí (v reálném životě spojená se závazkem; naproti tomu záporná čísla mohou existovat i bez toho, abychom měli deprese a vznikaly nám žaludeční vředy)[2].

Připustíme-li skutečnost, že už jednou v životě jsme přijali matematický model, který nelze dost dobře realizovat v životě (realizovat neznamená totéž co zužitkovat), nebude nás již tolik trápit, že se nyní budeme pokoušet o totéž znova. Začněme proto přemýšlet o komplexních číslech. Až příliš často se vznik komplexních čísel motivuje tak, že „komplexní čísla zavádíme proto, abychom mohli odmocňovat záporná čísla“. Bohužel už málokdo se trápí otázkou: Proč někdo potřebuje odmocňovat záporná čísla? Samo o sobě toto vypadá tak, že matematici zavedli komplexní čísla z dlouhé chvíle. Ukážeme si, že tomu bylo jinak.

Prvním impulsem k tomu, aby lidé začali uvažovat nad odmocninou ze záporných čísel vzešel z Cardanových vzorců[3]. Jedná se o vzorce, pomocí kterých můžeme najít kořeny kubické rovnice $ax^3 + bx^2 + cx + d = 0$. Brzy si matematici všimli, že korektně odvozené vzorce jsou v případě, kdy má rovnice tři reálné řešení, nepoužitelné, protože po dosazení musíme najít druhou odmocninu se záporného čísla (například rovnice $x^3-6x^2+11x-6 = 0$ má kořeny $x_0 = 1$, $x_1 = 2$ a $x_3 = 3$; zkuste k výpočtu užít Cardanovy vzorce). Prvotní pokusy se snažily najít chybu ve vzorcích. Přesto se později ukázalo, že úvahy musíme směřovat jiným směrem. Cardáno totiž, aniž si to uvědomil, pracoval ve svém důkazu s předpokladem, že lze každé číslo odmocnit.

Od Cardánových vzorců vedla ke komplexním číslům dlouhá cesta. Až Carl Friedrich Gauss teorii komplexních čísel završil svou větou, které se do dneška přezdívá „Hlavní věta algebry“. Komplexní čísla nezůstaly pouze „metodou“ řešení některých matematických úloh, ale postupně se ukázalo, že také hrají nenahraditelnou úlohu v mnohých fyzikálních teoriích.

Přestože je teorie komplexních čísel značně vzdálena přirozenému vnímání světa, význam v odborných aplikacích je již dnes takový, že alespoň základní znalost komplexních

[2]Na stejné téma existuje vtip vystihující přemýšlení matematiků. Stojí tři vědci – biolog, fyzik a matematik – před budovou, do které vešli dva lidé a z níž vyšli tři. Biolog má ihned jasno, lidé se rozmnožili. Fyzik po chvíli přemýšlení dojde k závěru, že se jedná o chybu v měření. Matematik o chvíli později zajásá: „Už vím, co se stalo. Za chvíli vejde do budovy ještě jeden člověk a nebude tam nikdo.“

[3]Původní tvar vypadal tak, že

$$x = \sqrt[3]{\frac{-q}{2} + \sqrt[2]{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{-q}{2} - \sqrt[2]{\frac{q^2}{4} + \frac{p^3}{27}}},$$

kde $p = b - \frac{a^2}{3}$ a $q = c + \frac{2a^3+9ab}{27}$.

čísel je součástí už středoškolského vzdělávání.

Definice 19 *Množinu všech prvků ve tvaru $a + bi$, kde $a, b \in \mathbb{R}$, označme $\mathbb{C}$ a nazvěme komplexními čísly*[4] *(symbol i nazýváme komplexní jednotku). Na množině komplexních čísel zavadíme operace součtu a součinu následovně:*

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i,$$

$$(a_1 + b_1 i) \cdot (a_2 + b_2 i) = (a_1 \cdot a_2 - b_1 \cdot b_2) + (a_1 \cdot b_2 + a_2 \cdot b_1)i.$$

Definice může být motivována dvěma způsoby. Nejčastěji argumentujeme tím, že těleso $\mathbb{R}$ rozšiřujeme o hodnotu $\sqrt{-1}$, kterou značíme i. Platí tedy $i^2 = -1$. Z předpokladů (především z očekávané distributivity) plyne zavedení součtu a součinu.

Alternativně můžeme vzít množinu polynomů nad $\mathbb{R}$ s jedinou proměnnou i. Množina polynomů vzhledem ke klasickému sčítání a násobení tvoří komutativní okruh (viz [BlI, BlII]). Na tomto okruhu potom zavedeme kongruenci $\sim$ takovou, že polynomy $f(i)$ a $g(i)$ jsou ekvivalentní, jestliže polynom $f(i) - g(i)$ je dělitelný polynomem $i^2 + 1$ (důkaz toho, že zavedená relace je kongruencí, je totožný s důkazem rozkladu tělesa $\mathbb{Z}$ na třídy modulo n ve Větě 64). Potom vidíme, že platí $i^2 \sim -1$ (protože polynom $i^2 + 1$ dělí sám sebe), a proto i^n je ekvivalentní s jedním z prvků ± 1 nebo $\pm i$. Nyní lze ukázat, že každý polynom $a_n i^n + a_{n-1} i^{n-1} + \cdots + a_1 i + a_0$ je ekvivalentní s některým polynomem ve tvaru $a + bi$. Vzniklá struktura je proto izomorfní s námi definovanými komplexními čísly.

Věta 54 *Algebraická struktura $(\mathbb{C}, +, \cdot)$ je komutativní těleso obsahující těleso $(\mathbb{R}, +, \cdot)$.*

Důkaz: Operace sčítání je zřejmě komutativní a asociativní, přičemž nulovým prvkem je $0 + 0i$ a opačným prvkem k číslu $a + bi$ je číslo $(-a) + (-b)i$. Proto $(\mathbb{C}, +)$ je komutativní grupa.

Komutativita násobení je zřejmá a asociativitu stejně jako distributivitu lze snadno ověřit výpočtem (v případě, že přijmeme definici přes faktorizaci množiny polynomů, plyne asociativita a distributivita přímo z věty o faktorovém okruhu). Jednotkový prvek je $1 + 0i$.

Zbývá dokázat, že ke každému nenulovému číslu existuje inverzní prvek. Dokážeme, že

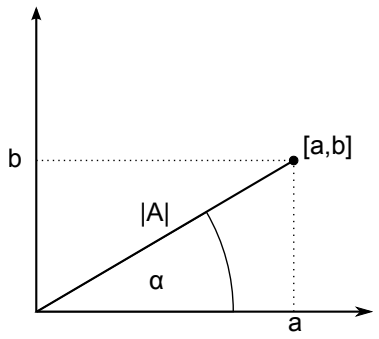
$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i.$$

Protože $a + bi$ je nenulový prvek platí, že $a \neq 0$ nebo $b \neq 0$, a tedy také $a^2 + b^2 \neq 0$. Nyní platí:

$$(a - bi) \cdot \left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i \right) = \frac{a^2 + b^2}{a^2 + b^2} - \frac{ab - ab}{a^2 + b^2} i = 1 + 0i.$$

Nyní zbývá dokázat, že těleso reálných čísel je podtělesem čísel komplexních. Hledané vnoření $f : \mathbb{R} \longrightarrow \mathbb{C}$ je definováno $f(x) = x + 0i$. □

[4] Někdy se množina komplexních čísel chápe jako množina $\mathbb{R}^2$. Je určitě jedno, zda-li uspořádanou dvojici značíme (a, b), nebo $a + bi$.



Obrázek 7.1 Znázornění komplexního čísla v rovině.

Stejně tak jako reálná čísla znázorňujeme na přímku, je obvyklé znázorňovat těleso komplexních čísel na rovinou. Komplexní číslo $a + bi$ se potom zobrazí na bod se souřadnicemi $[a, b]$ (rovina představující komplexní čísla se obvykle nazývá *Gaussova rovinou*). Tento způsob zobrazení komplexního čísla inspiruje k zápisu pomocí polárních souřadnic, kterému říkáme goniometrický tvar komplexního čísla.

Jestliže máme libovolné komplexní číslo $a + bi = A \in \mathbb{C}$, potom definujeme jeho *absolutní hodnotu*[5] $|A| = \sqrt{a^2 + b^2}$ (v Gaussově rovině představuje vzdálenost obrazu čísla od počátku souřadnicového systému). Číslo *komplexně sdružené* definujeme jako číslo ve tvaru $\overline{A} = a - bi$. Snadno nyní ověříme, že platí

$$\sqrt{A \cdot \overline{A}} = \sqrt{(a + bi)(a - bi)} = \sqrt{a^2 + b^2} = |A|. \qquad (*)$$

Díky tomuto vztahu můžeme vyslovit:

Lemma 18 *Jestliže $A, B \in \mathbb{C}$, potom platí $\overline{A} \cdot \overline{B} = \overline{A \cdot B}$ a $|A| \cdot |B| = |A \cdot B|$.*

Důkaz: Jestliže $A = a_1 + b_1 i$ a $B = a_2 + b_2 i$, potom platí,

$$\overline{A \cdot B} = \overline{(a_1 + b_1 i) \cdot (a_2 + b_2 i)} = \overline{(a_1 \cdot a_2 - b_1 \cdot b_2) + (a_1 \cdot b_2 + a_2 \cdot b_1)i} =$$

$$(a_1 \cdot a_2 - b_1 \cdot b_2) - (a_1 \cdot b_2 + a_2 \cdot b_1)i = (a_1 - b_1 i) \cdot (a_2 - b_2)i = \overline{A} \cdot \overline{B}.$$

Navíc také platí $|A|^2 \cdot |B|^2 = A \cdot \overline{A} \cdot B \cdot \overline{B} = (A \cdot B) \cdot (\overline{A \cdot B}) = |A \cdot B|^2$. □

Jestliže označíme α úhel, který svírá kladná poloosa x s orientovanou polopřímkou začínající počátkem a jdoucí přes bod $[a, b]$, který vizualizuje číslo A (viz Obrázek 7.1), potom vidíme, že $\cos \alpha = \frac{a}{|A|}$ a $\sin \alpha = \frac{b}{|A|}$. V tomto okamžiku můžeme upravit

$$A = a + bi = |A| \cos \alpha + i|A| \sin \alpha = |A|(\cos \alpha + i \sin \alpha.)$$

[5] Odmocninu a její existenci jsme v předchozích částech neodvozovali, přesto její jednoznačnou existenci a definici nalezne čtenář v 9. kapitole. Pro správné pochopení je naprosto dostatečné správné intuitivní vnímání pojmů. Celkově v kapitole komplexních čísel budeme užívat aparát, který je předmětem jiných matematických disciplín. Je tomu tak proto, abychom ukázali nejdůležitější vlastnosti komplexních čísel v širším kontextu.

Výrazu na pravé straně říkáme *goniometrický tvar čísla A*. Význam tohoto tvaru pro aritmetiku nám ukáže následující Moiverova[6] věta.

Věta 55 *Jestliže $A, B \in \mathbb{C}$ jsou komplexní čísla v goniometrickém tvaru $A = |A|(\cos\alpha + i\sin\alpha)$ a $B = |B|(\cos\beta + i\sin\beta)$, potom platí:*

(i) $A \cdot B = |A \cdot B|(\cos(\alpha+\beta) + i\sin(\alpha+\beta))$,

(ii) $A^n = |A|^n(\cos n\alpha + i\sin n\alpha)$ *pro libovolné* $n \in \mathbb{N}$.

Důkaz: S ohledem na vzorce cosinu a sinu součtu úhlů a vzhledem k předchozímu lematu můžeme počítat:

$$\begin{aligned} A \cdot B &= |A|(\cos\alpha + i\sin\alpha)|B|(\cos\beta + i\sin\beta) = \\ &= |A| \cdot |B|((\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \sin\beta\cos\alpha)) = \\ &= |A \cdot B|(\cos(\alpha+\beta) + i\sin(\alpha+\beta)). \end{aligned}$$

Druhou část věty dokážeme snadno z dokázané části matematickou indukcí. □

Moiverovu větu užíváme k řešení binomických rovnic (tedy k nalezení všech komplexních n-tých odmocnin z komplexního čísla). Pomocí této věty také můžeme snadno nalézt goniometrický tvar inverzního čísla k nenulovému komplexnímu číslu, a to tak, že jestliže $A = |A|(\cos\alpha + i\sin\alpha)$, potom platí $A^{-1} = \frac{1}{|A|}(\cos(-\alpha) + i\sin(-\alpha))$. Správnost vztahu můžeme ověřit pomocí předchozí věty součinem:

$$A \cdot A^{-1} = |A|(\cos\alpha + i\sin\alpha)\frac{1}{|A|}(\cos(-\alpha) + i\sin(-\alpha)) = \cos 0 + i\sin 0 = 1 - 0i.$$

Dalším navazujícím tématem je také takzvaný *Eulerův vzorec*, který definuji komplexní mocninu kladného reálného čísla. Jedním ze způsobů jeho odvození je užitá Taylorova rozvoje (přesněji MacLaurinovy řady) funkce. Připomeňme, že platí:

$$f(x) = \sum_{n=0}^{\infty} \frac{1}{n!} f^{(n)}(0)x^n.$$

MacLaurinovy řady pro funkce $\sin x$, $\cos x$, a e^x vypadají následovně:

$$e^x = 1 + x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \frac{1}{4!}x^4 + \frac{1}{5!}x^5 + \cdots,$$

$$\cos x = 1 - \frac{1}{2!}x^2 + \frac{1}{4!}x^4 - \frac{1}{6!}x^6 + \frac{1}{8!}x^8 - \cdots,$$

$$\sin x = x - \frac{1}{3!}x^3 + \frac{1}{5!}x^5 - \frac{1}{7!}x^7 + \frac{1}{9!}x^9 - \cdots.$$

[6] Moiverova věta je druhá část následující věty.

Dosadíme-li proměnnou x v rozvoji funkce e^x hodnotu $i \cdot \alpha$, dostaneme rovnost

$$\begin{aligned} e^{\alpha \cdot i} &= 1 + (\alpha \cdot i) + \frac{1}{2!}(\alpha \cdot i)^2 + \frac{1}{3!}(\alpha \cdot i)^3 + \frac{1}{4!}(\alpha \cdot i)^4 + \cdots = \\ &= (1 - \frac{1}{2!}\alpha^2 + \frac{1}{4!}\alpha^4 - \cdots) + i \cdot (\alpha - \frac{1}{3!}\alpha^3 + \frac{1}{5!}\alpha^5 - \frac{1}{7!}\alpha^7 - \cdots) = \\ &= \cos\alpha + i \cdot \sin\alpha. \end{aligned}$$

Odvozený vztah $e^{\alpha \cdot i} = \cos\alpha + i\sin\alpha$ se nazývá Eulerův vzorec. Využít jej můžeme mimo jiné k úpravě goniometrického tvaru komplexního čísla na tvar, který se nazývá *exponenciální tvar komplexního čísla*.

$$A = |A|(\cos\alpha + i\sin\alpha) = |A|e^{\alpha \cdot i}.$$

Věta 55, která popisuje násobení komplexních čísel v goniometrickém tvaru (resp. Moiverova věta) se nám v kontextu s exponenciálním tvarem komplexního čísla mění na větu o komplexní mocnině. Jestliže $A = |A|e^{\alpha \cdot i}$ a $B = |B|e^{\beta \cdot i}$, potom

$$A \cdot B = |A|e^{\alpha \cdot i} \cdot |B|e^{\beta \cdot i} = |A \cdot B|e^{\alpha \cdot i + \beta \cdot i} = |A \cdot B|e^{(\alpha+\beta) \cdot i}$$

a také navíc

$$A^n = (|A|e^{\alpha \cdot i})^n = |A|^n (e^{\alpha \cdot i})^n = |A|^n e^{n \cdot \alpha \cdot i}.$$

Na závěr ještě připomeneme historicky mimořádně důležitou větu, které se dodnes přezdívá Základní věta algebry. Tato věta nakonec ukázala, že hlavní problém, který vedl k zavedení komplexních čísel – tedy problém řešení algebraických rovnic, byl zavedením komplexních čísel vyřešen. Větu uvedeme bez patřičného důkazu, který čtenář nalezne například zde [**?**].

Věta 56 *Každý polynom $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ nad komplexními čísly $\mathbb{C}$ stupně alespoň 1 má v množině komplexních čísel alespoň jeden kořen x_0 (tedy platí $f(x_0) = 0$).*

Důsledkem je, že každý polynom stupně n má právě n kořenů a tedy $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ lze psát ve tvaru $f(x) = a(x - x_1)\cdots(x - x_n)$, kde $x_1, \cdots x_n \in \mathbb{C}$ jsou právě kořeny polynomu (až na násobnost řešení).

Kapitola 8

Hyperkomplexní čísla

Komplexní čísla nejsou posledním existujícím číselným oborem. Teoretická matematika zná ještě minimálně dvě rozšíření komplexních čísel na takzvaná hyperkomplexní čísla. Myšlenkou tohoto rozšiřování je opakování principu zdvojování, který jsme poprvé uplatnili při konstrukci komplexních čísel.

Prvním problémem všech hyperkomplexních struktur je jejich užitečnost a aplikovatelnost. Přestože jsou hyperkomplexní čísla úzce spojena s fyzikálními strukturami (např. částicové fyziky), je sporné, zda-li tyto struktury jsou opravdu v daných aplikacích nezbytné nebo nenahraditelné. Jejich vlastnosti a aplikace jsou ovšem neustále velmi intenzivně studovány, a lze proto očekávat, že naše porozumění hyperkomplexním číslům bude přinášet stále se zvětšující význam této teorie.

Cílem této kapitole je pouze ukázat čtenáři existenci takovýchto struktur. K hlubšími studiu doporučujeme odbornou literaturu (např. [KaSo]).

Následující úvaha byla poprvé prezentována irským matematikem Williamem Rowanem Hamiltonem v roce 1843. Všimněme se, že komplexní čísla vznikla zdvojením reálných čísel do tvaru $a+bi$, kde $a, b \in \mathbb{R}$. Pokusíme se tento postup zopakovat. Představme si, že zavedeme čísla ve tvaru $A+Bj$, kde $A, B \in \mathbb{C}$ a j představuje novou imaginární jednotku (platí proto $j^2 = -1$). Jestliže $A = a + bi$ a $B = c + di$, potom dostáváme tvar

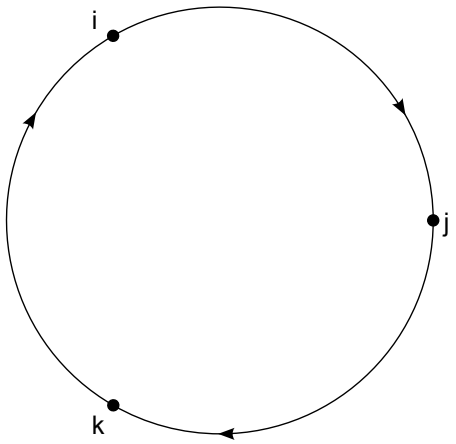
$$A + Bk = (a + bi) + (c + di)j = a + bi + cj + dij,$$

kde $a, b, c, d \in \mathbb{R}$. Zbývá tedy dořešit, co je vlastně hodnotu $i \cdot j$. Hamilton potom označil součin imaginárních jednotek $i \cdot j$ jako novou imaginární jednotku k. Čísla v tomto tvaru se nazývají (Hamiltonovy) kvaterniony, přičemž množinu všech kvaternionů značíme $\mathbb{H}$. Shrneme tedy prvky ve tvaru:

$$a + bi + cj + dk,$$

kde $a, b, c, d \in \mathbb{R}$ a i, j a k jsou imaginární jednotky nazýváme kvaterniony. Součet kvaternionů je zřejmý (probíhá po složkách, stejně jako u komplexních čísel). Abychom mohli zavést součin, musíme znát součiny imaginárních jednotek. Tyto jsou definovány následovně:

$\cdot$	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1



Obrázek 8.1 Násobení komplexních jednotek u kvaternionů.

Tato definice je inspirována následujícím „kruhovým“ schématem (viz Obrázek 8.1; při násobení proti směru šipky je výsledek záporný), kdy násobení po směru orientace dává ve výsledku následující člen a násobení proti směru dává prvek opačný (záporný). Výsledkem je, že platí následující věta:

Věta 57 *Algebraická struktura kvaternionů* $(\mathbb{H}, +, \cdot)$ *tvoří nekomutativní těleso.*

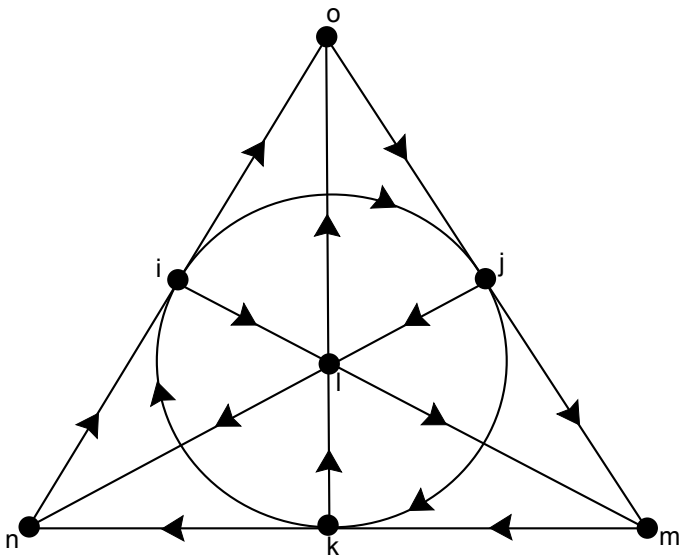
Ještě jedním opakováním principu zdvojení dostaneme prvky ve tvaru:

$$a + bi + cj + dk + +el + fm + gn + ho,$$

kde $a, b, c, d, e, f, g, h \in \mathbb{R}$, a navíc i, j, k, l, m, n, a o jsou imaginární jednotky (tedy jejich druhá mocnina je rovná -1). Takováto čísla nazýváme *oktoniony* a množinu oktonionů značíme $\mathbb{O}$. Operace sčítání oktonionů probíhá po složkách a násobení je definováno následující tabulkou (resp. schématem z Obrázku 8.2).

$\cdot$	i	j	k	l	m	n	o
i	-1	k	$-j$	m	$-l$	$-o$	n
j	$-k$	-1	i	n	o	l	$-m$
k	j	$-i$	-1	o	$-n$	m	$-l$
l	$-m$	$-n$	$-o$	-1	i	j	k
m	l	$-o$	n	$-i$	-1	$-k$	j
n	o	$-l$	$-m$	$-j$	k	-1	$-i$
o	$-n$	m	l	$-k$	$-j$	i	-1

Výsledná struktura již nemá asociativní ani komutativní násobení, ale pouze alternativní (tj. $(x \cdot y) \cdot y = x \cdot (y \cdot y)$). Ve struktuře lze zavést mocniny a dělení nenulovým



Obrázek 8.2 Násobení komplexních jednotek u oktonionů.

prvkem. Stejně jako všechny dosud zkoumané číselné struktury i oktoniony jsou v jistém smyslu univerzální strukturou, platí totiž, že všechny tzv. Hurwiczovy algebry (normované algebry s dělením) nad číselnými tělesy jsou isomorfní s jednou ze struktur $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ nebo $\mathbb{O}$.

Připomeňme, že právě oktoniony souvisí s Liovými grupami, které představují významné fyzikální struktury. Oktoniony přitahují stále větší pozornost teoretických fyziků, kteří v této struktuře hledají univerzální částicovou teorii.

Kapitola 9

Mocniny

V následující kapitole si zavedeme základní typy mocnin a dokážeme některé souvislosti. Mocninu definujeme následovně:

Definice 20 *Mějme pologrupu* $\mathbf{G} = (G, \cdot)$*. Potom definujeme pro libovolné* $x \in G$ *mocninu* x^n *matematickou indukcí tak, že* $x^1 = x$ *a* $x^{n+1} = x \cdot x^n$*.*

Nejprve si uvědomme, že matematickou indukcí (přesněji předpokladem pátého Peanova axiomu) lze přímo dokázat, že mocnina je pro libovolné $n \in \mathbb{N}$ korektně definována. V případě, že v pologrupě užíváme místo multiplikativní symboliky $\cdot$ symboliku aditivní $+$, potom se mocnina obvykle značí $n \times x$. Dokážeme si první větu.

Věta 58 *Jestliže* $\mathbf{G} = (G, \cdot)$ *je pologrupa, potom pro libovolné prvky* $x, y \in G$ *a libovolná čísla* $m, n \in \mathbb{N}$ *platí*[1]*:*

i) $x^m \cdot x^n = x^{m+n}$,

ii) $(x^m)^n = x^{m \cdot n}$,

iii) jestliže existuje neutrální prvek e*, potom* $e^n = e$*,*

iv) jestliže je pologrupa komutativní, potom platí také $(x \cdot y)^n = x^n \cdot y^n$*.*

Důkaz: ad i) Podle definic součinu platí $x^1 \cdot x^n = x \cdot x^n = x^{n+1}$. Nechť nyní $x^m \cdot x^n = x^{m+n}$ pro některá pevně zvolená čísla $m, n \in \mathbb{N}$. Potom platí podle definice mocniny $x^{m+1} \cdot x^n = x \cdot x^m \cdot x^n = x \cdot x^{m+n} = x^{1+m+n}$. Z principu matematické indukce plyne tvrzení.

ad ii) Z definice mocniny dostáváme $(x^m)^1 = x^m = x^{1 \cdot m}$. Nechť nyní pro některá libovolná, ale pevně zvolená čísla platí $(x^m)^n = x^{m \cdot n}$. Potom vzhledem k dokázané části věty platí $(x^m)^{n+1} = x^m \cdot (x^m)^n = x^m \cdot x^{n \cdot m} = x^{m+m \cdot n} = x^{(n+1) \cdot m}$. Vzhledem k principu matematické indukce je věta dokázána.

ad iii) Jistě platí $e^1 = e$. Jestliže $e^n = e$, potom protože e je neutrální prvek, platí také $e^{n+1} = e \cdot e^n = e^n = e \cdot e = e$. Z principu matematické indukce plyne tato část věty.

ad iv) Z definice mocniny plyne $(x \cdot y)^1 = x \cdot y = x^1 \cdot y^1$. Předpokládejme, že platí navíc $(x \cdot y)^n = x^n \cdot y^n$. Nyní vzhledem k definici mocniny a vzhledem k předpokládané komutativitě můžeme počítat $(x \cdot y)^{n+1} = (x \cdot y) \cdot (x \cdot y)^n = x \cdot y \cdot x^n \cdot y^n = x \cdot x^n \cdot y \cdot y^n = x^{n+1} \cdot y^{n+1}$. Z principu matematické indukce plyne tvrzení. □

[1] Všimněte si, jak vypadají následující výroky přepsané do aditivní symboliky. Například *i)* $m \times x + n \times x = (m + n) \times x$, *ii)* $m \times (n \times x) = (m \cdot n) \times x$ apod.

Lemma 19 *Jestliže* $\mathbf{G} = (G, \cdot)$ *je pologrupa s jednotkovým prvkem. Nechť k některému prvku* $x \in G$ *existuje inverzní prvek* x^{-1}*. Potom pro libovolné* $n \in \mathbb{N}$ *platí, že* $(x^{-1})^n = (x^n)^{-1}$.

Důkaz: Tvrzení dokážeme matematickou indukcí. Nejprve $(x^1)^{-1} = x^{-1} = (x^{-1})^1$. Předpokládejme proto nyní, že platí pro některé libovolné, ale pevně zvolené $n \in \mathbb{N}$ rovnost $(x^n)^{-1} = (x^{-1})^n$. Potom také dostaneme (s ohledem na Lemma 1(iii)) $(x^{-1})^{n+1} = x^{-1} \cdot (x^{-1})^n = x^{-1} \cdot (x^n)^{-1} = (x \cdot x^n)^{-1} = (x^{n+1})^{-1}$. Lemma vyplývá z principu matematické indukce. □

Definice 21 *Mějme grupu* $\mathbf{G} = (G, \cdot)$*. Potom pro* $n \in \mathbb{N}$ *je definovaná mocnina v Definici 20 pro nulu platí* $x^0 = e$*, kde* e *je neutrální prvek. Jestliže je prvek* $n \in \mathbb{Z}$ *záporný (tedy* $-n \in \mathbb{N}$*), potom definujeme mocninu* $x^n = (x^{-1})^{-n}$*. Vzhledem k Větě 24 máme jednoznačně definováno mocninu* x^z *pro libovolné* $z \in \mathbb{Z}$.

Věta 59 *Jestliže* $\mathbf{G} = (G, \cdot)$ *je grupa, potom pro libovolné prvky* $x, y \in G$ *a libovolná čísla* $m, n \in \mathbb{Z}$ *platí:*

i) $x^m \cdot x^n = x^{m+n}$,

ii) $(x^m)^n = x^{m \cdot n}$,

iii) pro neutrální prvek e *platí* $e^n = e$,

iv) jestliže je grupa komutativní, potom platí také $(x \cdot y)^n = x^n \cdot y^n$.

Důkaz: V důkazu celé věty budeme velmi intenzivně využívat Věty 58, tedy skutečnosti, že tato věta je pro přirozené čísla dokázána.

i) Předpokládejme, že $m, n, \in \mathbb{Z}$. Pro čísla $m, n \in \mathbb{N}$ je již věta dokázaná. Jestliže $m = 0$, potom $x^0 \cdot x^n = e \cdot x^n = x^n = x^{0+n}$ (analogicky pro případ $n = 0$). Jestliže $-m, -n \in \mathbb{N}$, a tedy také $-m - n = -(m + n) \in \mathbb{N}$, potom lze vzhledem k definici mocniny a předchozí větě počítat $x^m \cdot x^n = (x^{-1})^{-m} \cdot (x^{-1})^{-n} = (x^{-1})^{-m-n} = x^{m+n}$.

Konečně může nastat případ, kdy $-m, n \in \mathbb{N}$. Důkaz se zde rozpadá na tři možnosti. Nejprve $-m < n$, potom $n+m \in \mathbb{N}$ a platí $x^m \cdot x^n = (x^{-1})^{-m} \cdot x^n = (x^{-m})^{-1} \cdot x^{-m} \cdot x^{n+m} = x^{m+n}$ (toto plyne ze skutečnosti, že $-m, n+n \in \mathbb{N}$, a tedy podle Věty 58 $x^{-m} \cdot x^{n+m} = x^n$). Jestliže $-m = n$, potom $m + n = 0$, a tedy $x^m \cdot x^n = (x^{-m})^{-1} \cdot x^n = (x^n)^{-1} \cdot x^n = e = x^0 = x^{m+n}$. Konečně poslední možností je, že $-m > n$, kdy $-(m + n) \in \mathbb{N}$. Potom platí, že $x^m \cdot x^n = (x^{-1})^{-m} \cdot x^n = (x^{-1})^{-m-n} \cdot (x^{-1})^n \cdot x^n = x^{m+n} \cdot (x^n)^{-1} \cdot x^n = x^{m+n}$.

iii)Pro $n \in \mathbb{N}$ je tvrzení dokázáno ve Větě 58(iii). Pro $n = 0$ tvrzení ihned plyne z definice. Konečně, jestliže $-n \in \mathbb{N}$, potom $e^n = (e^{-1})^{-n} = e$.

ii) Tvrzení dokážeme analogicky jako v předchozím případě rozborem na jednotlivé případy. Jestliže $m, n \in \mathbb{N}$ je tvrzení totožné s Větou 58(ii). Pokud $m = 0$, potom vzhledem k dokázané části věty platí $(x^0)^n = e^n = e = x^0 = x^{0 \cdot n}$. Analogicky pro $n = 0$. V následujících částech budeme užívat Lemma 19 . Jestliže $-m, -n \in \mathbb{N}$, a tedy také $m \cdot n \in \mathbb{N}$, potom platí, že $(x^m)^n = (((x^{-1})^{-m})^{-1})^{-n} = (((x^{-1})^{-1})^{-m})^{-n} = (x^{-m})^{-n} =$

$x^{(-m)\cdot(-n)} = x^{m\cdot n}$. Konečně, jestliže $-m, n \in \mathbb{N}$, potom $-m \cdot n \in \mathbb{N}$, a proto také platí $(x^m)^n = ((x^{-1})^{-m})^n = (x^{-1})^{-m\cdot n} = x^{m\cdot n}$.

iv) Jestliže $n \in \mathbb{N}$, potom je tvrzení dokázáno ve Větě 58(iv). Pro $n = 0$ platí $(x\cdot y)^0 = e = e \cdot e = x^0 \cdot y^0$. Pokud $-n \in \mathbb{N}$, potom vzhledem ke komutativitě operace $\cdot$ a Větě 58 platí $(x \cdot y)^n = ((x \cdot y)^{-n})^{-1} = (x^{-n})^{-1} \cdot (y^{-n})^{-1} = x^n \cdot y^n$. □

9.1 Mocniny kladných reálných čísel

V jistém smyslu nejpodstatnější části mocnin je definice mocniny (a tedy i obecné odmocniny) na reálných číslech. Je již jedno, zda-li budeme pracovat s reálnými čísly konstruovanými Dedekindovými řezy nebo pomocí fundamentálních posloupností. V tomto okamžiku budeme reálná čísla vnímat jako uspořádanou strukturu $(\mathbb{R}, +, \cdot)$ s větou o supremu (a tedy i infimu). Připomeňme ještě, že těleso reálných čísel je archimedovské. Mějme libovolné kladné reálné číslo $x \in \mathbb{R}^+$. Dokážeme, že množina

$$\{y \in \mathbb{R}^+ \mid y^n \leq x\}$$

je neprázdná a shora omezená. V prvé řadě platí, že pro libovolné $x \in \mathbb{R}^+$ existuje $m \in \mathbb{N}$ takové, že platí $\frac{1}{x} < m \leq m^n$, a proto $(\frac{1}{m})^n = \frac{1}{m^n} < x$. Studovaná množina je neprázdná. Nyní budeme hledat horní závoru této množiny. Jestliže $0 < x \leq 1$, potom pro libovolné $y \in \mathbb{R}^+$ takové, že $y^n \leq x$ musí platit, že $y \leq 1$ (v opačném případě platí $x \leq 1 = 1^n < y^n$ což je spor). V tomto případě je horní závorou množiny číslo 1. Pokud $1 < x$, a $y^n < x$ potom $y \leq x$ (jinak $x \leq y$ dává $1 < y$, a tedy $y < y^n$, což dohromady dává $x < y^n$ – spor). Máme dokázáno, že výše určená množina má horní závoru (buďto 1, nebo x). V každém případě můžeme podle věty o supremu definovat:

Definice 22 *Jestliže $x \in \mathbb{R}^+$, potom pro $n \in \mathbb{N}$ definujeme*

$$\sqrt[n]{x} = \sup\{y \in \mathbb{R}^+ \mid y^n \leq x\}.$$

K tomu, abychom mohli vyslovit a dokázat základní tvrzení o mocninách, potřebujeme následující technické tvrzení.

Lemma 20 *Jestliže $n \in \mathbb{N}$ je takové, že $1 < n$, a nechť $x \in \mathbb{R}$ je takové, že $0 < x < 1$, potom $(1 - x)^n > 1 - nx$*

Důkaz: Lemma dokážeme matematickou indukcí. Pro $n = 2$ platí $(1-x)^2 = 1-2x+x^2 > 1 - 2x$. Předpokládejme nyní, že $(1 - x)^n > 1 - nx$. Potom lze počítat:

$$\begin{aligned}(1-x)^{n+1} &= (1-x)\cdot(1-x)^n > \\ &= (1-x)\cdot(1-nx) = \\ &= 1-(n+1)x+nx^2 > \\ &> 1-(n+1)x.\end{aligned}$$

□

Věta 60 *Mějme kladná reálná čísla $x, \alpha \in \mathbb{R}^+$ a přirozené číslo $n \in \mathbb{N}$ takové, že $2 \leq n$, potom platí:*

i) Jestliže $\alpha < x^n$, potom existuje $y \in \mathbb{R}^+; y < x$ splňující $\alpha < y^n$.

ii) Jestliže $x^n < \alpha$, potom existuje $y \in \mathbb{R}^+; x < y$ splňující $y^n < \alpha$.

Důkaz: i) Protože platí $\alpha < x^n$, potom $0 < \frac{\alpha}{x^n} < 1$. Z tohoto plyne, že $0 < 1 - \frac{\alpha}{x^n} < 1$, a proto také

$$0 < \frac{1}{n} \cdot \left(1 - \frac{\alpha}{x^n}\right) < \frac{1}{n} < 1.$$

Označíme si

$$y = x \cdot \left(1 - \frac{1}{n} \cdot \left(1 - \frac{\alpha}{x^n}\right)\right).$$

Protože opět

$$0 < 1 - \frac{1}{n} \cdot \left(1 - \frac{\alpha}{x^n}\right) < 1,$$

platí také $y < x$. Konečně užitím Lemmatu 20 dostáváme:

$$\begin{aligned} y^n &= \left(x \cdot \left(1 - \frac{1}{n} \cdot \left(1 - \frac{\alpha}{x^n}\right)\right)\right)^n = \\ &= x^n \cdot \left(1 - \frac{1}{n} \cdot \left(1 - \frac{\alpha}{x^n}\right)\right)^n > \\ &> x^n \cdot \left(1 - n \cdot \frac{1}{n} \cdot \left(1 - \frac{\alpha}{x^n}\right)\right) = \\ &= x^n \cdot \left(1 - \left(1 - \frac{\alpha}{x^n}\right)\right) = \\ &= x^n \cdot \frac{\alpha}{x^n} = \\ &= \alpha. \end{aligned}$$

ii) Jestliže $x^n < \alpha$, potom $\frac{1}{\alpha} < \frac{1}{x^n} = (\frac{1}{x})^n$. Podle dokázané části věty existuje $y < \frac{1}{x}$ takové, že $\frac{1}{\alpha} < y^n$. Nyní již je snadno vidět, že platí $x < \frac{1}{y}$ a současně $(\frac{1}{y})^n = \frac{1}{y^n} < \alpha$. Hledaná hodnota je proto $\frac{1}{y}$. □

Nyní již můžeme vyslovit a především dokázat známá tvrzení, která u odmocnin automaticky očekáváme a dobře známe.

Věta 61 *Nechť $n \in \mathbb{N}$ a $x \in \mathbb{R}^+$, potom číslo $\sqrt[n]{x}$ je jediné kladné reálné číslo, jehož n-tou mocninou je právě číslo x.*

Důkaz: Dokážeme, že pro kladná reálná čísla platí $x \leq y$ tehdy a jen tehdy, jestliže $x^n \leq y^n$. Implikace zleva doprava plyne snadno z monotónnosti násobení kladným číslem. Jestliže $x^n \leq y^n$ platí tak, že $x \not\leq y$, potom z trichotomie uspořádaní plyne $y < x$. Nyní díky monotónnosti násobení kladným číslem dostáváme $y^n < x^n$, což je spor.

Nyní zvolme libovolné $x \in \mathbb{R}^+$, jehož odmocninu budeme studovat. Z dokázaného plyne, že množina $M = \{y \in \mathbb{R}^+ \,|\, x \leq y^n\}$ je právě množinou horních závor množiny $N = \{y \in \mathbb{R}^+ \,|\, y^n \leq x\}$ (jestliže $y_1 \in N$ a $y_2 \in M$, potom platí $y_1^n \leq x \leq y_2^n$, a tedy $y_1 \leq y_2$; opačně, pokud z je horní závora množiny N a současně $z^n < x$, potom podle Věty 60(ii) existuje $w \in \mathbb{R}^+$ takové, že $z < w$ a $w^n < x$, proto $w \in N$, a tedy z není horní závora množiny N, což je spor; dokázali jsme, že horní závora z množiny N musí splňovat $x \leq z^n$).

Dokázali jsme, že $\sqrt[n]{x} = \sup\{y \in \mathbb{R}^+ \,|\, y^n \leq x\} = \min\{y \in \mathbb{R}^+ \,|\, x \leq y^n\}$ (supremum je nejmenší horní závora). Proto platí $x \leq (\sqrt[n]{x})^n$. Pokud by platilo $x < (\sqrt[n]{x})^n$, potom podle Věty 60(i) existuje $y \in \mathbb{R}^+$ takové, že $y < \sqrt[n]{x}$ a současně $x < y^n$. Proto $y \in M$ (což je spor, protože podle definice je $\sqrt[n]{x}$ nejmenší prvek množiny M).

Dokázali jsme, že $x = (\sqrt[n]{x})^n$. Pokud navíc existuje $y \in \mathbb{R}^+$ takové, že $y^n = x = (\sqrt[n]{x})^n$, potom podle prvního odstavce tohoto důkazu musí také platit $y \sqrt[n]{x}$ (protože $y^n \leq (\sqrt[n]{x})^n$ a $y^n \geq (\sqrt[n]{x})^n$ dává $y \leq \sqrt[n]{x}$ a $y \geq \sqrt[n]{x}$). Proto existuje jediná kladná n-tá odmocnina čísla x. □

Aparát odmocniny nám umožňuje na kladných reálných číslech zavést mocninu s libovolným racionálním exponentem. Protože $(\mathbb{R}^+, \cdot)$ je komutativní grupa, máme již korektně definovány celočíselné mocniny (viz Definice 21 a Věta 59).

Lemma 21 *Mějme libovolné $x \in \mathbb{R}^+$. Potom platí:*

i) Jestliže $p \in \mathbb{Z}$ a $q \in \mathbb{N}$, potom platí:

$$\sqrt[p]{x^q} = \left(\sqrt[p]{x}\right)^q,$$

ii) Pokud $p_1, p_2 \in \mathbb{Z}$ a $q_1, q_2 \in \mathbb{N}$ jsou takové, že platí $\frac{p_1}{q_1} = \frac{p_2}{q_2}$. Potom:

$$\sqrt[q_1]{x^{p_1}} = \sqrt[q_2]{x^{p_2}}.$$

Důkaz: i) Podle Věty 59 platí $\left((\sqrt[p]{x})^q\right)^p = (\sqrt[p]{x})^{p \cdot q} = \left((\sqrt[p]{x})^p\right)^q = x^q$. Z Věty 61 o odmocnině a z předchozí rovnosti plyne $\sqrt[p]{x^q} = (\sqrt[p]{x})^q$.

ii) Z rovnosti $\frac{p_1}{q_1} = \frac{p_2}{q_2}$ ihned plyne rovnost $p_1 \cdot q_2 = p_2 \cdot q_1$. Označme tuto hodnotu $m = p_1 \cdot q_2 = p_2 \cdot q_1$, potom počítejme:

$$\left(\sqrt[q_1]{x^{p_1}}\right)^m = \left(\sqrt[q_1]{x^{p_1}}\right)^{q_1 \cdot p_2} = \left(\left(\sqrt[q_1]{x^{p_1}}\right)^{q_1}\right)^{p_2} = (x^{p_1})^{p_2} = x^{p_1 \cdot p_2} =$$

$$= (x^{p_2})^{p_1} = \left(\left(\sqrt[q_2]{x^{p_2}}\right)^{q_2}\right)^{p_1} = \left(\sqrt[q_2]{x^{p_2}}\right)^{q_2 \cdot p_1} = \left(\sqrt[q_2]{x^{p_2}}\right)^m.$$

Díky Věty 61 můžeme najít m-tou odmocninu z levé a pravé strany dokázané rovnosti, což přímo dokazuje naše tvrzení. □

Definice 23 *Jestliže $\frac{p}{q} \in \mathbb{Q}$ je takové, že $q \in \mathbb{N}$ (toto lze předpokládat bez újmy na obecnosti, protože $\frac{p}{q} = \frac{-p}{-q}$ a $q \neq 0$) a libovolné $x \in \mathbb{R}^+$, potom definujme:*

$$x^{\frac{p}{q}} = \sqrt[p]{x^q} \quad \left(= \left(\sqrt[p]{x}\right)^q\right).$$

Díky Lemmatu 21ii) víme, že předchozí definice je korektní (tedy hodnota definované mocniny nezávisí na volbě reprezentanta zlomku). Toto navíc umožňuje dokázat analogicky i následující větu.

Věta 62 *Pro libovolné prvky $x, y \in \mathbb{R}^+$ a libovolná racionální čísla $\frac{p}{q}, \frac{p_1}{q_1}, \frac{p_2}{q_2} \in \mathbb{Q}$ platí:*

i) $x^{\frac{p_1}{q_1}} \cdot x^{\frac{p_2}{q_2}} = x^{\frac{p_1}{q_1}+\frac{p_2}{q_2}}$,

ii) $(x^{\frac{p_1}{q_1}})^{\frac{p_2}{q_2}} = x^{\frac{p_1}{q_1}.\frac{p_2}{q_2}}$,

iii) $1^{\frac{p}{q}} = 1$,

iv) $(x \cdot y)^{\frac{p}{q}} = x^{\frac{p}{q}} \cdot y^{\frac{p}{q}}$.

Důkaz: i) Díky Větě 59(iv) můžeme počítat:

$$\begin{aligned}
\left(x^{\frac{p_1}{q_1}} \cdot x^{\frac{p_2}{q_2}}\right)^{q_1 \cdot q_2} &= (\sqrt[q_1]{x^{p_1}} \cdot \sqrt[q_2]{x^{p_2}})^{q_1 \cdot q_2} = \\
&= \left(\sqrt[q_1]{x^{p_1}}\right)^{q_1 \cdot q_2} \cdot \left(\sqrt[q_2]{x^{p_2}}\right)^{q_1 \cdot q_2} = \\
&= \left(\left(\sqrt[q_1]{x^{p_1}}\right)^{q_1}\right)^{q_2} \cdot \left(\left(\sqrt[q_2]{x^{p_2}}\right)^{q_2}\right)^{q_1} = \\
&= (x^{p_1})^{q_2} \cdot (x^{p_2})^{q_1} = \\
&= x^{p_1 \cdot q_2} \cdot x^{p_2 \cdot q_1} = \\
&= x^{p_1 \cdot q_2 + p_2 \cdot q_1} = \\
&= \left(\sqrt[q_1 \cdot q_2]{x^{p_1 \cdot q_2 + p_2 \cdot q_1}}\right)^{q_1 \cdot q_2} = \\
&= \left(x^{\frac{p_1 \cdot q_2 + p_2 \cdot q_1}{q_1 \cdot q_2}}\right)^{q_1 \cdot q_2} = \\
&= \left(x^{\frac{p_1}{q_1}+\frac{p_2}{q_2}}\right)^{q_1 \cdot q_2}.
\end{aligned}$$

Podle Věty 61 můžeme provést $q_1 \cdot q_2$-odmocninu z dokázané rovnosti, která dokončuje důkaz.

ii) Analogicky jako v předchozím případě platí:

$$\begin{aligned}
\left(\left(x^{\frac{p_1}{q_1}}\right)^{\frac{p_2}{q_2}}\right)^{q_1 \cdot q_2} &= \left(\left(\sqrt[q_2]{\left(\sqrt[q_1]{x^{p_1}}\right)^{p_2}}\right)^{q_2}\right)^{q_1} = \\
&= \left(\left(\sqrt[q_1]{x^{p_1}}\right)^{p_2}\right)^{q_1} = \\
&= \left(\left(\sqrt[q_1]{x^{p_1}}\right)^{q_1}\right)^{p_2} = \\
&= (x^{p_1})^{p_2} = \\
&= x^{p_1 \cdot p_2} = \\
&= \left(\sqrt[q_1 \cdot q_2]{x^{p_1 \cdot p_2}}\right)^{q_1 \cdot q_2} = \\
&= \left(x^{\frac{p_1 \cdot p_2}{q_1 \cdot q_2}}\right)^{q_1 \cdot q_2}.
\end{aligned}$$

Odmocníme-li dokázanou rovnost $q_1 \cdot q_2$-tou odmocninou, dostaneme tvrzení:

iii) Pro $p \in \mathbb{N}$ platí $1^p = 1$ (podle Věty 59(iii)). Proto také $\sqrt[q]{1} = 1$ (viz Věta 61). Dohromady dostáváme $1^{\frac{p}{q}} = \sqrt[q]{1^p} = \sqrt[q]{1} = 1$.

iv) Podle předchozích vět opět můžeme počítat:

$$\begin{aligned}
\left(x^{\frac{p}{q}} \cdot y^{\frac{p}{q}}\right)^q &= \left(\sqrt[q]{x^p} \cdot \sqrt[q]{y^p}\right)^q = \\
&= \left(\sqrt[q]{x^p}\right)^q \cdot \left(\sqrt[q]{y^p}\right)^q = \\
&= x^p \cdot y^p = \\
&= (x \cdot y)^p = \\
&= \left(\sqrt[q]{(x \cdot y)^p}\right)^q = \\
&= \left((x \cdot y)^{\frac{p}{q}}\right)^q.
\end{aligned}$$

Najdeme-li q-tou odmocninu z hledané rovnosti, dostaneme hledanou větu. □

Dosavadní teorie lze ještě rozšířit o mocniny kladných reálných čísel reálnou mocninou. Jestliže $a \in \mathbb{R}^+$ a $x \in \mathbb{R}$, potom lze definovat mocninu a^x jako

$$a^x = \begin{cases} \inf\{a^y \mid y \in \mathbb{Q} \text{ a navíc } x \leq y\}, & \text{jestliže platí } 1 \leq a, \\ \sup\{a^y \mid y \in \mathbb{Q} \text{ a navíc } x \leq y\}, & \text{jestliže platí } 1 > a. \end{cases}$$

K tomu, abychom dokázali předchozí věty i pro tuto mocninu, musíme dokázat spojitost funkce $f(x) = a^x$. Zájemce odkážeme na podrobnější literaturu (např. [BlI, BlII]).

Kapitola 10

Poziční číselné soustavy

Základním způsobem zápisu čísel je takzvaný z-adický zápis, kde $z \in \mathbb{N}$ je libovolné přirozené číslo takové, že $1 < z$. Pro nás nejobvyklejší dekadický zápis není vždy nejvýhodnější (například počítačová věda pracuje s binární nebo hexadecimální – tj. šestnáctkovou – soustavou). Základní myšlenka z-adického zápisu je obsažena v následující větě.

Věta 63 *Jestliže $z \in \mathbb{N}$ je takové, že $1 < z$, potom pro libovolné $n \in \mathbb{N}$ existuje jediná posloupnost prvků $a_0, \ldots, a_k \in \{0, 1, \ldots, z-1\}$, kde $a_k \neq 0$ splňující*

$$n = a_0 z^0 + a_1 z^1 + \cdots + a_k z^k.$$

Důkaz: Libovolné číslo n můžeme dělit se zbytkem číslem z.[1] Z konečnosti každého čísla $n \in \mathbb{N}$ plyne, že existují konečné posloupnosti prvků $r_0, r_1, \ldots, r_k = 0 \in \mathbb{N}$, dále $a_0, \ldots, a_n \in \{0, \ldots, z-1\}$ takových, že platí:

$$\begin{aligned} n &= z \cdot r_0 + a_0, \\ r_0 &= z \cdot r_1 + a_1, \\ &\cdots \\ r_{i-1} &= z \cdot r_i + a_i, \\ &\cdots \\ r_{k-1} &= z \cdot r_k + a_k. \end{aligned}$$

Nyní dokážeme, že posloupnost $a_0, \ldots, a_k$ je námi hledanou posloupností. Z předchozích rovností a ze skutečnosti, že $r_k = 0$, dostáváme:

$$\begin{aligned} a_0 &= n - z \cdot r_0, \\ a_1 &= r_0 - z \cdot r_1, \\ &\cdots \\ a_i &= r_{i-1} - z \cdot r_i, \end{aligned}$$

[1] Vydělíme se zbytkem číslo n číslem z. Nejprve vezmeme maximální $m \in \mathbb{N}$ takové, že $n \geq m \cdot z$. a poté označíme $r = n - m \cdot z$. Snadno $0 \leq r < z$ (jinak by platilo, že $n \geq (m+1) \cdot z$, což je spor s maximalitou m). Potom platí, že $n = m \cdot z + r$. Platí tedy, že $n : z = m$ se zbytkem r.

$$\begin{aligned} &\cdots \\ a_{k-1} &= r_{k-2} - z \cdot r_{k-1}, \\ a_k &= r_{k-1}. \end{aligned}$$

Proto také platí:

$$\begin{aligned} a_0 &= n - z \cdot r_0, \\ z \cdot a_1 &= z \cdot r_0 - z^2 \cdot r_1, \\ &\cdots \\ z^i \cdot a_i &= z^i \cdot r_{i-1} - z^{i+1} \cdot r_i, \\ &\cdots \\ z^{k-1} \cdot a_{k-1} &= z^{k-1} \cdot r_{k-2} - z^k \cdot r_{k-1}, \\ z^k \cdot a_k &= z^k \cdot r_{k-1}. \end{aligned}$$

Nyní sečteme předchozí rovnosti:

$$a_0 + z \cdot a_1 + \cdots z^i \cdot a_i + \cdots + z^{k-1} \cdot a_{k-1} + z^k \cdot a^k =$$

$$n - z \cdot r_0 + z \cdot r_0 - z^2 \cdot r_1 + \cdots + z^i \cdot r_{i-1} - z^{i+1} \cdot r_i + \cdots + z^{k-1} \cdot r_{k-2} - z^k \cdot r_{k-1} + z^k \cdot r_{k-1} = n.$$

Opačně, platí-li rovnost

$$n = a_0 z^0 + a_1 z^1 + \cdots + a_k z^k$$

za daných podmínek věty, potom je posloupnost $a_0, \ldots, a_n$ evidentně posloupnost zbytků při postupném dělení čísla n číslem z. Protože taková posloupnost je jediná, je také dokázána věta. □

Posloupnost prvků $a_0, \cdots, a_k$ obvykle slouží k takzvanému z-adickému zápisu čísla. Obvykle postupujeme tak, že každému z čísel $0, \cdots, z-1$ přiřadíme jeden znak (číslici) a potom posloupnost číslic $a_k a_{k-1} \cdots a_1 a_0$ je zápisem našeho čísla v z-adické soustavě.

Důkaz předchozí věty nám navíc dává návod, jak najít příslušný z-adický rozvoj pro konkrétní číslo. Například, budeme se snažit najít trojkový zápis čísla 1025. Potom platí:

$$\begin{aligned} 1025 &= 3 \cdot 341 + 2 \\ 341 &= 3 \cdot 113 + 2 \\ 113 &= 3 \cdot 37 + 2 \\ 37 &= 3 \cdot 12 + 1 \\ 12 &= 3 \cdot 4 + 0 \\ 4 &= 3 \cdot 1 + 1 \\ 1 &= 3 \cdot 0 + 1. \end{aligned}$$

Potom trojkový zápis čísla 1025 je 1101222. Opačně snadno ověříme, že platí:

$$1025 = 2 \cdot 3^0 + 2 \cdot 3^1 + 2 \cdot 3^2 + 1 \cdot 3^3 + 0 \cdot 3^4 + 1 \cdot 3^5 + 1 \cdot 3^6.$$

Zápis celého čísla v z-adickém rozvoji lze již jednoduše rozšířit ze zápisu přirozených čísel, a to především díky Věty 24, která říká, že každé celé číslo je buďto nulou nebo přirozeným číslem, nebo je opačným číslem k přirozenému číslu. Proto přidáním 0 a čísel ve tvaru $-a_k a_{k-1} \dots a_0$, která představují záporná čísla, dostáváme zápis libovolného celého čísla.

Jak je čtenáři jistě dobře známo, zavádíme i z-adický rozvoj pro reálná čísla (v případě desítkové soustavy tento rozvoj nazýváme desetinným rozvojem). Hlavní myšlenka této konstrukce je zápis reálného čísla pomocí členů snadno konstruovatelné fundamentální posloupnosti. Mějme reálné číslo $x \in \mathbb{R}$ takové, že $0 \leq x < 1$, potom platí, že $0 \leq z \cdot x < z$ a tedy existuje maximální číslice $a_1 \in \{0, \dots, z-1\}$ taková, že $a_1 \leq z \cdot x$ a proto platí, že $0 < z \cdot x - a_1 < 1$. Označíme-li $x_2 = z \cdot x - a_1$, můžeme úvahu opakovat (tedy dostaneme $a_2 \in \{0, \dots, z-1\}$ splňující $0 \leq z \cdot x_2 - a_2 < 1$). Celkově dostáváme posloupnost číslic $a_1, \dots, a_i, \dots \in \{0, \dots, z-1\}$ takových, že $x_{i+1} = z \cdot x_i - a_i$, kde $x = x_1$. Z tohoto přímo dostáváme rovnosti:

$$\frac{a_1}{z} = x - \frac{x_2}{z}$$
$$\frac{a_i}{z^i} = \frac{x_i}{z^{i-1}} - \frac{x_{i+1}}{z^i}.$$

Vezmeme-li libovolné $n \in \mathbb{N}$, potom také platí

$$\sum_{i=1}^{n} \frac{a_i}{z^i} = x - \frac{x_{n+1}}{z^n}.$$

Uvědomíme-li si navíc, že $0 \leq x_n < 1$ platí pro všechna $n \in \mathbb{N}$, a tedy také $0 \leq \frac{x_{n+1}}{z^n} < \frac{1}{z^n}$, potom můžeme dedukovat, že $\lim \frac{x_{n+1}}{z^n} = 0$. Dohromady proto platí

$$\lim_{n\to\infty} \sum_{i=1}^{n} \frac{a_i}{z^i} = \lim_{n\to\infty} \left(x - \frac{x_{n+1}}{z^n} \right) = x - \lim_{n\to\infty} \left(\frac{x_{n+1}}{z^n} \right) = x - 0 = x.$$

Posloupnost číslic $a_1 a_2 \dots a_i \dots$ jednoznačně určuje číslo $x \in \mathbb{R}$ takové, že $0 \leq x < 1$, a to tak, že

$$\lim_{n\to\infty} \sum_{i=1}^{n} \frac{a_i}{z^i} = x.$$

Jak bylo navíc ukázáno výše, ke každému takovému x daná posloupnost (číselný rozvoj) existuje. Tohoto využíváme k zápisu kladného reálného čísla. Libovolné kladné reálné číslo $x \in \mathbb{R}^+$ může být zapsáno jako posloupnost číslic $a_n a_{n-1} \dots a_0 a_{-1} \dots$, kde platí

$$x = \sum_{i=n}^{-\infty} \frac{a_i}{z^i}.$$

Jistou nevýhodou je, že v případě, kdy pro všechny číslice od některého a_k platí $a_i = z-1$, má jedno číslo dva možné zápisy (typickým příkladem je $0,\overline{9} = 1$). Protože se jedná o jedinou nejednoznačnost, užíváme takovéhoto zápisu reálných čísel velice často.

Desetinný zápis reálných čísel je ve skutečnosti určení reálného čísla podle fundamentální posloupnosti (posloupnost má limitu, a proto je podle Věty 41 fundamentální). Výpočty s desetinným zápisem se výborně algoritmizují, což přineslo významný rozvoj celé aritmetice.

Kapitola 11

Základní kritéria dělitelnosti celých čísel

Ukážeme si základní možnosti k určování kriterií dělitelnosti malými čísly v oboru integrity $\mathbb{Z}$. Kapitola prezentuje pouze nejzákladnější metody určování kritérií.

Připomeňme, že na množině celých čísel zavádíme relaci takovou, že $x|y$ platí tehdy a jen tehdy, jestliže existuje $z \in \mathbb{Z}$ takové, že $x \cdot z = y$. Potom tuto skutečnost čteme „x dělí y“.

Definice 24 *Řekneme, že dvě čísla $x, y \in \mathbb{Z}$ jsou ekvivalentní modulo n, kde $n \in \mathbb{N}$ je libovolné, ale pevně zvolené číslo, platí-li $n|x - y$. Tuto skutečnost potom zapisujeme $x \equiv y \pmod{n}$.*

Definice nám vlastně říká, že dvě celá čísla jsou ekvivalentní v relaci $x \equiv y \pmod{n}$, právě když mají stejný zbytek při dělení číslem n.

Věta 64 *Relace $x \equiv y \pmod{n}$ je kongruence na oboru integrity (tedy okruhu) $\mathbb{Z}$. Faktorové okruhy potom nazýváme okruhy zbytkových tříd a značíme je $\mathbb{Z}_n$.*

Důkaz: Protože $n \cdot 0 = 0 = x - x$, platí $n|x - x$ a také $x \equiv x \pmod{n}$ pro libovolné $x \in \mathbb{Z}$. Relace je tedy reflexivní. Jestliže $x \equiv y \pmod{n}$, potom $n|x - y$, a proto existuje $z \in \mathbb{Z}$ takové, že $n \cdot z = x - y$. Snadno nyní platí $n \cdot (-z) = -(x - y) = y - x$, a tedy $y \equiv x \pmod{n}$. Relace je proto také symetrická. Předpokládejme nyní, že $x \equiv y \pmod{n}$ a $y \equiv z \pmod{n}$, potom $n|x - y$ a $n|y - z$. Existují proto hodnoty $z_1, z_2 \in \mathbb{Z}$ takové, že platí $n \cdot z_1 = x - y$ a $n \cdot z_2 = y - z$. Dostáváme také rovnost $n \cdot (z_1 + z_2) = n \cdot z_1 + n \cdot z_2 = (x - y) + (y - z) = x - z$. Proto platí $n|x - z$ a také $x \equiv z \pmod{n}$. Dohromady jsme dokázali, že relace $\equiv$ je relace ekvivalence.

Jestliže $x_1 \equiv y_1 \pmod{n}$ a $x_2 \equiv y_2 \pmod{n}$, potom také $n|x_1 - y_1$ a $n|x_2 - y_2$. Opět takto dostáváme existenci čísel $z_1, z_2 \in \mathbb{Z}$ takových , že $n \cdot z_1 = x_1 - y_1$ a $n \cdot z_2 = x_2 - y_2$. Proto $n \cdot (z_1 + z_2) = n \cdot z_1 + n \cdot z_2 = (x_1 - y_1) + (x_2 - y_2) = (x_1 + x_2) - (y_1 + y_2)$. Dokázali jsme, že platí $n|(x_1 + y_1) - (x_2 + y_2)$, a tedy také $x_1 + x_2 \equiv y_1 + y_2 \pmod{n}$.

Dále můžeme počítat:

$$\begin{aligned} x_1 \cdot x_2 - y_1 \cdot y_2 &= x_1 \cdot x_2 - x_1 \cdot y_2 + x_1 \cdot y_2 - y_1 \cdot y_2 = \\ &= x_1 \cdot (x_2 - y_2) + y_2 \cdot (x_1 - y_1) = \\ &= x_1 \cdot n \cdot z_2 + y_2 \cdot n \cdot z_1 = \\ &= n \cdot (x_1 \cdot z_2 + y_2 \cdot z_1). \end{aligned}$$

Proto platí $n|x_1 \cdot x_2 + y_1 \cdot y_2$ a dohromady také $x_1 \cdot x_2 \equiv y_1 \cdot y_2 \pmod{n}$. □

Předcházející věta nám dává již dostatečný aparát k nalezení kritérií dělitelnosti jednotlivými čísly.

Připomeňme, že libovolné přirozené číslo $a \in \mathbb{N}$ reprezentujeme pomocí dekadického zápisu

$$a_n a_{n-1} \dots a_1 a_0 = \sum_{i=0}^{n} 10^i \cdot a_i = a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n,$$

kde $a_0, \dots, a_n$ jsou číslice v rozmezí 0 až 9.

Kritérium dělitelnosti číslem 2.

Snadno ověříme, že platí $10 \equiv 0 \pmod{2}$, a tedy pro $n \in \mathbb{N}$ takové, že $1 \leq n$ platí také $10^n \equiv 10 \cdot 10^{n-1} \equiv 0 \cdot 10^{n-1} \equiv 0 \pmod{2}$. Proto také

$$a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n \equiv a_0 + 0a_1 + \cdots + 0a_n \equiv a_0 \pmod{2}.$$

Tímto jsme dokázali, že číslo a dává při dělení číslem 2 stejný zbytek jako číslice a_0, a tedy a je dělitelné 2 tehdy a jen tehdy, když a_0 je dělitelné 2. Navíc poslední číslice je dělitelná dvěma jenom v případě, že se jedná o některou z následujících číslic 0, 2, 4, 6 a 8.

Kritérium dělitelnosti číslem 3.

Platí $10 \equiv 1 \pmod{3}$, a tedy také $10^n \equiv 1^n \equiv 1 \pmod{3}$ pro všechna $n \geq 1$. Nyní můžeme počítat:

$$a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n \equiv a_0 + a_1 + \cdots + a_n \pmod{3}.$$

Proto číslo a dává při dělení číslem 3 stejný zbytek jako číslo $a_0 + \cdots + a_n$. Dohromady můžeme říci, že číslo a je dělitelné 3, právě když jeho ciferný součet (součet číslic v dekadickém zápisu) je dělitelný číslem 3.

Kritérium dělitelnosti číslem 4.

Platí ekvivalence $100 \equiv 0 \pmod{4}$. Proto také pro každé $n \geq 2$ můžeme počítat $10^n \equiv 10^{n-2} \cdot 100 \equiv 10^{n-2} \cdot 0 \equiv 0 \pmod{4}$. Platí proto také:

$$a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n \equiv a_0 + 10a_1 + 0a_2 + \cdots + 0a_n \equiv a_0 + 10a_1 \pmod{4}.$$

Dokázali jsem, že číslo je dělitelné 4 právě když jeho poslední dvojčíslí je dělitelné 4.

Kritérium dělitelnosti číslem 5.

Jelikož $10 \equiv 0 \pmod{5}$, platí také pro každé $n \geq 1$, že $10^n \equiv 10 \cdot 10^{n-1} \equiv 0 \cdot 10^{n-1} \equiv 0 \pmod{5}$. Dohromady dostáváme:

$$a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n \equiv a_0 + 0a_1 + \cdots + 0a_n \equiv a_0 \pmod{5}.$$

Dokázali jsme, že číslo a je dělitelné 5, právě když jeho poslední číslice a_0 je dělitelná pěti. Navíc a_0 je dělitelná 5 jenom v případě, že se jedná o 0 nebo 5.

Kritérium dělitelnosti číslem 6.

Jestliže platí $6|a$ pro $a \in \mathbb{Z}$, potom existuje $z \in \mathbb{Z}$ takové, že $6z = a$, ale také $2 \cdot 3 \cdot z = a$. Proto $2|a$ a $3|a$.

Předpokládejme opačně, nechť $2|a$ a $3|a$, potom a je společným násobkem čísel 2 a 3. Proto také (podle definice nejmenšího společného násobku) platí $nsn(2,3)|a$, a tedy $6|a$.

Dohromady jsme dokázali, že číslo a je dělitelné 6, právě když je dělitelné 2 a 3.

Kritérium dělitelnosti číslem 7.

Vidíme, že platí $10 \equiv 3 \pmod 7$. Proto $10^2 \equiv 3^2 \equiv 2 \pmod 7$ a konečně $10^3 \equiv 10^2 \cdot 10 \equiv 2 \cdot 3 \equiv 6 \equiv -1 \pmod 7$. Z uvedeného poznatku můžeme usoudit, že pro všechna $n \geq 3$ platí $10^n \equiv 10^3 \cdot 10^{n-3} \equiv -10^{n-3} \pmod 7$, a proto také platí:

$$a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n \equiv a_0 + 10a_1 + 100a_2 - a_3 - 10a_4 - 100a_5 + a_6 \cdots \pmod 7.$$

Dohromady dostáváme, že číslo a je dělitelné 7 tehdy a jen tehdy, je-li 7 dělitelné číslo $a_2a_1a_0 - a_5a_4a_3 + a_8a_7a_6 - \cdots$.

Kritérium dělitelnosti číslem 8.

Platí $1000 \equiv 0 \pmod 8$, a proto pro všechna $n \geq 3$ platí $10^n \equiv 10^3 \cdot 10^{n-3} \equiv 0 \cdot 10^{n-3} \equiv 0 \pmod 8$. Platí proto:

$$a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n \equiv a_0 + 10a_1 + 0a_2 + \cdots + 0a_n \equiv a_0 + 10a_1 + 100a_3 \pmod 8.$$

Dohromady jsme dokázali, že číslo a je dělitelné 8, právě když jeho poslední trojčíslí je dělitelné 8.

Kritérium dělitelnosti číslem 9.

Platí $10 \equiv 1 \pmod 9$, a tedy také $10^n \equiv 1^n \equiv 1 \pmod 9$. Nyní můžeme počítat:

$$a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n \equiv a_0 + a_1 + \cdots + a_n \pmod 9.$$

Proto můžeme říci, že číslo a je dělitelné 9, právě když jeho ciferný součet je dělitelný číslem 9.

Kritérium dělitelnosti číslem 10.

Platí $10 \equiv 0 \pmod{10}$, a tedy pro $n \in \mathbb{N}$ takové, že $1 \leq n$, platí také $10^n \equiv 10 \cdot 10^{n-1} \equiv 0 \cdot 10^{n-1} \equiv 0 \pmod{10}$. Proto také

$$a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n \equiv a_0 + 0a_1 + \cdots + 0a_n \equiv a_0 \pmod{10}.$$

Proto je a je dělitelné 10, tehdy a jen tehdy, když a_0 je dělitelné 10. Navíc poslední číslice je dělitelná 10 jenom v případě, že se jedná o 0. Číslo a je dělitelné 10 právě když $a_0 = 0$.

Kritérium dělitelnosti číslem 11**.**

Platí, že $10 \equiv -1 \pmod{11}$, proto pro každé $n \in \mathbb{N}$ platí, že $10^n \equiv (-1)^n \pmod{11}$. Proto platí, že

$$a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n \equiv a_0 - a_1 + a_2 - a_3 + \cdots \pmod{11}.$$

Dokázali jsme proto, že a je dělitelné číslem 11 tehdy a jen tehdy, je-li číslem 11 dělitelné číslo $a_0 - a_1 + a_2 - a_3 + \cdots$.

Literatura

[BlI] Blažek, J.: *Algebra a teoretická aritmetika I.*, SPN Praha, 1983.

[BlII] Blažek, J., Koman, M., Vojtášková, B.: *Algebra a teoretická aritmetika II.*, SPN Praha, 1985.

[Dav] Davenport, H.: *The Higher Arithmetic: An Introduction to the Theory of Numbers (7th ed.),*, Cambridge University Press, Cambridge, UK, 1999, ISBN 0-521-63446-6.

[GGSK] Gavalec, M., Gedeonová, E., Smítal, J., Katriňák, T.: *Algebra a teoretická aritmetika*, Bratislava: Alfa, 1985.

[KaSo] Kantor, I.L., Solodovnikov A.S. : *Hypercomplex numbers: an elementary introduction to algebras*; translated by A. Shenitzer (original in Russian). New York: Springer-Verlag, c. 1989.

[Zed1] Zedník, J.: *Algebra a teoretická aritmetika*, Univerzita Palackého, 1993.

[Zed2] Zedník, J.: *Reálná čísla podle Cantora*, Olomouc : Rektorát Univerzity Palackého, 1989.