Univerzita Karlova
Pedagogická fakulta
Katedra matematiky a didaktiky matematiky

BAKALÁŘSKÁ PRÁCE

Číselné obory a soustavy
Main and Other Number Systems

Jakub Michal

Vedoucí práce: prof. RNDr. Jarmila Novotná, CSc.

Studijní program: Specializace v pedagogice

Studijní obor: Matematika se zaměřením na vzdělávání

2018

Prohlašuji, že jsem bakalářskou práci na téma Číselné obory a soustavy vypracoval pod vedením vedoucí práce samostatně za použití v práci uvedených pramenů a literatury. Dále prohlašuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

12. července 2018

. . . .

podpis

Poděkování

Rád bych poděkoval prof. RNDr. Jarmile Novotné, CSc., za odborné vedení práce, poskytnutí cenných rad a za čas, který mi při tvorbě práce věnovala.

Anotace

Tato bakalářská práce má za cíl shromáždit informace o oborech čísel přirozených, celých, racionálních, reálných a komplexních čísel, shrnout jejich historii, konstrukci a ukázat některé vlastnosti každého z oborů, jako zda je obor spočetný nebo uspořádaný. Také jsou ukázány vlastnosti aritmetických operací, které jsou na každém z oborů definovány. V úvodu práce je pozornost věnována pojmu číslo a historii nuly. Následují kapitoly o číselných oborech zmíněných výše a v poslední kapitole jsou stručně představeny další typy čísel.

Klíčová slova

Matematika, číslo, číselný obor, historie matematiky, vlastnosti čísel

Annotation

The goal of this bachelor thesis is to gather information on natural numbers, integers, real numbers and complex numbers, to make a synopsis of their history, to describe their construction and to show some of each system properties such as countability or ordering. Properties of operations which are defined on each system are shown as well. Introduction of thesis is focused on concept of number itself and history of number zero. Chapters about each abovementioned number system follow. Last chapter briefly introduces other number types.

Key Words

Mathematics, number, number system, history of mathematics, number properties

Obsah

1 Úvod

Práci zabývající se číselnými obory jsem si vybral hned z několika důvodů. Jednak jimi lze dobře demonstrovat vývoj matematiky, myšlení a překonávání mezí v matematice tak, jak šly dějiny. Také jejich optikou můžeme dobře nazřít koncepce chápání světa v různých epochách, což je něco, co mně osobně přijde velice zajímavé. Také mě, stejně jako celé lidstvo v průběhu času, vždy fascinovaly mnohé paradoxy, které právě kolem číselných oborů vyvstávají. Dalším z důvodů a inspirací, proč jsem si dané téma vybral, mi byl předmět zapsaný na Filosofické fakultě UK, který se zabýval právě filosofií čísla a matematiky a na pojem číselný obor velice často narážel ve velice zajímavých souvislostech.

Cílem práce je shromáždit informace o číselných oborech z literatury jak vědecké, tak popularizační. Dalším cílem je popsat historii druhů čísel, konstrukci číselných oborů a zavedení operací sčítání a násobení. Dále ukážeme některé z vlastností jako spočetnost každého z oborů nebo se zamyslíme, jakou algebraickou strukturu spolu s operacemi na něm definovanými obor tvoří.

Práce je rozdělena do devíti kapitol. První kapitola je věnována pojmu čísla jako takového. Stručně je zde zmíněna také historie nuly. V prvních kapitolách jsou zavedeny důležité pojmy, se kterými se setkáme v celé práci. Dále následují kapitoly o přirozených číslech, celých číslech, racionálních číslech, reálných číslech, komplexních číslech a v závěrečné kapitole jsou stručně zmíněny kvaterniony a další číselné obory.

Každá další kapitola věnující se číselnému oboru je rozdělena do několika částí. Je vysvětleno, jak byla tato čísla prvně objevena, a také je popsána historie jejich vzniku. Dále je každý číselný obor zkonstruován pomocí axiomů, vět a definic tak, jak je pro dnešní matematiku typické. Také je pro každý obor ukázáno, zda je spočetný, či nikoliv. Uvedeno je také, jakou algebraickou strukturu obor s operacemi na něm definovanými tvoří.

2 Číslo

Ottův slovník naučný (1893) stanovuje číslo jako entitu určující kolikost stejnorodých věcí. Je-li vyjádřeno s jednotkou, je konkrétním a bez jednotky abstraktním. Právě ona abstraktnost z čísel činí univerzální nástroj, bez kterého by dnešní svět vypadal úplně jinak. Ovšem přestože potřeba věci počítat byla pro lidi typickou již od počátku jejich existence, o čemž svědčí četné nálezy kostí či oblázků se zářezy symbolizujícími počet, k číslům v podobě, ve které je známe dnes, vedla dlouhá cesta.

Hegel, německý filosof, ve své knize *Fenomenologie ducha* (1960) popisuje vznik pojmu čísla pomocí zákonu dvojí negace. Říká, že k tomu, abychom mohli určit počet, je potřeba nejprve negovat rozdíly mezi sčítanými entitami, které každou z nich tvoří jedinečnou, a najít pouze shodné jmenovatele sčítaných entit (Hegel nazývá Für-Sich-Sein, jedná se o to, co daná věc musí mít, aby byla tou věcí), jelikož není možné sčítat různé. Ovšem po tomto prvotním znegování by stále nebylo možné součet provést, jelikož popřením prvotní rozdílnosti bychom entitu sjednotili v jednu (n-krát to samé je stále jedno a to samé), a proto je potřeba negovat znovu a najít prvotně popřenou odlišnost. (Kolman, 2017)

Hegelův model vzniku čísla jasně ilustruje, jak obtížným procesem bylo přijít s universálními pojmy označujícími nejen počet, ale i pořadí. Nástroji, které by fungovaly bez ohledu na to, co počítáme nebo kdo počítá. Ovšem než lidstvo dospělo ke konstruktu, který by byl sdělitelný, společný a jasný, byl potřebný vývoj dlouhý až sto padesát tisíc let, který je stručně popsán v kapitole 2.1.

Henry B. Fine ve své knize *Number-System of Algebra* (1907) o čísle říká, že se jedná o tu vlastnost skupiny předmětů, která zůstává nezměněnou po všech změnách provedených na této skupině tak dlouho, dokud nenarušíme jejich separovanost (soudružnost skupiny) od všech ostatních věcí. Můžeme tedy měnit polohu, uspořádání, vztah jednoho k druhému a dokonce i charakter těchto předmětů, ale jejich počet bude stále neměnnou vlastností této skupiny.

2.1 Historie čísla

Nejjednodušší a pravděpodobně první použitou metodou k vyjádření počtu věcí ve skupině je reprezentace věcí samotných, ať už pomocí obrázku nebo jejich slovního označení. Tento způsob ovšem není počítáním v pravém slova smyslu, jelikož neupouští od vlastností sčítaného a nesoustředí se pouze na jeho množství. O počítání můžeme poprvé mluvit teprve tehdy, kdy jedna skupina předmětů byla použita k reprezentaci množství obsaženého v nějaké jiné skupině. Pak již nezáleželo na charakteru věcí v každé ze skupin, ale pouze na jejich sdílené vlastnosti, a to právě počtu. (Fine, 1907)

V knize *The Number-System of Algebra* (Fine, 1907) je vývoj primitivních čísel, tedy čísel, která se objevila jako první v různých kulturách, popsán ve třech fázích. Vývoj začíná u symbolů gestikulačních, pokračuje přes symboly sdílené řeči a končí u symbolů, které je možné zapsat.

2.1.1 Čísla vyjádřená pomocí gestikulace

Nejpřirozenější člověku bylo přiřazování předmětů, které počítal, k jednotlivým prstům rukou. Důvody k tomu jsou hned dva. Jednak se jedná o skupinu, kterou máme neustále při sobě, ale také jsou jednotlivé prsty od sebe funkcí a podobou jen velmi málo odlišné, takže je vlastně jednodušší jejich odlišnosti ignorovat. To je pro skupinu, která slouží jako skupina, se kterou porovnáváme, ideální vlastnost. Pokud totiž naše srovnávací skupina je jen málo diferencovatelná, je mnohem snadnější upustit od zbývajících odlišností. (Fine, 1907)

Dalším důkazem, že počítání na prstech bylo upřednostněno před jinými metodami, je podle Finea (1907) to, že téměř každý systém číselného vyjádření, který je nám známý, je buď o základu pět, deset, dvacet, nebo jejich kombinací. Podle Finea není náhoda, že čísla odpovídají právě počtu prstů na jedné, dvou a čtyřech lidských končetinách.

Přesvědčit se o správnosti předpokladu, že počítání na prstech bylo prvotním způsobem určování počtu, můžeme také u současných kmenů žijících mimo civilizaci. Přestože domorodci nemají slova vyjadřující množství větší než dva nebo tři, jsou schopni, a také skutečně určují počet pomocí signalizace na prstech. Fine uvádí jako příklady domorodý kmen ze státu Victoria v Austrálii nebo kmen Bororů z Brazílie. Vychází přitom z knihy *Primitive Culture* (Tylor, 1871).

2.1.2 Čísla vyjádřená pomocí slova

Fine (1907) dále popisuje vznik slov označujících množství. Jak říká, čísla se tímto způsobem začala šířit mnohem později než gestikulací. Upozorňuje na fakt, že tam, kde se dá zpětně dopátrat, jak slovo označující množství od jedné do dvaceti vzniklo, je to obvykle odvozeno právě ze symbolů značících jednotlivé prsty, nebo se jedná o skupiny předmětů, které byly pro všechny známé, a mohly tedy být použity jako sdílený etalon. V mnoha kmenech je proto například číslo pět označováno slovem, které také znamená „ruka“, slovo deset slovem „ruce“ či výraz pro dvacet je homonymem pro „celého člověka“. Dvojka je často významem převzatým ze slov jako „oči“, „uši“ nebo „křídla“. Zajímavým příkladem uvedeným Fineem (1907) jsou Tamanakové z Orinoka, jejichž slovo pro číslo pět znamená „celá ruka“. Šestku značí výrazem znamenajícím „jeden z druhé ruky“, a tak dále až po devítku, deset logicky znamená „obě ruce“. Dále pokračují s prsty u nohou. Pro dvacítku použijí výraz „jeden indián“…

Jako další národy, jejichž jazyk byl bohatým na slova popisující čísla, uvádí Fine (1907) ze stejného zdroje (*Primitive Culture*, Tylor, 1871) mimo jiné Inuity nebo Aztéky. Ke dvojce ještě dodává příklady kultur z knihy *Short History of*

Greek Mathematics (Gow, 1884). V čínštině výraz pro slovo dva znamená „uši“ a v tibetštině „křídla“.

U většiny rozvinutých jazyků už bohužel nelze zpětně vypátrat původní smysl slov pro čísla užívaná na jejich území v dnešní době. (Fine, 1907)

2.1.3 Čísla vyjádřená pomocí písma

Pomocí desíti symbolů $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ jsme schopni zapsat libovolné racionální číslo. Nyní popíšeme, proč se jedná právě o tyto symboly, proč je jich deset a proč jsou uspořádány v pořadí, v jakém je dnes známe.

První metody zjišťování počtu byly založeny na bijektivním přiřazování. Počet zářezů či předmětů, se kterými bylo množství srovnáváno, ovšem při velké kvantitě sčítaného představoval problém jak v přehlednosti, tak praktičnosti. Přesto už tento způsob komunikace měl výhody oproti předchozím dvěma. Jsou jimi trvalost, kdy vyznačené zářezy vydržely po tisíce let, a také možnost vyznačit obrovské množství, které bychom nedokázali pomocí gest či slov připodobnit. (Fine, 1907)

Problém nepřehlednosti, způsobený velkým množstvím znaků, byl v různých kulturách řešen odlišnými způsoby. Nejprve se začaly v hebrejské, řecké a egyptské formě zápisu objevovat symboly značící větší množství, díky čemuž bylo možné zapsat číslo na menším prostoru. Toto rozšíření systému „zářezů“ ovšem nebylo dostatečné pro velká čísla, kdy bylo nutné vymýšlet další a další nové symboly, které na nepřehlednosti a nesdílitelnosti jen přidávaly. (King, 2017)

Velkou změnou, a také krokem k zápisu čísel v poziční soustavě, byla čísla římská. Zde již určitou roli hrálo místo, na kterém se daný symbol vyskytl. Pokud je znak s menší hodnotou před znakem s hodnotou větší, odčítáme hodnotu menšího od většího. V dobách Říma byly povoleny ovšem jen tyto možnosti, kdy se menší číslo odečítalo od většího: IX, XL, XC, CD, CM. Další možnosti, se kterými se dnes můžeme setkat, se začaly objevovat až ve středověku. Symboly, které Římané používali, byly mocniny desítky: I, X, C, M a jejich poloviny: V, L, D. Stejně jako u jiných, starších kultur (např. Egypt) symboly vznikly jako připodobnění našim prstům pro čísla $I, II, III, IIII$, tvaru dlaně pro V. Desítku připodobnili dvěma rukám, což označlili jako dvě opačná V, z nichž vznikl symbol X. Znaky C a M jsou z latinských slov *centum* znamenajícím sto a *mille*, které překládáme jako tisíc. (Crilly, 2010)

Co se římských zlomků týče, existoval symbol pro polovinu S. Zlomky Římané vyjadřovali pomocí dvanáctkové soustavy, ač zbylou aritmetiku prováděli v soustavě desítkové. (Crilly, 2010)

Hodnota číslice se však i u římských čísel stále odvíjí od zástupného znaku, nikoliv od pozice, a velká čísla tak byla stále problémem. Dalším nedostatkem je zde absence znaku pro nulu a obtížnost operací sčítání a násobení.

Pozn. 1. Francouzský král *Ludvík XIV.* preferoval zápis svého jména jako *Ludvik XIIII.* Díky jeho nařízení se také setkáme na ciferníku hodin se zápisem čtyřky jako *IIII*, jak by ji zapsali i Římané, a ne jako středověké *IV.* (Crilly, 2010)

Nejefektivnějším řešením tedy bylo přijít se systémem, který se bude odvíjet od pozice znaku. Tímto způsobem je možné zapsat i velká čísla za pomoci jednoho symbolu, kde jeho kvantita určí násobek čísla odpovídajícího pozici, na které se nachází.

Poziční zápis se vyvinul ve třech různých kulturách. Nezávisle na sobě ho objevili Babyloňané, Číňané a Aztékové. Z Asie se dostal poziční způsob zápisu čísel do Evropy kolem osmého století. Evropský systém je desítkový a využívá deset různých znaků, díky čemuž již není nutné pro násobnost číslice psát stejný symbol několikrát na dané místo zápisu. Velice podobný systém byl vyvinut i Mayskou civilizací. Mayský systém obsahoval také symbol pro nulu. Kultury, které sice poziční soustavu znaly, ale nepoužívaly zástupný symbol značící prázdné místo v zápisu, pouze vynechávaly místo, což vedlo ke značnému ztížení čitelnosti a chybám. Největším problém pak bylo, jak rozlišit například čísla 20 a 200, kdy bylo vynechané místo na konci (viz 2.2). (King, 2017)

Symboly užívané pro reprezentaci deseti znaků desítkové soustavy se lišily kulturu od kultury. Ty, se kterými se dnes setkáváme, se pravděpodobně vyvinuly ze symbolů používaných na severu Afriky v regionu Maghreb spadajícím pod arabskou říši. Čísla dnes známá jako indoevropská nahradila v běžném užití čísla římská počátkem patnáctého století.

Jak již bylo zmíněno při popisu čísel římských, desítkový systém (*decimal system*) byl oblíbený v mnoha kulturách zřejmě právě proto, že jako lidé jsme na číslo deset zvyklí díky naší morfologii (viz kapitola 2.1.1). Stejně lze odůvodnit užití systému dvacítkového u Aztéků (*vigesimal system*). (King, 2017)

Další historicky významné systémy o jiném základu jsou babylónská čísla šedesátková (*sexigesimal system*). Tento systém byl pravděpodobně zvolen pro dělitelnost za sebou jdoucími čísly $1, 2, 3, 4, 5, 6$. Podobně vhodný je systém dvanáctkový (*duodecimal system*), díky vlastnosti dvanáctky být dělitelnou $2, 3, 4, 6$. Dělitelnost ulehčila práci s často užívanými zlomky, jelikož takto měly racionální hodnoty. Proto se s těmito soustavami setkáváme dodnes v běžném životě při měření času a úhlů a stejně tak v jazyce s výrazy jako kopa nebo tucet. (Lundyová, 2010; Ted-Ed, 2017)

V kapitole 2.1.1 bylo zmíněno, že kultury využívaly zejména čísla o základu pět, deset, dvacet nebo jejich kombinace. Za příklad pětkové soustavy (*quinary system*) uvádí Fine (1907) z knihy *Primitive Culture* (1871) polynéskou číselnou řadu a jako příklad dvacítkové (*vigesimal system*) uvádí z Cantorovy knihy *Geschichte der Mathematik* zápis Mayů z Yucatánu, kteří mají speciální slova pro 20, 400, 8 000 a 160 000.

Co se smíšených soustav, tedy soustav kombinujících čísla o různých základech, týče, už jsme zmínili Římany a jejich desítkovou a dvanáctkovou soustavu. Dalšími jsou například Aztékové, kteří kombinovali dvacítkovou a pětkovou soustavu. Fine (1907) stanovuje podle *Primitive Culture* (1871) závěr, že pětková a dvacítková soustava se častěji objevuje u méně rozvinutých kultur, zatímco desítková u pokročilejších.

Ve světě informatiky se setkáme nejčastěji se soustavou o základu dvě (*binary system*). Méně často programátoři také používají soustavu osmičkovou nebo šestnáctkovou, ve kterých je zápis velkých čísel podstatně kratší. (Crilly, 2010; Ted-Ed, 2017)

2.2 Nula

„Nula je hybnou silou pokroku. To, že toto vzdušné 'nic' obdrželo nejen pouhou pozici, jméno, obrázek, symbol, ale i prospěšnou funkci, je typické pro hinduisty, kterým za ni vděčíme.“

G. B. Halsted (Crilly, 2010, s. 7)

Zvláštní zmínku si zaslouží historie nuly, která je důležitá nejen, chceme-li pomocí čísla ukázat, že množství sčítané entity je žádné, ale také jako významný symbol v pozičním zápisu čísel.

Nula se objevila v historii na minimálně čtyřech místech, a to nezávisle na sobě. Babyloňané používali již kolem roku 400 před naším letopočtem symbol dvou klínů značící prázdné místo ve sloupci jejich šedesátkové soustavy. Mayská kultura užívala obdobně symbolu mušle. Staří Indové zase používali kruhový symbol značící otisk v písku, který zůstane po zvednutí oblázku z písčitého povrchu, což je dokonalá metafora pro něco, co už není. Z tohoto symbolu se vyvinula nula značená tak, jak ji známe. (Lundyová, 2010)

Zatímco Babyloňané se spoléhali při rozpoznání zapsaných čísel pouze na kontext čísla při rozlišování mezi řády, v moderním zápisu čísel nám nula umožní určit řád konkrétně, stejně jako zapsat čísla velmi malá, či naopak opravdu velká. K tomuto účelu byl znak podobný naší nule poprvé použit Ptolemaiem, který z poznatků Babyloňanů vycházel. (Crilly, 2010)

Přestože historie nuly je dlouhá, jako číslo (a ne pouhý zástupný symbol) ji poprvé popsal, i s jejími základními vlastnostmi nutnými dodržovat k jejímu používání, až indický matematik Brahmagupta v roce 628 našeho letopočtu. Jeho axiomy pro nulu byly následující:

1. Součet nuly a kladného čísla je kladný.
2. Součet nuly a záporného čísla je záporný.
3. Součet kladného a záporného čísla je jejich rozdíl; pokud však mají stejnou hodnotu, výsledkem je nula.
4. Nula dělená záporným nebo kladným číslem je buď nula, nebo výsledek zapisujeme ve tvaru zlomku, jehož čitatel je roven nule a jmenovatel má konečnou hodnotu.

(Crilly, 2010, s. 7)

Nulu jako číslo s těmito vlastnostmi pak přinesl roku 1202 západnímu světu Leonardo Pisánský (známý jako Fibonacci) v díle *Liber Abaci* (1202), ovšem nebyla brána jako plnohodnotná číslice. (Crilly, 2010)

To s sebou ovšem přineslo celou řadu problémů, které bylo nutné vyřešit. Jedním z nich bylo stanovit, čemu se rovná výraz $\frac{a}{0}$. Indický matematik Bháskara, žijící ve dvanáctém století, přišel s myšlenkou, že $\frac{a}{0} = \infty$, jelikož čím menším číslem dělíme, tím větší číslo dostáváme. Pro tuto vlastnost výraz považoval za božský. Fine (The Number-System of Algebra, 1907, s. 71) Bháskarovu ideu o nekonečnosti výrazu formuluje takto: „*Hodnota* $\frac{a}{0}$ *nepodléhá žádné změně, jakkoliv* *je zvětšena, nebo zmenšena.“* Ovšem tím se problém pouze zkomplikoval, jelikož nekonečno není číslo a ani se neřídí aritmetickými zákony. (Fine, 1907; Crilly 2010; Heeffer, 2011)

Dalším problémem byl výraz $\frac{0}{0}$, který po vyjádření neznámé říká, že se může rovnat čemukoliv (neurčitý výraz).

Nejjednodušším řešením tedy bylo dělení nulou zakázat. (Crilly, 2010)

3 Číselné obory

Na gymnáziích se se zavedením číselných oborů setkáváme hned v úvodu studia. V učebnici *Matematika pro gymnázia, Základní poznatky* (Bušek, Calda, 1992) jsou číselné obory definovány ve druhé kapitole jako množina všech čísel určitého druhu, ve které jsou definovány bez omezení operace sčítání a násobení.

Z definice je evidentní, že žáci již mají jistou představu o tom, že existují různé *druhy* čísel ze školy základní.

Definice 1. Množina všech čísel určitého druhu, ve které jsou definovány bez omezení operace sčítání a násobení, se nazývá číselný obor. Značit ho budeme $\mathbb{C}_{\mathbb{O}}$.

(Bušek, Calda, 1992, s. 12)

Pozn. 2. Pokud bychom v angličtině hledali vhodný ekvivalent pojmu číselný obor, zjistíme, že takto úzce definovanou strukturu najdeme obvykle jako podmnožinu širšího pojmu. Obory tak v literatuře často spadají do jedné z následujících skupin:

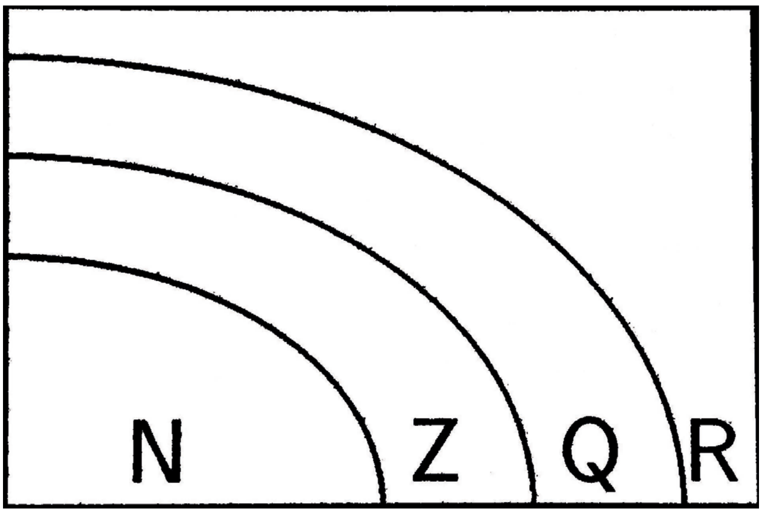
- **Number sets** - Pojem je velice široký, zahrnuje totiž veškeré číselné množiny, a tedy i obory.
- **Number types** - Pojem rozdělující čísla na typy podle druhu zápisu, základu, znaménka, parity, dělitelnosti a mnoha dalších vlastností. Číselné obory pak obvykle nalezneme pod kategorií **main number types**.
- **Number systems** - pojem nejužší a nejbližší našim oborům, ovšem zahrnuje stejně jako předcházející pojem i čísla o jiných základech, poziční/nepoziční číselné modely a další. Pojem **main number systems** popisuje číselné obory, jak je známe. Označení number system je použito v knize *The Number System* (Thurston, 1956), která je jedním ze zdrojů práce. (Vzhledem k tomu,

že byla celá věnována přístupům ke konstrukci číselných oborů, nebylo třeba v názvu publikace úže specifikovat, že se jedná o main number systems.)

V dalším textu se setkáme také s výrazy podobor a nadobor. Přestože jsem se s tímto označením v literatuře nesetkal, je dosti intuitivní již z obrázku 1. Pro úplnost pojmy definujeme v definici 2.

Definice 2. Nadoborem $\mathbb{A}$ oboru $\mathbb{B}$ budeme rozumět takový obor, který je definován na nadmnožině množiny, na níž je definován obor $\mathbb{B}$. Obdobně budeme mluvit o podoboru.

Číselné obory, které budeme dále zkoumat, budou uvedeny právě v takovém pořadí, že každý další obor bude nadoborem předešlého, jak znázorňuje obrázek 1 převzatý z učebnice *Matematika pro gymnázia* (Bušek, Calda, 1992). Na rozdíl od ilustrace ovšem budeme věnovat pozornost také oboru komplexních čísel.



Obrázek 1: Znázornění vztahů mezi obory (Bušek, Calda, 1992, s. 13)

Věta 1. *Pro každý číselný obor* $\mathbb{C}_{\mathbb{O}}$ *platí:*

$$\forall a, b, c \in \mathbb{C}_{\mathbb{O}}: \qquad (a+b)+c = a+(b+c),$$

$$\forall a, b \in \mathbb{C}_{\mathbb{O}}: \qquad a+b = b+a,$$

$$(\cdot) \quad \exists 0 \in \mathbb{C}_{\mathbb{O}} \quad \forall a \in \mathbb{C}_{\mathbb{O}}: \qquad a+0 = a,$$

$$\exists 1 \in \mathbb{C}_{\mathbb{O}} \quad \forall a \in \mathbb{C}_{\mathbb{O}}: \qquad a \cdot 1 = a,$$

$$\forall a, b \in \mathbb{C}_{\mathbb{O}}: \qquad a \cdot b = b \cdot a,$$

$$\exists 1 \in \mathbb{C}_{\mathbb{O}} \quad \forall a \in \mathbb{C}_{\mathbb{O}}: \qquad a \cdot 1 = a,$$

$$\forall a, b, c \in \mathbb{C}_{\mathbb{O}}: \qquad a(b+c) = ab+ac$$

** Platí v případě, kdy bereme přirozená čísla s nulou, pro případ bez nuly je tvrzení (3) platné až pro nadobory oboru* $\mathbb{N}$.

(Pavlicová, 2010)

Důkaz věty bude u jednotlivých oborů proveden zvlášť.

3.1 Číselné obory jako algebraické struktury

Vzhledem k tomu, co říká definice 1, se lze na číselné obory dívat optikou algebraických struktur. Algebraická struktura je totiž množinou, na níž je bez omezení definována alespoň jedna operace/relace. Přesně to je podle definice 1 splněno pro každý číselný obor. Proto bude mít smysl se u každé kapitoly zabývat tím, jakou strukturu daná množina čísel s operacemi sčítání a násobení tvoří.

4 Čísla přirozená

Ve článku *What are numbers, and what is their meaning?* (Burris, 2001), který pojednává o publikacích Richarda Dedekinda *Continuity and irrational numbers* (1872) a *What are numbers, and what is their meaning?* (1888), se dočteme, že přirozená čísla byla v osmdesátých letech devatenáctého století velkou filosofickou otázkou. Burris se zmiňuje v tomto kontextu o Gaussově dopisu zaslaném roku 1830. Gauss v dopise říká, že čísla jsou odlišná od prostoru a času v tom, že jen čísla jsou produktem naší mysli. Na to navazuje Dedekind slovy o tom, že touto optikou osvobozenosti prvků od všeho jiného obsahu (abstrakce) lze na přirozená čísla nahlížet jako na prostý výtvor lidské mysli. Jak Burris dodává, je tento pohled v rozporu s Kroneckerovou pozdější poznámkou:

„Přirozená čísla jsou od Boha, vše ostatní je dílo člověka.“

Leopold Kronecker, 1886 (Kubínová, Novotná, 1997, s. 139)

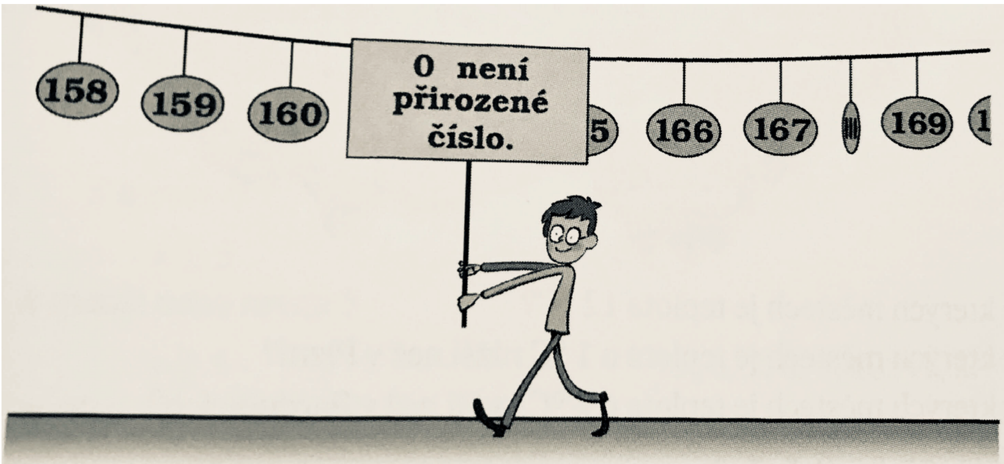
Citace od Leopolda Kroneckera ukazuje, že čísla přirozená byla vnímána jako něco natolik jasného, že je není třeba definovat, něco, co existuje od nepaměti a je nám intuitivně známé. S Kroneckerovou citací se také setkáváme například i v názvu knihy Stephena Hawkinga *God Created the Integers: The Mathematical Breakthroughs That Changed History* (2005). Zajímavostí je, že v názvu knihy citát mluví o *integers*. Stejně tak v Kroneckerovi vlastní němčině je v citátu použit výraz *ganzen Zahlen*, tedy celá čísla. Do češtiny je však citát překládán tak, jak byl uveden výše, tedy hovořící o číslech přirozených. To může být částečně vysvětleno jak mnohostí výrazů popisujících přirozená a celá čísla (viz poznámka 7), tak vývojem a posunem jazyka a matematických pojmů. Ovšem v článku Burrise

(2001) se vyskytuje citát s výrazem *natural numbers*, jak ho chápeme dnes.

Jak bylo popsáno v kapitole 2, přirozené číslo lze interpretovat mnoha způsoby, ať už z pohledu filosofie, jazykovědy, nebo vlastnostmi předmětů v reálném světě.

Co se matematické definice přirozených čísel týče, neexistovala až do konce devatenáctého století. Stejně tak se ani žáci na základních a středních školách s axiomatickou definicí čísel nesetkávají.

V učebnici pro základní školy *MATEMATIKA pro 6. ročník základní školy, 1. díl* (Odvárko, Kadleček, 1997) jsou přirozená čísla zavedena jako čísla $1, 2, 3, 4, \ldots$ a znázorněním na číselné ose. Učebnice také jasně zavádí, že nula není přirozené číslo. To *demonstruje* i následující obrázek 2 převzatý z téže učebnice.



Obrázek 2: Nula není přirozené číslo (Odvárko, Kadleček, 1997, s. 4)

Pozn. 3. My se však k nule budeme stavět tak, jak je uvedeno v poznámkách 5 a 6, které následují po definici 3.

Přestože se definice z učebnice pro základní školy může jevit jako jasná a triviální, je za ní dlouhý vývoj myšlení a konstrukce, která je vysvětlena v kapitole 4.1 a vychází z knihy *The Number System* (Thurston, 1956).

4.1 Počítání & srovnávání

Pokud chceme vědět, v jaké z množin je více prvků, zdá se být nejjasnějším způsobem, jak rozhodnout, spočítat prvky v jedné a druhé množině a výsledek porovnat. Ovšem nejjasnější způsob není nejjednodušším. Nejen člověk, ale i některá zvířata dokáží rozeznat už rychle od pohledu, že v závorce [*******] je více hvězdiček než v případě závorky [***]. Stejně tak některá zvířata mají schopnost rozeznat rozdíl mezi množstvím ve dvou časových údajích, například vejdou-li do domu tři lidé a vyjdou dva, vědí, že jeden je stále uvnitř. Toto dokáží rozeznat přes to, že neexistuje jediný důkaz, že by uměla počítat. (Thurston, 1956)

Existuje zde tedy rozdíl mezi počítáním a porovnáváním. V knize *The Number System* (Thurston, 1956) je tento rozdíl dále ilustrován na příkladu domorodého kmenu, který zná čísla do dvaceti. Dokáže rozeznat rozdíl mezi skupinami o 17 a 18 členech jejich spočítáním. Ale nedokáže spočítat skupiny o 25 a 75 členech. Použijí zde metodu srovnávání a dokáží poznat již na první pohled, která skupina je větší. Rozdíl mezi dvěma skupinami je od oka evidentní a pro případ takto extrémního rozdílu si kmen vystačil s prostým pozorováním. Ovšem existuje ještě jedna metoda, která by fungovala jak v případě skupin o 17 a 18 členech, tak u skupin větších než 20, kde nemusí být rozdíl na pohled patrný.

Thurston (1956) metodu ilustruje na příkladě s tanečníky. Mistr chce vědět, jaké pohlaví je v tanečním sále zastoupeno více členy. Vyzve tedy tanečníky, aby se párovali tak, že každý muž si najde tanečnici a obráceně. Pokud zbyde muž/muži, je více mužů. Pokud zbyde žena/ženy, je více žen. Pokud nezbyde nikdo, množiny jsou zastoupeny rovnoměrně.

Tento princip bijektivního zobrazení množiny na druhou pro rozhodnutí o mohutnostech množin byl intuitivně znám člověku mnohem dříve, než vůbec dokázal počítat nebo čísla jakkoliv zapisovat. V knize *The Number System* (1956) Thurston princip nazývá jednoduše „matching“, tedy přiřazování.

4.2 Zavedení přirozených čísel

Thurston dále popisuje, jak vznikla přirozená čísla:

1. Uvažujme posloupnost [*], [**], [***], [****], ... Pokud je možné množinu toho, co sčítáme, přiřadit k množině hvězdiček v [*], řekneme, že počet prvků množiny je jedna. Je-li obdobně možné ji přiřadit k množině [**], řekneme, že počet prvků je dva... Obdobně pro další čísla.

   Pozn. 4. Tento přístup zavedení čísla je blízký definici čísla ze sedmé knihy Eukleidových Základů (300 př. n. l.):

   i) „Jednotka jest, dle níž každé věci říká se jedna.“

   ii) „Číslo pak je množství složené z jednotek.“

   (Servít, 1907, s. 103).

2. Pro konstrukci čísel, jak je známe, nyní již stačí nahradit nešikovné symboly * obvyklými symboly. Tedy: [1], [1,2], [1,2,3], [1,2,3,4], ...

   Každá ze závorek obsahuje n-tici, jejíž pořadí musí být neměnné. Tyto množiny nazveme standardními.

3. Po přiřazení množiny k některé ze standardních množin stačí znát poslední číslo v závorce, abychom znali počet sčítaného. (Taková čísla čeština označuje pojmem ordinální.) Zavedeme následující označení, kdy každé uspořádané n-tici přiřadíme její poslední prvek. Symbol $\leftrightarrow$ značí přiřazení n-tice k číslu:

$$\begin{aligned} [1] &\leftrightarrow 1, \\ [1,2] &\leftrightarrow 2, \\ [1,2,3] &\leftrightarrow 3, \\ &\dots \\ [1,2,3,\dots,n] &\leftrightarrow n. \end{aligned}$$

Z této konstrukce čísel pro počítání množství Thurston (1956) dedukuje závěr, a sice že vše, co je potřeba k počítání, je uspořádaná sada různých symbolů, která pokračuje do nekonečna.

Takto definovaná čísla už nesou jisté vlastnosti, které mají přirozená čísla definovaná pomocí Peanových axiomů, například, že každé číslo má svého následníka (viz definice 3), nebo vlastnost, že různá čísla mají různé následníky (viz definice 3).

4.2.1 Peanovy axiomy

Definice 3. Peanovy axiomy

1) $0 \in \mathbb{N}$,

2) $\forall a \in \mathbb{N} \quad \exists! \sigma(a)$, kde $\sigma(a)$ nazýváme následníkem čísla a,

3) $\sigma(a) = \sigma(b) \implies a = b$,

4) $\nexists a, \sigma(a) = 0$,

5) Nechť V je vlastnost přirozených čísel a nechť:

   I. Pro nulu vlastnost V platí.

   II. Jestliže vlastnost V platí pro a, platí vlasnost V i pro $\sigma(a)$.

   Pak platí vlastnost V pro všechna přirozená čísla.

(Kubínová, Novotná, 1997)

Jak je popsáno ve skriptech *Posloupnosti a řady* (Kubínová, Novotná, 1997), lze pro tento systém vytvořit také množinový model následujícím způsobem:
Na množině $\mathbb{N}$ je definována nula a zobrazení σ: $\mathbb{N} \longrightarrow \mathbb{N}$ a platí:

(i) σ je injektivní,

(ii) $0 \notin \sigma(\mathbb{N})$,

(iii) Nechť $U \subset \mathbb{N}$ má tyto vlastnosti:

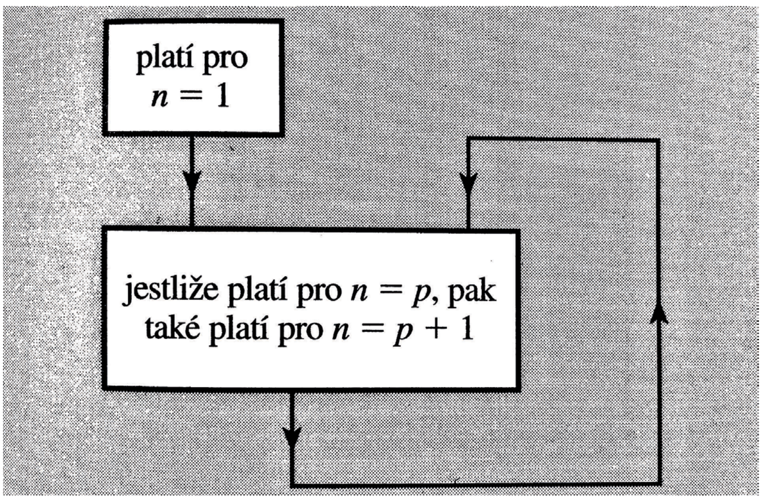
a) $0 \in U$,

b) $n \in U \implies \sigma(n) \in U$.

Pak $U = \mathbb{N}$.

- Třetí Peanův axiom říká, že zobrazení σ je prosté zobrazení množiny přirozených čísel do množiny přirozených čísel.

- Pátý Peanův axiom nazýváme axiomem indukce. Je na něm založena známá metoda důkazu vlastností přirozených čísel. Následující schéma 3 ze strany 87 knihy *1089 a další parádní čísla* od Davida Achesona princip ilustrativně znázorňuje.



Obrázek 3: Myšlenka principu matematické indukce (Acheson, 2006, s. 87)

Tento bod je někdy zaměňován za následující axiom:

5*) Nejsou jiná přirozená čísla než ta, která vzniknou z axiomů 1) a 2).

Následující věta ukazuje, že jsou oba axiomatické systémy ekvivalentní:

Věta 2. *Systém Peanových axiomů* $1) - 5)$ *je ekvivalentní se systémem* $1) - 4), 5^{\star})$.

Ekvivalence dvou systémů z věty 2 je zřejmá.

Pozn. 5. Nulu v definici 3 chápeme jako první prvek množiny přirozených čísel. Pokud z nějakého důvodu nulu jako takovou nepovažujeme za přirozené číslo, chápeme nulu v definici 2 jako jedničku.

Pozn. 6. Abychom předcházeli nedorozuměním, která by mohla být vyvolána zahrnutím či nezahrnutím nuly do množiny přirozených čísel, budeme v dalším textu, kde to bude mít význam, rozlišovat následující značení:

- $\mathbb{N}$ značí množinu přirozených čísel bez nuly,
- $\mathbb{N}_0$ značí množinu přirozených čísel včetně nuly.

Pozn. 7. Také je důležité zde zmínit, že v anglické literatuře (např. *The Number-System* [Thurston, 1956]) se nesetkáváme pouze s pojmem **natural numbers**, ale také **whole numbers**. **Whole numbers** ovšem nejsou chápána jako naše celá čísla, nýbrž právě jako čísla přirozená zahrnující nulu (tedy nezáporná). Pro celá čísla angličtina používá termín **integers**. Často je také v literatuře (např. *Number-System of Algebra* [Fine, 1907]) používán pouze výraz **Positive integers**, tedy kladná celá čísla.

4.3 Operace na množině přirozených čísel

Definice 4. Sčítání přirozených čísel je zobrazení $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, definované předpisem:

$$\forall a, b \in \mathbb{N} : a + b = \sigma^b(a).$$

Definice 5. Sčítání přirozených čísel definujeme za pomoci axiomu 5) z definice 3 takto:

(i) $\forall a \in \mathbb{N} : a + 0 = a$,

(ii) $\forall a, b \in \mathbb{N} : a + \sigma(b) = \sigma(a + b)$.

Věta 3. $\forall a, b \in \mathbb{N} : \sigma(a) + b = \sigma(a + b)$.

Důkaz. K důkazu použijeme matematickou indukci. Zvolme $a \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že tvrzení platí pro $b = 0$:

$$\sigma(a) + 0 = \sigma(a + 0).$$

Podle definice 5 se levá strana rovná $\sigma(a)$ a pravá také $\sigma(a)$. Pro $b = 0$ a libovolné přirozené a tvrzení platí.

II. Předpokládejme, že pro $b \in \mathbb{N}$ platí $\sigma(a) + b = \sigma(a + b)$. Ověříme, že pak platí také $\sigma(a) + \sigma(b) = \sigma(a + \sigma(b))$:

$$\sigma(a) + \sigma(b) \overset{def.\,5}{=} \sigma(\sigma(a) + b) \overset{ind.předpoklad}{=} \sigma(\sigma(a + b)) \overset{def.\,5}{=} \sigma(a + \sigma(b)).$$

Tvrzení je pravdivé pro všechna $a, b \in \mathbb{N}$. □

Věta 4. *Definice sčítání na množině přirozených čísel 4 a 5 definují totožnou operaci.*

Důkaz. Sčítání z definice 4 budeme pro důkaz značit $+_1$. Obdobně sčítání z definice 5 označíme $+_2$.

K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b \in \mathbb{N}$ platí:

$$\forall a, b \in \mathbb{N} : a +_1 b = a +_2 b.$$

Zvolme $a \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že rovnost platí pro $b = 0$. Chceme dokázat, že $a +_1 0 =$ $= a +_2 0$. Levá strana se podle definice 5 rovná a. Pravá se také podle definice 5 rovná a. Tedy tvrzení platí pro $b = 0$ a libovolné přirozené a.

II. Nyní předpokládáme, že pro nějaké b přirozené platí $a +_1 b = a +_2 b$. Ověříme, že pak platí $a +_1 \sigma(b) = a +_2 \sigma(b)$:

$$a +_1 \sigma(b) \overset{def. 4}{=} \sigma^{\sigma(b)}(a) = (\sigma \circ \sigma^b)(a) = \sigma(\sigma^b(a)) = \sigma(a +_1 b) =$$
$$\overset{ind. předpoklad}{=} \sigma(a +_2 b) \overset{def. 5}{=} a +_2 \sigma(b).$$

Definice 4 a 5 definují stejnou operaci.

□

Věta 5. $\forall a, b, c \in \mathbb{N}$:

1) $a + b = b + a$, *(sčítání je komutativní)*

2) $(a + b) + c = a + (b + c)$, *(sčítání je asociativní)*

3) $0 + a = a + 0 = a$, *(nula je neutrální prvek vzhledem ke sčítání)*

4) $a + c = b + c \implies a = b$,
$a + b = 0 \implies (a = 0 \land b = 0)$. *(pravidla pro krácení)*

Důkaz. K většině důkazů použijeme matematickou indukci z definice 3. Také budeme používat definici 5.

1) Nejprve dokážeme komutativitu sčítání. K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b \in \mathbb{N}$ platí:

$$a + b = b + a.$$

Zvolme $a \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že rovnost platí pro $b = 0$. Chceme dokázat, že $a + 0 =$ $= 0 + a$. Levá strana se podle definice 5 rovná a. Pravá je podle definice 4 rovna $\sigma^a(0)$, což je také rovno a. Tedy komutativita platí pro libovolné a přirozené a $b = 0$.

II. Nyní předpokládáme, že pro $b \in \mathbb{N}$ platí $a + b = b + a$. Ověříme, že pak platí také $a + \sigma(b) = \sigma(b) + a$:

$$a + \sigma(b) \overset{def.\,5}{=} \sigma(a + b) \overset{ind.předpoklad}{=} \sigma(b + a) \overset{def.\,3}{=} \sigma(b) + a.$$

Sčítání je tedy komutativní pro všechna $a, b \in \mathbb{N}$.

2) Dokážeme asociativitu sčítání. K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b, c \in \mathbb{N}$ platí:

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

Zvolme $a, b \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že rovnost platí pro $c = 0$. Chceme dokázat, že $(a+$ $+b) + 0 = a + (b + 0)$:

$$\left.\begin{aligned} L &: (a + b) + 0 \overset{def.5}{=} a + b \\ P &: a + (b + 0) \overset{def.5}{=} a + b \end{aligned}\right\} L = P.$$

Tedy asociativita sčítání platí pro libovolná přirozená a, b a $c = 0$.

II. Nyní předpokládejme, že pro nějaké c přirozené platí $(a+b)+c = a+(b+c)$. Ověříme, že pak platí také $(a + b) + \sigma(c) = a + (b + \sigma(c))$:

Nejprve upravíme levou stranu rovnosti:

$$L = (a+b)+\sigma(c) \overset{def.5}{=} \sigma((a+b)+c) \overset{ind.předpoklad}{=} \sigma(a+(b+c)) \overset{def.5}{=} a+\sigma(b+c).$$

Nyní upravíme stranu pravou:

$$P = a + (b + \sigma(c)) \overset{def.5}{=} a + \sigma(b + c).$$

Levá strana se rovná pravé.

Sčítání je tedy asociativní pro všechna $a, b, c \in \mathbb{N}$.

3) Platí, že $0+a = a+0 = a$? Víme již, že sčítání přirozených čísel je komutativní, platí tedy, že $a + 0 = 0 + a$. Z definice 5 také víme, že $a + 0 = a$. 0 je tedy neutrálním prvkem pro sčítání přirozených čísel.

4) Dokážeme první pravidlo pro krácení. K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b, c \in \mathbb{N}$ platí:

$$a + c = b + c \Rightarrow a = b.$$

Zvolme $a, b \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že tvrzení platí pro $c = 0$. Chceme dokázat, že $a + 0 = = b + 0 \Rightarrow a = b$:

$$\left.\begin{aligned} L &: a + 0 \overset{def.5}{=} a \\ P &: b + 0 \overset{def.5}{=} b \end{aligned}\right\}\text{Tedy } a = b.$$

První pravidlo pro krácení tedy platí pro libovolná přirozená a, b a $c = 0$.

II. Nyní předpokládejme, že platí $(a+c = b+c) \Rightarrow a = b$ pro nějaké přirozené c. Ověříme, že pak platí také: $(a + \sigma(c) = b + \sigma(c)) \Rightarrow a = b$. Upravíme levou a pravou stranu předpokladu implikace:

$$\left.\begin{aligned} L &: a + \sigma(c) \overset{def.5}{=} \sigma(a + c) \\ P &: b + \sigma(c) \overset{def.5}{=} \sigma(b + c) \end{aligned}\right\}\text{Tedy } \sigma(a + c) = \sigma(b + c).$$

Peanův axiom 3) (viz definice 3) říká, že pokud se následníci dvou čísel rovnají, rovnají se čísla samotná. Tedy:

$$\sigma(a + c) = \sigma(b + c) \Rightarrow a + c = b + c.$$

Z indukčního předpokladu víme, že jestliže $a + c = b + c$, pak $a = b$.

$(a + c = b + c) \Rightarrow a = b$ tedy platí pro všechna $a, b, c \in \mathbb{N}$.

5) Platí $\forall a, b \in \mathbb{N} : a + b = 0 \Rightarrow (a = 0 \wedge b = 0)$?

   Důkaz povedeme sporem. Předpokládejme, že $\exists a, b \in \mathbb{N} : (a \neq 0 \vee b \neq 0) \wedge$ $\wedge (a+b = 0)$. Podle definice sčítání 4 přepíšeme $a+b$ jako $\sigma^b(a)$. Pro a, b mohou nastat následující situace:

   (a) $a \neq 0 \Rightarrow \sigma^b(a)$ je b-tým následníkem nenulového čísla a. Je-li $b = 0$, dostáváme $\sigma^0(a) = a$. Je-li $b \neq 0$, pak nenulový následník nenulového čísla rozhodně není nula (viz definice 3, axiom 4). To je spor s předpokladem, že $a + b = \sigma^b(a) = 0$.

   (b) $b \neq 0 \Rightarrow \sigma^b(a)$ je b-tým následníkem čísla a. Pokud je a nenulové, dostáváme případ, kdy jsou obě čísla nenulová, popsaný ve druhé části (a). Pokud je $a = 0$ nula, je b-tý následník nuly roven nenulovému číslu b. A to je spor s předokladem, že $a + b = \sigma^b(a) = 0$.

   Platí i druhé pravidlo pro krácení.

$\square$

Definice 6. Násobení přirozených čísel je zobrazení $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, definované předpisem:

$$\forall a, b \in \mathbb{N} : a \cdot b = (\sigma^a)^b(0).$$

Násobení přirozených čísel lze definovat také následujícím způsobem:

Definice 7. Násobení je operace splňující tyto podmínky:

(i) $\forall a \in \mathbb{N} : a \cdot 0 = 0$,

(ii) $\forall a, b \in \mathbb{N} : a \cdot \sigma(b) = a \cdot b + a$.

Věta 6. *Definice násobení 6 a 7 definují totožnou operaci.*

Důkaz. Násobení z definice 6 budeme v důkazu značit jako $\cdot_1$. Obdobně násobení z definice 7 označíme jako $\cdot_2$.

K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b \in \mathbb{N}$ platí:

$$\forall a, b \in \mathbb{N} : a \cdot_1 b = a \cdot_2 b.$$

Zvolme $a \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že rovnost platí pro $b = 0$. Chceme dokázat, že $a \cdot_1 0 = a \cdot_2 0$. Levou a pravou stranu rovnosti přepíšeme podle příslušných definic násobení:

$$\left.\begin{aligned} L &: a \cdot_1 0 \overset{def.6}{=} (\sigma^a)^0(0) = 0 \\ P &: a \cdot_2 0 \overset{def.7}{=} 0 \end{aligned}\right\} L = P.$$

Definice 6 a 7 definují stejnou operaci pro a libovolné přirozené a $b = 0$.

II. Nyní předpokládáme, že pro nějaké b přirozené platí $a \cdot_1 b = a \cdot_2 b$. Ověříme, že pak platí také $a \cdot_1 \sigma(b) = a \cdot_2 \sigma(b)$:

$$\begin{aligned} &a \cdot_1 \sigma(b) = (\sigma^a)^{\sigma(b)}(0) = (\sigma^a \circ (\sigma^a)^b)(0) = \sigma^a((\sigma^a)^b(0)) = \sigma^a(a \cdot_1 b) = \\ &= a \cdot_1 b + a \overset{ind.předpoklad}{=} a \cdot_2 b + a = a \cdot_2 \sigma(b). \end{aligned}$$

Definice násobení přirozených čísel 6 a 7 tedy definují totožnou operaci.

□

Pozn. 8. Kde nebude hrozit nedorozumění, můžeme místo $a \cdot b$ psát pouze ab.

Definice 8. Prvek $\sigma(0)$ budeme značit 1 a nazývat jedničkou.

Věta 7. *Pro relaci $>$ na množině přirozených čísel definovanou takto:*

$$m > n \Leftrightarrow \exists r \in \mathbb{N} - \{0\} : m = n + r,$$

platí následující vlastnosti:

a) je tranzitivní,

b) je trichotomická.

Důkaz. a) Máme dokázat tranzitivitu relace $>$, tedy ptáme se, zda pro všechna $a, b, c \in \mathbb{N}$ platí:

$$(a > b) \wedge (b > c) \Rightarrow a > c.$$

Přepíšeme levou stranu implikace podle definice:

$$\exists r_1, r_2 \in \mathbb{N} - \{0\} : (a = b + r_1) \wedge (b = c + r_2).$$

Dosadíme do první rovnosti za b:

$$a = c + r_2 + r_1 = c + r_3, \text{ kde } r_3 = r_2 + r_1.$$

Protože r_3 je součet dvou nenulových přirozených čísel r_1, r_2, tedy také přirozené nenulové číslo, platí podle definice relace $>$, že $a > c$. Relace je tedy tranzitivní.

b) Dále máme dokázat, že relace je trichotomická. To znamená, že se ptáme, zda platí:

$$\forall a, b \in \mathbb{N} : (a > b) \oplus (b > a) \oplus (a = b),$$

kde symbol $\oplus$ značí logickou spojku XOR.
Z definice $+$ plyne, že nemůže nastat, že $(a = b) \wedge (a > b)$ nebo $(a = b) \wedge (b > a)$. Zbývá tedy ukázat, že nemůže nastat případ, kdy $(a > b) \wedge (b > a)$. Tvrzení dokážeme sporem. Předpokládejme, že:

$$\exists r_1, r_2 \in \mathbb{N} - \{0\} : a = b + r_1, b = a + r_2.$$

Dosadíme za b do první rovnosti:

$$a = a + r_2 + r_1 = a + (r_1 + r_2),$$

aby však tato rovnost platila, musela by obě čísla r_1, r_2 být rovna nule. To je však ve sporu s předpokladem, že $r_1, r_2 \neq 0$. Relace $>$ je tedy trichotomická.

$\square$

Pozn. 9. Relace $>$ je tranzitivní i trichotomická (viz věta 7). Je tedy uspořádáním na množině $\mathbb{N}$.

Věta 8. $\forall a, b \in \mathbb{N} : \sigma(b) \cdot a = b \cdot a + a.$

Důkaz. K důkazu použijeme matematickou indukci. Zvolme $b \in \mathbb{N}$ libovolné.

I. Ukážeme, že pro $a = 0$ tvrzení platí:

$$\sigma(b) \cdot 0 = b \cdot 0 + 0,$$

levá strana je podle definice 7 rovna nule. Pravá strana za využití věty 5 a definice 7 je také rovna nule. Tedy tvrzení pro libovolné přirozené b a $a = 0$ platí.

II. Předpokládejme, že pro nějaké a přirozené platí $\sigma(b) \cdot a = b \cdot a + a$. Ukážeme, že potom platí i pro $\sigma(a)$. Tedy, že platí:

$$\sigma(b) \cdot \sigma(a) = b \cdot \sigma(a) + \sigma(a).$$

Začneme upravovat levou stranu rovnosti:

$$\sigma(b) \cdot \sigma(a) \overset{def.\,7}{=} \sigma(b) \cdot a + \sigma(b) \overset{ind.\,předpoklad}{=} b \cdot a + a + \sigma(b) =$$
$$\overset{věta\,5}{=} a + \sigma(b) + b \cdot a \overset{věta\,3}{=} \sigma(a) + b + b \cdot a \overset{věta\,5}{=} \sigma(a) + b \cdot a + b =$$
$$\overset{def.\,7}{=} \sigma(a) + b \cdot \sigma(a) \overset{věta\,5}{=} b \cdot \sigma(a) + \sigma(a).$$

Tvrzení je tedy pravdivé pro všechna $a, b \in \mathbb{N}$. $\square$

Věta 9. $\forall a, b, c \in \mathbb{N}:$

1) $a \cdot b = b \cdot a$, *(násobení je komutativní)*

2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, *(násobení je asociativní)*

3) $0 \cdot a = a \cdot 0 = 0$, *(nula je tzv. agresivní prvek vzhledem k násobení)*

4) $1 \cdot a = a \cdot 1 = a$, *(jednička je neutrální prvek vzhledem k násobení)*

5) $(a + b) \cdot c = a \cdot c + b \cdot c$, *(násobení je distributivní vzhledem ke sčítání)*

6) $(c \neq 0 \wedge a \cdot c = b \cdot c) \implies a = b$,
$a \cdot b = 0 \implies (a = 0 \vee b = 0)$. *(pravidla pro krácení)*

Důkaz. 1) Nejprve ukážeme, že násobení je komutativní. K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b \in \mathbb{N}$ platí:

$$a \cdot b = b \cdot a.$$

Zvolme $a \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že tvrzení platí $b = 0$. Chceme tedy ukázat, že $a \cdot 0 = = 0 \cdot a$:

$$\left.\begin{aligned} L &: a \cdot 0 \overset{def.7}{=} 0 \\ P &: 0 \cdot a \overset{def.6}{=} (\sigma^0)^a(0) = 0 \end{aligned}\right\} L = P.$$

Komutativita násobení tedy platí pro libovolné a a $b = 0$.

II. Nyní předpokládejme, že platí $a \cdot b = b \cdot a$ pro $b \in \mathbb{N}$. Ověříme, že pak platí také $a \cdot \sigma(b) = \sigma(b) \cdot a$.:

$$a \cdot \sigma(b) \overset{def.7}{=} a \cdot b + a \overset{\text{věta}\,5}{=} a + a \cdot b \overset{ind.předpoklad}{=} a + b \cdot a \overset{\text{věta}\,8}{=} \sigma(b) \cdot a.$$

Násobení je tedy komutativní pro všechna $a, b \in \mathbb{N}$.

5) Nyní dokážeme distributivitu násobení vzhledem ke sčítání, kterou později využijeme k důkazu asociativity násobení. K důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b, c \in \mathbb{N}$ platí:

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

Zvolme $a, b \in \mathbb{N}$ libovolně.

I. Ukážeme, že tvrzení platí pro $c = 0$. Chceme dokázat, že $(a + b) \cdot 0 = = a \cdot 0 + b \cdot 0$. Z definice násobení 7 platí, že levá i pravá strana jsou rovny nule, a tedy se rovnají. Pro a, b libovolné přirozené a $c = 0$ distributivita násobení vzhledem ke sčítání platí.

II. Předpokládejme nyní, že platí $(a+b) \cdot c = a \cdot c + b \cdot c$ pro $c \in \mathbb{N}$. Dokážeme, že pak platí $(a + b) \cdot \sigma(c) = a \cdot \sigma(c) + b \cdot \sigma(c)$:

$$\left.\begin{aligned} L &: (a + b) \cdot \sigma(c) \overset{def.7}{=} (a + b) \cdot c + (a + b) \\ P &: a \cdot \sigma(c) + b \cdot \sigma(c) \overset{def.7}{=} a \cdot c + a + b \cdot c + b \overset{\star}{=} (a + b) \cdot c + (a + b) \end{aligned}\right\} L = P.$$

$\star$: Využili jsme komutativitu sčítání z věty 5 a indukční předpoklad.

Násobení je tedy distributivní vzhledem ke sčítání pro všechna $a, b, c \in \mathbb{N}$.

2) Nyní už můžeme ukázat, že násobení je asociativní. I zde k důkazu použijeme matematickou indukci. Ptáme se, zda pro všechna $a, b, c \in \mathbb{N}$ platí:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Zvolme $a, b \in \mathbb{N}$ libovolně.

I. Nejprve ukážeme, že asociativita násobení platí pro $c = 0$. Chceme dokázat, že $(a \cdot b) \cdot 0 = a \cdot (b \cdot 0)$:

$$\left.\begin{aligned} L &: (a \cdot b) \cdot 0 \overset{def.7}{=} 0 \\ P &: a \cdot (b \cdot 0) \overset{def.7}{=} a \cdot 0 \overset{def.7}{=} 0 \end{aligned}\right\} L = P.$$

Asociativita násobení tedy platí pro libovolná přirozená čísla a, b a $c = 0$.

II. Nyní předpokládáme, že platí $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ pro nějaké c přirozené. Ukážeme, že pak platí $(a \cdot b) \cdot \sigma(c) = a \cdot (b \cdot \sigma(c))$:

$$\left.\begin{aligned} L &: (a \cdot b) \cdot \sigma(c) \overset{def.7}{=} (a \cdot b) \cdot c + a \cdot b \overset{ind.předpoklad}{=} a \cdot (b \cdot c) + a \cdot b \\ P &: a \cdot (b \cdot \sigma(c)) \overset{def.7}{=} a \cdot (b \cdot c + b) \overset{distrib.nás.}{=} a \cdot (b \cdot c) + a \cdot b \end{aligned}\right\} L = P$$

Násobení je tedy asociativní pro všechna $a, b, c \in \mathbb{N}$.

3) Agresivita nuly vyplývá z definice 7 a již dokázané komutativity násobení.

4) Je 1 neutrální prvek vzhledem k násobení? Z již dokázané komutativity víme, že $1 \cdot a = a \cdot 1$. Také víme, že jednička je $\sigma(0)$. Za využití definice 7 dostáváme:

$$a \cdot \sigma(0) = a \cdot 0 + a = 0 + a.$$

Nula je neutrální prvek ke sčítání. Tedy $0 + a = a$.

1 je proto neutrálním prvkem vzhledem k násobení.

6) Nejprve dokážeme sporem druhé pravidlo pro krácení:

$$a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0).$$

Předpokládejme, že $\exists a, b \in \mathbb{N} : a \neq 0 \wedge b \neq 0 \wedge (a \cdot b = 0)$. Přepíšeme $a \cdot b$ podle definice 6:

$$a \cdot b = (\sigma^a)^b(0).$$

Pokud jsou však čísla a, b nenulová, pak $(\sigma^a)^b(0)$ nemůže být rovno nule, jelikož nula není následníkem žádného přirozeného čísla (viz definice 3, axiom 4). To je spor s předpokladem, že $(a \cdot b = 0)$ a původní věta o krácení platí.

Nyní dokážeme první z pravidel pro krácení. Ptáme se, zda pro všechna $a, b, c \in$ $\in \mathbb{N}$ platí:

$$(c \neq 0 \wedge a \cdot c = b \cdot c) \Rightarrow a = b.$$

Použijeme opět důkaz sporem. Předpokládejme, že $\exists a, b, c \in \mathbb{N} : a \neq b \wedge a \cdot c =$ $= b \cdot c \wedge c \neq 0$. Protože $a \neq b$, víme z věty 7, že nastává buď případ $a > b$, nebo $b > a$. Bez újmy na obecnosti můžeme předpokládat, že $a > b$. Platí potom, že $\exists d \in \mathbb{N} - \{0\} : a = b + d$. Potom $(b + d) \cdot c = b \cdot c$. Využijeme distributivitu násobení vzhledem ke sčítání a dostaneme $b \cdot c + d \cdot c = b \cdot c$. Podle věty 5 zkrátíme $b \cdot c$. Potom $d \cdot c = 0$. Z druhého pravidla o krácení víme, že $d = 0 \vee c = 0$. Protože podle předpokladu je $d \neq 0$, je 0 rovno c. To je ale spor s předpokladem, že $c \neq 0$. Původní věta o krácení je pravdivá.

□

Pozn. 10. Definice a věty v kapitole 4.3 vycházejí ze skript *Posloupnosti a řady* (Kubínová, Novotná, 1997). Důkazy také vycházejí ze stejných skript, případně byly rozšířeny. Věty 3 a 8 jsou vlastní. Důkazy vět 3, 5, 8 a 9 jsou také vlastní.

4.4 Spočetnost

Pomocí přirozených čísel definujeme spočetnost, kterou se budeme zabývat i u nadoborů.

Definice 9. Množinu M nazveme spočetnou, jestliže existuje bijektivní zobrazení množiny M na množinu $\mathbb{N}$.

Pozn. 11. Je-li množina spočetná, lze ji chápat jako posloupnost.

Věta 10. *Množina přirozených čísel je spočetná množina.*

Důkaz. Plyne přímo z definice. Hledáme zobrazení $f\colon \mathbb{N} \to \mathbb{N}$, které je bijektivní. To splňuje například $f(x) = x$. □

Věta 11. *Množina přirozených čísel je nekonečná množina.*

Důkaz. Tvrzení dokážeme sporem. Předpokládejme, že existuje největší prvek množiny přirozených čísel m:

$$\exists m \in \mathbb{N} \quad \forall n \in \mathbb{N} : m \geqq n.$$

Z definice 3 však víme, že pro každý prvek $\mathbb{N}$ existuje jeho následník, který je také prvkem $\mathbb{N}$. Tedy i pro m existuje $\sigma(m)$. Pro takové číslo platí:

$$\sigma(m) > m.$$

To je ovšem ve sporu s předpokladem, že m je největším prvkem množiny $\mathbb{N}$. Množina přirozených čísel je tedy nekonečnou množinou. □

Pozn. 12. Indický matematik Ramanujan ukázal, že součet všech přirozených čísel je roven číslu $\frac{-1}{12}$. Způsob jeho argumentace a metodu sumace divergentní řady popisuje například článek *Divergent Series: why 1+2+3+. . . =-1/12* (Cais, 2010) dostupný online z http://math.arizona.edu/~cais/Papers/Expos/div.pdf.

4.5 Přirozená čísla jako algebraická struktura

Na množině přirozených číslech jsme definovali operace sčítání a násobení. Množina s nimi tvoří hned několik významných algebraických struktur.

Definice 10. Monoid je algebraická struktura s jednou vnitřní operací. Pro operaci platí, že je asociativní a má neutrální prvek.

(Bečvář, 2005)

Věta 12. *Množina* $\mathbb{N}_0$ *spolu s operací* $+$ *tvoří komutativní monoid.*

Důkaz.

1. $\forall a, b \in \mathbb{N}_0 : (a + b) \in \mathbb{N}_0$,
2. $\exists n \in \mathbb{N}_0 \quad \forall a \in \mathbb{N}_0 : n + a = a + n = a$,
3. $\forall a, b \in \mathbb{N}_0 : a + b = b + a$.

Uzavřenost operace $+$ na množině $\mathbb{N}$ platí podle definice 4. Bod druhý, tedy existence neutrálního prvku, platí podle věty 5. Komutativita sčítání je zaručena také z věty 5. □

Věta 13. *Množina* $\mathbb{N}_0$ *spolu s operací* $\cdot$ *tvoří komutativní monoid.*

Důkaz.

1. $\forall a, b \in \mathbb{N}_0 : (a \cdot b) \in \mathbb{N}_0$,
2. $\exists n \in \mathbb{N}_0 \quad \forall a \in \mathbb{N}_0 : n \cdot a = a \cdot n = a$,
3. $\forall a, b \in \mathbb{N}_0 : a \cdot b = b \cdot a$.

Uzavřenost operace násobení na množině přirozených čísel zaručuje definice 6. Existence neutrálního prvku stejně tak jako komutativita vyplývá z věty 9. □

Definice 11. Polookruh je algebraická struktura se dvěma vnitřními operacemi $+$ a $\cdot$. Vzhledem ke sčítání tvoří komutativní monoid a vzhledem k násobení monoid. Operace násobení je vzhledem ke sčítání distributivní.

(Hruša, 1970)

Věta 14. *Množina* $\mathbb{N}_0$ *tvoří spolu s operacemi* $+$ *a* $\cdot$ *polookruh.*

Důkaz. Podle vět 12 a 13 platí, že struktura $(\mathbb{N}, +)$ i struktura $(\mathbb{N}, \cdot)$ tvoří komutativní monoid.

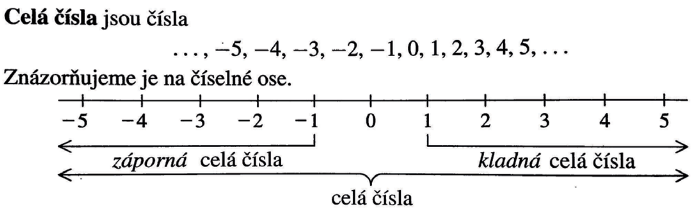
Distributivita pak plyne z věty 9. $\square$

Pozn. 13. Přestože by se množina přirozených čísel mohla zdát jako probádaná, stále ji matematici se zájmem studují. V roce 2013 například český matematik Vopěnka v knize *Nová infinitní matematika* přišel se závěrem, že množina všech přirozených čísel neexistuje.

5 Celá čísla

Pozn. 14. Pokud bychom se drželi historického vývoje číselných oborů, následovala by nyní čísla, která by byla racionální a zároveň nezáporná. My ovšem budeme postupovat podle schématu 1. Pokud bychom totiž nyní definovali čísla racionální, museli bychom po zavedení celých čísel zvlášť dodatečně zavést záporná racionální čísla.

Na základní škole jsou zavedena celá čísla jako čísla kladná, nula a čísla záporná. Záporná jsou taková čísla, která jsou opačná k číslům kladným vzhledem k operaci sčítání. Dále jsou znázorněna na číselné ose, jak ukazuje obrázek 4 z učebnice *MATEMATIKA [1] pro 7. ročník základní školy* (Odvárko, Kadleček, 1998).



Obrázek 4: Celá čísla na číselné ose (Odvárko, Kadleček, 1998, s. 39)

Ve středoškolské učebnici *Matematika pro gymnázia, Základní poznatky z matematiky* (Bušek, Calda, 1992) se o celých číslech hovoří pouze jako o druhu čísel, který umožňuje vyjádřit změnu/nárůst/úbytek. Dále je zavedeno značení $\mathbb{Z}$ (z německého *Zahlen*, což jsou v překladu *čísla*). Nakonec učebnice uvádí věty o operacích sčítání a násobení. Konkrétně jsou uvedeny věty o jejich uzavřenosti, asociativitě, komutativitě, existenci neutrálního prvku, opačných prvků a distributivitě.

Zavedení celých čísel na základní i střední škole předpokládá jisté intuitivní chápání toho, jak budou čísla na ose uspořádána (o tom blíže kapitola 5.4), fungování aritmetických operací na oboru, i toho, že vůbec nějaká záporná čísla mohou existovat. K objevu záporných čísel však vedla dlouhá cesta, jak je popsáno dále.

5.1 Historie záporných a celých čísel

Fine (1907) o záporných číslech říká, že na rozdíl od čísel komplexních a iracionálních, která byla objevena skrze problémy geometrie, záporná čísla vycházejí z řešení algebraických rovnic. Proto je existence celých čísel těsně spjata právě s historií řešení rovnic.

Definice 12. Nechť V, W jsou dva výrazy, z nichž alespoň jeden obsahuje proměnnou. Jsou-li $x_1, x_2, \ldots, x_n$ všechny proměnné, které jsou obsaženy buď ve V, nebo W, nazýváme zápis $V = W$ rovnicí o n neznámých $x_1, x_2, \ldots, x_n$. Výraz V je levá strana, výraz W pravá strana rovnice. Speciálně zápis tvaru $V = 0$, kde V obsahuje alespoň jednu proměnnou, je rovnice v základním tvaru.

(Novotná, Trch, 1993)

O rovnicích se poprvé dočteme ve staroegyptském spisu písaře Ahmese (2000 př. n. l.), který řeší rovnice s jednou neznámou, kterou označuje slovem *hau* znamenajícím *kupa*. Crilly (2007) uvádí jako první Babyloňany, kteří pracovali dokonce s kvadratickými rovnicemi, a to až dva tisíce let před naším letopočtem. (Fine, 1907)

5.1.1 Záporná čísla v Řecku?

V raném Řecku byly hlavním tématem matematiky problémy z oblasti geometrie. Přístup k nim byl čistě syntetický. Algebraizace se objevuje teprve u Eukleida ve třetím století před naším letopočtem a to stále ve spojitosti s geometrickými problémy. Dánský matematik Zeuthen ve svém díle *Die Lehre von den Kegelschnitten im Altertum* (1886) zkoumá práci *Conics* (2. století př. n. l.) matematika Apollónia z Pergy žijícího ve druhém století před naším letopočtem a dochází k závěru, že autor musel využívat algebraického aparátu k popisu geometrických zákonitostí, o kterých hovoří. (Fine, 1907)

Rovnice se poté objevuje až ve spisech Hera z Alexandrie okolo roku 120 před naším letopočtem. Hero měl za cíl složité geometrické pravdy učinit použitelnými a srozumitelnými pro práci zeměměřičů. Geometrii formuloval do vět a problémy řešil pomocí rovnic, ze kterých se tak stal plnohodnotný nástroj geometrů. Hero řešil i rovnice kvadratické. (Fine, 1907)

Poslední z významných řeckých matematiků Diofantos z Alexandrie žijící ve třetím století našeho letopočtu zásadně přispěl k rozvoji teorie týkající se algebraických rovnic a jejich symbolismu. Diofantos využíval označení pro rovnost, neznámou nebo mocninu neznámé. Dále používal speciální znak pro odčítání, zatímco pro sčítání nikoliv. Dvě čísla se sčítala, pokud stála za sebou. Dále se zde také neobjevovaly obecné znaky pro známé hodnoty. Společně se značením přišla i nová pravidla pro algebraické operace. Dále pak Diofantos popsal pravidla pro sčítání, odečítání a násobení polynomů. (Fine, 1907)

Rovnice, které řešil, jsou následujícího tvaru:

1. $ax^m = bx^n$,
2. $ax^2 + bx = c$,
3. $ax^2 + c = bx$,
4. $ax^2 = bx + c$,
5. $y^2 = ax^2 + bx + c$,

kde koeficienty jsou nezáporná čísla. (Proto rozlišujeme případy 2, 3 a 4.)

Dále se v díle *Aritmetika* (Diofantos, 3. st. n. l.) objevuje i jedna rovnice kubická.

Řešením rovnice typu 5 nazýval Diofantos libovolnou dvojici $[x, y]$, pro kterou byla rovnice po dosazení pravdivá. Diofantos ve svém díle nediskutoval počet řešení a za uspokojivé považoval nalezení jednoho řešení, a to i v případě, kdy jich má daná rovnice nekonečně mnoho.

V *Aritmetice* (3. st. n. l.) také nenajdeme popsané obecné postupy výpočtů daných typů rovnic, nýbrž řešení konkrétních příkladů. (Fine, 1907)

Přesto lze vysledovat, jakým způsobem Diofantos a před ním také Hero řešili rovnici typu 3:

$$\begin{aligned} ax^2 + c &= bx, \\ a^2x^2 + ac &= abx, \\ a^2x^2 - abx + \left(\frac{b}{2}\right)^2 &= \left(\frac{b}{2}\right)^2 - ac, \\ ax - \frac{b}{2} &= \sqrt{\left(\frac{b}{2}\right)^2 - ac}, \\ x &= \frac{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 - ac}}{a}. \end{aligned}$$

Za řešení Diofantos považoval pouze takové případy, kdy číslo pod odmocninou bylo nezáporné a zároveň druhou mocninou přirozeného čísla. Zatímco dnes bychom za řešení $x^2 = a$, kde $a \in \mathbb{N}$, považovali $\pm\sqrt{a}$, Difantos bral v potaz pouze řešení s kladným znaménkem. Z toho a z faktu, že Diofantos byl posledním z velkých řeckých matematiků, Fine usuzuje, že řecká matematika o záporných (natož komplexních) číslech nikdy neuvažovala.

Pozn. 15. Fine upozorňuje, že rovnice, které dnes známe pod názvem Diofantické, se v žádném z Diofantových děl nevyskytují. Nazvány po řeckém matematikovi byly zřejmě pro jeho zásluhy v oblasti řešení rovnic jako takových.

5.1.2 Al-Chorezmí

Další pokrok, co se řešení rovnic týče, pak příchází z východu s prací matematika Al-Chorezmího (z jehož jména pochází slovo *algoritmus*). Ve své knize *Hisáb* *al-džabr wa-l-muqábala* (Al-Chorezmí, 825) se zabývá řešitelností lineárních a kvadratických rovnic. V knize se také objevuje slovo *al-džabr* znamenající *skládat dohromady*, které později dalo jméno tomu, co dnes známe jako *algebra*. (Crilly, 2007)

„U Diofanta algebra nebyla ničím více než uměním, jež řeší numerické problémy, mezi kterými neníž souvislosti; v Indii je povýšena na důstojnost vědy se svými vlastními obecnými metodami a koncepty.“

(Fine, 1907, s. 70)

5.1.3 Indie a objev záporných čísel

Na poznání Řeků navázali indičtí astronomové a matematici Árjabhata, Brahmagupta a Bháskara. Geometrii přijali od Hera a neučinili v ní další významné pokroky. Zato algebra přejatá od Diofanta v rukou indických matematiků byla rozvíjena a obohacena o velké množství poznatků. Indové začali více pracovat s obecnými symboly a zaváděli universální značení. Sčítání a odčítání byly značeny obdobně jako u Diofanta, jen nad odčítaným byla napsána tečka. Dále měli symboly pro násobení, dělení nebo odmocninu. (Fine, 1907)

Největším přínosem symbolismu indických matematiků je jejich přístup k odčítání. Na rozdíl od Diofanta, který mezi menšenec a menšitel vložil symbol značící odečítání, v Indii byl symbol odčítání přímo součástí menšitele. To znamená, že problém odčítání byl převeden na problém přičítání záporného čísla. Dalším důsledkem této formy zápisu je fakt, že číslo odečítané nyní mohlo stát samo jako plnohodnotný koeficient v rovnici. (Fine, 1907)

Bháskara dále objevil další vlastnosti odmocnin, uvědomil si, že znaménko po odmocnění může být jak kladné, tak záporné. Díky tomu již byl schopen nacházet oba kořeny kvadratických rovnic. Také zmínil, že odmocnit záporné číslo není možné. Fine tuto poznámku považuje za první výrok týkající se čísel komplexních v historii matematiky. (Fine,1907)

O kladných číslech se zprvu hovořilo jako o *means* znamenajícím *prostředky* a záporných jako o *debt*, tedy *dluh*. (Fine, 1907)

5.1.4 Cardano a Viète

Pro úplnost ještě uvádíme další dva významné matematiky, kteří se zasloužili o rozvoj algebry a řešení rovnic. Prvním byl Cardano, který dokázal, že algebraické rovnice stupně menšího nebo rovného čtyřem je možno řešit algebraicky, tj. vyjádřit kořeny pomocí koeficientů a operací sčítání, odčítání, násobení, dělení, umocnění a odmocnění. Také byl prvním, kdo uspokojivě odůvodnil existenci záporných řešení lineárních rovnic a přijal existenci záporných kořenů odmocniny. (Crilly, 2007; Heffeer, 2011)

Druhým byl Viète, který výrazy začal zapisovat pomocí písmen a přinesl nové metody řešení rovnic. (Crilly, 2007; Heffeer, 2011)

5.2 Descartova Geometrie

Na významu záporná čísla však nabyla až s vydáním dvojice Descarteových knih *Géométrie* (1637). Knihy byly počátkem analytické geometrie. Descartes se snažil veškeré problémy matematiky převést na rovnice a začal právě u geometrie.

Fine (1907) popisuje, jak Descartes v knize *Géométrie, Livre II.* (1637) převáděl křivky na rovnice. Postupoval tak, že známé označil pro nás konvenčním způsobem $a, b, c \ldots$ a neznámé x, y. Obecně poté popisoval každý bod křivky ve vztahu ke zvolené *line of reference* (budeme překládat jako *vztažná přímka*) způsobem, kde nejprve spustil kolmici z bodu křivky ke vztažné přímce a vzdálenost křivky od paty označil y. Vzdálenost paty kolmice od pevně zvoleného bodu na vztažné přímce označil x. Rovnicí křivky rozuměl takovou rovnici, která je platná pro každou dvojici x a y, kterou dostaneme v každém bodě křivky.

Před Descartem ležel problém, jak rozlišit případy, kdy křivka je na jedné, nebo druhé „straně“ vztažné přímky. Jelikož y označovalo pouze vzdálenost od přímky, ztrácela se z rovnice tato informace a například dvě rovnoběžné přímky s přímkou vztažnou, kde jedna by ležela „nad ní“ a druhá „pod ní“ ve stejné vzdálenosti, by měly stejnou rovnici. Descartes proto zavedl, že před délkou kolmic ležících na opačné „strany“ od přímky vztažné budou stát opačná znaménka. (Fine, 1907)

Tento konstrukt čísla záporná postavil na roveň číslům kladným. Nyní byla nepostradatelnými a přestala být něčím nepředstavitelným, jelikož měla reálnou aplikaci, kterou bylo možné graficky znázornit. (Fine, 1907)

Pozn. 16. V předchozím textu jsme mluvili o tzv. vztažné přímce. Z dnešního pohledu by se jednalo o osu x, pevně zvolený bod by byl počátek soustavy souřadnic a délky x, y bychom nazvali souřadnicemi. Fine (1907) píše, že Descartes sám nepoužíval pevně zvolenou soustavu os, kterou dnes známe pod jeho jménem jako kartézskou.

5.3 Konstrukce celých čísel

V konstrukci budeme postupovat podle následujících kroků tak, jak je uvedeno ve skriptech *Posloupnosti a řady* (Kubínová, Novotná, 1997, s. 146):

1. Konstrukce množiny $\mathbb{Z}$
   a) Na $\mathbb{N} \times \mathbb{N}$ zadefinujeme vhodnou relaci. Označíme ji $\sim$.
   b) Ověříme, že $\sim$ je ekvivalencí na $\mathbb{N}$.
   c) Rozklad množiny $\mathbb{N} \times \mathbb{N}$ podle ekvivalence $\sim$ nazveme množinou $\mathbb{Z}$.
2. Vytvoření Abelovy grupy $(\mathbb{Z}, +)$
   a) Definujeme operaci sčítání na $\mathbb{Z}$.

b) Ověříme, že struktura $(\mathbb{Z}, +)$ je skutečně Abelova grupa.

c) Najdeme souvislost mezi $(\mathbb{N}, +)$ a $(\mathbb{Z}, +)$.

d) Izomorfně vnoříme $(\mathbb{N}, +)$ do $(\mathbb{Z}, +)$.

1.a) Relaci na $\mathbb{N} \times \mathbb{N}$ definujeme takto:

$$(a, b) \sim (c, d) \Leftrightarrow (a + d = c + b).$$

(Kubínová, Novotná, 1997)

Pozn. 17. V relaci jsou tedy například dvojice $(1, 2)$ a $(4, 5)$ protože:

$$1 + 5 = 4 + 2.$$

1.b)

Věta 15. *Relace* $\sim$ *na* $\mathbb{N} \times \mathbb{N}$ *je ekvivalence.*

Důkaz. Chceme ukázat, že $\sim$ je reflexivní, symetrická a tranzitivní.

i) $\sim$ je reflexivní $\Leftrightarrow \forall (a, b) \in (\mathbb{N} \times \mathbb{N}) : (a, b) \sim (a, b)$.

Pro $\forall a, b \in \mathbb{N}$ platí, že $a + b = a + b$. Z toho podle definice $\sim$ plyne $(a, b) \sim (a, b)$.

Relace $\sim$ je reflexivní.

ii) $\sim$ je symetrická $\Leftrightarrow (\forall (a, b), (c, d) \in (\mathbb{N} \times \mathbb{N}) : (a, b) \sim (c, d) \Rightarrow (c, d) \sim \sim (a, b))$.

Platí $(a, b) \sim (c, d)$. Z toho vyplývá $a + d = c + b$. To lze díky symetrii relace $=$ zapsat jako $c + b = a + d$, což z definice relace $\sim$ platí právě tehdy, když $(c, d) \sim (a, b)$.

Relace $\sim$ je symetrická.

iii) $\sim$ je tranzitivní $\Leftrightarrow (\forall (a,b),(c,d),(e,f) \in (\mathbb{N} \times \mathbb{N}))$:
$((a,b) \sim (c,d) \wedge (c,d) \sim (e,f)) \Rightarrow ((a,b) \sim (e,f))$.

Vyjdeme z předpokladů, které přepíšeme pomocí definice, tedy:

$$a + d = c + b,$$
$$c + f = e + d.$$

K první rovnosti přičteme f, ke druhé b. Získáváme tedy:

$$a + d + f = c + b + f,$$
$$c + f + b = e + d + b.$$

Pravá strana první rovnosti se rovná levé straně druhé (využijeme komutativitu přirozených čísel). Proto tedy platí:

$$a + d + f = e + d + b.$$

Můžeme využít pravidlo pro krácení z věty 5. Tím získáme rovnost $a + f = e + b$, což je ale z definice relace $\sim$ právě $(a,b) \sim (e,f)$. Relace $\sim$ je tedy tranzitivní relací.

Ukázali jsme, že relace je reflexivní, symetrická i tranzitivní, a je tedy ekvivalencí na $\mathbb{N} \times \mathbb{N}$. $\square$

1.c)

Definice 13. Množinou celých čísel $\mathbb{Z}$ nazveme rozklad na $\mathbb{N} \times \mathbb{N}$ podle ekvivalence $\sim$. Třídy tohoto rozkladu jsou prvky množiny $\mathbb{Z}$. Tedy platí:

$$\mathbb{Z} = \{T_{(a,b)}; (a,b) \in \mathbb{N} \times \mathbb{N}\}, T_{(a,b)} = \{(x,y) \in \mathbb{N} \times \mathbb{N}; (x,y) \sim (a,b)\}.$$

(Kubínová, Novotná, 1997)

2.a) Nyní na množině $\mathbb{Z}$, kterou jsme sestrojili, definujeme operaci $+$ takto:

Definice 14. $\forall T_{(a,b)}, T_{(c,d)} \in \mathbb{Z} : T_{(a,b)} + T_{(c,d)} = T_{(a+c,b+d)}$.

Aby byla definice 14 korektní, musí splňovat následující dvě podmínky:

i) $T_{(a+c,b+d)} \in \mathbb{Z}$,

ii) $\forall (x,y) \in T_{(a,b)}, \forall (u,v) \in T_{(c,d)} : (x+u, y+v) \in T_{(a+c,b+d)}$.

i) platí, jelikož každý prvek $T_{(x,y)}$, kde $x, y \in \mathbb{N}$, je z množiny $\mathbb{Z}$, tedy i $T_{(a+c,b+d)}$. (Součet dvou přirozených čísel je znovu přirozené číslo podle definice 4.)

ii) je nutné ověřit:

$$\forall (x,y) \sim (a,b), \forall (u,v) \sim (c,d) : (x+u, y+v) \sim (a+c, b+d).$$

Opět přepíšeme předpoklady podle definice relace $\sim$: $(x+b = a+y) \wedge (u+d = c+v)$. Rovnosti sečteme a dostáváme $x+b+u+d = a+y+c+v$. Využijeme komutativitu sčítání přirozených čísel (viz věta 5) a poslední rovnost přepíšeme jako $x+u+b+d = a+c+y+v$, což ale je právě $(x+u, y+v) \sim (a+c, b+d)$. Tedy i druhá podmínka pro korektnost definice sčítání je splněna.

(Kubínová, Novotná, 1997)

2.b) Ptáme se, zda množina $\mathbb{Z}$ s operací $+$ tvoří Abelovu grupu.

Věta 16. *Struktura* $(\mathbb{Z}, +)$ *je Abelovou grupou.*

(Kubínová, Novotná, 1997)

Důkaz. Aby struktura byla Abelovou grupou, musí platit:

i. $T_{(a,b)}, T_{(c,d)} \in \mathbb{Z} \Rightarrow T_{(a,b)} + T_{(c,d)} \in \mathbb{Z}$,

ii. $\forall T_{(a,b)}, T_{(c,d)} \in \mathbb{Z} : T_{(a,b)} + T_{(c,d)} = T_{(c,d)} + T_{(a,b)}$,

iii. $\forall T_{(a,b)}, T_{(c,d)}, T_{(e,f)} \in \mathbb{Z} : (T_{(a,b)} + T_{(c,d)}) + T_{(e,f)} = T_{(a,b)} + (T_{(c,d)} + T_{(e,f)})$,

iv. $\exists T_{(x,y)} \in \mathbb{Z} \quad \forall T_{(a,b)} \in \mathbb{Z} : T_{(a,b)} + T_{(x,y)} = T_{(x,y)} + T_{(a,b)} = T_{(a,b)}$,

v. $\forall T_{(a,b)} \in \mathbb{Z} \quad \exists T_{(x,y)} \in \mathbb{Z} : T_{(a,b)} + T_{(x,y)} = T_{(0,0)}$.

i. Uzavřenost operace + byla jednou z ověřovaných podmínek po zavedení definice 14. Sčítání celých čísel je tedy vnitřní operace na množině $\mathbb{Z}$.

ii. Pro důkaz komutativity přepíšeme zvlášť levou a zvlášť pravou stranu rovnosti:

$$\left.\begin{aligned} L &= T_{(a,b)} + T_{(c,d)} = T_{(a+c,b+d)} \\ P &= T_{(c,d)} + T_{(a,b)} = T_{(c+a,d+b)} \overset{def.\,5}{=} T_{(a+c,b+d)} \end{aligned}\right\} L = P.$$

Sčítání celých čísel je komutativní.

iii. Dokážeme asociativitu sčítání celých čísel. Chceme ukázat, že pro všechna $T_{(a,b)}, T_{(c,d)}, T_{(e,f)} \in \mathbb{Z}$ platí $\Big(T_{(a,b)} + T_{(c,d)}\Big) + T_{(e,f)} = T_{(a,b)} + \Big(T_{(c,d)} + T_{(e,f)}\Big)$. Pro sčítání použijeme definici 14. Upravíme zvlášť levou a pravou stranu rovnosti a ukážeme, že se strany rovnají:

$$\left.\begin{aligned} L &= \Big(T_{(a,b)} + T_{(c,d)}\Big) + T_{(e,f)} = \Big(T_{(a+c,b+d)}\Big) + T_{(e,f)} = T_{(a+c+e,b+d+f)} \\ P &= T_{(a,b)} + \Big(T_{(c,d)} + T_{(e,f)}\Big) = T_{(a,b)} + \Big(T_{(c+e,d+f)}\Big) = T_{(a+c+e,b+d+f)} \end{aligned}\right\} L = P.$$

Sčítání celých čísel je asociativní.

iv. Dokážeme existenci neutrálního prvku. Zvolme za hledanou třídy $T_{(n,n)}$, kde $n \in \mathbb{N}$. Ověříme, že platí $T_{(a,b)} + T_{(n,n)} = T_{(a,b)}$. Vyjdeme z rovnosti $a+b+n = a+b+n$, kde $a, b, n \in \mathbb{N}$. Využijeme komutativitu a asociativitu sčítání přirozených čísel podle věty 5 a dostáváme rovnost $a + (b + n) =$ $= (a + n) + b$. Pak ovšem z definice relace $\sim$ platí $(a, b) \sim (a + n, b + n)$.

Podle definice 13 platí, že pokud $(a, b) \sim (a+n, b+n)$, pak se rovnají i třídy $T_{(a,b)}$ a $T_{(a+n,b+n)}$. Platí:

$$T_{(a,b)} = T_{(a+n,b+n)}.$$

Pravá strana rovnosti lze podle definice 14 přepsat jako $T_{(a,b)} + T_{(n,n)}$. Tudíž víme, že platí:

$$T_{(a,b)} + T_{(n,n)} = T_{(a,b)}.$$

Že $T_{(a,b)} + T_{(n,n)} = T_{(n,n)} + T_{(a,b)}$, už víme z dokázané komutativity sčítání celých čísel. $T_{(n,n)}$ je tedy neutrálním prvkem vzhledem ke sčítání celých čísel.

Pozn. 18. Podle definice 13 platí, že třída $T_{(n,n)} = T_{(0,0)}$.

v. Dokážeme existenci opačných prvků. Nechť $T_{(a,b)} \in \mathbb{Z}$. Dokážeme, že pro $T_{(b,a)} \in \mathbb{Z}$ platí $T_{(a,b)} + T_{(b,a)} = T_{(0,0)}$. Vyjdeme z rovnosti $a + b = a + b$, kde $a, b \in \mathbb{N}$. Využijeme komutativitu a neutrálnost prvku 0 vzhledem ke sčítání přirozených čísel podle věty 5 a dostáváme rovnost $a+b+0 = = 0 + b + a$. Pak z definice relace $\sim$ platí $(a + b, b + a) \sim (0, 0)$. Podle definice relace $\sim$ platí, že pokud $(a + b, b + a) \sim (0, 0)$, pak se rovnají i třídy $T_{(a+b,b+a)}$ a $T_{(0,0)}$. Tudíž platí:

$$T_{(a+b,b+a)} = T_{(0,0)}.$$

Levá strana rovnosti lze rozepsat podle definice 14 jako $T_{(a,b)} + T_{(b,a)}$. Tudíž platí:

$$T_{(a,b)} + T_{(b,a)} = T_{(0,0)}.$$

Opačným prvkem pro každý prvek $T_{(a,b)} \in \mathbb{Z}$ je prvek ve tvaru $T_{(b,a)} \in \mathbb{Z}$.

Množina celých čísel s operací + je tedy Abelovou grupou. □

2.c) Přirozená čísla nejsou podmnožinou čísel celých. Ovšem můžeme zkonstruovat podstrukturu $(\mathbb{Z}', +)$, která bude se stukrurou $(\mathbb{N}, +)$ izomorfní. (Kubínová, Novotná, 1997)

Věta 17. *Ve struktuře* $(\mathbb{Z}, +)$ *existuje podstruktura* $(\mathbb{Z}', +)$*, která je s* $(\mathbb{N}, +)$ *izomorfní.*

Důkaz. Zkonstruujeme $(\mathbb{Z}', +)$:

$$\mathbb{Z}' = \{T_{(z,0)}; z \in \mathbb{N}\}, + \text{ je zúžením operace sčítání ze } \mathbb{Z} \text{ na } \mathbb{Z}'.$$

Aby platilo, že $(\mathbb{N}, +)$ je izomorfní s $(\mathbb{Z}', +)$, musí existovat bijektivní zobrazení $\varphi : \mathbb{N} \to \mathbb{Z}$, pro které navíc platí: $\forall x, y \in \mathbb{N} : \varphi(x + y) = \varphi(x) + \varphi(y)$.

Zobrazení definujeme takto:

$$\forall x \in \mathbb{N} : \varphi(x) = T_{(x,0)}.$$

(Kubínová, Novotná, 1997, s. 147)

Je bijektivní?

- Nejprve ukážeme, že zobrazení φ je injektivní. Ukážeme, že platí:

  $$\forall x_1, x_2 \in \mathbb{N} : x_1 \neq x_2 \Rightarrow \varphi(x_1) \neq \varphi(x_2).$$

  Tvrzení dokážeme sporem. Předpokládejme, že $\exists x_1, x_2 \in \mathbb{N}(x_1 \neq x_2) \wedge$ $\wedge(\varphi(x_1) = \varphi(x_2))$. Pak se ovšem $T_{(x_1,0)} = T_{(x_2,0)}$, což nastává právě tehdy, když $(x_1, 0) \sim (x_2, 0)$. Pak platí $x_1 + 0 = x_2 + 0$, což podle věty 5 přepíšeme jako $x_1 = x_2$. To je spor s předpokladem, že x_1 a x_2 jsou různá.

  Zobrazení φ je injektivní.

- Ukážeme, že zobrazení φ je surjektivní. Tedy že platí:

$$\forall T_{(x,0)} \in \mathbb{Z} \quad \exists x \in \mathbb{N} : \varphi(x) = T_{(x,0)}.$$

  Z definice celých čísel platí, že pro každý prvek $T_{(a,b)}$ jsou $a, b \in \mathbb{N}$. Tedy i x z celého čísla $T_{(x,0)}$ je přirozené číslo. Pro x platí $\varphi(x) = T_{(x,0)}$.

  Zobrazení φ je surjektivní.

Zobrazení φ je injektivní i surjektivní. Je tedy bijekce.

Ověříme, zda platí:

$$\varphi(x + y) = \varphi(x) + \varphi(y).$$

Obě strany rovnosti přepíšeme podle definice zobrazení φ:

$$\left.\begin{aligned} L &= \varphi(x + y) = T_{(x+y,0)} = T_{(x,0)} + T_{(y,0)} \\ P &= \varphi(x) + \varphi(y) = T_{(x,0)} + T_{(y,0)} \end{aligned}\right\} L = P.$$

Platí tedy $\varphi(x+y) = \varphi(x)+\varphi(y)$. Struktura $(\mathbb{Z}', +)$ je izomorfní se strukturou $(\mathbb{N}, +)$. □

2.d) Jestliže položíme $\forall x \in \mathbb{N} : x \equiv T_{(x,0)}$, je $\mathbb{N} \subset \mathbb{Z}$. (Kubínová, Novotná, 1997, s. 148)

Věta 18. $\forall T_{a,b} \quad \exists! c \in \mathbb{N} : \left(T_{(a,b)} = T_{(c,0)}\right) \vee \left(T_{(a,b)} = T_{(0,c)}\right).$

Důkaz. Podle věty 7 platí pro přirozená čísla a, b právě jedna z následujících možností:

- $a < b : \exists! c \in \mathbb{N} - \{0\} : a + c = b$, pak

$$T_{(a,b)} = T_{(a,a+c)} = T_{(a+0,a+c)} = T_{(a,a)} + T_{(0,c)} = T_{(0,0)} + T_{(0,c)} = T_{(0,c)}$$

- $a = b : T_{(a,b)} = T_{(a,a)} = T_{(0,0)}$, c položíme rovno nule a platí.

- $a > b : \exists! c \in \mathbb{N} - \{0\} : b + c = a$ pak,

$$T_{(a,b)} = T_{(b+c,b)} = T_{(b+c,b+O)} = T_{(b,b)} + T_{(c,0)} = T_{(0,0)} + T_{(c,0)} = T_{(c,0)}.$$

Jednoznačnost plyne z krácení přirozených čísel (viz věta 5). □

(Kubínová, Novotná, 1997, s. 148)

Pozn. 19. Typy tříd z věty 18 budeme nazývat a značit takto:

- Množinu $\{T_{(c,0)} \in \mathbb{Z}; c \neq 0\}$ nazveme množinou kladných celých čísel a její prvky kladnými čísly. Budeme ji značit $\mathbb{Z}^+$. Třídu $T_{(c,0)}$ budeme značit zkráceně c.

- Množinu $\{T_{(0,c)} \in \mathbb{Z}; c \neq 0\}$ nazveme množinou záporných celých čísel a její prvky zápornými čísly. Budeme ji značit $\mathbb{Z}^-$. Třídu $T_{(0,c)} = -T_{(c,0)}$ budeme značit zkráceně $-c$.

- Nulu nebudeme zahrnovat ani do jedné z množin $\mathbb{Z}^+, \mathbb{Z}^-$. Budeme ji považovat za číslo, které není ani kladné, ani záporné. Třídu $T_{(0,0)}$ budeme značit 0.

  Platí tedy, že $\mathbb{Z} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+$.

(Kubínová, Novotná, 1997)

Definice 15. Operaci násobení $\odot$ na celých číslech definujeme jako:

$$\begin{aligned} a \odot b &= a \cdot b \quad \forall a, b \in \mathbb{N}; \\ &= (-a) \cdot (-b) \quad \forall a, b \in \mathbb{Z}^-; \\ &= -((-a) \cdot b)) \quad \forall a \in \mathbb{Z}^-, b \in \mathbb{N}; \\ &= -(a \cdot (-b)) \quad \forall a \in \mathbb{N}, b \in \mathbb{Z}^-. \end{aligned}$$

(Kubínová, Novotná, 1997)

Pozn. 20. Násobení celých čísel lze zavést také pomocí tříd:

$$\forall T_{(a,b)}, T_{(c,d)} \in \mathbb{Z} : T_{(a,b)} \cdot T_{(c,d)} = T_{(a \cdot c + b \cdot d, a \cdot d + b \cdot c)}.$$

Aby byla definice násobení korektní, musí splňovat následující dvě podmínky:

i) $T_{(a \cdot c + b \cdot d, a \cdot d + b \cdot c)} \in \mathbb{Z}$,

ii) $\forall (x, y) \in T_{(a,b)}, \forall (u, v) \in T_{(c,d)} : (x \cdot u + y \cdot v, x \cdot v + y \cdot u) \in T_{(a \cdot c + b \cdot d, a \cdot d + b \cdot c)}$.

Pozn. 21. Násobení celých čísel jsme definovali pomocí násobení čísel přirozených $(\cdot)$, proto se přenáší vlastnost komutativity, asociativity, distributivity násobení vzhledem ke sčítání, existence neutrálního prvku a pravidla krácení pro násobení z $\mathbb{N}$ na $\mathbb{Z}$.

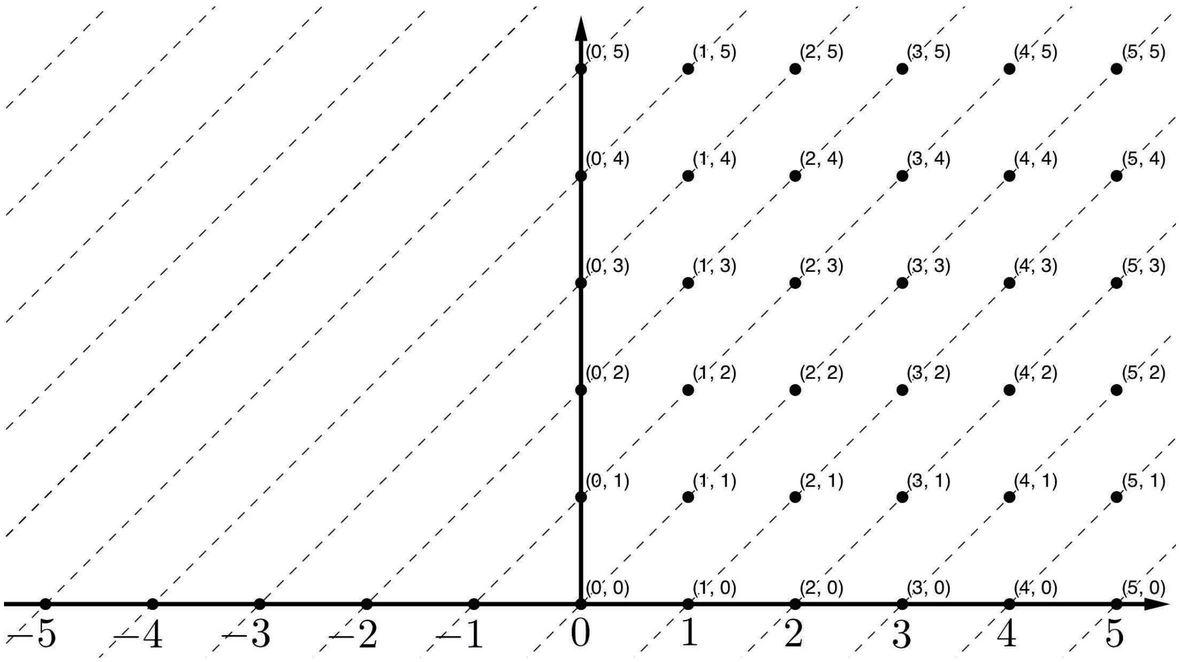
Pozn. 22. Definice 15 využívá podobné logiky jako Euler při argumentaci, proč mínus krát mínus dává plus (viz 5.4.2), a sice té, že popíše všechny případy, které mohou nastat pro pravou stranu.

Třídy ekvivalence po zavedení značení z poznámky 19 můžeme znázornit obrázkem 5. Souřadnice bodů odpovídají uspořádaným dvojicím přirozených čísel, šrafovaná čára znázorňuje třídu ekvivalence. Číslo na konci této čáry odpovídá označení této třídy, tedy označení prvku množiny celých čísel.

Pozn. 23. Věty, důkazy a definice v kapitole 5.3 jsou převzaty ze skript (Kubínová, Novotná, 1997). Důkazy vět 15 a první dva body důkazu 16 jsou vlastní, třetí bod vychází také ze skript (Kubínová, Novotná, 1997).

5.4 Celá čísla a číselná osa

V úvodu kapitoly 5 jsme zmínili číselnou osu jako způsob grafické interpretace celých čísel na základní škole. S chápáním číselné osy v souvislosti se zápornými čísly



Obrázek 5: Rozklad podle ekvivalence (vlastní obrázek)

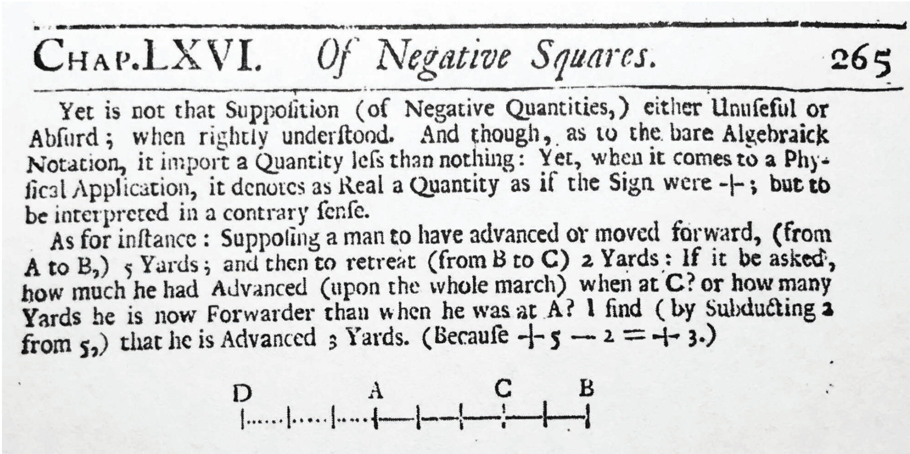
ovšem vznikla v historii celá řada problémů, jimiž se v sedmnáctém a osmnáctém století zabývali matematici jako Euler, Leibnitz nebo d'Alembert. (Heeffer, 2011)

Jak v článku *Historical objections against the number line* (2011) říká Heeffer, je důležité rozumět těmto problémům, které v chápání koncept záporných čísel na ose způsobil v historii, zejména pro učitele, kteří tak snáze dokáží porozumět obtížím žáků s uchopením záporných čísel.

Definice 16. Číselnou osou rozumíme reprezentaci čísel na přímce, na níž jsou body představující celá/reálná čísla. Vzdálenost mezi body číselně odpovídá rozdílu mezi příslušnými čísly. V západní kultuře obvykle znázorňujeme vodorovně, tak, že kladná čísla jsou směrem vpravo, záporná vlevo od nuly. (Heeffer, 2011)

Jako první číselnou osu představil Wallis ve své knize *Algebra* (1685) v souvislosti se slovní úlohou o vzdálenosti (viz obrázek 6). (Heeffer, 2011)

Heeffer (2011) se zamýšlí nad přínosy a nedostatky tohoto modelu. Model od-



CHAP. LXVI. *Of Negative Squares.* 265

Yet is not that Suppoſition (of Negative Quantities,) either Unuſeful or Abſurd; when rightly underſtood. And though, as to the bare Algebraick Notation, it import a Quantity leſs than nothing: Yet, when it comes to a Phyſical Application, it denotes as Real a Quantity as if the Sign were +; but to be interpreted in a contrary ſenſe.

As for inſtance: Suppoſing a man to have advanced or moved forward, (from A to B,) 5 Yards; and then to retreat (from B to C) 2 Yards: If it be asked, how much he had Advanced (upon the whole march) when at C? or how many Yards he is now Forwarder than when he was at A? I find (by Subducting 2 from 5,) that he is Advanced 3 Yards. (Becauſe $+5 - 2 = +3$.)

Obrázek 6: První výskyt číselné osy v knize Wallise *Algebra* (1685)

Obrázek převzat od Heeffera (2011, s. 14).

povídá množině $\mathbb{Z}$ v tom, že pro každé číslo existuje číslo větší i menší, a stejně tak osa, tedy přímka, lze „protáhnout" do nekonečna na obou jejích stranách. Osa také dobře znázorňuje rozdíly mezi čísly a v případě racionálních čísel je vhodným nástrojem pro představu, mezi která dvě celá čísla zlomek patří. Jako nedostatky osy Heeffer (2011) spatřuje znázornění aritmetických operací jako násobení, dělení nebo poměry v kombinaci se záporným číslem. Dále si klade otázku, zda je umístění nuly jako předělu mezi kladnými a zápornými čísly zejména pro žáky intuitivní a zda je představení celých čísel osou vůbec vhodné. Z tohoto důvodu zmiňuje problémy, se kterými se v historii matematici potýkali a o nichž budou následující kapitoly.

5.4.1 Poměr

Jako první na problémy s osou a intuitivním chápáním celých čísel upozornil Arnauld. V knize *Geometry* (1667) zmínil vlastnost, že pokud zvolíme přirozené číslo

n větší než jedna, poměr čísel $n+1$ ku $n-1$ bude vždy větší než poměr převrácený:

$$\frac{n+1}{n-1} > \frac{n-1}{n+1},$$

jakmile však k přirozeným číslům na ose přidáme opačná čísla (stále za podmínky, že nedělíme nulou), přestává vlastnost, že větší číslo ku menšímu je větší než menší číslo ku většímu, platit. Uvádí to na následujícím případu:

$$\frac{1}{-1} > \frac{-1}{1},$$

to evidentně neplatí. (Heeffer, 2011)

5.4.2 Mínus krát mínus

Dále Heeffer (2011) uvádí součin dvou záporných čísel. Vlastnost, kterou dnes známe (viz definice 15), není, jak říká, z osy patrná.

Čemu je roven takový součin, se zabýval v pojednání *Aliabraa argibra* (1344) Dardi. Vysvětlil na konkrétním příkladě za využití distributivity, proč se součin dvou záporných čísel musí rovnat číslu kladnému:

$$64 = 8 \cdot 8 = (10-2)(10-2) = 100 - 20 - 20 + ((-2)(-2)),$$

aby rovnost platila, musí se součin $(-2)(-2)$ rovnat 4.

Obecněji vztahy mezi znaménky stanovil na konci patnáctého století Paciolli v díle *Summa* (1494). Viz obrázek 7 a 8. (Heeffer, 2011)

Ve volném překladu z italštiny tabulka na obrázku 7 stanoví:

„Součin kladného s kladným je kladný."

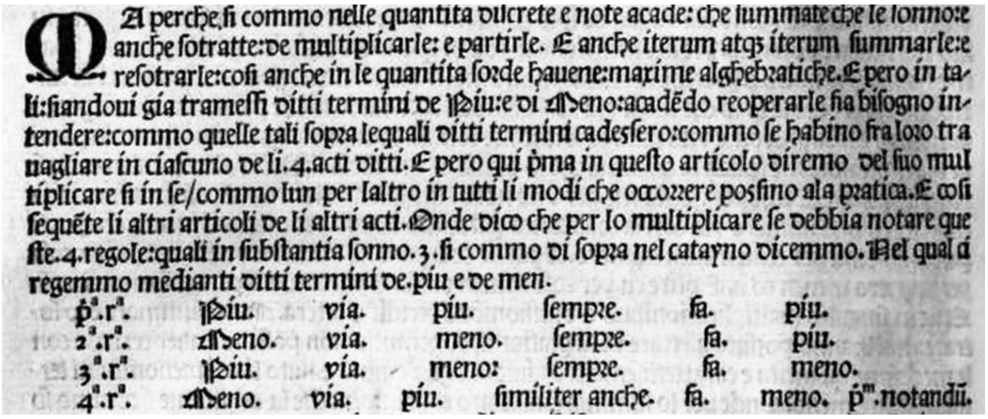
„Součin záporného se záporným je kladný."

„Součin kladného se záporným je záporný."

„Součin záporného s kladným je záporný."

Obdobně tabulka v překladu na obrázku 8 popisuje:

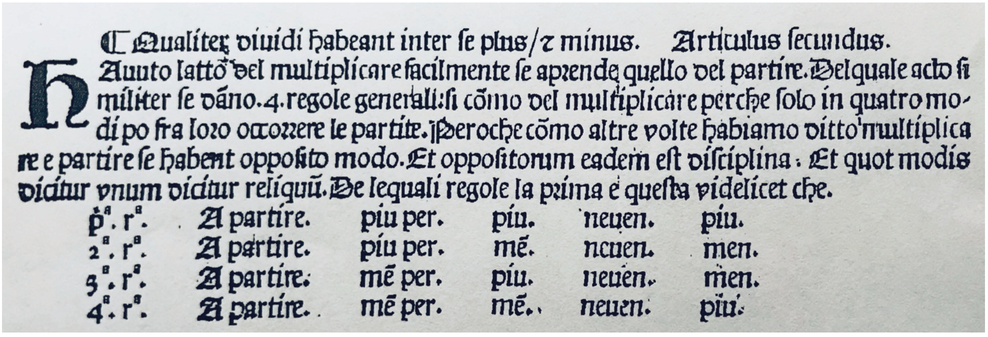
„Podíl kladného s kladným je kladný."



Ma perche, si commo nelle quantita discrete e note acade: che summate che le sonno: e anche sotratte: de multiplicarle: e partirle. E anche iterum atq3 iterum summarle: e resotrarle: cosi anche in le quantita sorde hauene: maxime algebratiche. E pero in tali: siandoui gia tramessi ditti termini de Piu: e di Meno: acadēdo reoperarle fia bisogno intendere: commo quelle tali sopra lequali ditti termini cadessero: commo se habino fra loro tra nagliare in ciascuno de li.4.acti ditti. E pero qui pma in questo articolo diremo del suo multiplicare si in se/commo lun per laltro in tutti li modi che occorrere posino ala pratica. E cosi sequēte li altri articoli de li altri acti. Onde dico che per lo multiplicare se debbia notare queste.4.regole: quali in substantia sonno.3.si commo di sopra nel catayno dicemmo. Nel qual dirigemmo medianti ditti termini de.piu e de men.

$p^a.r^a.$	Piu.	via.	piu.	sempre.	fa.	piu.	
$2^a.r^a.$	Meno.	via.	meno.	sempre.	fa.	piu.	
$3^a.r^a.$	Piu.	via.	meno:	sempre.	fa.	meno.	
$4^a.r^a.$	Meno.	via.	piu.	similiter anche.	fa.	meno.	p^m.notandū.

Obrázek 7: Pravidla pro znaménka při násobení (Paciolli, 1494, s. 112)



Qualiter diuidi habeant inter se plus/& minus. Articulus secundus.

Hauuto lattō del multiplicare facilmente se aprende quello del partire. Del quale acto similiter se dāno.4.regole generali: si cōmo del multiplicare perche solo in quatro modi po fra loro occorrere le partite. Peroche cōmo altre volte habiamo ditto multiplicare e partire se habent opposito modo. Et oppositorum eadem est disciplina: Et quot modis dicitur vnum dicitur reliquū. De lequali regole la prima e questa videlicet che.

$p^a.r^a.$	A partire.	piu per.	piu.	neuen.	piu.
$2^a.r^a.$	A partire.	piu per.	mē.	neuen.	men.
$3^a.r^a.$	A partire.	mē per.	piu.	neuen.	men.
$4^a.r^a.$	A partire.	mē per.	mē.	neuen.	piu.

Obrázek 8: Pravidla pro znaménka při dělení (Paciolli, 1494, s. 113)

„Podíl kladného se záporným je záporný.“

„Podíl záporného s kladným je záporný.“

„Podíl záporného se záporným je kladný.“

Důležitým pozorováním na tabulkách je, že zcela upustily od hodnot a pravidla jsou stanovena zcela obecně. (Paciolli, 1494; Heeffer, 2011)

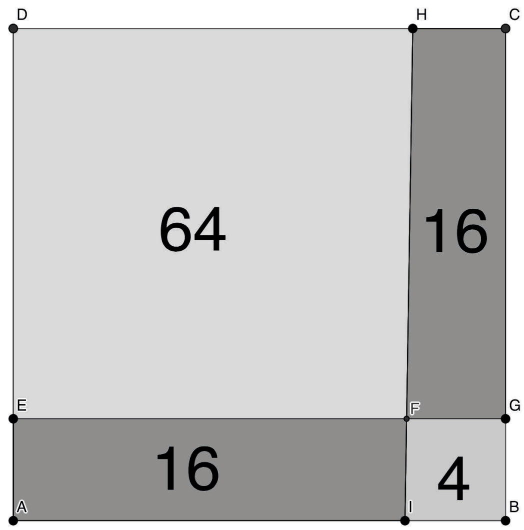
Dardiho argumentaci zpochybnil Cardano v dílech *De Aliza Regulae* (1570) a *Sermo de plus and minus* (1663). Vyšel ze stejného příkladu jako Dardi a tvrdil, že stejně, jako z něj můžeme usuzovat, že mínus krát mínus dává plus, můžeme také říct, že plus krát plus dává mínus. Cardano argumentoval takto:

1. Mějme čtverec $ABCD$ o délce strany 10 (viz obrázek 9).
2. Obsah čterce $IBGF$ je roven 4 a obsahy shodných obdélníků $AIFE$ a $FGCH$ jsou rovny 16.
3. Obsah čtverce $EFHD$ je tedy 64.
4. Abychom ze 100 dostali 64, musíme odebrat obdélník $ABGE$ a $IBCH$.
5. Tím jsme ovšem odebrali čtverec $IBGF$ dvakrát, musíme ho tedy jednou přičíst.

Neboli:

$$100 - (10 \cdot 2) - (10 \cdot 2) + (2 \cdot 2) = 64.$$

To je rovno $(10 - 2) \cdot (10 - 2)$ stejně, jako tomu bylo v případě Dardiho, ovšem podle Cardana je přičtená čtyřka důsledek dvojnásobného odečtení čtverce, nikoliv součinu $(-2) \cdot (-2)$. (Heeffer, 2011)



Obrázek 9: Dardi vs. Cardano (vlastní obrázek)

Cardano uzavřel svůj argument slovy, že stejně jako můžeme tvrdit, že mínus krát mínus dává plus, můžeme říct, že mínus krát mínus dává mínus (Heeffer, 2011). Heeffer soudí, že Cardano chtěl touto demonstrací poukázat, že je třeba i zákonitosti, které jsou obecně příjmány nebo se jeví jako samozřejmé, zakotvit v definicích a blíže prozkoumat. Odůvodnění matematiků tehdejší doby včetně Dardiho pro Cardana nebylo uspokojivé, a tak ukázal, jak jednoduše lze Dardiho argumentaci napadnout.

5.4.3 Podíl větší než nekonečno

Wallis v *Arithmetica Infinitorium* (1656) představuje v souvislosti s problematikou kvadratury křivek, kterou se zabýval, myšlenku, že dělíme-li kladné číslo záporným, dostáváme číslo větší než nekonečno. Úvahu stavěl na tom, že čím menším číslem dělíme, tím větší číslo dostáváme. Dělíme-li nulou, dostáváme podle Wallise nekonečno (původně Bháskarova myšlenka, viz 2.2), a překročíme-li tuto mez a dělíme stále menšími čísly, dostaneme čísla větší než samotné nekonečno. (Heeffer, 2011)

Ke stejnému závěru dospěl v textu *De seriebus divergentibus* (1746) Euler (Heeffer, 2011). Euler zavedl rozdělení na dvě záporna:

1. Záporno prvního druhu je takové, které dostaneme, odečteme-li od čísla a jeho následníka $\sigma(a)$.

2. Jako záporno druhého druhu Euler chápal výsledek dělení kladného čísla záporným, tedy například $\frac{1}{-1}$, nebo případy, kdy se sčítaly divergentní řady a výsledky byly záporné.

(Heeffer, 2011)

První druh jsou záporná čísla menší než nula. Druhý druh jsou záporná čísla větší než nekonečno. To Euler demonstroval na obdobném příkladu jako Wallis:

$$\frac{1}{3}, \frac{1}{2}, \frac{1}{1}, \frac{1}{0}, \frac{1}{-1}, \frac{1}{-2}, \ldots,$$

směrem zleva do prava čísla rostou, až dosáhnou nekonečna, a tak budou podle Eulera růst i nadále až přes nekonečno. (Heeffer, 2011)

Heeffer zmiňuje miskoncepce mnohých historiků (Kline, Dunham, Sandifer, …), kteří tato pozorování interpretovali tak, že Euler s Wallisem tvrdili, že záporná čísla na ose nemají místo vlevo od nuly, nýbrž za nekonečnem. Euler sám ve své knize elementární algebry (1822) napsal, že záporná čísla jsou méně než ničím. To také demonstroval na ose tím, že od nuly odečítal opakovaně -1 (obdoba následníka v přirozených číslech). Dále přišel s argumentem, proč součin dvou záporných čísel je kladný. Řekl, že víme-li, že mínus krát plus je mínus, musí mínus krát mínus mít jiný výsledek, tedy plus. (Heeffer, 2011)

D'Alembert v *Encyclopédie* (1761-1790) o záporných číslech zmiňuje: „Záporné kvantity jsou ty, které jsou ovlivněny znaménkem mínus a které jsou několika matematiky považovány za menší než nula. Poslední myšlenka je chybná, jak bude za moment vidno." (d'Alembert, 1785, s. 445) Argumentoval poté tím, že nemůžeme tvrdit, že záporná čísla jsou menší než nula, protože ne vždy musí přejít z kladných do záporných právě přes nulu. To ukázal na příkladu $y = x - a$, který přes nulu z kladných do záporných vždy přejde, a poté na příkladu $y = \frac{1}{x-a}$, kdy z kladných do záporných nepřecházíme přes nulu, nýbrž nekonečno (pro hodnotu $x = a$). Proto není podle d'Alemberta možné říkat, že záporná čísla jsou vždy menší než nula. (Heeffer, 2011)

5.5 Spočetnost

Věta 19. *Množina celých čísel je spočetná.*

Důkaz. Celá čísla přerovnáme do následující posloupnosti:

$$0, 1, -1, 2, -2, 3, -3 \dots$$

Podle definice 9 je množina spočetná, právě když existuje bijektivní zobrazení f na přirozená čísla. To zajisté existuje, můžeme ho definovat například následujícím způsobem:

$$
\begin{aligned}
f(0) &= 1,\\
f(1) &= 2,\\
f(-1) &= 3,\\
f(2) &= 4,\\
f(-2) &= 5,\\
&\dots
\end{aligned}
$$

$\square$

Věta 20. *Množina celých čísel je nekonečná množina.*

Důkaz. Celá čísla jsou nadoborem přirozených čísel (definice 2). Dále platí věta 11. Z toho plyne, že i množina celých čísel je nekonečná. $\square$

5.6 Uspořádání celých čísel

Definice 17. Relace $<$, kterou nazveme uspořádáním na $\mathbb{Z}$, je definována takto:

$$\forall a, b \in \mathbb{Z} : a < b \Leftrightarrow b + (-a) \in \mathbb{Z}^+.$$

(Kubínová, Novotná, 1997)

Věta 21. *Relace $<$ je na $\mathbb{Z}$ tranzitivní a trichotomická.*

Důkaz. i. Nejprve dokážeme tranzitivitu relace $<$. Chceme ukázat, že pro všechna $a, b, c \in \mathbb{Z}$ platí $[(a < b) \wedge (b < c)] \Rightarrow (a < c)$. Víme, že $b + (-a) = u$, kde $u \in \mathbb{Z}^+$. Také víme, že $c + (-b) = v$, kde $v \in \mathbb{Z}^+$. K oběma stranám rovnosti $b + (-a) = u$ přičteme číslo $a \in \mathbb{Z}$. Dostaneme $b = u + a$. Do druhé rovnosti dosadíme za b a dostaneme rovnost $c + (-u - a) = v$. K oběma stranám přičteme u. Dostaneme $c - a = v + u$, $v, u \in \mathbb{Z}^+$, proto i součet u a v, který označíme w, je ze $\mathbb{Z}^+$. $c - a = w, w \in \mathbb{Z}^+$, přepíšeme podle definice relace $<$ jako $a < c$.

Relace je tedy tranzitivní.

ii. Nyní ukážeme, že relace $<$ je trichotomická. Chceme ukázat, že pro všechna $a, b \in \mathbb{Z}$ platí právě jedna z možností $a < b, a = b, a > b$. Zajisté platí právě jedna z možností, buď $b+(-a) \in \mathbb{Z}^+$, nebo $a+(-b) \in \mathbb{Z}^+$, a nebo $a+(-b) = 0$.

Relace $<$ je trichotomická

Relace $<$ je uspořádáním na $\mathbb{Z}$. □

Množina $(\mathbb{Z}, <)$ není dobře uspořádaná množina, jelikož nemá nejmenší prvek.

5.7 Celá čísla jako algebraická struktura

Definice 18. Strukturu $(O, +, \cdot)$ nazveme oborem integrity, pokud platí:

- $(O, +)$ je Abelova grupa.
- Násobení je asociativní, komutativní a má neutrální prvek. Násobení je distributivní vzhledem ke sčítání.
- Ve struktuře neexistují dělitelé nuly, tedy platí:

$$\forall a, b \in O : a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0).$$

Věta 22. *Celá čísla spolu s operacemi + a · tvoří obor integrity.*

Důkaz. Podle věty 16 víme, že struktura $(\mathbb{Z}, +)$ tvoří Abelovu grupu. Z definice 15 víme, že pro násobení celých čísel platí stejné vlastnosti jako pro násobení přirozených čísel, tedy asociativita, komutativita, existence neutrálního prvku i distributivita. Stačí ukázat, že v $\mathbb{Z}$ neexistují dělitelé nuly. Chceme ukázat, že pro všechna

$T_{(a,b)}, T_{(c,d)} \in \mathbb{Z}$ platí:

$$\Big(T_{(a,b)} \cdot T_{(c,d)} = 0\Big) \Rightarrow \Big(T_{(a,b)} = 0 \vee T_{(c,d)} = 0\Big)\,.$$

Předpokládejme, že $T_{(a,b)} \cdot T_{(c,d)} = 0$ a bez újmy na obecnosti předpokládejme, že $T_{(a,b)} \neq 0$. Chceme ukázat, že pak platí $T_{(c,d)} = 0$. Podle poznámky 20 pro součin celých čísel platí:

$$T_{(a,b)} \cdot T_{(c,d)} = T_{(a\cdot c+b\cdot d, a\cdot d+b\cdot c)}.$$

Z předpokladu víme, že se součin čísel $T_{(a,b)}, T_{(c,d)}$ rovná nule. Proto:

$$T_{(a\cdot c+b\cdot d, a\cdot d+b\cdot c)} = 0.$$

Podle poznámky 18 a věty 19 platí:

$$\Big(T_{(a\cdot c+b\cdot d, a\cdot d+b\cdot c)} = 0\Big) \Leftrightarrow (a \cdot c + b \cdot d = a \cdot d + b \cdot c).$$

Protože $a \neq b$, je podle věty 7 buď $a > b$, nebo $b > a$.

i) Předpokládejme nejprve, že $a > b$. Pak existuje $k \in \mathbb{N} - \{0\} : a = b + k$. Do rovnosti $a \cdot c + b \cdot d = a \cdot d + b \cdot c$ dosadíme za a:

$$(b + k) \cdot c + b \cdot d = (b + k) \cdot d + b \cdot c.$$

Využijeme distributivitu násobení vzhledem ke sčítání přirozených čísel podle věty 9:

$$b \cdot c + k \cdot c + b \cdot d = b \cdot d + k \cdot d + b \cdot c.$$

Zkrátíme podle věty 5 a dostaneme:

$$k \cdot c = k \cdot d.$$

Protože $k \neq 0$, můžeme použít vlastnost krácení podle věty 9 a dostaneme:

$$c = d.$$

Potom platí $T_{(c,d)} = T_{(c,c)} = 0$, což jsme právě chtěli ukázat.

ii) Nyní předpokládejme, že $b > a$. Pak existuje $k \in \mathbb{N} - \{0\} : b = a + k$. Do rovnosti $a \cdot c + b \cdot d = a \cdot d + b \cdot c$ dosadíme za b:

$$a \cdot c + (a + k) \cdot d = a \cdot d + (a + k) \cdot c.$$

Využijeme distributivitu násobení vzhledem ke sčítání přirozených čísel podle věty 9:

$$a \cdot c + a \cdot d + k \cdot d = a \cdot d + a \cdot c + k \cdot c.$$

Zkrátíme podle věty 5 a dostaneme:

$$k \cdot d = k \cdot c.$$

Protože $k \neq 0$, můžeme použít vlastnost krácení podle věty 9 a dostaneme:

$$d = c.$$

Potom platí $T_{(c,d)} = T_{(c,c)} = 0$, což jsme právě chtěli ukázat.

Na $\mathbb{Z}$ neexistují dělitelé nuly a struktura $(\mathbb{Z}, +, \cdot)$ je obor integrity. $\square$

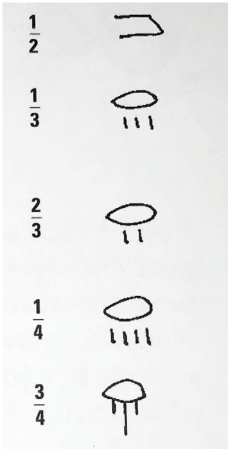
6 Čísla racionální

Racionální čísla jsou taková čísla, která, jak už název napovídá, lze vyjádřit jako poměr (z latinského *ratio*) ve tvaru zlomku $\frac{a}{b}$, kde $a, b \in \mathbb{N}$. Pro obor racionálních čísel použijeme označení $\mathbb{Q}$ z německého *Quotient*, které překládáme kvocient nebo také podíl.

O racionálních číslech se také někdy mluví jako o číslech souměřitelných. Eukleidés souměřitelné veličiny definoval takto: „Souměřitelnými zovou se veličiny, které touž měrou se měří; nesouměřitelnými pak, jimž míra žádná nemůže státi společnou.“ (Servít, 1907, s. 159)

Fine (1907) o zlomcích tvrdí, že z umělých čísel (těmi rozumí všechna čísla kromě přirozených) jako jediné nevznikly primárně jako abstraktní matematický konstrukt, ale proto, že měly v běžném životě své užití. To dokládá tím, že se objevují nejen v nejstarších matematických spisech Babyloňanů a Egypťanů, ale také Římanů, kteří se rozvoji matematiky příliš nevěnovali. Zlomky používali také řečtí kupci dávno před tím, než byly přijaty matematiky. Pokud byl etalon (jednotka [viz pozn. 4]) příliš velký, byl rozdělen na menší části. Tyto části se postupně staly další jednotkou. Tento princip je patrný například u peněz, kdy vznikaly nové druhy mincí nižší hodnoty. Poté došlo k abstrakci od mincí a vztah jednotky k jednotce menší začal být používán obecně i pro jiné předměty. Tímto principem vznikly například zlomky Římanů. Používali slova pro mince *uncia* nebo *sicilicus*, která byla částmi mince *as*, jež byla jednotkou. U jiných kultur však došlo k posunu od slov označujících mince k prostému numerickému vztahu. (Fine, 1907)

V matematicky vyspělejším Egyptě zavedli zlomky obecněji, i se značením. Tento systém je známý z nejstaršího matematického textu, *Rhindského papyru* (Ahmes, 2000 př.n.l). Jejich systém vycházel z tzv. kmenových zlomků. Kmenovými zlomky rozuměli takové zlomky, jejichž čitatel byl roven jedné. Další zlomky pak vyjadřovali pomocí zlomků kmenových, až na některé výjimky, které z praktických důvodů měly vlastní symbol, jak je vidět na obrázku 10 (např. $\frac{2}{3}, \frac{3}{4} \ldots$). (Crilly, 2010)



Obrázek 10: Zlomky Egypťanů (Crilly, 2010, s. 15)

Jak by Egypťané vyjádřili například zlomek $\frac{5}{7}$, uvádí Crilly na následujícím příkladu:

$$\frac{5}{7} = \frac{1}{3} + \frac{1}{4} + \frac{1}{8} + \frac{1}{168}.$$

Navíc Egypťané používali v součtu každý kmenový zlomek nejvýše jednou. Jak vidno, není tento způsob praktický a pro svou obtížnost nebyl příliš rozšířený.

Crilly ještě dodává, že některé zlomky je možné zapsat více způsoby. Například zlomek $\frac{5}{7}$ by bylo možné zapsat také takto:

$$\frac{5}{7} = \frac{1}{2} + \frac{1}{7} + \frac{1}{14},$$

což je kratší způsob. Do dnešní doby není znám způsob, jak obecně najít nejkratší rozklad na kmenové zlomky. (Crilly, 2010)

Zhruba o 150 let dříve se podobný systém objevil i u Babyloňanů (Crilly, 2010). Na rozdíl od Egypťanů, jejichž kořenové zlomky měly všechny stejný čitatel, Babyloňané měli zlomky se společnou vlastností ve jmenovateli, kde vždy najdeme nějakou mocninu čísla 60. U zlomků zapisovali pouze čitatel, mocnina jmenovatele závisela na pořadí, ve kterém byl další sčítanec zapsán. Například $\frac{27}{80} = \frac{20}{60} + \frac{15}{60^2}$ bychom podle Babyloňanů zapsali jako 20 15. (Fine, 1907)

Znovu zde chybělo znaménko operace, a muselo tak být jasné pouze z následnosti, že se jedná o sčítání (Fine, 1907). Jak Babyloňané rozlišili prostý součet čísel od součtu zlomků, Fine nezmiňuje.

Systém zlomků v šedesátkové soustavě byl ve vědě využíván až do šestnáctého století, kdy byl nahrazen soustavou desítkovou. Pro měření úhlů je však používán dodnes. (Fine, 1907)

Stejně jako Řekové rozlišovali mezi „čistou geometrií“ a geometrií řešenou aritmetickými metodami, rozlišovali také mezi „čistou aritmetikou“ a „uměním výpočtů“. Zlomky spadaly do kategorie umění výpočtů, jelikož byly Řeky považovány za umělý konstrukt, který nepatří do čisté vědy. Zlomky se tak objevují u geometrů Archimeda nebo Hera, ani jeden je však neuznává jako matematické objekty, nýbrž jen jako prostředky výpočtu. Zlomek $\frac{3}{2}$ by zapsali $\gamma' \ \beta'' \ \beta''$. (Fine, 1907)

V *Eukleidových Základech* (300 př.n.l.) jsou popsány některé vlastnosti zlomků, například v následující větě: „Když je číslo čísla dílem a jiné jiného je týmž dílem, též součet obou týmž dílem bude součtu, jakým jedno jednoho.“ (Servít, 1907, s. 107) nebo také ve větě: „Když je číslo čísla dílem, jakým odečtené odečteného, také zbytek zbytku týmž dílem bude, jakým celek celku.“ (Servít, 1907, s. 108).

Fine (1907) ovšem dodává, že Eukleidés zlomky chápal pouze v roli poměru geometrických objektů a nezapisoval je, ani s nimi neprováděl aritmetické výpočty jako s abstraktními čísly. To prováděl až Diophantos (Fine, 1907).

Zlomkovou čáru v podobě, v jaké ji dnes známe, dal světu Pisánský (Fibonacci) na počátku 13. století. Na konci století 16. Stevin přešel od zlomků o základu mocniny čísla 60 ke zlomkům o základu mocniny čísla 10. (Crilly, 2010)

6.1 Konstrukce racionálních čísel

Chceme vytvořit strukturu $(\mathbb{Q}, \cdot)$. Motivací je zkonstruovat taková čísla, aby byla vždy řešitelná rovnice:

$$a \cdot x = b.$$

Také chceme, aby pro tato čísla platily aritmetické zákony. (Thurston, 1956)

1. Ukážeme, že rovnice v tomto tvaru může mít pouze jedno řešení. To dokážeme sporem. Předpokládejme, že rovnice má řešení dvě. Označme tato řešení například $p, q \in \mathbb{Z} : p \neq q$:

   $$a \cdot p = b = a \cdot q.$$

   Podle věty 9 zkrátíme, a dostaneme tak:

   $$p = q,$$

   což je spor s předpokladem, že $p \neq q$. Rovnice má tedy pouze jedno řešení. Řešení je závislé na a, b, proto by jeho označení mělo zahrnovat a i b. Zavedeme označení pro řešení $\frac{b}{a}$. (Thurston, 1956)
   Víme, že někdy mají různé rovnice tohoto typu stejná řešení, například $2x = 10$ a $3x = 15$. Zajímá nás, kdy se tak děje. Předpokládejme tedy, že dvojice rovnic $a \cdot x = b$ a $c \cdot x = d$ má stejné řešení $x = r$. Platí tedy:

   $$a \cdot r = b \wedge c \cdot r = d.$$

   Obě strany rovnosti $a \cdot r = b$ vynásobíme $d \in \mathbb{Z}$:

   $$(a \cdot r) \cdot d = b \cdot d = b \cdot (c \cdot r).$$

   Využijeme komutativitu a asociativitu násobení (věta 9):

   $$(a \cdot d) \cdot r = (b \cdot c) \cdot r.$$

Zkrátíme r podle věty 9 a zjišťujeme, že jestliže mají rovnice stejné řešení, pak platí $a \cdot d = b \cdot c$. (Thurston, 1956)

Naopak platí-li, že $a \cdot d = b \cdot c$ a r řeší rovnici $a \cdot x = b$, tedy $a \cdot r = b$, pak tuto rovnost vynásobíme $c \in \mathbb{Z}$:

$$(a \cdot r) \cdot c = b \cdot c = a \cdot d,$$

využijeme asociativitu násobení (věta 9):

$$a \cdot (r \cdot c) = a \cdot d,$$

zkrátíme a použijeme komutativitu (obojí věta 9):

$$c \cdot r = d.$$

To znamená, že r řeší i rovnici $c \cdot x = d$. Pro řešení jsme zavedli označení $\frac{b}{a} = r$. Jak vidno, mezi řešeními tedy platí následující ekvivalence:

$$\frac{b}{a} = \frac{d}{c} \Leftrightarrow a \cdot d = b \cdot c.$$

(Thurston, 1956)

Relace = ve výrazu $\frac{b}{a} = \frac{d}{c}$ je ekvivalencí (označme tuto relaci $\approx$) definovanou na množině $M = \mathbb{Z} \times (\mathbb{Z} - \{0\})$. Platí:

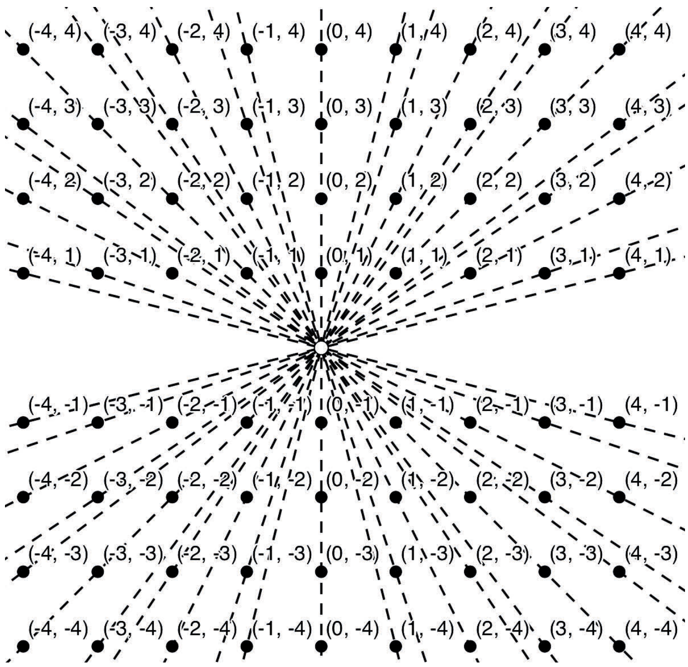
$$\forall a, c \in \mathbb{Z} \quad \forall b, d \in (\mathbb{Z} - \{0\}) : (a, b) \approx (c, d) \Leftrightarrow a \cdot c = b \cdot d.$$

2. Množinu $\mathbb{Q}$ racionálních čísel definujme jako rozklad množiny M podle ekvivalence $\approx$. Třídy tohoto rozkladu jsou prvky množiny $\mathbb{Q}$. Tedy platí:

$$\mathbb{Q} = \{T_{(a,b)}; (a, b) \in M\}, T_{(a,b)} = \{(c, d) \in M; (a, b) \approx (c, d)\}.$$

(Kubínová, Novotná, 1997)

Třídy rozkladu podle ekvivalence $\approx$ znázorňuje obrázek 11. Přerušovaná čára znázorňuje třídu ekvivalence a body na ní prvky, které do dané třídy spadají. Počátek přitom nepatří do žádné ze tříd, stejně tak jako každý bod osy x.



Obrázek 11: Třídy ekvivalence racionálních čísel (vlastní obrázek)

3. Na množině $\mathbb{Q}$ definujeme operaci násobení.

Definice 19. Operaci $\cdot$ na množině $\mathbb{Q}$ zavedeme takto:

$$\forall T_{(a,b)}, T_{(c,d)} \in \mathbb{Q} : T_{(a,b)} \cdot T_{(c,d)} = T_{(a\cdot c, b\cdot d)}.$$

(Kubínová, Novotná, 1997)

Pro korektnost definice musí platit, že:

i) $T_{(a\cdot c, b\cdot d)} \in \mathbb{Q}$,

ii) $\forall (x,y) \in T_{(a,b)}, \forall (u,v) \in T_{(c,d)} : (x \cdot u, y \cdot v) \in T_{(a \cdot c, b \cdot d)}$.

Podle definice množiny racionálních čísel i) platí. Čísla a, c jsou ze $\mathbb{Z}$ a čísla b, d jsou prvky $\mathbb{Z} - \{0\}$. Tedy i součin celých čísel bude celé číslo a součin nenulových čísel bude nenulový. To odpovídá definici množiny $\mathbb{Q}$.

Pro ověření ii) je třeba zjistit, zda platí:

$$\forall (x,y) \approx (a,b), \forall (u,v) \approx (c,d) : (x \cdot u, y \cdot v) \approx (a \cdot c, b \cdot d).$$

Přepíšeme předpoklady podle definice relace $\approx$:

$$\forall (x,y) \approx (a,b) \Leftrightarrow x \cdot a = y \cdot b,$$
$$\forall (u,v) \approx (c,d) \Leftrightarrow u \cdot c = v \cdot d.$$

Vynásobíme mezi sebou levé a pravé strany rovností a dostáváme $x \cdot a \cdot u \cdot c = y \cdot b \cdot v \cdot d$. To je podle definice relace $\approx$ a za využití komutativity násobení $(x \cdot u, y \cdot v) \approx (a \cdot c, b \cdot d)$.

Definice násobení na $\mathbb{Q}$ je tedy korektní.

4. Ukážeme, že struktura $(\mathbb{Q}, \cdot)$ je komutativní monoid. Jeho jednotkovým prvek je $T_{(1,1)}$.

Věta 23. *Struktura* $(\mathbb{Q}, \cdot)$ *tvoří komutativní monoid.*

Důkaz. Aby struktura byla komutativní monoid, je zapotřebí, aby byla asociativní, komutativní a existoval neutrální prvek vzhledem k operaci.

(a) Začneme důkazem asociativity. Chceme ukázat, že platí:

$$\forall T_{(a,b)}, T_{(a,b)}, T_{(a,b)} \in \mathbb{Q} : (T_{(a,b)} \cdot T_{(c,d)}) \cdot T_{(e,f)} = T_{(a,b)} \cdot (T_{(c,d)} \cdot T_{(e,f)}).$$

Součiny přepíšeme podle definice násobení v $\mathbb{Q}$:

$$T_{(a \cdot c, b \cdot d)} \cdot T_{(e,f)} = T_{(a \cdot c \cdot e, b \cdot d \cdot f)} = T_{(a,b)} \cdot T_{(c \cdot e, d \cdot f)}.$$

Struktura je asociativní.

(b) Ptáme se, zda je struktura komutativní. Ukážeme, že platí:

$$\forall T_{(a,b)}, T_{(c,d)} \in \mathbb{Q} : T_{(a,b)} \cdot T_{(c,d)} = T_{(c,d)} \cdot T_{(a,b)}.$$

Součiny přepíšeme podle definice násobení v $\mathbb{Q}$ a ukážeme, že platí:

$$T_{(a\cdot c, b\cdot d)} = T_{(c\cdot a, d\cdot b)}.$$

Čísla a, c jsou prvky $\mathbb{Z}$ a čísla b, d jsou prvky $\mathbb{Z} - \{0\}$. Násobení celých čísel je komutativní, tedy $a \cdot c = c \cdot a$ a $b \cdot d = d \cdot b$. Proto $T_{(a\cdot c, b\cdot d)} =$ $= T_{(c\cdot a, d\cdot b)}$. Násobení racionálních čísel je tedy komutativní.

(c) Nyní ověříme, že prvek $T_{(1,1)}$ je neutrálním prvkem vzhledem k operaci $\cdot$. Chceme ukázat platnost tvrzení:

$$\forall T_{(a,b)} \in \mathbb{Q} : T_{(a,b)} \cdot T_{(1,1)} = T_{(1,1)} \cdot T_{(a,b)} = T_{(a,b)}.$$

Komutativita operace $\cdot$ byla dokázána v (b). Stačí tedy ukázat, že platí:

$$T_{(a,b)} \cdot T_{(1,1)} = T_{(a,b)}.$$

Přepíšeme levou stranu rovnosti podle definice násobení racionálních čísel:

$$T_{(a,b)} \cdot T_{(1,1)} = T_{(a\cdot 1, b\cdot 1)}.$$

Chceme ukázat, že platí:

$$T_{(a\cdot 1, b\cdot 1)} = T_{(a,b)}.$$

Protože čísla a, b jsou prvky $\mathbb{Z}$, víme, že platí $a \cdot 1 = a$ a $b \cdot 1 = b$. Levá strana rovnosti se rovná pravé, a násobení racionálních čísel tak má opravdu neutrální prvek $T_{(1,1)}$.

Struktura $(\mathbb{Q}, \cdot)$ tedy tvoří komutativní monoid. Neutrálním prvkem je $T_{(1,1)}$.

$\square$

5. Chceme sestrojit takovou strukturu, aby vzhledem k násobení existovaly inverzní prvky k nenulovým racionálním číslům. Označíme $\mathbb{Q}_0 = \{T_{(a,b)} \in \in \mathbb{Q}; a \neq 0\}$. Existuje ke každému prvku z $\mathbb{Q}_0$ inverzní prvek vzhledem k operaci $\cdot$? Ukážeme, že pro každý prvek $T_{(a,b)} \in \mathbb{Q}_0$ existuje inverzní prvek ve tvaru $T_{(b,a)} \in \mathbb{Q}_0$:

$$T_{(a,b)} \cdot T_{(b,a)} = T_{(a \cdot b, b \cdot a)} = T_{(a \cdot b, a \cdot b)} = T_{(1,1)}.$$

Tím je ověřeno, že $T_{(b,a)}$ je inverzním prvkem pro $T_{(a,b)}$. Struktura $(\mathbb{Q}_0, \cdot)$ je tedy Abelova grupa.

6. Chceme izomorfně vnořit $\mathbb{Z}$ do $\mathbb{Q}$. Množinu tříd ekvivalence, které mají reprezentanta $(a, 1), a \in \mathbb{Z}$, označme $\mathbb{Q}'$. Definujme zobrazení f takto:

$$f : (\mathbb{Z}, \cdot) \to (\mathbb{Q}', \cdot), f(a) = T_{(a,1)}.$$

Zobrazení f je izomorfismem. Označíme $\mathbb{Q}'_0$ množinu tříd z $\mathbb{Q}$, které mají reprezentanta $(p, 1), p \in \mathbb{Z} - \{0\}$. Zúžení izomorfismu na $\mathbb{Z} - \{0\}$ je izomorfismem mezi strukturami $(\mathbb{Z} - \{0\}, \cdot)$ a $(\mathbb{Q}' \bigcap \mathbb{Q}'_0, \cdot)$.

(Kubínová, Novotná, 1997, s. 153)

6.1.1 Značení

Platí $f : (\mathbb{Z}, \cdot) \to (\mathbb{Q}', \cdot), f(a) = T_{(a,1)}$, je izomorfismus, můžeme tedy prvky ve tvaru $T_{(a,1)}$ značit a.

Také platí, že každý prvek $\mathbb{Q}$ lze rozepsat jako následující součin:

$$T_{(a,b)} = T_{(a,1)} \cdot T_{(1,b)} = T_{(a,1)} \cdot (T_{(b,1)})^{-1} = a \cdot b^{-1}.$$

Prvek a^{-1} označíme $\frac{1}{a}$. V dalším textu $T_{(a,b)}$ budeme značit $\frac{a}{b}$.

(Kubínová, Novotná, 1997)

6.2 Operace na množině racionálních čísel

6.2.1 Vlastnosti operace násobení na množině $\mathbb{Q}$

Operaci $\cdot$ v $\mathbb{Q}$ jsme definovali takto:

$$\forall T_{a,b}, T_{c,d} \in \mathbb{Q} : T_{(a,b)} \cdot T_{(c,d)} = T_{(a \cdot c, b \cdot d)}.$$

Použijeme-li označení zavedené v kapitole 6.1.1, můžeme tuto definici přepsat takto:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

(Kubínová, Novotná, 1997)

Věta 24. *$\forall \frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$:*

1) $\frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b}$, *(komutativita)*

2) $\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right)$, *(asociativita)*

3) $\frac{1}{1} \cdot a = a$, *(1 je neutrální prvek)*

4) $\frac{a}{b} \cdot \frac{0}{1} = \frac{0}{1} = 0$, *(nula je agresivní prvek)*

5) $\frac{a}{b} \neq 0 \Rightarrow \left(\left(\frac{a}{b} \cdot \frac{c}{d} = \frac{a}{b} \cdot \frac{e}{f}\right) \Rightarrow \frac{c}{d} = \frac{e}{f}\right)$, *(pravidlo pro krácení)*

6) $\frac{a}{b} \neq 0 \Rightarrow \exists \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$. *(existence inverzních prvků)*

Důkaz. 1. Ukážeme, že platí $\frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b}$. Začneme upravovat levou stranu:

$$L = \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d} \overset{\star}{=} \frac{c \cdot a}{d \cdot b} = \frac{c}{d} \cdot \frac{a}{b} = P.$$

$\star$: Využili jsme komutativitu násobení celých čísel.

$L = P$, násobení racionálních čísel je tedy komutativní.

2. Chceme ukázat, že platí $\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right)$.

$$L = \left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \left(\frac{a \cdot c}{b \cdot d}\right) \cdot \frac{e}{f} = \frac{(a \cdot c) \cdot e}{(b \cdot d) \cdot f} \overset{\star}{=} \frac{a \cdot (c \cdot e)}{b \cdot (d \cdot f)} =$$
$$= \frac{a}{b} \cdot \left(\frac{c \cdot e}{d \cdot f}\right) = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right) = P.$$

$\star$: Využili jsme asociativitu násobení celých čísel.

$L = P$, násobení racionálních čísel je tedy asociativní.

3. Ověříme platnost $\frac{1}{1} \cdot a = a$.

$$\frac{1}{1} \cdot a \overset{viz\, 6.1.1}{=} 1 \cdot a \overset{\star}{=} a.$$

$\star$: Využili jsme toho, že jednička je neutální prvek vzhledem k násobení na množině celých čísel.

Jednička je neutrálním prvkem vzhledem k násobení i pro racionální čísla.

4. Dokážeme platnost $\frac{a}{b} \cdot \frac{0}{1} = 0$.

$$\frac{a}{b} \cdot \frac{0}{1} = \frac{a \cdot 0}{b \cdot 1} \overset{\star}{=} \frac{0}{b} = T_{(0,b)} = T_{(0,0)} = 0.$$

$\star$: V čitateli jsme využili toho, že nula je agresivním prvkem vzhledem k násobení celých čísel. Ve jmenovateli jsme využili neutrálnosti prvku 1 vzhledem k násobení celých čísel.

Nula je tedy agresivní vzhledem k násobení racionálních čísel.

6. Nejprve dokážeme existenci inverzních prvků vzhledem k násobení. Dokážeme, že pro všechna $\frac{a}{b} \in \mathbb{Q} - \{0\} \quad \exists (\frac{a}{b})^{-1} : \frac{a}{b} \cdot \left(\frac{a}{b}\right)^{-1} = 1$.

   Nechť $\frac{a}{b} \in \mathbb{Q} - \{0\}$. Ukážeme, že $\left(\frac{a}{b}\right)^{-1}$ je $\frac{b}{a}$:

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{b \cdot a} = \frac{a \cdot b}{a \cdot b} = T_{(a \cdot b, a \cdot b)} = T_{(1,1)} = 1.$$

   Pro každý prvek $\mathbb{Q}$ kromě nuly existuje inverzní prvek vzhledem k násobení.

5. Nyní můžeme dokázat pravidlo pro krácení. Ukážeme, že pro všechna $\frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$ a $\frac{a}{b} \in \mathbb{Q} - \{0\}$ platí $\left(\frac{a}{b} \cdot \frac{c}{d} = \frac{a}{b} \cdot \frac{e}{f}\right) \Rightarrow \left(\frac{c}{d} = \frac{e}{f}\right)$.

   Protože $\frac{a}{b} \neq 0$, existuje podle 6) inverzní prvek $\frac{b}{a}$. Obě strany rovnosti $\frac{a}{b} \cdot \frac{c}{d} = \frac{a}{b} \cdot \frac{e}{f}$ inverzním prvkem $\frac{b}{a}$ vynásobíme:

$$\begin{aligned} \frac{b}{a} \cdot \frac{a}{b} \cdot \frac{c}{d} &= \frac{b}{a} \cdot \frac{a}{b} \cdot \frac{e}{f}, \\ 1 \cdot \frac{c}{d} &= 1 \cdot \frac{e}{f}, \\ \frac{c}{d} &= \frac{e}{f}. \end{aligned}$$

   Pravidlo pro krácení tedy platí.

$\square$

6.2.2 Definice a vlastnosti operace sčítání na množině $\mathbb{Q}$

Definice 20. Sčítání racionálních čísel definujeme takto:

$$\forall \frac{a}{b}, \frac{c}{d} \in \mathbb{Q} : \frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d}.$$

(Kubínová, Novotná, 1997)

Zapsáno pomocí tříd:

$$T_{(a,b)} + T_{(c,d)} = T_{(a \cdot d + c \cdot b, b \cdot d)}.$$

Takto definovaná operace + na $\mathbb{Q}$ splňuje podmínky:

i) $T_{(a\cdot d+c\cdot b, b\cdot d)} \in \mathbb{Q}$,

ii) $\forall (x,y) \in T_{(a,b)}, \forall (u,v) \in T_{(c,d)} : (x \cdot v + u \cdot y, y \cdot v) \in T_{(a\cdot d+c\cdot b, b\cdot d)}$.

Proto je korektní.

Věta 25. *Pro všechna $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$ platí následující vlastnosti:*

1) $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$, *(komutativita)*

2) $\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right)$, *(asociativita)*

3) $\frac{a}{b} + \frac{0}{1} = \frac{a}{b}$, *(nula je neutrální prvek)*

4) $\exists \frac{x}{y} : \frac{a}{b} + \frac{x}{y} = 0$, *(existence opačných prvků)*

5) $\left(\frac{a}{b} + \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{a}{b} \cdot \frac{e}{f} + \frac{c}{d} \cdot \frac{e}{f}$. *(násobení je distributivní vzhledem ke sčítání)*

Důkaz. 1) Dokážeme, že platí $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$.

$$L = \frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d} \overset{\star}{=} \frac{c \cdot b + a \cdot d}{d \cdot b} = \frac{c}{d} + \frac{a}{b} = P.$$

$\star$: Využili jsme komutativitu násobení a komutativitu sčítání celých čísel.

$L = P$, sčítání racionálních čísel je tedy komutativní.

2) Ukážeme, že platí $\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right)$.

$$\left.\begin{aligned} L &= \left(\tfrac{a}{b} + \tfrac{c}{d}\right) + \tfrac{e}{f} = \tfrac{a\cdot d+c\cdot b}{b\cdot d} + \tfrac{e}{f} = \tfrac{(a\cdot d+c\cdot b)\cdot f+e\cdot b\cdot d}{b\cdot d\cdot f} \overset{\star}{=} \tfrac{a\cdot d\cdot f+c\cdot b\cdot f+e\cdot b\cdot d}{b\cdot d\cdot f} \\ P &= \tfrac{a}{b} + \left(\tfrac{c}{d} + \tfrac{e}{f}\right) = \tfrac{a}{b} + \tfrac{c\cdot f+e\cdot d}{d\cdot f} = \tfrac{a\cdot d\cdot f+(c\cdot f+e\cdot d)\cdot b}{b\cdot d\cdot f} \overset{\star}{=} \tfrac{a\cdot d\cdot f+c\cdot b\cdot f+e\cdot b\cdot d}{b\cdot d\cdot f} \end{aligned}\right\} L = P.$$

$\star$: Využili jsme distributivitu a komutativitu celých čísel.

$L = P$, sčítání racionálních čísel je tedy asociativní.

3) Ukážeme, že platí $\frac{a}{b} + \frac{0}{1} = \frac{a}{b}$.

$$\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + 0 \cdot b}{b \cdot 1} \stackrel{\star}{=} \frac{a + 0}{b} = \frac{a}{b}.$$

$\star$: Využili jsme toho, že jednička je jednotkový prvek a nula agresivní prvek vzhledem k násobení celých čísel.

Nula je neutrální prvek vzhledem ke sčítání racionálních čísel.

4) Dokážeme existenci opačných prvků. Nechť $\frac{a}{b} \in \mathbb{Q}$. Dokážeme, že pro $\frac{-a}{b} \in \mathbb{Q}$ platí $\frac{a}{b} + \frac{-a}{b} = 0$.

Existence plyne z existence opačných prvků pro celá čísla. Stačí ukázat, že $\frac{-a}{b}$ je opačné číslo k $\frac{a}{b}$:

$$\frac{a}{b} + \frac{-a}{b} = \frac{a \cdot b + (-a) \cdot b}{b \cdot b} \stackrel{\star}{=} \frac{0}{b \cdot b} = 0,$$

$\star$: Využili jsme vlastnosti opačného prvku pro celá čísla.

Platí, že pro každé racionální číslo existuje opačný prvek vzhledem ke sčítání a je pro každé číslo $\frac{a}{b}$ ve tvaru $\frac{-a}{b}$.

5) Dokážeme, že násobení racionálních čísel je distributivní vzhledem ke sčítání. Chceme ukázat, že pro všechna $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$ platí $\left(\frac{a}{b} + \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{a}{b} \cdot \frac{e}{f} + \frac{c}{d} \cdot \frac{e}{f}$.
Upravíme každou stranu rovnosti zvlášť:

$$\left.\begin{aligned} L &= \left(\tfrac{a}{b} + \tfrac{c}{d}\right) \cdot \tfrac{e}{f} = \left(\tfrac{a \cdot d + c \cdot b}{b \cdot d}\right) \tfrac{e}{f} = \tfrac{(a \cdot d + c \cdot b) \cdot e}{b \cdot d \cdot f} \stackrel{\star}{=} \tfrac{a \cdot d \cdot e + c \cdot b \cdot e}{b \cdot d \cdot f} \\ P &= \tfrac{a}{b} \cdot \tfrac{e}{f} + \tfrac{c}{d} \cdot \tfrac{e}{f} = \tfrac{a \cdot e}{b \cdot f} + \tfrac{c \cdot e}{d \cdot f} = \tfrac{a \cdot e \cdot d \cdot f + c \cdot e \cdot b \cdot f}{b \cdot f \cdot f \cdot d \cdot e} \stackrel{\star}{=} \tfrac{f}{f} \cdot \tfrac{a \cdot d \cdot e + c \cdot b \cdot e}{b \cdot d \cdot f} = \tfrac{a \cdot d \cdot e + c \cdot b \cdot e}{b \cdot d \cdot f} \end{aligned}\right\} L = P$$

$\star$: Využili jsme distributivitu násobení vzhledem ke sčítání na celých číslech.

$L = P$, tedy násobení racionálních čísel je distributivní vzhledem ke sčítání.

□

Pozn. 24. Důkazy vět 24, 25 jsou vlastní. Věty pocházejí ze skript *Posloupnosti a řady* (Kubínová, Novotná, 1997).

6.3 Spočetnost

Věta 26. *Množina racionálních čísel je nekonečnou množinou.*

Důkaz. Nekonečná množina $\mathbb{Z}$ je podmnožinou množiny $\mathbb{Q}$. Proto je i množina $\mathbb{Q}$ nekonečná. $\square$

Věta 27. *Množina racionálních čísel je spočetná množina.*

Důkaz. Proto, abychom mohli racionální čísla snadno bijektivně přiřadit k přirozeným, zapíšeme je do matice:

$$\begin{array}{cccccc}
\frac{0}{1} & \frac{1}{1} & \frac{-1}{1} & \frac{2}{1} & \frac{-2}{1} & \cdots \\[1em]
\frac{0}{2} & \frac{1}{2} & \frac{-1}{2} & \frac{2}{2} & \frac{-2}{2} & \cdots \\[1em]
\frac{0}{3} & \frac{1}{3} & \frac{-1}{3} & \frac{2}{3} & \frac{-2}{3} & \cdots \\[1em]
\frac{0}{4} & \frac{1}{4} & \frac{-1}{4} & \frac{2}{4} & \frac{-2}{4} & \cdots \\[1em]
\frac{0}{5} & \frac{1}{5} & \frac{-1}{5} & \frac{2}{5} & \frac{-2}{5} & \cdots \\[1em]
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Nyní zlomky seřadíme do posloupnosti tak, jak je znázorněno na obrázku 12.

Prvky matice tedy řadíme po diagonálách. Posloupnost, kterou dostáváme, je:

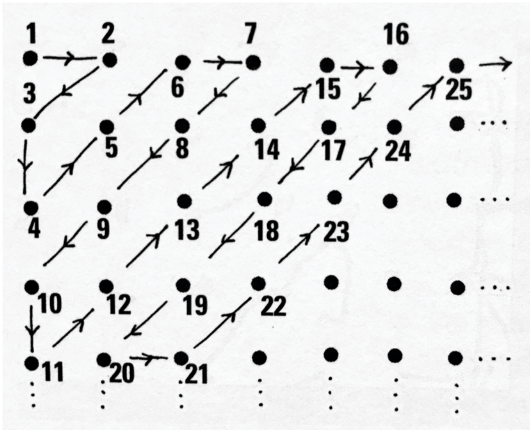
$$\frac{0}{1}, \frac{1}{1}, \frac{0}{2}, \frac{-1}{1}, \frac{1}{2} \cdots$$

Z definice 9 víme, že můžeme-li množinu chápat jako posloupnost, je spočetná. Tedy množina racionálních čísel je spočetnou množinou.

$\square$

6.4 Uspořádání na množině racionálních čísel

Pozn. 25. Každé racionální číslo $\frac{a}{b}$ lze zapsat ve tvaru podílu tak, že $b > 0$ (Kubínová, Novotná, 1997). Toho využijeme v důkazu věty 28.



Obrázek 12: Způsob, jakým řadíme racionální čísla z matice do posloupnosti (Crilly, 2010, s. 30)

Definice 21. Relace $<$ je na $\mathbb{Q}$ definována takto:

$$\forall \frac{a}{b}, \frac{c}{d} \in \mathbb{Q} \quad (a, b > 0) : \frac{a}{b} < \frac{c}{d} \Leftrightarrow a \cdot d < c \cdot b$$

(Kubínová, Novotná, 1997, s. 153)

Věta 28. *Relace $<$ je na $\mathbb{Q}$ tranzitivní a trichotomická.*

Důkaz. i. Nejprve dokážeme tranzitivitu relace $<$. Chceme ukázat, že pro všechna $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$ platí $\left[\left(\frac{a}{b} < \frac{c}{d}\right) \wedge \left(\frac{c}{d} < \frac{e}{f}\right)\right] \Rightarrow \left(\frac{a}{b} < \frac{e}{f}\right)$. Předpokládejme také, že čísla $b, d, f \in \mathbb{Z}$ jsou větší, než nula (viz poznámka 25). Podle definice 21 platí:

$$\left(\frac{a}{b} < \frac{c}{d}\right) \Leftrightarrow a \cdot d < c \cdot b,$$
$$\left(\frac{c}{d} < \frac{e}{f}\right) \Leftrightarrow c \cdot f < e \cdot d.$$

Vynásobíme první nerovnost číslem f a druhou nerovnost číslem b. Obě čísla jsou kladná celá. Platí:

$$(a \cdot d \cdot f < c \cdot b \cdot f) \wedge (b \cdot c \cdot f < b \cdot e \cdot d).$$

Čísla a, b, c, d, e, f jsou celá. Pro celá čísla je relace $<$ tranzitivní (viz. věta 21). Proto:

$$a \cdot d \cdot f < b \cdot e \cdot d.$$

Protože d je kladné celé číslo a proto, že násobení celých čísel je komutativní, platí:

$$a \cdot f < e \cdot b.$$

Podle definice 21 pak tedy $\frac{a}{b} < \frac{e}{f}$.

Relace $<$ je na množině racionálních čísel tranzitivní.

ii. Nyní ukážeme, že relace $<$ je na množině racionálních čísel trichotomická. Chceme ukázat, že pro všechna $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ platí právě jedna z možností $\frac{a}{b} < \frac{c}{d}$, $\frac{a}{b} = \frac{c}{d}$, $\frac{a}{b} > \frac{c}{d}$.

Podle věty 21 je relace $<$ trichotomická pro celá čísla. Tedy pro všechna $a, b, c, d \in \mathbb{Z}$ nastává právě jedna z možností:

(a) $a \cdot d = c \cdot b$,

(b) $a \cdot d < c \cdot b$,

(c) $a \cdot d > c \cdot b$.

Proto i na racionálních číslech je relace $<$ trichotomická.

Relace $<$ je tranzitivní a trichotomická na množině racionálních číslech. Je tedy uspořádáním na $\mathbb{Q}$. □

6.5 Racionální čísla jako algebraická struktura

Definice 22. Algebraickou strukturu $(T, +, \cdot)$ nazveme tělesem, jestliže $(T, +)$ a $(T - \{0\}, \cdot)$ tvoří Abelovu grupu a operace $\cdot$ je distributivní vzhledem k operaci $+$.

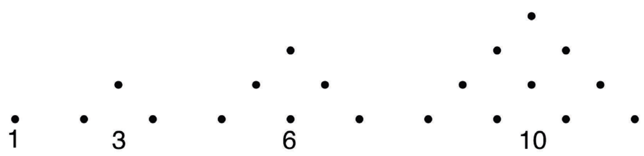
Věta 29. *Struktura* $(\mathbb{Q} - \{0\}, +, \cdot)$ *tvoří těleso.*

Důkaz. Že struktura $(\mathbb{Q}, +)$ je Abelovou grupou, jsme ověřili ve větě 25. Obdobně jsme ukázali, že $(\mathbb{Q} - \{0\}, \cdot)$ tvoří Abelovu grupu ve větě 24. Ve stejné větě jsme dokázali také distributivitu násobení vzhledem ke sčítání.

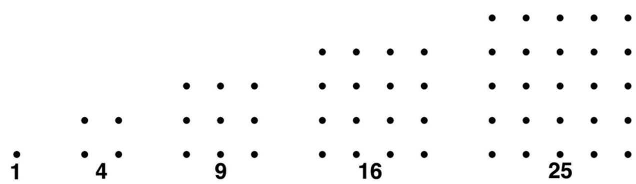
Struktura $(\mathbb{Q} - \{0\}, +, \cdot)$ tvoří těleso. $\square$

7 Čísla reálná

Objev nesouměřitelných čísel je připisován Pythagorovi, který žil v šestém století před naším letopočtem, a jeho stoupencům. Pro Pythagorejce a antickou matematiku, včetně aritmetiky, je typické interpretovat všechny zákonitosti pomocí geometrie. Dokonce od Řeků pocházejí i pojmy jako čísla trojúhelníková (viz obrázek 13) nebo čtvercová (viz obrázek 14). (Fine, 1907; Crilly, 2010; Kolman, 2008)



Obrázek 13: Trojúhelníková čísla (vlastní obrázek)



Obrázek 14: Čtvercová čísla (vlastní obrázek)

Právě při zkoumání čísel čtvercových si Pythagoras všiml vztahu mezi čtverci trojky, čtyřky a pětky. Tedy, že platí $3^2 + 4^2 = 5^2$. Stejně tak věděl, že trojúhelník o těchto délkách stran je pravoúhlý. Pythagorovi se povedlo větu zobecnit i geometricky ukázat její platnost. Ovšem když začal hledat trojice čísel odpovídající délkám stran pravoúhlých trojúhelníků, narazil na problém.

Řekové se zabývali tzv. *teorií měření* (Crilly, 2010). Ta spočívala v tom, že chceme-li změřit délku úsečky AB měřidlem (jednotkou) délky CD, budeme měřidlo přikládat n-krát. Pokud se po n-tém přiložení konec úsečky AB a konec měřidla překrývají, je délka úsečky AB právě n (vzhledem k jednotce). Pokud měřidlo přesáhlo, prodloužíme úsečku AB na dvojnásobek její délky a postup opakujeme. Pokud se konce překryjí, je délka úsečky AB počtem přiložení měřidla k prodloužené úsečce dělený násobností délky úsečky AB v úsečce prodloužené. Pokud měřidlo znovu přesáhne, prodloužíme původní úsečku AB na trojnásobek atd.

Řekové věřili, že po konečně mnoha prodlouženích úsečky AB se konce prodloužené úsečky a měřidla překryjí, a bude tak možné vyjádřit délku měřené úsečky ku měřidlu jako poměr nějakých dvou celých čísel. Délky, pro které tato vlastnost platí, nazýváme souměřitelné. (Crilly, 2010, Fine, 1907, Kolman, 2008)

Pozn. 26. V Eukleidových základech (Servít, 1907) jsou jako souměřitelné veličiny označeny takové veličiny, pro něž existuje společná míra, a nesouměřitelné takové, pro které společná míra neexistuje.

Pythagoras chtěl tímto způsobem změřit délku přepony pravoúhlého trojúhelníku, jehož odvěsny měly délku jednotky. Hledal tedy délku úhlopříčky čtverce. Za jednotku, pomocí které měřil, zvolil délku strany čtverce. Najít délku úhlopříčky se mu ovšem nedařilo. Pythagorejcům se podařilo ukázat, že délka úhlopříčky čtverce není s délkou jeho strany souměřitelná. (Fine, 1907; Kolman, 2008)

Věta 30. *Strana a úhlopříčka čtverce jsou nesouměřitelné.*

Důkaz. Větu dokážeme sporem. Předpokládejme, že úhlopříčka U a strana S čtverce jsou souměřitelné. Pak mají poměr jako nějaká dvě celá čísla $u, s \in \mathbb{Z}$. Podle Pythagorovy věty platí $u^2 = 2s^2$.
Pokud jsou čísla u, s soudělná, tedy pokud $\exists c \in \mathbb{N} - \{0, 1\} : u = c \cdot \alpha, s = c \cdot \beta$, pak tvar $(c \cdot \alpha)^2 = 2 \cdot (c \cdot \beta)^2$ zkrátíme c^2 a dostáváme:

$$\alpha^2 = 2 \cdot \beta^2.$$

Protože se α^2 rovná dvojnásobku β^2, můžeme říct, že α je sudé číslo. Jelikož jsme vydělili c^2, čísla α, β jsou nesoudělná, musí β být liché číslo.
Je-li α sudé číslo, existuje $\gamma \in \mathbb{N}$ takové, že $\alpha = 2 \cdot \gamma$. Když dosadíme za α do rovnosti $\alpha^2 = 2 \cdot \beta^2$, dostáváme:

$$(2 \cdot \gamma)^2 = 2 \cdot \beta^2,$$

což je po umocnění:

$$4 \cdot \gamma^2 = 2 \cdot \beta^2,$$

obě strany vydělíme dvěma:

$$2 \cdot \gamma^2 = \beta^2.$$

Z toho plyne, že β je sudé číslo. To je spor s nesoudělností čísel α, β. Ke sporu jsme došli také proto, že číslo je buď sudé, nebo liché, ale β je současně sudé i liché.
Délka hrany čtverce a jeho úhlopříčky jsou tedy nesouměřitelné. □

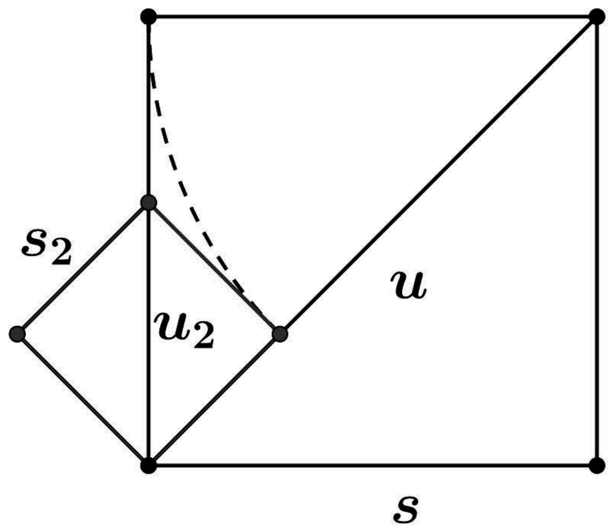
(Servít, 1907; Fine, 1907; Kolman, 2008)

Důkaz věty lze provést i graficky:

Důkaz. Mějme čtverec o délce strany s a délce úhlopříčky u. Přeneseme délku strany s na u. Nad zbývající délkou strany u sestavíme čtverec. Délku jeho strany označíme s_2 a délku jeho úhlopříčky u_2 (viz obrázek 15).

Předpokládejme nyní, že je možné změřit s pomocí u, nebo opačně, tedy, že existuje společná míra s a u. Označíme ji E.
Pro délky menšího ze čtverců však platí:

- $s_2 = u - s$,
- $u_2 = s - s_2$ (je vidět z deltoidu, v němž je vepsán oblouk kružnice na obrázku 15).



Obrázek 15: Nesouměřitelnost délek strany a úhlopříčky čtverce (vlastní obrázek)

Proto by společná míra u, s byla i společnou mírou u_2, s_2. Konečným počtem opakování stejné konstrukce pro vzniklé menší čtverce dostaneme pro libovolné E stranu a úhlopříčku, které budou kratší než E, tedy E nemůže být společnou měrou a to je spor. □

(Kolman, 2008)

Pozn. 27. Čísla, která jsou nesouměřitelná, tedy je nemožné je zapsat jako podíl dvou celých čísel, dnes nazýváme iracionální. Slovo pochází z latinského slova *ratio*, znamenajícího *poměr*, a předpony, vyjadřující zápor. Slovo *ratio* ovšem také znamená rozum, a proto by se slovo *iracionální* dalo přeložit i jako *stojící mimo rozum.*

Z práce se čtvercovými čísly Řekové usoudili, že rovnice $x^2 = 2$ nemá řešení, jelikož neznali žádné číslo, které by ji splňovalo. Ovšem právě takové číslo se objevovalo v geometrii jako poměr úhlopříčky jednotkového čtverce k jeho straně.

Thurston (1956) soudí, že objev iracionálních čísel mohl přispět k tomu, proč se antičtí matematici přestali věnovat aritmetice a soustředili se na geometrii. (Thurston, 1956)

7.1 Konstrukce reálných čísel

7.1.1 Axiomatická výstavba oboru reálných čísel

Definice 23. Množinu $\mathbb{R}$ nazveme množinou reálných čísel, jestliže platí následující axiomy:

1. Na množině $\mathbb{R}$ je definována operace sčítání $+, + : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$. Operace přiřazuje každé dvojici $x, y \in \mathbb{R} \times \mathbb{R}$ prvek $x + y \in \mathbb{R}$. Sčítání má tyto vlastnosti:

   a) $\exists 0 \in \mathbb{R} \quad \forall a \in \mathbb{R} : 0 + a = a + 0 = a,$ *(nula je neutrální prvek pro +)*

   b) $\forall a \in \mathbb{R} \quad \exists (-a) \in \mathbb{R} : a + (-a) = (-a) + a = 0,$ *(existence opačných prvků)*

   c) $\forall a, b, c \in \mathbb{R} : a + (b + c) = (a + b) + c,$ *(asociativita)*

   d) $\forall a, b \in \mathbb{R} : a + b = b + a.$ *(komutativita)*

2. Na množině $\mathbb{R}$ je definována operace násobení $\cdot, \quad \cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$. Operace přiřazuje každé dvojici $x, y \in \mathbb{R} \times \mathbb{R}$ prvek $x \cdot y \in \mathbb{R}$. Násobení má tyto vlastnosti:

   a) $\exists 1 \in \mathbb{R} \quad \forall a \in \mathbb{R} : 1 \cdot a = a \cdot 1 = a,$ *(jednička je neutrální prvek vzhledem k $\cdot$)*

   b) $\forall a \in \mathbb{R} - \{0\} \quad \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = 1,$ *(existence inverzních prvků)*

   c) $\forall a, b, c \in \mathbb{R} : a \cdot (b \cdot c) = (a \cdot b) \cdot c,$ *(asociativita)*

d) $\forall a, b \in \mathbb{R} : a \cdot b = b \cdot a.$ *(komutativita)*

3. $\forall a, b, c \in \mathbb{R} : a \cdot (b + c) = (a \cdot b) + (a \cdot c).$ *($\cdot$ je distributivní vzhledem k $+$)*

4. Na množině $\mathbb{R}$ je definována relace nerovnost $<$, která splňuje tyto podmínky:

   a) $\forall a, b, c \in \mathbb{R} : (a < b \wedge b < c) \Rightarrow a < c,$ *(tranzitivita)*

   b) $\forall a, b \in \mathbb{R}$: $a < b \oplus a = b \oplus a > b.$ *(trichotomie)*

5. Axiom vazby operací a uspořádání: $\forall a, b, c \in \mathbb{R}$:

   a) $a < b \Rightarrow a + c < b + c,$

   b) $(0 < a \wedge 0 < b) \Rightarrow 0 < a \cdot b.$

6. Axiom úplnosti: $(A, B \subset \mathbb{R} : \forall a \in A, \forall b \in B : a < b) \Rightarrow \exists c \in \mathbb{R} : a < c < b.$

(Kubínová, Novotná, 1997, s. 154-155)

Pozn. 28. Thurston (1956) k názvu reálných čísel píše, že nejsou *reálná* proto, že by byla v nějakém ohledu reálnější než podobory, nýbrž proto, že jsou v některých vlastnostech *reálnější* než jejich nadobory. Například je možné znázornit je na číselné ose.

7.1.2 Cantorova konstrukce oboru reálných čísel

Pro zavedení oboru reálných čísel Cantorovou konstrukcí je potřeba nejprve definovat, co je *cauchyovská* posloupnost.

Definice 24. Posloupnost $a = \{a_n\}_{n=1}^{\infty}, a_n \in \mathbb{Q}$, je cauchyovská, jestliže:

$$\forall \varepsilon > 0 \quad \exists n_0 \in \mathbb{N} \quad \forall m, n \in \mathbb{N}; m, n > n_0 : |a_m - a_n| < \varepsilon.$$

(Kubínová, Novotná, 1997, s. 155)

Definice 25. Nechť $a = \{a_n\}_{n=1}^{\infty}, b = \{b_n\}_{n=1}^{\infty}$ jsou posloupnosti racionálních čísel. Definujeme:

- $a + b = \{a_n + b_n\}_{n=1}^{\infty}$,
- $a - b = \{a_n - b_n\}_{n=1}^{\infty}$,
- $a \cdot b = \{a_n \cdot b_n\}_{n=1}^{\infty}$,
- $\frac{a}{b} = \left\{\frac{a_n}{b_n}\right\}_{n=1}^{\infty}$ pro $b_n \neq 0$.

(Kubínová, Novotná, 1997, s. 155)

Nyní zavedeme množinu všech cauchyovských posloupností F.

$$F = \{a; a = \{a_n\}_{n=1}^{\infty} \text{ je cauchyovská posloupnost racionálních čísel}\}.$$

Dále definujeme relaci $\sim$ na F:

$$a \sim b \Leftrightarrow \lim_{n\to\infty}(a_n - b_n) = 0.$$

Ukážeme, že relace $\sim$ je ekvivalence na F:

- Je relace $\sim$ reflexivní? Ukážeme, že $\forall a \in F : a \sim a$. Přepíšeme relaci podle definice:

  $$a \sim a \Leftrightarrow \lim_{n\to\infty}(a_n - a_n) = 0.$$

  To platí, relace je tedy reflexivní.

- Je relace $\sim$ symetrická? Ukážeme, že $\forall a, b \in F : a \sim b \Rightarrow b \sim a$. Obě strany přepíšeme podle definice relace $\sim$:

  $$L : a \sim b \Leftrightarrow \lim_{n\to\infty}(a_n - b_n) = \lim_{n\to\infty}(a_n) - \lim_{n\to\infty}(b_n) = 0 \Rightarrow \lim_{n\to\infty}(a_n) = \lim_{n\to\infty}(b_n),$$

$P: b \sim a \Leftrightarrow \lim\limits_{n\to\infty}(b_n - a_n) = \lim\limits_{n\to\infty}(b_n) - \lim\limits_{n\to\infty}(a_n) = 0 \Rightarrow \lim\limits_{n\to\infty}(b_n) = \lim\limits_{n\to\infty}(a_n).$

Tedy dostáváme $\lim_{n\to\infty}(a_n) = \lim_{n\to\infty}(b_n) \Rightarrow \lim_{n\to\infty}(b_n) = \lim_{n\to\infty}(a_n)$, a relace $\sim$ je proto symetrická.

- Je relace $\sim$ tranzitivní? Ukážeme, že $\forall a, b, c \in F : (a \sim b \wedge b \sim c) \Rightarrow a \sim c$. Začneme přepsáním předpokladu podle definice relace $\sim$:

$$\lim_{n\to\infty}(a_n - b_n) = 0 \quad \wedge \quad \lim_{n\to\infty}(b_n - c_n) = 0.$$

Chceme ukázat, že pak $\lim_{n\to\infty}(a_n - c_n) = 0$:

$$\lim_{n\to\infty}(a_n - c_n) = \lim_{n\to\infty}(a_n - c_n) + \lim_{n\to\infty}(b_n) - \lim_{n\to\infty}(b_n) = \lim_{n\to\infty}(a_n) -$$
$$- \lim_{n\to\infty}(c_n) + \lim_{n\to\infty}(b_n) - \lim_{n\to\infty}(b_n) = \lim_{n\to\infty}(a_n - b_n) + \lim_{n\to\infty}(b_n - c_n) = 0.$$

Protože $\lim_{n\to\infty}(a_n - c_n) = 0$, platí $a \sim$c.

Relace $\sim$ je na F tranzitivní.

Protože je relace $\sim$ reflexivní, symetrická i tranzitivní, jedná se o ekvivalenci na F.

Množinu $\mathbb{R}$ reálných čísel definujeme jako rozklad množiny F podle ekvivalence $\sim$. Třídy tohoto rozkladu jsou prvky množiny $\mathbb{R}$. Tedy platí:

$$\mathbb{R} = \{T_a; a \in F\}, T_a = \{x \in F; x \sim a\}.$$

Na množině $\mathbb{R}$ zavedeme operace $+$ a $\cdot$.

Definice 26. Sčítání na množině $\mathbb{R}$ definujeme:

$$\forall T_a, T_b \in \mathbb{R} : T_a + T_b = T_{a+b}.$$

Pozn. 29. Pro korektnost definice 26 je ještě třeba ověřit, že součet nezávisí na volbě reprezentantů tříd a že $T_{a\cdot b} \in \mathbb{R}$.

Definice 27. Odčítání na množině $\mathbb{R}$ definujeme:

$$\forall T_a, T_B \in \mathbb{R} : T_a - T_b = T_{a-b}.$$

Pozn. 30. V důkazech vět 31 a 32 použijeme následující vlastnosti limit posloupností. Ty vycházejí z (Kubínová, Novotná, 1997, s. 23) a (Kubínová, Novotná, 1997, s. 35).

1. Nechť $\lim_{n\to\infty} a_n = 0$ a posloupnost $\{b_n\}_{n=1}^{\infty}$ je omezená. Pak existuje limita $\lim_{n\to\infty}(a_n \cdot b_n)$ a je rovna 0.

2. Je-li $\lim_{n\to\infty} a_n = a \in \mathbb{R}$, $\lim_{n\to\infty} b_n = b \in \mathbb{R}$, pak:

   a) $\exists \lim_{n\to\infty}(a_n + b_n)$ a platí $\lim_{n\to\infty}(a_n + b_n) = a + b$,

   b) $\exists \lim_{n\to\infty}(a_n \cdot b_n)$ a platí $\lim_{n\to\infty}(a_n \cdot b_n) = a \cdot b$,

   c) pro $b \neq 0 \quad \exists \lim_{n\to\infty} \frac{a_n}{b_n}$ a platí $\lim_{n\to\infty} \frac{a_n}{b_n} = \frac{a}{b}$.

Věta 31. $\forall T_a, T_b, T_c \in \mathbb{R}$ *platí:*

1) $(T_a + T_b) + T_c = T_a + (T_b + T_c)$, *(asociativita)*

2) $T_a + T_b = T_b + T_a$, *(komutativita)*

3) $T_a + T_{\{0,0,\dots\}} = T_a$, *($T_{\{0,0,\dots\}}$ je neutrální prvek)*

4) $T_a + (T_b - T_a) = T_b$. *(existence inverzních prvků)*

Důkaz. 1. Dokážeme, že sčítání reálných čísel je asociativní:

$$(T_a + T_b) + T_c = T_{(a+b)} + T_c = T_{(a+b)+c} \stackrel{\star}{=} T_{a+(b+c)} = T_a + T_{(b+c)} = \\ = T_a + (T_b + T_c).$$

$\star$: Využili jsme asociativitu sčítání racionálních čísel (viz věta 25).

Sčítání je asociativní pro všechna $T_a, T_b, T_c \in \mathbb{R}$.

2. Chceme ukázat, že sčítání reálných čísel je komutativní:

$$T_a + T_b = T_{(a+b)} \stackrel{\star}{=} T_{b+a} = T_b + T_a.$$

$\star$: Využili jsme komutativitu sčítání racionálních čísel (viz věta 25).

Sčítání je komutativní pro všechna $T_a, T_b \in \mathbb{R}$.

3. Chceme ukázat, že $T_{\{0,0,\dots\}}$ je neutrálním prvkem vzhledem ke sčítání:

$$T_a + T_{\{0,0,\dots\}} = T_{(a+0)} \stackrel{\star}{=} T_a.$$

$\star$: Využili jsme toho, že 0 je neutrální prvek vzhledem ke sčítání racionálních čísel (viz věta 25).

$T_{\{0,0,\dots\}}$ je neutrálním prvkem pro všechna $T_a \in \mathbb{R}$ vzhledem ke sčítání.

4. A nakonec platnost tvrzení $T_a + (T_b - T_a) = T_b$:

$$T_a + (T_b - T_a) = T_a + T_{(b-a)} = T_{(a+b-a)} \stackrel{\star}{=} T_{(b+0)} = T_b.$$

$\star$: Využili jsme komutativitu a vlastnost opačných prvků vzhledem ke sčítání racionálních čísel (viz věta 25).

Pro každé reálné číslo T_a existuje opačné číslo vzhledem ke sčítání ve tvaru $-T_a$.

$\square$

Definice 28. Násobení na množině $\mathbb{R}$ definujeme:

$$\forall T_a, T_b \in \mathbb{R} : T_a \cdot T_b = T_{(a\cdot b)}.$$

Pozn. 31. Pro korektnost definice 28 je ještě třeba ověřit, že součin nezávisí na volbě reprezentantů tříd a to, že $T_{a\cdot b} \in \mathbb{R}$.

Definice 29. Dělení na množině $\mathbb{R}$ definujeme:

$$\forall T_a, T_b \in \mathbb{R} : \frac{T_a}{T_b} = T_{\frac{a}{b}}; T_b \neq T_{\{0,0,\dots\}}.$$

Věta 32. $\forall T_a, T_b, T_c \in \mathbb{R}$ *platí:*

1) $(T_a \cdot T_b) \cdot T_c = T_a \cdot (T_b \cdot T_c)$, *(asociativita)*

2) $T_a \cdot T_b = T_b \cdot T_a$, *(komutativita)*

3) $T_a \cdot T_{\{1,1,\dots\}} = T_a$, *($T_{\{1,1,\dots\}}$ je neutrální prvek)*

4) $T_b \cdot \frac{T_a}{T_b} = T_a; T_b \neq T_{\{0,0,\dots\}}$, *(existence inverzních prvků)*

5) $(T_a + T_b) \cdot T_c = T_a \cdot T_c + T_b \cdot T_c$. *(distributivita násobení vzhledem ke sčítání)*

Důkaz. 1. Dokážeme asociativitu násobení reálných čísel:

$$(T_a \cdot T_b) \cdot T_c = T_{(a \cdot b)} \cdot T_c = T_{[(a \cdot b) \cdot c]} \stackrel{\star}{=} T_{[a \cdot (b \cdot c)]} = T_a \cdot T_{(b \cdot c)} = T_a \cdot (T_b \cdot T_c).$$

$\star$: Využili jsme asociativitu násobení racionálních čísel (viz věta 24).

Násobení je asociativní pro všechna $T_a, T_b, T_c \in \mathbb{R}$.

2. Chceme ukázat, že násobení reálných čísel je komutativní:

$$T_a \cdot T_b = T_{(a \cdot b)} \stackrel{\star}{=} T_{(b \cdot a)} = T_b \cdot T_a.$$

$\star$: Využili jsme komutativitu násobení racionálních čísel (viz věta 24).

Násobení je komutativní pro všechna $T_a, T_b \in \mathbb{R}$.

3. Ukážeme, že $T_{\{1,1,\dots\}}$ je neutrálním prvkem vzhledem k násobení reálných čísel:

$$T_a \cdot T_{\{1,1,\dots\}} = T_{(a \cdot 1)} \stackrel{\star}{=} T_a.$$

$\star$: Využili jsme toho, že 1 je neutrální prvek vzhledem k násobení racionálních čísel (viz věta 24).

$T_{\{1,1,\dots\}}$ je neutrálním prvkem vzhledem k násobení pro všechna $T_a \in \mathbb{R}$.

4. Chceme ukázat, že $\forall T_a, T_b, T_c \in \mathbb{R}$ platí tvrzení $T_b \cdot \frac{T_a}{T_b} = T_a$.

$$T_b \cdot \frac{T_a}{T_b} = T_b \cdot T_{\frac{a}{b}} = T_{b \cdot \frac{a}{b}} \stackrel{\star}{=} T_a.$$

$\star$: Využili jsme vlastnosti inverzních prvků vzhledem k násobení racionálních čísel (viz věta 24).

Pro každé reálné číslo $T_a \neq T_{\{0,0,\dots\}}$ existuje inverzní prvek ve tvaru $\frac{1}{T_a}$.

5. Nakonec dokážeme distributivitu násobení vzhledem ke sčítání:

$$(T_a + T_b) \cdot T_c = T_{(a+b)} \cdot T_c = T_{[(a+b)\cdot c]} \stackrel{\star}{=} T_{(a \cdot c + b \cdot c)} = T_a \cdot T_c + T_b \cdot T_c.$$

$\star$: Využili jsme distributivity násobení vzhledem ke sčítání racionálních čísel (viz věta 25).

Násobení je distributivní vzhledem ke sčítání pro všechna $T_a, T_b, T_c \in \mathbb{R}$.

$\square$

Pozn. 32. Definice a věty v kapitole 7.1.2 vycházejí ze skript Posloupnosti a řady (Kubínová Novotná, 1997).

7.1.3 Konstrukce pomocí Dedekindových řezů

Jiný způsob konstrukce reálných čísel popsal Richard Dedekind. Jeho metoda je založena na takzvaných *řezech.*

Předpokládejme, že existuje způsob rozdělení množiny všech racionálních čísel na dvě množiny. Množinu A a množinu B. Přitom platí, že pro každý prvek $b \in B$ je větší než každý prvek a množiny A. Takové rozdělení nazýváme řezem na množině racionálních čísel. (Courant, Robbins, 1996)

Formálně tedy definujeme:

Definice 30. Dedekindovým řezem A/B na množině racionálních čísel nazveme uspořádanou dvojici $[A, B]$, kde A, B jsou množiny racionálních čísel, pro které platí:

(1) $A \neq \emptyset \wedge B \neq \emptyset$,

(2) pro každé $a \in A$ a $b \in B$ platí $a < b$, a tedy i $A \cap B = \emptyset$,

(3) $A \cup B = \mathbb{Q}$.

(Kolman, 2008, s. 99; Kubínová, Novotná, 1997)

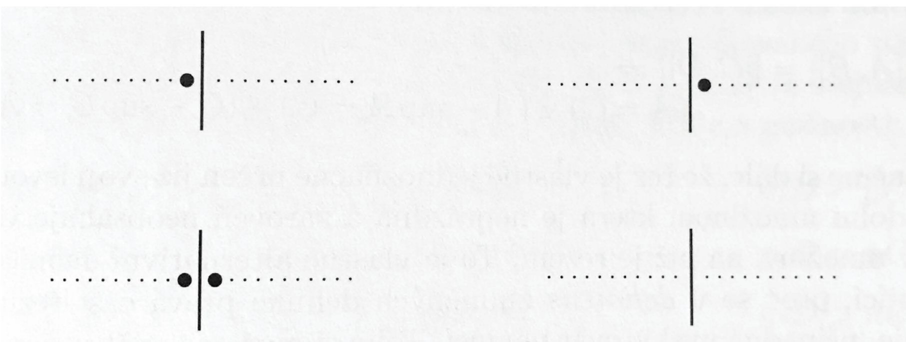
Pro řez mohou nastat pouze následující tři případy podle toho, zda existuje supremum/infimum na A, B (viz obrázek 16):

1) Existuje supremum $a' \in A$, které je zároveň infimem množiny B. (viz obrázek 16 vpravo nahoře)

2) Existuje infimum množiny $b' \in B$, které je zároveň supremum množiny A (viz obrázek 16 vlevo nahoře).

3) Neexistuje ani supremum v A, ani infimum v B. (viz obrázek 16 vpravo dole)

(Kolman, 2008; Courant, Robbins, 1996)



Obrázek 16: Dedekindovy řezy (Kolman, 2008, s. 101)

Pozn. 33. Pro případ 1) platí, že supremum množiny A je infimem množiny B, a pro případ 2) obráceně. Případy se liší pouze tím, do které z množin A, B supremum/infimum náleží. (Kolman, 2008)

Případ, že by existovalo supremum $a' \in A$ a infimum $b' \in B$, kdy $a' \neq b'$, nemůže nastat. Důvodem je, že například racionální číslo p, které je aritmetickým průměrem a' a b', by bylo větší než a' a menší než b', a tedy nepatřilo ani do A, ani do B, což je ve sporu s definicí řezu. (Courant, Robbins, 1996)
V případě 3) řez podle Dedekinda definuje iracionální číslo (viz obrázek 16 vlevo dole). (Kolman 2008; Courant, Robbins, 1996)

7.1.4 Definice iracionálních čísel pomocí vnořených intervalů

Definice 31. Uvažujme posloupnost intervalů $I_1, I_2, I_3, \dots, I_n, \dots$ na množině racionálních čísel takovou, že každý další interval je obsažen v intervalech předešlých, a takovou, že velikost intervalu se s rostoucím n neomezeně blíží nule. Takovou posloupnost nazveme posloupností vnořených intervalů (*nested intervals*).

(Courant, Robbins, 1996)

Věta 33. *Pro každou posloupnost vnořených intervalů existuje právě jeden bod, který je obsažen v každém z nich.*

(Courant, Robbins, 1996)

Pozn. 34. Věta je pod názvem *Cantorova věta o vnořených intervalech* dokázána například na stranách 13-14 v textu *Učební text k přednášce matematická analýza I* (Klazar, 2007). Dostupné online na: https://kam.mff.cuni.cz/~klazar/analyzaI.pdf.

Definice 32. Bod z věty 33 nazveme reálným číslem. Nejedná-li se o číslo racionální, pak se jedná o číslo iracionální.

(Courant, Robbins, 1996)

7.2 Spočetnost

Věta 34. *Množina reálných čísel je nekonečnou množinou.*

Důkaz. Množina reálných čísel obsahuje všechna čísla racionální. Množina racionálních čísel je nekonečná, tedy i množina reálných čísel je nekonečná. □

Věta 35. *Množina reálných čísel není spočetnou množinou.*

Důkaz. Předpokládejme, že množina reálných čísel je spočetná. Je-li spočetná, pak existuje její bijektivní zobrazení na $\mathbb{N}$. Seřaďme všechna reálná čísla do následující posloupnosti $\{a_n\}$:

$$\begin{aligned} a_1 &= 0, u_1 u_2 u_3 u_4 u_5 \dots \\ a_2 &= 0, v_1 v_2 v_3 v_4 v_5 \dots \\ a_3 &= 0, w_1 w_2 w_3 w_4 w_5 \dots \\ &\vdots \end{aligned}$$

Nyní pomocí tzv. Cantorovy diagonalizační metody sestrojíme prvek $a_c \in \mathbb{R}$ ve tvaru $0, c_1 c_2 c_3 c_4 c_5 \dots$, pro který platí, že prvek $c_1 \neq u_1$, prvek $c_2 \neq v_2$, prvek $c_3 \neq w_3$, ...
Takový prvek ovšem nebyl v posloupnosti $\{a_n\}$, přičemž jsme předpokládali, že v posloupnosti $\{a_n\}$ jsou všechny prvky $\mathbb{R}$. To je spor a bijektivní zobrazení reálných čísel na čísla přirozená neexistuje. □

7.3 Uspořádání na množině reálných čísel

Věta 36. *Relace $<$, zavedená jako 4. axiom axiomatické výstavby oboru reálných čísel (viz kapitola 7.1.1), je uspořádáním na množině reálných čísel.*

Důkaz. Axiom 4. v kapitole 7.1.1 také říká, že je relace $<$ na $\mathbb{R}$ tranzitivní a trichotomická. Proto se jedná o uspořádání na $\mathbb{R}$. □

7.4 Reálná čísla jako algebraická struktura

Věta 37. *Reálná čísla spolu s operacemi $+$ a $\cdot$ tvoří těleso.*

Důkaz. Vlastnosti tělesa plynou z vět 31 a 32. $\square$

8 Komplexní čísla

Posledním na gymnáziích probíraným oborem je obor komplexních (imaginárních) čísel. V učebnici *Matematika pro gymnázia, Komplexní čísla* (Calda, 1994) jsou komplexní čísla definována takto: „**Komplexním číslem** nazveme výraz tvaru $a + b\mathrm{i}$, kde a, b jsou reálná čísla a i je číslo, pro něž $\mathrm{i}^2 = -1$. V komplexním čísle $a + b\mathrm{i}$ se číslo a nazývá **reálná část**, číslo b - nikoli $b\mathrm{i}$ - **imaginární část**; číslo i se nazývá **imaginární jednotka**.“ (Calda, 1994, s. 12)

Motivací k zavedení komplexních čísel je požadavek na řešení rovnic typu $x^2 + 1 = 0$ (Fine, 1907). Historicky však potřeba zavést komplexní čísla vzešla z rovnic kubických. Acheson (2002) na straně 167 demonstruje potřebu komplexních čísel na příkladu $x^3 = 15x + 4$. Když Cardano popsal v šestnáctém století vzoce pro řešení kubických rovnic (viz poznámka 35), dostal se jejich použitím ke tvaru (Acheson, 2002):

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} = \sqrt[3]{2 + 11\sqrt{-1}} + \sqrt[3]{2 - 11\sqrt{-1}}.$$

Bez čísel komplexních bychom nyní učinili závěr, že rovnice nemá řešení, jelikož $\sqrt{-121}$ neexistuje. Ovšem Cardano si uvědomoval, že reálné řešení existuje, rovnice je splněna pro $x = 4$. Roku 1572 tento problém vyřešil Rafael Bombelli. (Crilly, 2010; Acheson, 2002).

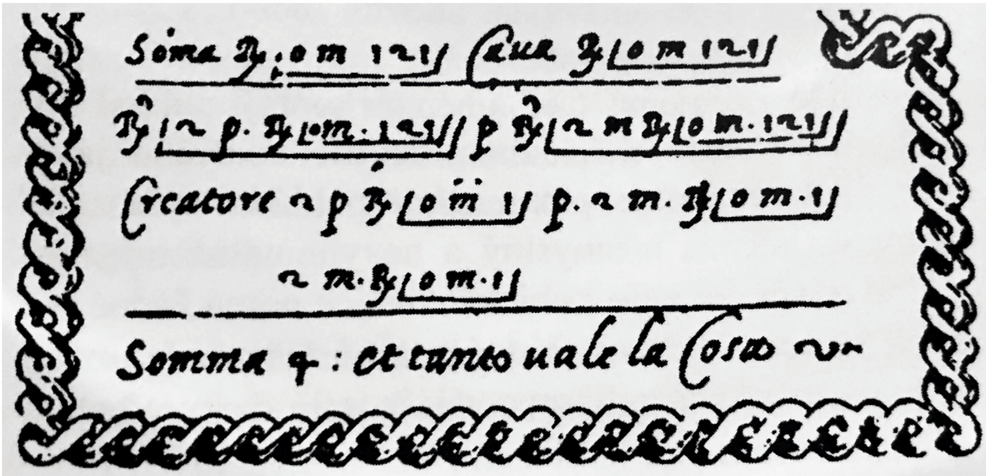
Bombelli s $\sqrt{-1}$ pracoval jako s běžným číslem. Pro vyřešení Cardanova problému umocnil výraz $2 + \sqrt{-1}$ na třetí. Tak dostal výraz $8 + 12\sqrt{-1} - 6 - \sqrt{-1} = = 2 + 11\sqrt{-1}$. Platí tedy, že $(2 + \sqrt{-1})^3 = 2 + 11\sqrt{-1}$, a obdobně bychom pro $(2 - \sqrt{-1})^3$ dostali $2 - 11\sqrt{-1}$. Platí proto:

$$\sqrt[3]{2 + 11\sqrt{-1}} + \sqrt[3]{2 - 11\sqrt{-1}} = \sqrt[3]{(2 + \sqrt{-1})^3} + \sqrt[3]{(2 - \sqrt{-1})^3} = 4,$$

což je reálným řešením rovnice. (Acheson, 2002)

Pozn. 35. Rovnice $x^3 = 15x + 4$ má ještě kořeny $x = -2 \pm \sqrt{3}$, které bychom dopočítali buď vydělením rovnice polynomem $(x - 4)$ a následným dořešením kvadratické rovnice, nebo také z Cardanových vzorců, které jsou uvedeny například v *Mathematical Handbook of Formulas and Tables* (Spiegel, Liu, 1968, s. 32).

Na obrázku 17 je vidět, jak Bombelli pracuje s výrazem odmocnina (zapsaným jinak, než jsme dnes zvyklí) z $0\,m\,121$, kde m značí znaménko minus. (Acheson, 2002)



Obrázek 17: Bombelli v knize *L'Algebra* (1572) pracuje s $\sqrt{-121}$, (Acheson, 2002, s. 168)

Euler roku 1777 jako první pro $\sqrt{-1}$ použil symbol i (Crilly, 2010). Fine (1907) za prvního označil Gausse.

Rozdělení čísel na reálná a imaginární není podle Finea (1907) zcela vhodné. O číslech komplexních říká, že nejsou o nic více imaginární, než čísla záporná nebo zlomky. Název imaginární pochází pravděpodobně z úst Reného Descarta. Existence imaginárních čísel byla otázkou filosofů, zatímco pro matematiky je komplexní jednotka pouhým znakem, stejně jako například znaménko minus. (Crilly, 2010; Fine, 1907).

„Hamilton považoval komplexní čísla za uspořádanou dvojici reálných čísel (a, b)*, čímž odkryl jejich dvojrozměrný charakter a tajemnou* $\sqrt{-1}$ *zbavil kouzla.“* (Crilly, 2010, s. 35)

Hamilton začal komplexní čísla interpretovat jako uspořádané dvojice, čímž ukázal, že znak i je pouhým pozičním znakem, a tedy ničím nepředstavitelným nebo imaginárním. (Crilly, 2010)

Téměř ve stejné době komplexní čísla začali znázorňovat do roviny matematici Gauss a Argand. Proto při znároznění komplexních čísel do roviny mluvíme o Gaussově/Argandově rovině. (Courant, Robbins, 1996; Crilly, 2010; Calda, 1994)

Jako uspořádanou dvojici konstruujeme čísla i v následujícím zavedení.

8.1 Konstrukce komplexních čísel

Definice 33. Množinu $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ nazveme množinou komplexních čísel. Protože je $\mathbb{C}$ rovno kartézskému součinu, jsou prvky množiny $\mathbb{C}$ uspořádané dvojice $z = (a, b)$, kde $a, b \in \mathbb{R}$, pro které platí:

$$\forall a, b, c, d \in \mathbb{R} : (a, b) = (c, d) \Leftrightarrow (a = c \wedge b = d).$$

(Kubínová, Novotná, 1996, s. 163)

8.2 Operace na množině komplexních čísel

Definice 34. Sčítat a násobit komplexní čísla budeme takto:

$$\begin{aligned} \forall a, b, c, d \in \mathbb{R} :& (a, b) + (c, d) = (a + c, b + d), \\ & (a, b) \cdot (c, d) = (a \cdot c - b \cdot d, a \cdot d + b \cdot c). \end{aligned}$$

(Kubínová, Novotná, 1996, s. 163)

8.3 Spočetnost a mohutnost množiny komplexních čísel

Věta 38. *Množina komplexních čísel je nekonečná množina.*

Důkaz. Množina reálných čísel je nekonečná. Komplexní čísla jsou uspořádanou dvojicí reálných čísel. Proto jsou také nekonečná. □

Věta 39. *Množina komplexních čísel je nespočetná.*

Důkaz. Množina reálných čísel je nespočetná množina. Komplexní čísla jsou uspořádanou dvojicí reálných čísel. Proto musí být také nespočetná. □

8.4 Uspořádání na množině komplexních čísel

Pozn. 36. Množinu reálných čísel lze izomorfně vnořit do množiny čísel komplexních. Podrobný postup nebudeme pro rozsah práce uvádět. Těleso reálných čísel ztotožníme se strukturou $\mathbb{C}' = \{z; , z = (a, 0), a \in \mathbb{R}\}$. Dvojici $(a, 0)$ budeme značit a.

Označme $\mathrm{i} = (0, 1)$. Použijeme definici sčítání a násobení komplexních čísel. Pak můžeme každé komplexní číslo (a, b) zapsat ve tvaru $(a, 0) + (b, 0)\mathrm{i}$, tj. $a + b\mathrm{i}$.

Věta 40. *Množinu komplexních čísel nelze uspořádat.*

Důkaz. Větu dokážeme sporem. Předpokládejme, že existuje uspořádání $<$ na množině komplexních čísel. Pro uspořádání platí, že je-li $a \neq 0$, je $a^2 > 0$. Protože $\mathrm{i} \neq 0$, je $\mathrm{i}^2 = -1 > 0$. Obě strany poslední nerovnosti vynásobíme číslem -1 a dostáváme $1 < 0$. Číslo $\mathrm{i}^2 \neq 0$, proto $(\mathrm{i}^2)^2 = 1 > 0$.

Ukázali jsme, že $(1 > 0) \wedge (1 < 0)$. To je spor s trichotomií.

Množinu komplexních čísel nelze uspořádat.

□

8.5 Komplexní čísla jako algebraická struktura

Věta 41. *Množina komplexních čísel spolu s operacemi $+$ a $\cdot$ tvoří těleso.*

Důkaz. Musíme pro operaci $+$ ověřit následující vlastnosti pro všechna $z_1, z_2, z_3 \in$ $\in \mathbb{C}$:

1.a) $z_1 + z_2 \in \mathbb{C}$, *(uzavřenost operace)*

2.a) $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$, *(asociativita)*

3.a) $\exists 0 \in \mathbb{C} \quad \forall z \in \mathbb{Z} : z + 0 = 0 + z = z$, *(existence neutrálního prvku)*

4.a) $\forall z \in \mathbb{C} \quad \exists(-z) \in \mathbb{C} : z + (-z) = 0$, *(existence opačných prvků)*

5.a) $z_1 + z_2 = z_2 + z_1$. *(komutativita)*

Pro operaci $\cdot$ musíme ověřit následující vlastnosti pro všechna $z_1, z_2, z_3 \in \mathbb{C}$:

1.b) $z_1 \cdot z_2 \in \mathbb{C}$, *(uzavřenost operace)*

2.b) $(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$, *(asociativita)*

3.b) $\exists 1 \in \mathbb{C} \quad \forall z \in \mathbb{Z} : 1 \cdot z = z \cdot 1 = z$, *(existence neutrálního prvku)*

4.b) $\forall z \in \mathbb{C} - \{0\} \quad \exists z^{-1} \in \mathbb{C} : z \cdot z^{-1} = 1$, *(existence inverzních prvků)*

5.b) $z_1 \cdot z_2 = z_2 \cdot z_1$. *(komutativita)*

A navíc ještě musíme ověřit, že platí pro všechna $z_1, z_2, z_3 \in \mathbb{C}$:

1.c) $(z_1 + z_2) \cdot z_3 = z_1 \cdot z_3 + z_2 \cdot z_3$. *(násobení je distributivní ke sčítání)*

Pro důkaz budeme využívat tvaru komplexního čísla jako uspořádané dvojice reálných čísel, jejichž vlastnosti již známe. Nechť tedy $z_1 = (a, b), z_2 = (c, d)$ a $z_3 = (e, f)$, kde $a, b, c, d, e, f \in \mathbb{R}$.

1.a) Chceme ukázat, že $(a, b) + (c, d)$ patří také do množiny komplexních čísel. Sečteme čísla podle definice 34:

$$(a, b) + (c, d) = (a + c, b + d),$$

čísla a, b, c, d jsou reálná, tedy i součty čísel $a+c$ a $b+d$ jsou reálná čísla. Proto podle definice 33 je i součet komplexních čísel komplexním číslem a operace $+$ je vnitřní operací na množině komplexních čísel.

2.a) Znovu využijeme definici 34 a upravíme zvlášť levou a zvlášť pravou stranu rovnosti:

$$\left.\begin{aligned} L &= ((a, b) + (c, d)) + (e, f) = (a + c, b + d) + (e, f) = (a + c + e, b + d + f) \\ R &= (a, b) + ((c, d) + (e, f)) = (a, b) + (c + e, d + f) = (a + c + e, b + d + f) \end{aligned}\right\} L = P.$$

Sčítání je na množině komplexních čísel asociativní.

3.a) Dokážeme, že $(0, 0)$ je neutrální prvek pro operaci $+$. Využijeme k tomu definici 34:

$$(a, b) + (0, 0) = (a + 0, b + 0) \overset{\star}{=} (a, b),$$

$$(0, 0) + (a, b) = (0 + a, 0 + b) \overset{\star}{=} (a, b).$$

$\star$: Využili jsme větu 31.

Operace $+$ je na množině komplexních čísel asociativní.

4.a) Dokážeme, že opačným číslem k číslu (a, b) je komplexní číslo $(-a, -b)$. Opět využijeme definici 34:

$$(a, b) + (-a, -b) = (a - a, b - b) \overset{\star}{=} (0, 0).$$

$\star$: Využili jsme větu 31.

Opačným prvkem k prvku (a, b) je tedy opravdu prvek $(-a, -b)$. Značit ho budeme $-z$.

5.a) Pro důkaz komutativity znovu využijeme větu 34. Chceme ukázat, že pro všechna $(a,b),(c,d) \in \mathbb{C}$ platí $(a,b)+(c,d)=(c,d)+(a,b)$. Upravíme každou stranu rovnosti zvlášť:

$$\left.\begin{aligned} L &= (a,b)+(c,d) = (a+c,b+d) \\ R &= (c,d)+(a,b) = (c+a,d+b) \stackrel{\star}{=} (a+c,b+d) \end{aligned}\right\} L = P.$$

$\star$: Využili jsme větu 31.

Sčítání je na množině komplexních čísel komutativní.

1.b) Chceme ukázat, že součin dvou komplexních čísel je prvkem množiny komplexních čísel:

$$(a,b)\cdot(c,d) = (a\cdot c - b\cdot d, a\cdot d + b\cdot c),$$

a,b,c,d jsou reálná čísla, proto i $a\cdot c - b\cdot d$ a $a\cdot d + b\cdot c$ jsou podle věty 37 reálná čísla. Součin je tedy podle definice 33 prvkem množiny $\mathbb{C}$.

2.b) Dokážeme asociativitu násobení komplexních čísel. Chceme ukázat, že pro všechna $(a,b),(c,d),(e,f) \in \mathbb{C}$ platí $((a,b)\cdot(c,d))\cdot(e,f) = (a,b)\cdot((c,d)\cdot(e,f))$. Upravíme zvlášť levou a zvlášť pravou stranu rovnosti. Využijeme definici 34:

$$\begin{aligned} L &= ((a,b)\cdot(c,d))\cdot(e,f) = (a\cdot c - b\cdot d, a\cdot d + b\cdot c)\cdot(e,f) = \\ &= ((a\cdot c - b\cdot d)\cdot(e) - (a\cdot d + b\cdot c)\cdot f, (a\cdot c - b\cdot d)\cdot f + (a\cdot d + b\cdot c)\cdot e) = \\ &\stackrel{\star}{=} (a\cdot c\cdot e - b\cdot d\cdot e - a\cdot d\cdot f - b\cdot c\cdot f, a\cdot c\cdot f - b\cdot d\cdot f + a\cdot d\cdot e + b\cdot c\cdot e) = \\ &\stackrel{*}{=} (a\cdot c\cdot e - a\cdot d\cdot f - b\cdot c\cdot f - b\cdot d\cdot e, a\cdot c\cdot f + a\cdot d\cdot e + b\cdot c\cdot e - b\cdot d\cdot f), \\ R &= (a,b)\cdot((c,d)\cdot(e,f)) = (a,b)\cdot(c\cdot e - d\cdot f, c\cdot f + d\cdot e) = \\ &= (a\cdot(c\cdot e - d\cdot f) - b\cdot(c\cdot f + d\cdot e), a\cdot(c\cdot f + d\cdot e) + b\cdot(c\cdot e - d\cdot f)) = \\ &\stackrel{\star}{=} (a\cdot c\cdot e - a\cdot d\cdot f - b\cdot c\cdot f - b\cdot d\cdot e, a\cdot c\cdot f + a\cdot d\cdot e + b\cdot c\cdot e - b\cdot d\cdot f). \end{aligned}$$

$\star$: Využili jsme větu 32.

$*$: Využili jsme větu 31.

$L = P$. Násobení je tedy asociativní na množině komplexních čísel.

3.b) Dokážeme, že $(1,0)$ je neutrálním prvkem pro operaci $\cdot$. Využijeme k tomu definici 34:

$$(a,b)\cdot(1,0) = (a\cdot 1 - b\cdot 0, a\cdot 0 + b\cdot 1) \overset{\star}{=} (a,b),$$

$$(1,0)\cdot(a,b) = (1\cdot a - 0\cdot b, 1\cdot b + 0\cdot a) \overset{\star}{=} (a,b).$$

$\star$: Využili jsme věty 32 a 31.

Prvek $(1,0)$ je tedy neutrálním prvkem pro násobení komplexních čísel.

4.b) Předpokládejme, že inverzním prvkem čísla (a,b) vzhledem k násobení je $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$. Dokážeme, že opravdu je:

$$(a,b)\cdot\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right) = \left(\frac{a^2+b^2}{a^2+b^2}, \frac{-a\cdot b + a\cdot b}{a^2+b^2}\right) \overset{\star}{=} (1,0).$$

$\star$: Využili jsme větu 31.

Ke každému nenulovému komplexnímu číslu najdeme inverzní prvek ve tvaru $(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2})$.

5.b) Pro důkaz komutativity násobení upravíme obě strany rovnosti podle definice 34:

$$\left.\begin{aligned} L &= (a,b)\cdot(c,d) = (a\cdot c - b\cdot d, a\cdot d + b\cdot c) \\ P &= (c,d)\cdot(a,b) = (c\cdot a - d\cdot b, c\cdot b + d\cdot a) \overset{\star}{=} (a\cdot c - b\cdot d, a\cdot d + b\cdot c) \end{aligned}\right\} L = P.$$

$\star$: Využili jsme věty 32 a 31.

Násobení na množině komplexních čísel je komutativní.

1.c) Pro důkaz distributivity upravíme levou i pravou stranu podle definice 34 a ukážeme, že se rovnají:

$$
\begin{aligned}
L &= ((a,b)+(c,d))\cdot(e,f) = (a+c,b+d)\cdot(e,f) = \\
&= ((a+c)\cdot e-(b+d)\cdot f,(a+c)\cdot f+(b+d)\cdot e) = \\
&\overset{\star}{=} (a\cdot e+c\cdot e-b\cdot f-d\cdot f,a\cdot f+c\cdot f+b\cdot e+d\cdot e), \\
P &= (a,b)\cdot(e,f)+(c,d)\cdot(e,f) = (a\cdot e-b\cdot f,a\cdot f+b\cdot e)+ \\
&+(c\cdot e-d\cdot f,c\cdot f+d\cdot e) = (a\cdot e-b\cdot f+c\cdot e-d\cdot f, \\
&a\cdot f+b\cdot e+c\cdot f+d\cdot e), \\
L &= P.
\end{aligned}
$$

$\star$: Využili jsme větu 32.

Násobení je na množině komplexních čísel distributivní vzhledem ke sčítání.

Ukázali jsme, že struktura $(\mathbb{C},+)$ tvoří Abelovu grupu. Také jsme ukázali, že množina $(\mathbb{C}-\{0\},\cdot)$ tvoří Abelovu grupu a nakonec distributivitu násobení vzhledem ke sčítání. Struktura $(\mathbb{C},+,\cdot)$ je tedy tělesem. $\square$

9 Další číselné obory

Po zavedení komplexních (dvourozměrných) čísel se objevily snahy o popis dalších, vícerozměrných čísel. Hamilton se snažil o konstrukci čísel třírozměrných, spolu s operacemi + a ·, avšak neúspěšně. Snahu tedy vzdal a pokusil se o popis čísel čtyřrozměrných. To se mu nakonec povedlo. Taková čísla nazýváme kvaterniony a na rozdíl od čísel komplexních, která mají imaginární jednotku i, mají kvaterniony takovéto jednotky tři, obvykle označované i, j, k. (Crilly, 2010; Bečvář 2005)

Na úspěch Hamiltona se podařilo navázat s čísly osmirozměrnými (Cayleho čísla). Dále bylo ukázáno, že šestnáctirozměrná čísla nemohou existovat. (Crilly, 2010)

Díky rozvoji teorie her byla objevena tzv. čísla nadreálná. O nich se blíže dočteme např. v knize *Surreal Numbers* (Knuth, 1974). Dále se nadreálným číslům věnuje kniha *Which Numbers Are Real?* (Henle, 2012). V ní se dočteme i další informace o kvaternionech, nebo dokonce o číslech hyperkomplexních.

10 Závěr

Cílem této práce bylo shromáždit informace o oborech čísel přirozených, celých, racionálních, reálných a komplexních. Dále bylo cílem ukázat konstrukci oborů a jejich vlastnosti, jako například zda je obor spočetnou množinou nebo jaké vlastnosti mají operace na oborech definované.

K získání informací byly využity jak české, tak cizojazyčné (převážně anglické) publikace a další informační zdroje. Jelikož práce obahuje také historii číselných oborů, snažil jsem se používat i starých, původních knih. Ty byly bohužel často buď obtížně dohledatelné, volně nepřístupné, nebo psány jazykem, který neovládám. Proto jsem byl často nucen spokojit se s informacemi ze zdrojů sekundárních. Přesto se mi podařilo nastínit u každé z hlavních kapitol práce nejdůležitější informace o motivaci k zavedení i způsobu popsání oboru.

U každého oboru je popsán princip výstavby a zavedení aritmetických operací. Většina vět je dokázána. Pro rozsah práce a analogičnost vět mezi obory byly některé důkazy vynechány. Snaha byla také o propojení kapitol pomocí odkazů na věty, definice a poznámky z kapitol předcházejících. Společné vlastnosti, které byly u oborů zkoumány, jsou spočetnost a vlastnosti binárních operací, které byly na oborech definovány.

Před psaním práce jsem zamýšlel, že práce bude obsahovat větší množství paradoxů a zajímavostí spojených s číselnými obory. Ovšem po nastudování literatury jsem zjistil, že by tak práce nabyla obrovských rozměrů. Téma by tak snadno mohlo být samostatným zaměřením nějaké další práce. Přesto některé zajímavosti jsou alespoň naznačeny a za paradox lze považovat i například již zmíněnou spočetnost. Zaujala mě zejména kapitola o součinu záporných čísel nebo důkaz komutativity jak násobení, tak sčítání. Tyto vlastnosti jsou známé už od základní školy, přesto jsem se s uspokojivým vysvětlením setkal až při studiu materiálů pro tvorbu práce. Přitom se jedná o něco, co je častým dotazem nejednoho žáka nejen střední, ale už základní školy, stejně jako otázka, co je to vlastně číslo, na kterou odpovídám v prvních kapitolách.

11 Seznam použitých informačních zdrojů

[1] ACHESON, D. J. *1089 a další parádní čísla: [matematická dobrodružství].* Praha: Dokořán, 2006. ISBN 80-7363-025-7.

[2] BEČVÁŘ, Jindřich. *Lineární algebra.* Vyd. 3. Praha: Matfyzpress, 2005. ISBN 80-86732-57-6.

[3] BUŠEK, Ivan a Emil CALDA. *Matematika pro gymnázia: základní poznatky.* 3. upr. vyd. Praha: Prometheus, 1999. Učebnice pro střední školy. ISBN 80-7196-146-9.

[4] CALDA, Emil. *Matematika pro gymnázia.* 4. vyd. Praha: Prometheus, 2008. Učebnice pro střední školy (Prometheus). ISBN 978-80-7196-364-6.

[5] COURANT, Richard, Herbert. ROBBINS a Ian STEWART. *What is mathematics?: an elementary approach to ideas and methods.* 2nd ed. New York: Oxford University Press, 1996. ISBN 0-19-510519-2.

[6] CRILLY, A. J. *Matematika: 50 myšlenek, které musíte znát.* Praha: Slovart, 2010. ISBN 978-80-7391-409-7.

[7] D'ALEMBERT, Jean le Rond, l'Abbé BOSSUT &c. *Encyclopédie Méthodique: Mathématiques* [online]. Paris: Panckoucke, 1785 [cit. 2018-06-30]. Dostupné z https://books.google.cz/books?id=xk2toqVxRasC&printsec=frontcover&hl=cs&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

[8] FINE, Henry B. *The number-system of algebra treated theoretically and historically.* Second Edition. Boston, U.S.A: D.C.Heath & CO., Publishers, 1907.

[9] HEEFFER, Albrecht. *Historical Objections Against the Number Line.* 2011, 20(9), 863-880. DOI: 10.1007/s11191-011-9349-0. ISSN 0926-7220. Dostupné také z: http://link.springer.com/10.1007/s11191-011-9349-0.

[10] HRUŠA, Karel. *Polynomy v moderní algebře: pro účastníky matematické olympiády.* Praha: Mladá fronta, 1970. Škola mladých matematiků.

[11] KING, Allesandra. A brief history of numerical systems - Alessandra King. In: *Youtube* [online]. 19. 1. 2017 [cit. 2018-05-06]. Dostupné z: https://youtu.be/cZH0YnFpjwU. Kanál uživatele TED-Ed.

[12] KOLMAN, Vojtěch. *Bytí a číslo.* [přednáška]. Praha: Filosofická fakulta Univerzity Karlovy, 2017.

[13] KOLMAN, Vojtěch. *Filosofie čísla: základy logiky a aritmetiky v zrcadle analytické filosofie.* Praha: Filosofia, 2008. ISBN 978-80-7007-279-0.

[14] KUBÍNOVÁ, Marie a Jarmila NOVOTNÁ. *Posloupnosti a řady: matematická analýza, teoretická aritmetika.* Praha: Karolinum, 1997. ISBN 80-7184-564-7.

[15] LUNDYOVÁ, Miranda. Posvátná čísla. *Kvadrivium: čtyři svobodná umění: aritmetika, geometrie, hudba a astronomie.* Přeložil Stanislav PAVLÍČEK, přeložil Jiří PILUCHA, přeložil Helena NYKLOVÁ, přeložil Petr HOLČÁK, přeložil Robert TSCHORN. Praha: Dokořán, 2015. Pergamen. ISBN 978-80-7363-732-3.

[16] MURRAY R. SPIEGEL. *Mathematical handbook of formulas and tables.* 34. print. New York, NY [u.a.]: McGraw-Hill, 1995. ISBN 0070602247.

[17] NOVOTNÁ, Jarmila a Milan TRCH. *Algebra a teoretická aritmetika: sbírka příkladů : skripta pro posl. pedag. fakulty Univ. Karlovy.* Praha: Karolinum, 1993. ISBN 80-706-6717-6.

[18] ODVÁRKO, Oldřich a Jiří KADLEČEK. *Matematika pro 6. ročník základní školy, 1. díl.* 2. Vydání. Praha: Prometheus, 1999. ISBN 80-7196-142-6.

[19] ODVÁRKO, Oldřich a Jiří KADLEČEK. *Matematika pro 7. ročník základní školy: [učebnice zpracovaná podle učebních osnov vzdělávacího programu Základní škola]*. Praha: Prometheus, 1998. Učebnice pro základní školy. ISBN 80-719-6111-6.

[20] Ottův slovník naučný: illustrovaná encyklopædie obecných vědomostí, šestý díl [online]. Praha: J. Otto, 1893 [cit. 2018-06-27]. Dostupné z: http://kramerius4.nkp.cz/search/i.jsp?pid=uuid:5d12b090-e6e6-11e4-a794-5ef3fc9bb22f#monograph-monographunit-page_uuid:faf2fa20-0a74-11e5-b309-005056825209.

[21] PACIOLI, Luca. *Summa de arithmetica, geometria, proportioni et proportionalita*. Toscolano: Paganino de Paganini, 1523.

[22] PAVLICOVÁ, Vladimíra. *Webová aplikace pro výuku základních poznatků z matematiky na střední škole* [online]. 2010 [cit. 2018-06-27]. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/86737. Vedoucí práce Jarmila Robová.

[23] SERVÍT, František. *Eukleidovy základy: (Elementa)*. Praha: Jednota českých mathematiků, 1907.

[24] THURSTON, H. A. *The number-system*. London: Blackie, 1956.