ARITMETIKA 1

Jaroslav Beránek

0. Úvod

Tento text je určen pro studenty učitelství pro 1. stupeň základní školy. Jelikož se jedná o doplněk k základní studijní literatuře [1], nejsou v tomto textu uváděny důkazy jednotlivých tvrzení. Pro studium textu je nutno předpokládat znalosti základů algebry (množinové operace a jejich vlastnosti, binární relace a jejich vlastnosti, relace uspořádání a uspořádané množiny, relace ekvivalence a rozklad množiny, binární algebraické operace a jejich vlastnosti, algebraické struktury a jejich homomorfismy). Standardní je rovněž označení základních číselných množin:
$\boldsymbol{N}$ – množina všech přirozených čísel (samozřejmě včetně čísla nula)
$\boldsymbol{Z}$ – množina všech celých čísel
$\boldsymbol{Q}$ – množina všech racionálních čísel
$\boldsymbol{R}$ – množina všech reálných čísel
V učebnici [1] je množina všech celých čísel označována $\boldsymbol{C}$, my se však přidržíme tradičního označení množiny celých čísel jako $\boldsymbol{Z}$.

1. Přirozená čísla

Úmluva: Všude v dalším budeme mezi přirozená čísla počítat i číslo nula, byť to odporuje současné normě. Pro účel Vašeho studia je však nutné, abychom nulu za přirozené číslo považovali.

Úvod 1.0. Přirozená čísla se vyvíjela v myšlení lidí od nepaměti. Bylo by jistě velmi zajímavé studovat představy pravěkých lovců nebo např. občanů antického Řecka o pojetí množství a vyjádření počtu věcí či objektů, to však není účelem Vašeho studia. Objevuje se však problém, jak teoreticky vybudovat přirozená čísla a dokázat jejich vlastnosti (již víte z dřívějška, že množina $\boldsymbol{N}$ s operacemi sčítání a násobení tvoří komutativní polookruh s neutrálním prvkem). Teoreticky nejčastěji se přirozená čísla zavádějí pomocí Peanových axiomů jako prvky tzv. Peanovy množiny. Tento způsob je v matematické literatuře vždy využíván, je však zcela formální. Proto bývají k zavedení množiny $\boldsymbol{N}$ užívány i dva modely Peanovy množiny, tj. kardinální čísla konečných množin a ordinální čísla dobře uspořádaných konečných množin. Budeme tedy mluvit o třech možnostech zavedení přirozených čísel: Kardinální čísla, ordinální čísla a prvky Peanovy množiny. Výklad zahájíme Peanovou množinou.

Axiomy Peanovy množiny $\boldsymbol{P}$

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

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

a) $e \in M$,

b) $(\forall\, x \in P)\ x \in M \Rightarrow x^{|} \in M$, pak $M = P$.

Věta 1.1. Nechť $x \in P$, pak platí:

(1) $x \neq x^{|}$ **,**

(2) $x \neq e \Rightarrow (\exists\, u \in P)\ x = u^{|}$**.**

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

Věta 1.2. Peanova množina je nekonečná množina.

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

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

(2) Jestliže existuje ${}^{/}a$, pak ${}^{/}a \in U(a)$,

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

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

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

Poznámka 1.5. Z předchozího plyne, že Peanovu množinu můžeme považovat za teoretický model množiny přirozených čísel. V tomto případě prvek e je roven číslu 0, následovník $x^{|}$ je roven číslu $x + 1$ a modely úseků příslušných ke každému přirozenému číslu chápanému jako prvek množiny P si lze představit takto: $U(1) = \{0\}$, $U(2) = \{0, 1\}$, $U(3) = \{0, 1, 2\}$, $U(4) = \{0, 1, 2, 3\}$ atd. Je zřejmé, že počet prvků každého úseku je určen přirozeným číslem, jemuž daný úsek přísluší. Proto i v dalším textu je možné představit si porovnávání prvků Peanovy množiny (relaci uspořádání v množině P) a následně i operace sčítání a násobení v množině P pomocí množiny přirozených čísel. I když teoretický postup je opačný (z obecné teorie v množině P plynou speciální vlastnosti v množině přirozených čísel), je pro pochopení podstaty vhodné už na tomto místě využít množiny přirozených čísel jako modelu Peanovy množiny P. Poznamenejme dále, že existuje i možnost vybudovat axiomaticky Peanovu množinu tak, že prvek e je roven číslu 1. V tom případě je samozřejmě nutné všechny definice a tvrzení přeformulovat.

Relace uspořádání v množině *P*

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

Poznámka 1.7. Je zřejmé, že relace $<$ z definice 1.6. je antireflexivní, antisymetrická a tranzitivní, jedná se tedy skutečně o ostré uspořádání v množině P. Pro každé dva různé prvky

a, b množiny P vždy platí právě jeden ze vztahů $a \in U(b)$, $b \in U(a)$, proto je uspořádání $<$ lineární.

Věta 1.8. Nechť $a, b \in P$. Pak platí:
(1) $(\forall\, a \in P)\ a < a^{|}$;
(2) Mezi prvky $a, a^{|}$ neexistuje žádný prvek x množiny P s vlastností $a < x < a^{|}$);
(3) Množina $(P, \leq)$ je dobře uspořádaná množina.

Operace sčítání v množině *P*

Věta 1.9. Na množině P existuje právě jedna operace + taková, že pro každou dvojici x, y prvků množiny P platí:
(1) $x + e = x$,
(2) $x + y^{|} = (x + y)^{|}$.

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

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

Věta 1.12. V grupoidu $(P, +)$ platí pro každé tři prvky x, y, z množiny P implikace

$$x + y = x + z \Rightarrow y = z\,.$$

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

Operace sčítání je spojena s relací uspořádání řadou vztahů. Některé jsou uvedeny v následující větě. Povšimněte si, že tyto vztahy odpovídají běžně známým vztahům, užívaným při výpočtech.

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

Operace násobení v množině *P*

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

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

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

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

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

Operace násobení je spojena s relací uspořádání řadou vztahů. Některé jsou uvedeny v následující větě (zajímavá je analogie s obdobnými vztahy pro sčítání).

Věta 1.19. Nechť $x, y, z, u, v \in P, z \neq e$. Pak platí:

(1) $x < y \Leftrightarrow x \cdot z < y \cdot z$
(2) $x \cdot z = y \cdot z \Rightarrow x = y$
(3) $x \leq y, u \leq v \Rightarrow x \cdot u \leq y \cdot v.$

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

Poznámka 1.21. Z definice množiny P a popsaných vlastností relace uspořádání a operací sčítání a násobení v této množině vyplývá, že polookruh všech přirozených čísel $(\boldsymbol{N}, +, \cdot)$ je jedním z možných modelů polookruhu $(P, +, \cdot)$. Roli prvku e hraje číslo 0, následovníkem čísla x je číslo $x + 1$, úsek množiny $\boldsymbol{N}$ příslušný číslu n obsahuje všechna přirozená čísla od čísla 0 po číslo $n - 1$ atd. Je samozřejmé, že provádění operací sčítání a násobení podle vět 1.9. a 1.15. se nikde v praxi nepoužívá. O tom pojednáme v části o kardinálních číslech.

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

Přirozená čísla jako kardinální čísla konečných množin

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

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

Popíšeme-li výše uvedenou konstrukci populárně (a matematicky ne zcela přesně), pak kardinální číslo konečné množiny M je systém množin, který kromě dané množiny M obsahuje všechny množiny (nekonečně mnoho), které mají tentýž počet prvků jako množina

M. Tato jediná společná vlastnost všech těchto množin, tj. stejný počet prvků, je vyjádřena přirozeným číslem, které je kardinálním číslem množiny *M* definováno. Ve školské matematice na ZŠ proto říkáme, že přirozená čísla vyjadřují počty prvků konečných množin.

Přechod od struktury $(P, +, \cdot)$ k jejímu modelu $(\boldsymbol{N}, +, \cdot)$ lze popsat takto: Nechť $n \in P$ je libovolný prvek Peanovy množiny. Úsek množiny *P* příslušný k prvku *n* je množina $U(n) = \{e, e^{|}, e^{||}, e^{|||}, \ldots, {}^{/}n\}$. Tato množina je konečná, proto jistě náleží do některé třídy rozkladu $\mathcal{M}_{|\sim}$. Tato třída rozkladu je kardinálním číslem konečné množiny *U(n)* a odpovídající přirozené číslo je číslo *n.* Lze tedy tvrdit, že úsek *U(n)* obsahuje právě *n* prvků. Odtud prvku *e* odpovídá číslo *0,* prvku $e^{|}$ číslo *1,* prvku $e^{||}$ číslo *2* atd. Uspořádání přirozených čísel lze pak definovat ve shodě s definicí porovnávání prvků Peanovy množiny (každé číslo náležející do *U(n)* je menší než číslo *n*).

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

Definice 1.23. (Sčítání kardinálních čísel)
Nechť *A, B* jsou konečné množiny, nechť platí $A \cap B = \phi$. Pak definujeme

$$|A| + |B| = |A \cup B|.$$

Definice 1.24. (Násobení kardinálních čísel)
Nechť *A, B* jsou konečné množiny. Pak definujeme

$$|A| \cdot |B| = |A \times B|.$$

Definice 1. 25. (Porovnávání kardinálních čísel)
Nechť *A, B* jsou konečné množiny. Pak definujeme$|A| < |B|$, právě když množina A je ekvivalentní s vlastní podmnožinou množiny B.

Poznámka 1.26. Lze ukázat, že obě operace definované definicemi 1.24. a 1.25. mají všechny vlastnosti, které očekáváme od operací sčítání a násobení přirozených čísel. Povšimněme si nyní omezující podmínky $A \cap B = \phi$ v definici 1.24. V případě jejího vypuštění bude pro součet kardinálních čísel množin *A, B* platit vztah $|A| + |B| \geq |A \cup B|$, přičemž číslo na levé straně této neostré nerovnosti je obecně větší než číslo na pravé straně o počet prvků průniku obou množin. Platí tedy rovnost

$$|A| + |B| - |A \cap B| = |A \cup B|.$$

Z teoretického hlediska se jedná o princip inkluze a exkluze pro $n = 2$. Pokud jsou tedy množiny *A, B* disjunktní, pak $|A \cap B| = 0$ a předchozí rovnost přejde v definici sčítání kardinálních čísel podle definice 1.24.

Přirozená čísla jako ordinální čísla konečných množin

Teorii ordinálních čísel uvedeme pouze populární formou. Tato teorie je svým formálním matematickým popisem velmi komplikovaná a nepřehledná, přičemž její důležitost ve srovnání s kardinální teorií je nesrovnatelně menší. Půjde pouze o to, abyste intuitivně pochopili, o čem se v ordinální teorii jedná. Podrobné formulace naleznete v učebnici [1]. Opět se budeme zabývat pouze konečnými množinami. Poznamenejme úvodem, že teorie ordinálních čísel je „aplikace teorie kardinálních čísel na uspořádané množiny“. Víme již, že množina je ostře lineárně uspořádaná, jestliže je na ní definována relace antireflexivní,

antisymetrická, tranzitivní a souvislá. Pro každou konečnou ostře lineárně uspořádanou množinu pak platí, že každý její prvek má jednoznačně určené pořadí (jako např. ve frontě osob u pokladny v supermarketu). Lze tedy vždy označit první (nejmenší) a poslední (největší) prvek této množiny. Každá ostře lineárně uspořádaná konečná množina je též současně dobře uspořádaná (každá její neprázdná podmnožina má první prvek). Na systému $\mathcal{G}$ všech konečných dobře uspořádaných množin je definována relace podobnost $\approx$ (jde o analogii relace ekvivalence množin z teorie kardinálních čísel). Tato relace $\approx$ je reflexivní, symetrická a tranzitivní, je to tedy rovněž relace ekvivalence. Populárně lze konstatovat, že dvě konečné dobře uspořádané množiny jsou podobné, mají-li stejný počet prvků. Lze tedy analogicky definovat rozklad $\mathcal{G}\,|_{\approx}$ systému $\mathcal{G}$ určený ekvivalencí $\approx$. Třídy rozkladu $\mathcal{G}\,|_{\approx}$ se nazývají ordinální čísla. Ordinálním číslem konečné dobře uspořádané množiny M tedy rozumíme třídu rozkladu $\mathcal{G}\,|_{\approx}$, která obsahuje množinu M a všechny množiny s ní podobné. Ordinální číslo množiny M budeme označovat ord (M).

Popíšeme-li výše uvedenou konstrukci populárně (a matematicky ne zcela přesně), pak ordinální číslo konečné dobře uspořádané množiny M je systém dobře uspořádaných množin, který kromě dané dobře uspořádané množiny M obsahuje všechny dobře uspořádané množiny (nekonečně mnoho), které mají tentýž počet prvků jako množina M. Tato jediná společná vlastnost všech těchto množin, tj. stejný počet prvků, je vyjádřena přirozeným číslem, které je ordinálním číslem množiny M definováno. Lze tedy říci, že přirozená čísla vyjadřují počty prvků konečných dobře uspořádaných množin.

Porovnávání ordinálních čísel a operace s nimi se na ZŠ takřka nepoužívají, proto je na tomto místě neuvádíme. Lze je nalézt v učebnici [1].

Přirozená čísla a jejich vlastnosti

Existují tři možnosti zavedení přirozených čísel: jako čísla kardinální, čísla ordinální a prvky formálně zavedené Peanovy množiny. V praxi na školách je nejdůležitější a nejrozšířenější zavedení přirozených čísel jako čísel kardinálních, kdy přirozená čísla vyjadřují počty prvků konečných množin. Ve smyslu ordinálních čísel vyjadřují přirozená čísla počty prvků konečných dobře uspořádaných množin, zatímco přirozená čísla jako prvky Peanovy množiny jsou pouze symboly (nevyjadřují počet prvků). Tato poslední možnost se sice často vyskytuje v praxi (telefonní čísla, čísla občanských průkazů, bankovních kont, označení vozidel MHD, tažená čísla ve Sportce apod). Při zavádění přirozených čísel na 1. stupni ZŠ však důsledně zavádíme přirozená čísla jako počty prvků konečných množin, tzn. jako kardinální čísla. Některé základní vlastnosti přirozených čísel nyní uvedeme (jde pouze o výběr).

Definice 1. 27. (dělení se zbytkem v množině přirozených čísel)
Pro každá dvě přirozená čísla a, b ($b \neq 0$) existuje jediná dvojice přirozených čísel q, z ($z < b$) s vlastností $a = b \cdot q + z$. Číslo a se nazývá dělenec, číslo b se nazývá dělitel, číslo q se nazývá neúplný podíl a číslo z se nazývá zbytek.

Definice 1. 28. Nechť a, b jsou libovolná přirozená čísla. Nechť existuje přirozené číslo x s vlastností $a = b + x$. Potom přirozené číslo x nazveme rozdílem přirozených čísel a, b a píšeme $x = a - b$.

Definice 1. 29. Nechť a, b jsou libovolná přirozená čísla. Nechť existuje přirozené číslo x s vlastností $a = b \cdot x$. Potom přirozené číslo x nazveme podílem přirozených čísel a, b a píšeme $x = a : b$.

Základní vlastnosti operací sčítání a násobení plynou přímo z definice komutativního polookruhu s jednotkovým prvkem.

Předpokládáme, že všechny níže uvedené rozdíly a podíly přirozených čísel existují

- $(a-b)+b=a$ $\qquad (a+b)-b=a$
- $(a+b)-c=(a-c)+b=a+(b-c)$
- $a-(b-c)=(a+c)-b$ $\qquad a-(b+c)=(a-b)-c$
- $(a+c)-(b+c)=a-b$ $\qquad (a-c)-(b-c)=a-b$
- $(a:b).b=a$ $\qquad (a.b):b=a$
- $(a.b):c=(a:c).b=a.(b:c)$
- $a:(b:c)=(a.c):b$ $\qquad a:(b.c)=(a:b):c$
- $(a.c):(b.c)=a:b$ $\qquad (a:c):(b:c)=a:b$
- $a.0=0.a=0$
- $a+c=b+c \Rightarrow a=b$ $\qquad a.c=b.c \Rightarrow a=b\ (c\neq 0)$
- $a\neq 0 \wedge b\neq 0 \Rightarrow a.b\neq 0$ $\qquad a.b=0 \Rightarrow a=0 \vee b=0$
- $a>b \Leftrightarrow (\exists x\in N, x\neq 0)\ a=b+x$
- $a<b \Rightarrow a+c<b+c$ $\qquad a<b \Rightarrow a.c<b.c\ (c\neq 0)$
- $a+b=0 \Leftrightarrow a=b=0$ $\qquad a.b=1 \Leftrightarrow a=b=1$
- $a<b \wedge c<d \Rightarrow a+c<b+d$ $\qquad a<b \wedge c<d \Rightarrow a.c<b.d$

2. Celá čísla

Motivace 2.0. Známe již polookruh všech přirozených čísel a známe tedy všechny jeho vlastnosti a pravidla pro počítání s přirozenými čísly. Problémem ale je, že v oboru přirozených čísel nelze neomezeně odčítat ani dělit. Problém s odečítáním vyřešíme zavedením celých čísel. Obor celých čísel musí mít tedy následující vlastnosti:
1. Musí v něm platit všechna pravidla a vlastnosti operací jako v oboru přirozených čísel.
2. Musí být zajištěno neomezené odčítání každých dvou celých čísel.
3. Přirozená čísla musí být součástí (podmnožinou) celých čísel. Matematicky říkáme, že polookruh přirozených čísel lze izomorfně vnořit do oboru integrity celých čísel.

Konstrukce 2.1. Při konstrukci oboru integrity celých čísel postupujeme takto:
Vyjdeme z kartézského součinu $\boldsymbol{N} \times \boldsymbol{N}$, na kterém definujeme pro každé dvě dvojice $[a, b], [c, d] \in \boldsymbol{N} \times \boldsymbol{N}$ relaci $\sim$ vztahem:

$$[a, b] \sim [c, d] = a + d = b + c.$$

Tato relace je ekvivalence (je reflexivní, symetrická a tranzitivní), existuje tedy rozklad kartézského součinu $\boldsymbol{N} \times \boldsymbol{N}$ na třídy; tento rozklad budeme označovat $\boldsymbol{N} \times \boldsymbol{N} /_{\sim}$.

Definice 2.2. Třídy rozkladu $\boldsymbol{N} \times \boldsymbol{N} /_{\sim}$ kartézského součinu $\boldsymbol{N} \times \boldsymbol{N}$ určeného ekvivalencí $\sim$ se nazývají celá čísla. Celá čísla jsou tedy třídy navzájem ekvivalentních uspořádaných dvojic přirozených čísel.

Poznámka 2.3. Z definice relace ekvivalence $\sim$ plyne, že všechny navzájem ekvivalentní uspořádané dvojice přirozených čísel mají tentýž rozdíl mezi první a druhou složkou. Tento rozdíl určuje celé číslo, danou třídou definované. V dalším textu o celých číslech je proto nutno rozlišovat mezi případem, kdy $[a, b]$ bude označovat tuto jednu konkrétní uspořádanou dvojici přirozených čísel a případem, kdy bude hrát roli reprezentující dvojice nějakého celého čísla. V tomto druhém případě budeme užívat tučného označení $\boldsymbol{[a, b]}$. Platí tedy např. $\boldsymbol{[4, 2]} = \{[2, 0], [3, 1], [4, 2], [5, 3], [6, 4], ...\}$. Celé číslo je vždy reprezentováno nekonečnou množinou navzájem ekvivalentních uspořádaných dvojic přirozených čísel. Podle dohodnutého označení je nutno také rozlišovat následující vztahy: Např. pro uspořádané dvojice $[5, 3], [6, 4]$ platí $[5, 3] \neq [6, 4], [5, 3] \sim [6, 4],$ pro dvě celá čísla $\boldsymbol{[5, 3]}, \boldsymbol{[6, 4]}$ ale platí rovnost $\boldsymbol{[5, 3]} = \boldsymbol{[6, 4]},$ protože obě tyto dvojice jsou reprezentanty téže třídy rozkladu systému $\boldsymbol{N} \times \boldsymbol{N} |_{\sim}$. Poznamenejme, že v dalším textu budeme pro zjednodušení označovat celá čísla velkými tučnými písmeny, např. $\boldsymbol{A}, \boldsymbol{B},$ .... Toto označení není v rozporu s uvedenou konstrukcí; vždy lze přejít k reprezentaci pomocí uspořádaných dvojic, např. $\boldsymbol{A} = \boldsymbol{[a, b]}$, $\boldsymbol{B} = \boldsymbol{[c, d]}$, ...

Věta 2.4. Vnoření $\psi : \boldsymbol{N} \to \boldsymbol{Z}$ grupoidu $\boldsymbol{N}$ do grupy $\boldsymbol{Z}$ je definováno takto pro každý prvek $n \in \boldsymbol{N}$ předpisem

$$\psi (n) = \{[n, 0]; n \in \boldsymbol{N}\}.$$

Operace s celými čísly a jejich vlastnosti

Definice 2.5. Sčítání na množině celých čísel je definováno předpisem

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

Věta 2.6. Operace + z předchozí definice je komutativní, asociativní, má neutrální prvek ***0*** reprezentovaný dvojicí ***[n, n]*** pro libovolné $n \in N$ a ke každému celému číslu $A = [a, b]$ existuje právě jedno opačné číslo $-A = [b, a]$.

Věta 2.7. Algebraická struktura $(Z, +)$ je komutativní grupa, ve které jsou řešitelné základní rovnice, tj rovnice $A + X = B$ má vždy řešení v množině Z pro každá dvě celá čísla A, B.

Věta 2.8. V grupě $(Z, +)$ existuje právě jedna inverzní operace k operaci sčítání. Tato operace se nazývá odčítání a je definována vztahem $A - B = A + (-B)$.

Poznámka 2.9. Z předchozí věty a věty 2.6. lze odvodit početní pravidlo pro operaci odčítání:

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

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

Definice 2.10. Na množině Z definujme binární operaci $\cdot$ následujícím způsobem:

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

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

Věta 2.11. Grupoid $(Z, \cdot)$ je asociativní, komutativní a má neutrální prvek 1 reprezentovaný dvojicí $[n+1, n]$ pro libovolné $n \in N$.

Věta 2.12. V grupoidu $(Z, \cdot)$ pro každá tři celá čísla $x, y, z, x \neq 0$ platí implikace

$$x \cdot y = x \cdot z \Rightarrow y = z .$$

Věta 2.13. Operace násobení je v množině celých čísel svázána s operací sčítání distributivním zákonem, tj.

$$A, B, C \in Z: \; A \cdot (B + C) = A \cdot B + A \cdot C.$$

Věta 2.14. Algebraická struktura $(Z, +, \cdot)$ je komutativní okruh s neutrálním prvkem, který není tělesem. V tomto okruhu neexistují vlastní dělitelé nuly, je to tedy obor integrity.

Poznámka 2.15. V oboru integrity všech celých čísel $(Z, +, \cdot)$ platí řada tvrzení, běžně užívaných při výpočtech. Uveďme některé příklady.

Věta 2.16. Nechť $A, B, C \in Z$. Pak platí:
(1) $-(-A) = A$;
(2) $-(A + B) = (-A) + (-B)$;
(3) $-(A - B) = B - A$;
(4) $(A - (B - C) = (A + C) - B$;
(5) $(-A) \cdot B = A \cdot (-B) = -(A \cdot B)$.

Poznámka 2.17. Operace dělení není v množině $\boldsymbol{Z}$ neomezeně definované, proto nemůže existovat obecný vzorec pro výpočet podílu každých dvou celých čísel. Chceme-li zjistit podíl dvou celých čísel $\boldsymbol{A : B = X}$, je nutno postupovat podle definice podílu. Vztah $\boldsymbol{A : B = X}$ přepíšeme na tvar $\boldsymbol{A = B \cdot X}$, dosadíme za $\boldsymbol{A, B}$ reprezentující uspořádané dvojice a řešíme součin $\boldsymbol{A = B \cdot X}$ jako rovnici. V případě, že podíl existuje, je možno ho tímto postupem určit.

Relace uspořádání v množině celých čísel

Definice 2.18. Nechť $\boldsymbol{A = [a, b]}$ je celé číslo. Řekneme, že toto číslo je kladné a píšeme $\boldsymbol{A > 0}$, právě když platí $a > b$. Je-li $a = b$, pak číslo $\boldsymbol{A = 0}$; ve zbývajícím případě pro $a < b$ říkáme, že celé číslo $\boldsymbol{A}$ je záporné a píšeme $\boldsymbol{A < 0}$.

Poznámka 2.19. Je zřejmé, že jeden z předchozích případů vždy musí nastat. Každé celé číslo je tedy buďto kladné nebo záporné nebo je rovno nule. Existuje tedy rozklad množiny všech celých čísel na čísla kladná, nulu a čísla záporná. Ve shodě s běžnou terminologií zavádíme i označení $\boldsymbol{A \leq 0}$ a říkáme, že číslo $\boldsymbol{A}$ je nekladné, resp. v případě $\boldsymbol{A \geq 0}$ je toto číslo nezáporné.

Definice 2.20. Nechť $\boldsymbol{A, B}$ jsou celá čísla. Řekneme, že $\boldsymbol{A < B}$, právě když platí $\boldsymbol{A - B < 0}$. Je-li $\boldsymbol{A - B = 0}$, pak $\boldsymbol{A = B}$; ve zbývajícím případě pro $\boldsymbol{A - B > 0}$ pak platí $\boldsymbol{A > B}$.

Poznámka 2.21. Je zřejmé, že i v předchozí definici jeden z případů vždy musí nastat. Relace uspořádání všech celých čísel je tedy lineární. I zde se běžně užívá neostrá nerovnost $\boldsymbol{A \leq B}$ pro případ $\boldsymbol{A - B \leq 0}$ a analogicky $\boldsymbol{A \geq B}$ pro případ $\boldsymbol{A - B \geq 0}$.

Věta 2.22. Nechť $\boldsymbol{A}$ je celé číslo. Pak platí:
(1) $\boldsymbol{A > 0 \Rightarrow -A < 0}$.
(2) $\boldsymbol{A < 0 \Rightarrow -A > 0}$.

Věta 2.23. Nechť $\boldsymbol{A, B}$ jsou kladná celá čísla. Potom jejich součet $\boldsymbol{A + B}$ i součin $\boldsymbol{A \cdot B}$ jsou také kladná celá čísla.

Poznámka 2.24. Výše definovaná relace uspořádání v množině všech celých čísel je spojena s operacemi v této množině řadou vztahů. Uveďme alespoň některé.

Věta 2.25. Nechť $\boldsymbol{A, B, C, D}$ jsou libovolná celá čísla. Pak platí:
(1) Jestliže $\boldsymbol{A > B}$ a $\boldsymbol{C < 0}$, potom $\boldsymbol{AC < BC}$;
(2) Jestliže $\boldsymbol{A + C > B + C}$, potom $\boldsymbol{A > B}$;
(3) Jestliže $\boldsymbol{AC > BC}$ a $\boldsymbol{C > 0}$, potom $\boldsymbol{A > B}$;
(4) Jestliže $\boldsymbol{AC > BC}$ a $\boldsymbol{C < 0}$, potom $\boldsymbol{A < B}$;
(5) Jestliže $\boldsymbol{A > B}$ a $\boldsymbol{C > D}$, potom $\boldsymbol{A + C > B + D}$;
(6) Jestliže $\boldsymbol{A > B}$ a $\boldsymbol{C > D}$ a $\boldsymbol{C > 0}$ a $\boldsymbol{B > 0}$, potom $\boldsymbol{A \cdot C > B \cdot D}$.

Věta 2.26. Nechť $\boldsymbol{A, B}$ jsou libovolná celá čísla, přičemž $\boldsymbol{B \neq 0}$. Pak existuje jednoznačně určená dvojice celých čísel $\boldsymbol{Q, R}$ (přičemž $\boldsymbol{0 \leq R < |B|}$) s vlastností $\boldsymbol{A = B \cdot Q + R}$. Číslo $\boldsymbol{A}$ se nazývá dělenec, číslo $\boldsymbol{B}$ dělitel, číslo $\boldsymbol{Q}$ je podíl (někdy též neúplný podíl) a číslo $\boldsymbol{R}$ je zbytek. Proces nalezení čísel $\boldsymbol{Q, R}$ se nazývá dělení se zbytkem v množině celých čísel.

Definice 2.27. Absolutní hodnotu $|\boldsymbol{A}|$ celého čísla $\boldsymbol{A}$ definujeme takto:

(1) Je-li $A \geq 0$, pak $|A| = A$;
(2) Je-li $A < 0$, pak $|A| = -A$.

Věta 2.28. Nechť A, B jsou libovolná celá čísla, pak platí:
(1) $|A| = |-A|$;
(2) $A \leq |A|$;
(3) $|A|^2 = A^2$;
(4) $|A \cdot B| = |A| \cdot |B|$;
(5) $|A + B| \leq |A| + |B|$;
(6) $|A - B| \geq |A| - |B|$.

Poznámka 2.29. Vnoření $\psi : N \to Z$ grupoidu N do grupy Z je definováno pro každý prvek $n \in N$ předpisem $\psi(n) = \{[n,0];\ n \in N\}$. Každé celé kladné (tj. přirozené) číslo n je tedy reprezentováno dvojicí $[n, 0]$, číslo nula je reprezentováno dvojicí $[0, 0]$ a každé celé záporné číslo $-n$ je reprezentováno dvojicí $[0, n]$.

3. Racionální čísla

Motivace 3.0. Známe již obor integrity všech celých čísel a známe tedy všechny jeho vlastnosti a pravidla pro počítání s celými čísly. Problémem ale je, že v oboru celých čísel nelze neomezeně dělit. Problém s dělením vyřešíme zavedením racionálních čísel. Obor racionálních čísel musí mít tedy následující vlastnosti:
1. Musí v něm platit všechna pravidla a vlastnosti operací jako v oboru celých čísel.
2. Musí být zajištěno neomezené dělení každých dvou racionálních čísel (kromě dělení nulou).
3. Celá čísla musí být součástí (podmnožinou) racionálních čísel. Matematicky říkáme, že obor integrity celých čísel lze izomorfně vnořit do tělesa racionálních čísel.

Konstrukce 3.1. Při konstrukci tělesa racionálních čísel postupujeme takto:
Vyjdeme z kartézského součinu $Z \times Z - \{0\}$, na kterém definujeme pro každé dvě dvojice $[a, b], [c, d] \in Z \times Z - \{0\}$ relaci $\sim$ vztahem:

$$[a, b] \sim [c, d] = a \cdot d = b \cdot c.$$

Tato relace je ekvivalence (je reflexivní, symetrická a tranzitivní), existuje tedy rozklad kartézského součinu $Z \times Z - \{0\}$ na třídy; tento rozklad budeme označovat $Z \times Z - \{0\}/_\sim$.

Definice 3.2. Třídy rozkladu $Z \times Z - \{0\}/_\sim$ kartézského součinu $Z \times Z - \{0\}$ určeného ekvivalencí $\sim$ se nazývají racionální čísla. Racionální čísla jsou tedy třídy navzájem ekvivalentních uspořádaných dvojic celých čísel.

Poznámka 3.3. V dalším budeme kartézský součin $Z \times Z - \{0\}$ označovat M a nazývat množina všech zlomků. Protože se racionální čísla běžně vyjadřují pomocí zlomků, budeme uspořádané dvojice z množiny M zapisovat jako zlomky, tedy místo $[a, b]$ budeme psát $\frac{a}{b}$.
Odtud je také zřejmé, proč se v množině M pro druhé složky všech dvojic nepřipouští číslo nula.

Poznámka 3.4. Racionální čísla jsou podle této konstrukce třídami rozkladu $M\ |_{\sim}$, tedy třídami navzájem ekvivalentních zlomků. Vnoření $\psi : \boldsymbol{Z} \to \boldsymbol{Q}$ okruhu $\boldsymbol{Z}$ do tělesa $\boldsymbol{Q}$ je definováno pro každý prvek $z \in \boldsymbol{Z}$ předpisem

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

Poznámka 3.5. Analogicky jako u celých čísel budeme rozlišovat jeden konkrétní zlomek od racionálního čísla. Tučným označením $\frac{\boldsymbol{a}}{\boldsymbol{b}}$ budeme označovat stav, kdy tento zlomek bude reprezentovat racionální číslo, zatímco běžným způsobem $\frac{a}{b}$ budeme označovat tento jeden konkrétní zlomek. Platí tedy např. $\frac{\boldsymbol{3}}{\boldsymbol{4}} = \{\frac{3}{4}, \frac{6}{8}, \frac{3}{12}, \frac{-21}{-28}, ...\}$. Poznamenejme, že v dalším textu budeme pro zjednodušení označovat racionální čísla velkými tučnými písmeny, např. ***A,*** ***B,*** .... Toto označení není, tak jako u celých čísel, v rozporu s uvedenou konstrukcí; vždy lze přejít k reprezentaci pomocí uspořádaných dvojic, např. $\boldsymbol{A} = \frac{\boldsymbol{a}_1}{\boldsymbol{a}_2}$, $\boldsymbol{B} = \frac{\boldsymbol{b}_1}{\boldsymbol{b}_2}$, ...

Věta 3.6. Operace sčítání v množině všech racionálních čísel je definována vztahem $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$. Tato operace je komutativní, asociativní, má neutrální prvek, ke každému racionálnímu číslu existuje právě jedno číslo opačné a jsou řešitelné základní rovnice. Algebraická struktura $(\boldsymbol{Q}, +)$ je tedy komutativní grupa.

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

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

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

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

Věta 3.10. Operace násobení v množině všech racionálních čísel je definována vztahem $\frac{\boldsymbol{a}}{\boldsymbol{b}} \cdot \frac{\boldsymbol{c}}{\boldsymbol{d}} = \frac{\boldsymbol{ac}}{\boldsymbol{bd}}$. Tato operace je v množině $\boldsymbol{Q}$ komutativní, asociativní a má neutrální prvek. Tímto neutrálním prvkem je číslo $\boldsymbol{1}$ reprezentované třídou zlomků $\frac{\boldsymbol{a}}{\boldsymbol{a}}$. Algebraická struktura $(\boldsymbol{Q}, \cdot)$ je komutativní pologrupa s neutrálním prvkem. Operace násobení je distributivní vzhledem k operaci sčítání v množině všech racionálních čísel.

Poznámka 3.11. Budeme-li zkoumat i existenci inverzních prvků a řešitelnost základních rovnic vzhledem k operaci násobení v množině $\boldsymbol{Q}$, snadno zjistíme, že jediným prvkem, který neumožňuje platnost těchto vlastností, je číslo 0. Po jeho odstranění z množiny $\boldsymbol{Q}$ můžeme vyslovit následující větu.

Věta 3.12. (1) Algebraická struktura $(\boldsymbol{Q} - \{0\}, \cdot)$ je komutativní grupa.
(2) Algebraická struktura $(\boldsymbol{Q}, +, \cdot)$ je komutativní těleso.

Poznámka 3.13. Inverzním prvkem k racionálnímu číslu $\frac{a}{b}$ je číslo $\frac{b}{a}$. Toto číslo vždy jednoznačně existuje ($b \neq 0$ podle konstrukce racionálních čísel a $a \neq 0$ podle předpokladu z poznámky 3.11. a věty 3.12.), nazývá se převrácené číslo k číslu $\frac{a}{b}$ a označuje $\left(\frac{a}{b}\right)^{-1}$. Při označení racionálního čísla $\boldsymbol{A}$ se převrácené číslo kromě zápisu $\boldsymbol{A^{-1}}$ zapisuje též $\frac{1}{A}$. V množině $\boldsymbol{Q} - \{0\}$ jsme nyní připraveni k definici operace dělení.

Definice 3.14. Dělení v množině $\boldsymbol{Q} - \{0\}$ je definováno jako násobení převráceným číslem, tj. $\boldsymbol{A : B = A \cdot B^{-1}}$. Vyjádřeno pomocí definice operace násobení a převráceného čísla dostáváme

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

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

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

Relace uspořádání v množině racionálních čísel

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

Poznámka 3.19. Je zřejmé, že jeden z předchozích případů vždy musí nastat. Každé racionální číslo je tedy buďto kladné nebo záporné nebo je rovno nule. Existuje tedy rozklad množiny všech racionálních čísel na čísla kladná, nulu a čísla záporná. Ve shodě s běžnou

terminologií zavádíme i označení $A \leq 0$ a říkáme, že číslo A je nekladné, resp. v případě $A \geq 0$ je toto číslo nezáporné.

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

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

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

Definice 3.23. Uspořádání v množině racionálních čísel je husté, tzn.

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

Poznámka 3.24. Definice hustého uspořádání říká, že „mezi každá dvě různá racionální čísla lze vložit další racionální číslo“.

Desetinné rozvoje racionálních čísel

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

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

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

4. Reálná čísla

Poznámka 4.1. Podle definice 3.23 a poznámky 3.24 se „laickým pohledem“ zdá, že každý bod číselné osy je obrazem racionálního čísla. To však neplatí. Snadno lze dokázat, že na číselné ose jsou „mezery“; např. $\sqrt{2}$ je číslo, které zcela jistě existuje (délka úhlopříčky čtverce o straně 1), avšak není racionální (nelze ho vyjádřit pomocí zlomku).

Definice 4.2. Každá mezera v uspořádané množině $(\boldsymbol{Q}, <)$ určuje právě jedno iracionální číslo. Označíme-li množinu všech iracionálních čísel $\boldsymbol{I}$, pak pro množinu všech reálných čísel $\boldsymbol{R}$ platí $\boldsymbol{R} = \boldsymbol{Q} \cup \boldsymbol{I}$.

Věta 4.3.
(1) Lineárně uspořádaná množina $(\boldsymbol{R}, <)$ je spojitě uspořádaná (neobsahuje mezery).
(2) $\forall x, y \in \boldsymbol{R}, x < y; \exists z \in \boldsymbol{Q}: x < z < y$.
(3) Desetinný rozvoj iracionálních čísel je nekonečný a nikdy není periodický.
(4) Algebraická struktura $(\boldsymbol{R}, +, \cdot)$ je komutativní těleso.

Poznámka 4.4. Protože lineárně uspořádaná množina $(\boldsymbol{R}, <)$ neobsahuje mezery, lze konstatovat, že každý bod číselné osy je obrazem právě jednoho reálného čísla a naopak, každé reálné číslo lze jednoznačně znázornit na číselné ose.

Poznámka 4.5. Problém důkazu existence iracionálních čísel je velmi starý. Již v antickém Řecku se objevila tzv. první krize matematického myšlení, která se týkala „nesouměřitelnosti úseček“. V tehdejší matematice byla známá racionální čísla i to, že jakékoliv racionální číslo lze přesnou geometrickou konstrukcí zobrazit na číselné ose. Společně se znalostí hustoty uspořádání racionálních čísel byl tehdy všeobecně přijímán názor, že jiná čísla než racionální neexistují, že každé číslo lze vyjádřit zlomkem a že každý bod číselné osy je obrazem nějakého racionálního čísla. Objev faktu, že v jakémkoliv čtverci jsou jeho strana a úhlopříčka tzv. nesouměřitelné a že délku úhlopříčky nelze vyjádřit zlomkem (má-li strana čtverce délku a, má úhlopříčka délku $\sqrt{2}\,a$), způsobil v tehdejší době doslova pozdvižení, neboť nebylo známo, jak vzniklý problém vyřešit. Z teorie už víme, že princip nesouměřitelnosti znamená to, že lineárně uspořádaná množina racionálních čísel obsahuje mezery. Vyřešení problému nesouměřitelnosti, tj. zavedení iracionálních čísel, mohlo být úspěšně teoreticky ukončeno až mnohem později.

5. Číselné soustavy

Poznámka 9.1. Problematika zápisů čísel provází lidstvo už od starověku. Je známá řada poznatků o způsobech numerace během historického vývoje, např. numerace ve starém Egyptě a Mezopotámii, numerace antického Řecka a Říma nebo numerace starých Mayů. Jedná se o velmi zajímavé otázky, kterými se však na tomto místě nemůžeme zabývat. Konstatujme pouze, že během vývoje se vykrystalizovaly dva typy číselných soustav, a to poziční a nepoziční. Základní rozdíl je v tom, že nepoziční soustavy nerozlišují řád číslice v zápisu čísla, kdežto poziční soustavy ano. Většina numeračních soustav v dávné historii byla nepoziční (Egypt, Mezopotámie, Řecko, Řím), zatímco v dnešní době se užívají výhradně poziční soustavy. Jediná nepoziční soustava, se kterou se ještě dnes můžeme setkat, jsou římské číslice. Uvědomme si ovšem, že s římskými číslicemi nepočítáme (neprovádíme žádné početní výkony), slouží pouze jako zápisy letopočtů atp. Poziční soustavy, jak už bylo řečeno, rozlišují řád číslice. Proto je potřeba mít určen tzv. základ poziční číselné soustavy. Dnes se užívá pro běžné počítání výhradně soustava se základem deset (desítková soustava). Ve výpočetní technice se můžeme setkat ještě se soustavami, jejichž základem jsou některé mocniny čísla dvě (soustava dvojková, čtyřková, osmičková a šestnáctková). Pozičním číselným soustavám bude věnována tato kapitola. Budeme se zabývat převody zápisů čísel a početními výkony v nedesítkových číselných soustavách. Zřejmě se můžeme omezit pouze na

kladná čísla; začneme čísly přirozenými a následně si uvedeme i převody zápisů čísel racionálních.

Příklad 9. 2. Nepoziční soustavy nerozlišují řád číslice, zatímco poziční soustavy ano. Tedy např. v zápise římskými číslicemi je číslo I I I rovno třem, zatímco v desítkové soustavě je číslo 111 rovno sto jedenácti. Nepoziční soustavy nemají symbol pro nulu, který je naopak v pozičních soustavách nutný. Např. čísla stojedna, tisíc jedna jsou zapsána v desítkové soustavě 101, 1001, zatímco pomocí římských číslic C I, M I.

Věta 9. 3. Nechť z je pevně zvolené přirozené číslo větší než jedna, nechť a je libovolné přirozené číslo. Pak platí:
(1) Existuje přirozené číslo n s vlastností $z^n \leq a < z^{n+1}$.
(2) Číslo a lze vyjádřit právě jedním způsobem ve tvaru

$$a = a_n z^n + a_{n-1} z^{n-1} + a_{n-2} z^{n-2} + \ldots + a_2 z^2 + a_1 z + a_0 , \qquad (\star)$$

kde a_i , $i = 0, 1, 2, \ldots, n$ jsou nezáporná celá čísla menší než z.

Definice 9. 4. Nechť platí označení předchozí věty a pro čísla a, n platí vyjádření $(\star)$. Pak říkáme, že jsme číslo a vyjádřili v číselné soustavě o základu z. Zkráceně píšeme $a = (a_n a_{n-1} \ldots a_0)_z$, přičemž závorky lze v zápisu vynechat. Číslo z nazýváme základ číselné soustavy, symboly a_i , $i = 0, \ldots, n$ se nazývají číslice (cifry). O číslici a_i říkáme, že je řádu i, číslo z^i se nazývá jednotka řádu i pro $i = 0, \ldots, n$.

Poznámka 9. 5. Je-li $z > 10$, plyne z předchozí věty, že v soustavě o základu z musí existovat právě z různých cifer $0, 1, \ldots, z - 1$. Protože v běžně užívané desítkové soustavě máme k dispozici pouze deset cifer $0, \ldots, 9$, je nutno doplnit další symboly. Podle mezinárodní konvence se užívá $A = 10, B = 11, C = 12, D = 13, E = 14, F = 15$. Soustavy o základu větším než 16 se již nepoužívají, proto není potřeba zavádět další symboly.

Poznámka 9. 6. (Porovnávání čísel). V každé poziční číselné soustavě platí stejná pravidla pro porovnávání čísel jako v soustavě desítkové. Obsahuje-li zápis přirozeného čísla a v číselné soustavě o základu z právě n číslic (číslice nejvyššího řádu je nenulová), pak $z^{n-1} \leq a < z^n$. Jsou-li zapsána dvě přirozená čísla a, b v číselné soustavě o stejném základu (číslice nejvyššího řádu jsou nenulové), pak platí:
1. To číslo, v jehož zápisu je více číslic, je větší.
2. Mají-li zápisy obou čísel stejný počet číslic, pak je větší to číslo, v jehož zápisu číslice nejvyššího řádu označuje větší přirozené číslo.
3. Nechť dvě různá čísla a, b jsou zapsána v téže soustavě zápisem o stejném počtu číslic, tj. $(a_n a_{n-1} \ldots a_0)_z$, $(b_n b_{n-1} \ldots b_0)_z$. Existuje-li číslo k $(0 \leq k < n)$ s vlastností $a_i = b_i$ pro $i = n, n-1, \ldots, k+1, a_k \neq b_k$, pak větší je to číslo, v jehož zápise číslice řádu k označuje větší přirozené číslo.

Poznámka 9. 7. (Převádění zápisů přirozených čísel) Při převádění zápisu přirozeného čísla a z desítkové soustavy do číselné soustavy o základu z postupujeme tak, že číslo a vydělíme číslem z se zbytkem. V dalším kroku vezmeme neúplný podíl předchozího dělení a opět dělíme základem soustavy. Takto pokračujeme tak dlouho, dokud není neúplný podíl roven nule (po konečném počtu dělení tento případ musí nastat). Hledaný zápis čísla a v soustavě o základu z je určen všemi zbytky po všech provedených děleních, které napíšeme vedle sebe počínaje od posledního k prvnímu. Při praktickém převádění využíváme nejčastěji jednoduchou tabulku, kterou si ilustrujeme nejprve pro $a = 986, z = 4,$ pak pro $a = 2507, z =$

16. V tabulce o dvou sloupcích zapíšeme do záhlaví čísla *a, z*, do levého sloupce píšeme neúplné podíly a do pravého sloupce zbytky. Obrácený převod z nedesítkové do desítkové soustavy se provádí rozvojem v nedesítkové soustavě.

Příklad 9. 8.

986	*4*
246	*2*
61	*2*
15	*1*
3	*3*
0	*3*

$$986 = 33122_4 .$$

Zkouška: $3122_4 = 3 . 4^4 + 3 . 4^3 + 1 . 4^2 + 2 . 4 + 2 = 3 . 256 + 3 . 64 + 16 + 8 + 2 = 986.$

Příklad 9. 9.

2507	*16*
156	*11*
9	*12*
0	*9*

$$2057 = 9CB_{16} .$$

Zkouška: $9CB_{16} = 9 . 16^2 + 12 . 16 + 11 = 9 . 256 + 12 . 16 + 11 = 2304 + 192 + 11 = 2507.$
Povšimněme si, že v případě $z > 10$ přepisujeme dvouciferné zbytky pomocí písmen a opačně, při rozvoji čísla místi písmene použijeme příslušné dvouciferné číslo.

Poznámka 9. 10. Na základě poznámky 9.7. lze nyní převést zápis jakéhokoliv přirozeného čísla z desítkové soustavy do nedesítkové a naopak. V případě, že chceme převést zápis přirozeného čísla zapsaného v nedesítkové soustavě do jiné nedesítkové soustavy, je nejvýhodnější přechod přes desítkovou soustavu. Existují ovšem případy (a jsou hojně využívány zejména v informatice), kdy lze takový převod mezi dvěma nedesítkovými soustavami provést přímo. To lze provést tehdy, jestliže pro dva základy soustav z_1 , z_2 platí vztah $z_1 = z_2^n$ pro nějaké přirozené číslo n. S ohledem na praktické využití jsou důležité zejména přímé převody mezi soustavou dvojkovou a čtyřkovou, dvojkovou a osmičkovou, dvojkovou a šestnáctkovou, resp. mezi čtyřkovou a šestnáctkovou. Převody se provádí na základě následující věty:

Věta 9. 11. Nechť pro dva základy soustav z_1 , z_2 platí vztah $z_1 = z_2^n$ pro nějaké přirozené číslo n. Pak číslo zapsané n ciframi v číselné soustavě o základu z_2 lze zapsat jedinou cifrou v číselné soustavě o základu z_1 .

Příklad 9. 12. Převeďte číslo 110110010110_2 do soustavy se základem 8.
Víme, že $8 = 2^3$. Platí : $110101010110_2 = 1 . 2^{11} + 1 . 2^{10} + 0 . 2^9 + 1 . 2^8 + 0 . 2^7 + 1 . 2^6 + 0 . 2^5 + 1 . 2^4 + 0 . 2^3 + 1 . 2^2 + 1 . 2 + 0 = (1 . 2^2 + 1 . 2 + 0) . (2^3)^3 + (1 . 2^2 + 0 . 2 + 1) . (2^3)^2 + (0 . 2^2 + 1 . 2 + 0) . 2^3 + (1 . 2^2 + 1 . 2 + 0) = 6 . 8^3 + 5 . 8^2 + 2 . 8 + 6 = 6526_8$.

Poznámka 9. 13. Postup uvedený v předchozím příkladu je těžkopádný a nepřehledný. V praxi postupujeme tak, že při převodu zápisu přirozeného čísla ze základu z_2 na základ $z_1 =$

z_2^n zapíšeme dané číslo ve zkráceném tvaru v soustavě z_2, rozdělíme zprava na n-ciferné skupiny, přičemž každá taková skupina n cifer dá podle věty 9. 11. jednu cifru v soustavě z_1. Příklad 9.12. lze pak psát takto: $110110010110_2 = 110/110/010/110_2 = 6526_8$. Při opačném převodu postupujeme analogicky. Musíme si však uvědomit, že vždy vytváříme z každé cifry v soustavě z_1 skupinu n cifer v soustavě z_2, tedy např. $301_4 = 110001_2$, $301_8 = 011000001_2$, tzn. např. číslo nula je zapsáno v prvním případě dvěma nulami, zatímco ve druhém případě třemi nulami.

Poznámka 9.13. Pro počítání v nedesítkových soustavách platí stejná pravidla jako pro počítání v desítkové soustavě. Pravidla pro provádění písemného sčítání, odčítání, násobení a dělení v desítkové soustavě lze všechna „přenést“ i pro počítání v nedesítkové soustavě. Procvičení takových početních výkonů poznáte v semináři.

Poznámka 9.14. V závěru textu jsou jako přílohy dvě tabulky. První z nich obsahuje převody čísel od 0 do 40 do všech soustav od základu 2 až do základu 16, ve druhé tabulce jsou uvedeny převodní vztahy pro přímé převody mezi nedesítkovými soustavami v případech, kdy to je možné (až do základu 16).

6. Literatura

[1] DRÁBEK, JAROSLAV, a kol. *Základy elementární aritmetiky pro učitelství 1. stupně ZŠ*. 1. vyd. Praha: Státní pedagogické nakladatelství, 1985. 223 s., 14-521-85.

[2] VAŇUROVÁ, MILENA. *Aritmetika 2.* Elektronický učební kurz Pedagogické fakulty MU. Dostupné z elektronické adresy *https://moodlinka.ped.muni.cz/login/index.php*, citováno dne 14. 7. 2011.

Poziční číselné soustavy - počítání po jedné

Základ / Číslo	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	10	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	11	10	3	3	3	3	3	3	3	3	3	3	3	3	3
4	100	11	10	4	4	4	4	4	4	4	4	4	4	4	4
5	101	12	11	10	5	5	5	5	5	5	5	5	5	5	5
6	110	20	12	11	10	6	6	6	6	6	6	6	6	6	6
7	111	21	13	12	11	10	7	7	7	7	7	7	7	7	7
8	1000	22	20	13	12	11	10	8	8	8	8	8	8	8	8
9	1001	100	21	14	13	12	11	10	9	9	9	9	9	9	9
10	1010	101	22	20	14	13	12	11	10	A	A	A	A	A	A
11	1011	102	23	21	15	14	13	12	11	10	B	B	B	B	B
12	1100	110	30	22	20	15	14	13	12	11	10	C	C	C	C
13	1101	111	31	23	21	16	15	14	13	12	11	10	D	D	D
14	1110	112	32	24	22	20	16	15	14	13	12	11	10	E	E
15	1111	120	33	30	23	21	17	16	15	14	13	12	11	10	F
16	10000	121	100	31	24	22	20	17	16	15	14	13	12	11	10
17	10001	122	101	32	25	23	21	18	17	16	15	14	13	12	11
18	10010	200	102	33	30	24	22	20	18	17	16	15	14	13	12
19	10011	201	103	34	31	25	23	21	19	18	17	16	15	14	13
20	10100	202	110	40	32	26	24	22	20	19	18	17	16	15	14
21	10101	210	111	41	33	30	25	23	21	1A	19	18	17	16	15
22	10110	211	112	42	34	31	26	24	22	20	1A	19	18	17	16
23	10111	212	113	43	35	32	27	25	23	21	1B	1A	19	18	17
24	11000	220	120	44	40	33	30	26	24	22	20	1B	1A	19	18
25	11001	221	121	100	41	34	31	27	25	23	21	1C	1B	1A	19
26	11010	222	122	101	42	35	32	28	26	24	22	20	1C	1B	1A
27	11011	1000	123	102	43	36	33	30	27	25	23	21	1D	1C	1B
28	11100	1001	130	103	44	40	34	31	28	26	24	22	20	1D	1C
29	11101	1002	131	104	45	41	35	32	29	27	25	23	21	1E	1D
30	11110	1010	132	110	50	42	36	33	30	28	26	24	22	20	1E
31	11111	1011	133	111	51	43	37	34	31	29	27	25	23	21	1F
32	100000	1012	200	112	52	44	40	35	32	2A	28	26	24	22	20
33	100001	1020	201	113	53	45	41	36	33	30	29	27	25	23	21
34	100010	1021	202	114	54	46	42	37	34	31	2A	28	26	24	22
35	100011	1022	203	120	55	50	43	38	35	32	2B	29	27	25	23
36	100100	1100	210	121	100	51	44	40	36	33	30	2A	28	26	24
37	100101	1101	211	122	101	52	45	41	37	34	32	2B	29	27	25
38	100110	1102	212	123	102	53	46	42	38	35	32	2C	2A	28	26
39	100111	1110	213	124	103	54	47	43	39	36	33	30	2B	29	27
40	101000	1111	220	130	104	55	50	44	40	37	34	31	2C	2A	28

Přímé převody zápisů čísel

z = 2	z = 4
00	0
01	1
10	2
11	3

z = 2	z = 8
000	0
001	1
010	2
011	3
100	4
101	5
110	6
111	7

z = 2	z = 16
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

z = 4	z = 16
00	0
01	1
02	2
03	3
10	4
11	5
12	6
13	7
20	8
21	9
22	A
23	B
30	C
31	D
32	E
33	F

z = 3	z = 9
00	0
01	1
02	2
10	3
11	4
12	5
20	6
21	7
22	8