Přirozená čísla

Úmluva: Všude v dalším budeme mezi přirozená čísla počítat i číslo nula. Všude v této části se omezíme pouze na konečné množiny.

Poznámka. Existují tři možnosti zavedení přirozených čísel: jako čísla kardinální, čísla ordinální a prvky 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.

Přirozená čísla jako kardinální čísla konečných množin

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 $\mathscr{M}$ (označujeme ji $\sim$) je ekvivalencí v relačním smyslu

(zřejmě je reflexivní, symetrická a tranzitivní). Proto generuje jednoznačným způsobem rozklad na systému všech konečných množin $\mathscr{M}$. Třídy tohoto rozkladu se nazývají kardinální čísla. Kardinálním číslem konečné množiny M tedy rozumíme třídu ze systému $\mathscr{M}$, 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.

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

Varianta 2: Nechť A, B jsou konečné množiny. Pak definujeme $|A| < |B|$, právě když existuje prosté zobrazení **celé** množiny A **do** množiny B (nikoliv na celou množinu B).

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

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

Poznámka. Povšimněme si nyní omezující podmínky $A \cap B = \phi$ v předchozí definici. 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

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

Pokud jsou tedy množiny A, B disjunktní, pak $|A \cap B| = 0$ a předchozí rovnost přejde v definici sčítání kardinálních čísel podle definice.

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

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

Poznámka. Lze ukázat, že obě operace definované definicemi 1.24. a 1.25. mají všechny vlastnosti, které očekáváme od operací sčítání a násobení přirozených čísel.

Přirozená čísla jako ordinální čísla konečných množin

Poznamenejme úvodem, že teorie ordinálních čísel je ve své podstatě „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 (označujeme ji [M]). 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 **G** všech konečných dobře uspořádaných množin je definována relace podobnost ≈ (jde o analogii relace ekvivalence množin z teorie kardinálních čísel).

Dvě dobře uspořádané množiny [A], [B] jsou podobné, píšeme [A] ≈ [B], jestliže existuje podobné zobrazení f množiny [A] na množinu [B], pro které platí:

(1) f je vzájemně jednoznačné zobrazení množiny [A] na množinu [B], tedy $A \sim B$;
(2) zobrazení f zachovává uspořádání (mezi vzory a jejich obrazy).

Populárně lze konstatovat, že dvě konečné dobře uspořádané množiny jsou podobné, mají-li stejný počet prvků.
Relace podobnost ≈ je reflexivní, symetrická a tranzitivní, je to tedy rovněž relace ekvivalence. Lze tedy analogicky definovat rozklad **G** systému **G** určený ekvivalencí ≈ . Třídy rozkladu systému **G** se nazývají ordinální čísla. Ordinálním číslem konečné dobře uspořádané množiny [M] tedy rozumíme třídu ze systému **G**, která obsahuje množinu

[*M*] a všechny uspořádané množiny s ní podobné. Ordinální číslo uspořádané 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.

Poznámka: Další informace o ordinálních číslech uvedeme rovněž pouze populární formou. Jde o formálně složité formulace, přičemž ordinální čísla se v praxi na 1. stupni ZŠ používají jen velmi málo (sned jen u příkladů využívajících číselné osy).

Definice. Nechť [*M*] je uspořádaná množina, nechť $a \in [M]$. Pak úsek dobře uspořádané množiny [*M*] příslušný prvku *a* zapisujeme *U(a)* a definujeme jako dobře uspořádanou podmnožinu všech takových prvků množiny [*M*], které předchází v uspořádání před prvkem *a* v původním pořadí určeném v množině [*M*].

Poznámka. Populárně si lze představit úsek takto. Nechť uspořádaná množina [*M*] je reprezentována frontou osob stojící u pokladny v obchodě. Zvolíme-li libovolnou osobu

ve frontě, pak úsek příslušný této osobě je část fronty před tímto člověkem beze změny pořadí. Jakmile bude obsloužen tento úsek, je zvolená osoba na řadě. Je zřejmé, že úsek dobře uspořádané množiny [M] je vždy její vlastní podmnožinou.

Definice. (Porovnávání ordinálních čísel)
Varianta 1: Nechť [A], [B] jsou konečné dobře uspořádané množiny. Pak definujeme ord [A] < ord [B], právě když dobře uspořádaná množina [A] je podobná s některým úsekem dobře uspořádané množiny [B].

Varianta 2: Nechť A, B jsou konečné množiny. Pak definujeme ord [A] < ord [B], právě když existuje podobné zobrazení **celé** množiny [A] do množiny [B] (nikoliv na celou množinu B).

Definice. (Sčítání ordinálních čísel)
Nechť [A], [B] jsou konečné dobře uspořádané množiny, nechť platí $A \cap B = \phi$. Pak definujeme

$$\text{ord } [A] + \text{ord } [B] = \text{ord } [A \cup B] .$$

Definice. (Násobení ordinálních čísel)
Nechť [A], [B] jsou konečné dobře uspořádané množiny. Pak definujeme

$$\text{ord } [A] \cdot \text{ord } [B] = \text{ord } [A \times B] .$$

Poznámka. U definic sčítání i násobení ordinálních čísel je třeba určit také uspořádání v množinách [$A \cup B$], [$A \times B$]. Tato uspořádání uvedeme opět pouze populární formou.

Uspořádání v množině $[A \cup B]$ můžeme verbálně popsat pomocí tří podmínek:
1. Uspořádání prvků v množině $[A]$ zůstává beze změny.
2. Uspořádání prvků v množině $[B]$ zůstává beze změny.
3. Nejprve se do uspořádané množiny $[A \cup B]$ zařadí množina $[A]$, za ní pak množina $[B]$.

Příklad: Nechť $[A] = \lfloor\{a, b, c\}\rfloor$, $[B] = \lfloor\{u, v\}\rfloor$. Pak
$[A \cup B] = \lfloor\{a, b, c, u, v\}\rfloor$.

Uspořádání v množině $[A \times B]$ můžeme verbálně popsat pomocí následujících dvou podmínek. Připomeňme, že množina $A \times B$ obsahuje uspořádané dvojice.
Nechť $[a_1, b_1], [a_2, b_2] \in A \times B$ libovolně.
1. Je-li $b_1 < b_2$, pak $[a_1, b_1] < [a_2, b_2]$;
2. Je-li $b_1 = b_2$ a současně $a_1 < a_2$, pak $[a_1, b_1] < [a_2, b_2]$.

Rozhodující je tedy druhá složka, v případě její rovnosti pak rozhoduje první složka.Tomuto uspořádání se říká lexikografické, lidově též princip telefonního seznamu. Považujeme-li v telefonním seznamu dvojici „jméno, příjmení“ za uspořádanou dvojici, pak rozhodující je příjmení. V případě stejného příjmení pak rozhoduje křestní jméno, např.

Antonín Novák
Břetislav Novák
Cyril Novák
Čestmír Novák
Dušan Novák
Emil Novák
. . .
Xaver Novák
Zdeněk Novák

Příklad: $[A] = \lfloor\{a, b, c\}\rfloor$, $[B] = \lfloor\{u, v\}\rfloor$. Pak
$[A \times B] = \lfloor\{[a, u], [b, u], [c, u], [a, v], [b, v], [c, v]\}\rfloor$.

Peanova množina

Axiomy Peanovy množiny *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 $x^{\backslash}$.
(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) $(\forall\, x \in P)\ \ x \in M \Rightarrow x^{\backslash} \in M$, pak $M = P$.

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

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

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

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

Operace sčítání v množině P

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

(1) $x + e = x$ **,**

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

Věta 1.10. Operace $+$ je v množině P asociativní a komutativní a má neutrální prvek.

Operace násobení v množině P

Věta 1.11. Na množině P existuje právě jedna operace $\cdot$ (násobení) taková, že pro každou dvojici x, y prvků množiny P platí:

(1) $x \cdot e = e$ **,**

(2) $x \cdot y^{\backprime} = x \cdot y + x$.

Věta 1.12. Operace $\cdot$ je v množině P asociativní, komutativní, má neutrální prvek a s operací sčítání je svázána distributivním zákonem:

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

Věta 1.19. Algebraická struktura $(P, +, \cdot)$ je komutativní polookruh s neutrálním prvkem.

Poznámka 1.20. 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 1.11. se nikde v praxi nepoužívá.

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 výuce 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. 21. (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. 22. 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. 23. 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 $x = a : b$.

Poznámka 1. 24. Vlastnosti sčítání, násobení a porovnávání: :

Sčítání: ND, K, A, EN
Násobení: ND, K, A, EN $\cdot$ D +
Porovnávání: AR, AS, T, SO (ostré lineární uspořádání). Z vlastnosti SO plyne, že každá dvě přirozená čísla lze porovnat.

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

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

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.

Definice 2.2. Třídy rozkladu 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.
$\boldsymbol{[4, 2]} = \{[2, 0], [3, 1], [4, 2], [5, 3], [6, 4], \ldots\}$.
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 $\boldsymbol{[5, 3] = [6, 4]}$, protože obě tyto dvojice jsou reprezentanty téže třídy rozkladu systému $\boldsymbol{N \times N}$. Poznamenejme, že v dalším textu budeme pro zjednodušení označovat celá čísla velkými tučnými písmeny, např. $\boldsymbol{A, B, \ldots}$. Toto označení není v rozporu s uvedenou konstrukcí; vždy lze přejít k reprezentaci pomocí uspořádaných dvojic, např. $\boldsymbol{A = [a, b]}$, $\boldsymbol{B = [c, d]}$, ...

Operace s celými čísly a jejich vlastnosti

Definice 2.4. Sčítání na množině celých čísel je definováno předpisem

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

Věta 2.5. Operace + z předchozí definice je komutativní, asociativní, má neutrální prvek $\boldsymbol{0}$ reprezentovaný dvojicí $\boldsymbol{[n, n]}$

pro libovolné $n \in \boldsymbol{N}$ a ke každému celému číslu $\boldsymbol{A = [a, b]}$ existuje právě jedno opačné číslo $\boldsymbol{-A = [b, a]}$.

Věta 2.6. Algebraická struktura $\boldsymbol{(Z, +)}$ je komutativní grupa, ve které jsou řešitelné základní rovnice, tj rovnice $\boldsymbol{A + X = B}$ má vždy řešení v množině $\boldsymbol{Z}$ pro každá dvě celá čísla $\boldsymbol{A, B}$.

Věta 2.7. V grupě $\boldsymbol{(Z, +)}$ existuje právě jedna inverzní operace k operaci sčítání. Tato operace se nazývá odčítání a je definována vztahem $\boldsymbol{A - B = A + (-B)}$.

Poznámka 2.8. Z předchozí věty a věty 2.6. lze odvodit početní pravidlo pro operaci odčítání:

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

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

Definice 2.9. Na množině $\boldsymbol{Z}$ definujme binární operaci $\cdot$ následujícím způsobem:

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

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

Věta 2.10. Grupoid $\boldsymbol{(Z, \cdot)}$ je asociativní, komutativní a má neutrální prvek $\boldsymbol{1}$ reprezentovaný dvojicí $\boldsymbol{[n+1,n]}$ pro libovolné $n \in \boldsymbol{N}$.

Věta 2.11. V grupoidu $(\boldsymbol{Z}, \cdot)$ pro každá tři celá čísla x, y, z, $x \neq 0$ platí implikace

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

Věta 2.12. Operace násobení je v množině celých čísel svázána s operací sčítání distributivním zákonem, tj.

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

Věta 2.13. Algebraická struktura $(\boldsymbol{Z}, +, \cdot)$ je komutativní okruh s neutrálním prvkem, který není tělesem. V tomto okruhu neexistují vlastní dělitelé nuly, je to tedy obor integrity.

Poznámka 2.14. V oboru integrity všech celých čísel $(\boldsymbol{Z}, +, \cdot)$ platí řada tvrzení, běžně užívaných při výpočtech. Uveďme některé příklady.

Věta 2.15. Nechť $\boldsymbol{A, B, C \in Z}$. Pak platí:

(1) $\boldsymbol{-(-A) = A}$;

(2) $\boldsymbol{-(A + B) = (-A) + (-B)}$;

(3) $\boldsymbol{-(A - B) = B - A}$;

(4) $\boldsymbol{(A - (B - C) = (A + C) - B}$;

(5) $\boldsymbol{(-A) \cdot B = A \cdot (-B) = -(A \cdot B)}$.

Poznámka 2.16. 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 2.17. 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 2.18. 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.

Definice 2.19. Nechť $\boldsymbol{A, B}$ jsou celá čísla. Řekneme, že $\boldsymbol{A} < \boldsymbol{B}$, právě když platí $\boldsymbol{A} - \boldsymbol{B} < 0$. Je-li $\boldsymbol{A} - \boldsymbol{B} = 0$, pak $\boldsymbol{A} = \boldsymbol{B}$; ve zbývajícím případě pro $\boldsymbol{A} - \boldsymbol{B} > 0$ pak platí $\boldsymbol{A} > \boldsymbol{B}$.

Poznámka 2.20. Je zřejmé, že i v předchozí definici jeden z případů vždy musí nastat. Relace uspořádání všech celých čísel je tedy lineární.

Věta 2.21. Nechť $\boldsymbol{A}$ je celé číslo. Pak platí:
(1) $\boldsymbol{A} > 0 \Rightarrow -\boldsymbol{A} < 0$.
(2) $\boldsymbol{A} < 0 \Rightarrow -\boldsymbol{A} > 0$.

Věta 2.22. Nechť $\boldsymbol{A}$, $\boldsymbol{B}$ jsou kladná celá čísla. Potom jejich součet $\boldsymbol{A} + \boldsymbol{B}$ i součin $\boldsymbol{A} \cdot \boldsymbol{B}$ jsou také kladná celá čísla.

Poznámka 2.23. Výše definovaná relace uspořádání v množině všech celých čísel je spojena s operacemi v této množině řadou vztahů. Uveďme alespoň některé.

Věta 2.24. Nechť A, B, C, D jsou libovolná celá čísla. Pak platí:

(1) Jestliže $A > B$ a $C < 0$, potom $AC < BC$;
(2) Jestliže $A + C > B + C$, potom $A > B$;
(3) Jestliže $AC > BC$ a $C > 0$, potom $A > B$;
(4) Jestliže $AC > BC$ a $C < 0$, potom $A < B$;
(5) Jestliže $A > B$ a $C > D$, potom $A + C > B + D$;
(6) Jestliže $A > B$ a $C > D$ a $C > 0$ a $B > 0$, potom $A \cdot C > B \cdot D$.

Věta 2.25. Nechť A, B jsou libovolná celá čísla, přičemž $B \neq 0$. Pak existuje jednoznačně určená dvojice celých čísel Q, R (přičemž $0 \leq R < |B|$) s vlastností $A = B \cdot Q + R$. Číslo A se nazývá dělenec, číslo B dělitel, číslo Q je podíl (někdy též neúplný podíl) a číslo R je zbytek. Proces nalezení čísel Q, R se nazývá dělení se zbytkem v množině celých čísel.

Definice 2.26. Absolutní hodnotu $|A|$ celého čísla A definujeme takto:

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

Věta 2.27. 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 2.28. Vnoření $\psi : \boldsymbol{N} \to \boldsymbol{Z}$ grupoidu $\boldsymbol{N}$ do grupy $\boldsymbol{Z}$ je definováno pro každý prvek $n \in \boldsymbol{N}$ předpisem $\psi(n) = \{[n,0];\ n \in \boldsymbol{N}\}$. 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 $[0, n]$.

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 $\boldsymbol{C} \times \boldsymbol{C} - \boldsymbol{\{0\}}$, na kterém definujeme pro každé dvě dvojice $[a, b], [c, d] \in \boldsymbol{C} \times \boldsymbol{C} - \boldsymbol{\{0\}}$ 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 $\boldsymbol{C} \times \boldsymbol{C} - \boldsymbol{\{0\}}$ na třídy.

Definice 3.2. Třídy rozkladu kartézského součinu $\boldsymbol{C \times C - \{0\}}$ 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 $\boldsymbol{C \times C - \{0\}}$ 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 množiny M určeného ekvivalencí $\sim$, tedy třídami navzájem ekvivalentních zlomků. Vnoření $\psi : \boldsymbol{C} \to \boldsymbol{Q}$ okruhu $\boldsymbol{C}$ do tělesa $\boldsymbol{Q}$ je definováno pro každý prvek $z \in \boldsymbol{C}$ předpisem $\psi(z) = \frac{z}{1}$.

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. $\frac{\boldsymbol{3}}{\boldsymbol{4}} = \{\frac{3}{4}, \frac{6}{8}, \frac{3}{12}, \frac{-21}{-28}, \ldots\}$. Poznamenejme, že v dalším textu budeme pro zjednodušení označovat racionální čísla velkými tučnými písmeny, např. ***A, B,*** .... Toto označení není, tak jako u celých čísel, v rozporu s uvedenou konstrukcí;

vždy lze přejít k reprezentaci pomocí uspořádaných dvojic, např. $\boldsymbol{A} = \frac{a_1}{a_2}$, $\boldsymbol{B} = \frac{b_1}{b_2}$, ...

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 $(\boldsymbol{C}, +)$, není tedy nutné je na tomto místě znovu uvádět. Poznamenejme jen, že neutrálním prvkem je číslo $\boldsymbol{0}$ reprezentované třídou $\frac{0}{b}$ a opačným racionálním číslem k číslu $\frac{a}{b}$ je číslo $-\frac{a}{b}$, které lze reprezentovat buďto třídou $\frac{-a}{b}$ nebo třídou $\frac{a}{-b}$.

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

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

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 $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. Tato operace je

v množině $\boldsymbol{Q}$ komutativní, asociativní a má neutrální prvek. Tímto neutrálním prvkem je číslo $\boldsymbol{1}$ reprezentované třídou zlomků $\frac{a}{a}$. 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 $\boldsymbol{A, B, C} \in \boldsymbol{Q}$. Pak platí:

(1) $(\boldsymbol{A}^{-1})^{-1} = \boldsymbol{A}$;

(2) $(\boldsymbol{A} \cdot \boldsymbol{B})^{-1} = \boldsymbol{A}^{-1} \cdot \boldsymbol{B}^{-1}$;

(3) $(\boldsymbol{A} \cdot \boldsymbol{B}^{-1})^{-1} = \boldsymbol{B} \cdot \boldsymbol{A}^{-1}$;

(4) $(\boldsymbol{A} \cdot \boldsymbol{B}^{-1}) \cdot \boldsymbol{C}^{-1} = \boldsymbol{A} \cdot (\boldsymbol{B} \cdot \boldsymbol{C})^{-1}$;

(5) $\boldsymbol{A} \cdot (\boldsymbol{B} \cdot \boldsymbol{C}^{-1})^{-1} = (\boldsymbol{A} \cdot \boldsymbol{C}) \cdot \boldsymbol{B}^{-1}$.

Relace uspořádání v množině racionálních čísel

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

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

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.

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. Platí 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.

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

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

Desetinné rozvoje racionálních čísel

Věta 3.25. 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.