Věta 7. (Algoritmus násobení *víceciferných čísel v poziční soustavě.*) *Nechť*

$$x = (a_n a_{n-1} \dots a_1 a_0)_z, \quad y = (b_m b_{m-1} \dots b_1 b_0)_z .$$

Potom

$$x \,.\, y = x \,.\, (b_0)_z + x(b_1 0)_z + x(b_2 00)_z + \dots + x(b_m \underbrace{000\,.\,.0}_{m\text{-nul}})_z .$$

Důkaz. Protože zřejmě

$$y = (b_m 00 \dots 0)_z + \dots + (b_2 00)_z + (b_1 0)_z + (b_0)_z ,$$

plyne věta z distributivnosti násobení vzhledem ke sčítání.

Příklad 8. a) Obzvláště jednoduchý je algoritmus ve dvojkové soustavě, protože dílčí kroky pozůstávají pouze z násobení číslem 1.

$$\begin{array}{r}
(10110)_2 \\
\cdot\quad (1011)_2 \\
\hline
10110 \\
10110 \\
10110 \\
\hline
(11110010)_2
\end{array}$$

b) Uvedeme ještě ukázku z pětkové soustavy. Při násobení využíváme pětkové násobilky (tab. 31) a při sčítání pětkové sčitalky (tab. 28).

$$\begin{array}{rcr}
(2143)_5 & \rightarrow & (298)_{10} \\
\cdot\quad (203)_5 & \rightarrow & \cdot\quad (53)_{10} \\
\cline{1-1}\cline{3-3}
(12034) & & \\
4341 & & \\
\cline{1-1}\cline{3-3}
(1001134)_5 & \rightarrow & (15794)_{10}
\end{array}$$

KAPITOLA VII

ČÍSLA CELÁ A RACIONÁLNÍ

§ 1. Celá čísla

V kapitole V jsme ukázali, jak je možno vytvořit strukturu $(\mathbf{N}, +, \cdot, <)$, která odpovídá naší představě o přirozených číslech. V tomto paragrafu sestrojíme – vycházejíce ze struktury přirozených čísel – novou strukturu, odpovídající naší představě čísel celých. Označíme ji už předběžně $(\mathbf{Z}, +, \cdot, <)$, neboť se pochopitelně budeme zajímat o vlastnosti sčítání, násobení a uspořádání celých čísel.

Nejprve se však zaměříme pouze na operaci sčítání.

Víme, že struktura $(\mathbf{N}, +)$ je komutativní pologrupa, zatímco $(\mathbf{Z}, +)$ by měla být (podle naší představy celých čísel) grupa.

Dále víme, že ve struktuře $(\mathbf{N}, +)$ platí: jestliže k prvkům $x, y \in \mathbf{N}$ existuje $z \in \mathbf{N}$ tak, že $x = y + z$, existuje takové z právě jedno. Lze tedy v $\mathbf{N}$ definovat operaci, jež každé uspořádané dvojici (x, y) přiřadí právě zmíněný prvek z (pokud existuje). Tuto operaci je obvyklé nazývat rozdíl a značit ji „–", takže píšeme $z = x - y$. Operace „–" je zřejmě pouze parciální operací v $\mathbf{N}$, zatímco v $\mathbf{Z}$ by mělo být odčítání operací úplnou.

Tím získáváme dva náměty na „zlepšení" vlastností struktury $(\mathbf{N}, +)$. Avšak užitím znalostí z kap. II, §3 a §4 snadno nahlédneme, že jde v podstatě o totéž; jestliže vytvořená struktura bude grupa, bude v ní odčítání automaticky úplnou operací (stačí pro libovolné její prvky x, y položit $x - y = x + (-y)$, kde $-y$ je prvek opačný k y) a naopak, podaří-li se nám sestrojit strukturu, v níž operace „–" bude úplná, bude to současně struktura s opačnými prvky, a tedy grupa (k libovolnému jejímu prvku x je pak prvek $0 - x$ opačným prvkem).

K vytvoření struktury $(\mathbf{Z}, +)$ užijeme metody, jejíž původní myšlenka pochází od německého matematika L. Kroneckera (1823–1891). Budeme postupovat tak, že „připojíme" k $\mathbf{N}$ všechny ty rozdíly dvou přirozených čísel, které do $\mathbf{N}$ nepatří a rozšíříme operaci sčítání na celou takto vzniklou množinu.

Protože vlastní postup, kterým ze struktury $(\mathbf{N}, +)$ vytvoříme strukturu $(\mathbf{Z}, +)$ je komplikovanější, a protože později tohoto postupu ještě použijeme, zavedeme pro něj označení konstrukce (K) a v přehledu vyznačíme jednotlivé její kroky.

Konstrukce (K) *provedená na strukturu* $(\mathbf{N}, +)$ – konstrukce struktury $(\mathbf{Z}, +)$.

(A) Sestrojení množiny $\mathbf{Z}$.

(a) Definice vhodné relace v množině $\mathbf{N} \times \mathbf{N}$.

(b) Relace z (a) je ekvivalencí v $\mathbf{N} \times \mathbf{N}$.

(c) Množina $\mathbf{Z}$ je rozklad $\mathbf{N} \times \mathbf{N}$ podle této ekvivalence.

(B) Vytvoření struktury $(\mathbf{Z}, +)$ a ověření požadovaných vlastností.

(a) Definice operace $+$ v množině $\mathbf{Z}$.

(b) $(\mathbf{Z}, +)$ je komutativní grupa.

(c) Souvislost mezi strukturami $(\mathbf{N}, +)$ a $(\mathbf{Z}, +)$.

(d) Ztotožnění struktury $(\mathbf{N}, +)$ s izomorfní podstrukturou $(\mathbf{Z}_0, +)$ v $(\mathbf{Z}, +)$.

Nyní konkrétně provedeme jednotlivé body uvedeného postupu.

(A) *Vytvoření množiny* $\mathbf{Z}$.

(a) Sestrojíme množinu $\mathbf{N} \times \mathbf{N}$ všech uspořádaných dvojic přirozených čísel a na ní definujeme relaci $\approx$ tímto způsobem:

(1) $$(\forall x, y, x', y' \in \mathbf{N})\,(x, y) \approx (x', y') \Leftrightarrow x + y' = x' + y.$$

Povšimněte si, že formule $x + y' = x' + y$ nebyla v (1) zvolena náhodně, nýbrž proto, že popisuje (a to způsobem vyjádřitelným v $(\mathbf{N}, +)$) skutečnost, že dvojice (x, y) a (x', y') určují týž rozdíl.

(b) Snadno ověříme, že relace $\approx$ je ekvivalencí v množině $\mathbf{N} \times \mathbf{N}$. Její reflexívnost a symetričnost je zřejmá. Předpokládejme, že pro libovolně zvolená přirozená čísla x, y, x', y', x'', y'' platí

$$(x, y) \approx (x', y') \wedge (x', y') \approx (x'', y'').$$

Pak podle (1) je $x + y' = x' + y$ a zároveň $x' + y'' = x'' + y'$. Přičteme-li k první rovnosti y'' a k druhé y, dostaneme

$$x + y' + y'' = x' + y + y'' \wedge x' + y'' + y = x'' + y' + y,$$

odkud díky komutativnosti sčítání v $\mathbf{N}$ (viz kap. I, věta 1d)) plyne $x + y' + y'' = x'' + y' + y$. Užitím tvrzení e) téže věty obdržíme $x + y'' = x'' + y$, neboli $(x, y) \approx (x'', y'')$, čímž je ověřena i tranzitivnost relace $\approx$ v $\mathbf{N} \times \mathbf{N}$.

(c) Ekvivalence $\approx$ indukuje rozklad množiny $\mathbf{N} \times \mathbf{N}$ (viz kap. II, §2); tento rozklad označíme symbolem $\mathbf{Z}$, tedy

(2) $$\mathbf{Z} = (\mathbf{N} \times \mathbf{N})/\approx.$$

Prvky množiny $\mathbf{Z}$ jsou podmnožiny v $\mathbf{N} \times \mathbf{N}$, které budeme nazývat třídy rozkladu $\mathbf{Z}$ a označovat $T(x, y)$, přičemž pro každé $x, y \in \mathbf{N}$ je

(3) $$T(x, y) = \square \approx (x, y) = \{(u, v) \in \mathbf{N} \times \mathbf{N}; (u, v) \approx (x, y)\}.$$

Tedy třída $T(x, y)$ rozkladu $\mathbf{Z}$ se skládá – jak vyplývá z definice relace – právě ze všech těch uspořádaných dvojic přirozených čísel, jež určují týž rozdíl jako dvojice (x, y); dvojici (x, y) budeme nazývat reprezentantem třídy $T(x, y)$.

Je důležité si uvědomit, že táž třída rozkladu (2) může mít různé uspořádané dvojice za své reprezentanty. Z (3) a vlastností relace $\approx$ lze snadno nahlédnout, že platí (pro zjednodušení zde vynecháme obecné kvantifikátory, což budeme často činit i v dalším textu)

(4) $$T(x, y) = T(x', y') \Leftrightarrow (x, y) \approx (x', y').$$

Protože například $T(2, 6) = T(4, 8) = T(1, 5) = T(0, 4)$, má třída $T(2, 6)$ za své reprezentanty též dvojice $(4, 8)$, $(1, 5)$ atd., obecně každou dvojici (x', y') z $\mathbf{N} \times \mathbf{N}$, pro niž platí $(2, 6) \approx (x', y')$.

(B) *Vytvoření struktury* $(\mathbf{Z}, +)$ *a ověření požadovaných vlastností.*

(a) Na množině $\mathbf{Z}$ zavedeme sčítání (v souladu s tím, že třída $T(x, y)$ charakterizuje rozdíl čísel x a y) tímto způsobem:

(5) $$T(x, y) + T(u, v) = T(x + u, y + v).$$

K tomu, abychom ověřili, že formule (5) skutečně definuje operaci v množině $\mathbf{Z}$, je třeba ukázat, že pro každou volbu $x, y, u, v \in \mathbf{N}$ výsledná třída $T(x + u, y + v)$ jednak patří do $\mathbf{Z}$, jednak nezávisí na volbě reprezentantů (x, y) a (u, v), nýbrž pouze na třídách $T(x, y)$ a $T(u, v)$. První požadavek zřejmě platí. Druhý – dříve než si jej dokážeme – zformulujeme přesněji ve tvaru

$$(T(x, y) = T(x', y') \wedge T(u, v) = T(u', v')) \Rightarrow$$
$$\Rightarrow T(x + u, y + v) = T(x' + u', y' + v').$$

Nechť tedy jsou splněny předpoklady našeho tvrzení, pak podle (4) platí

$$(x, y) \approx (x', y') \wedge (u, v) \approx (u', v'),$$

odkud užitím (1) dostáváme

$$x + y' = x' + y \wedge u + v' = u' + v$$

a sečtením obou rovností získáme

$$(x + u) + (y' + v') = (y + v) + (x' + u').$$

Podle (1) je tedy

$$(x + u, y + v) \approx (x' + u', y' + v'),$$

odkud podle (4) vyplývá hledaná rovnost

$$T(x + u, y + v) = T(x' + u', y' + v').$$

Tedy „+“ je skutečně operací v $\mathbf{Z}$, takže $(\mathbf{Z}, +)$ je algebraická struktura.

(b) O této struktuře dokážeme následující větu:

Věta 1. *Struktura* $(\mathbf{Z}, +)$ *je komutativní grupa.*

Důkaz. Komutativnost a asociativnost struktury $(\mathbf{Z}, +)$ vyplývá z týchž vlastností struktury $(\mathbf{N}, +)$.

Nulovým prvkem struktury $(\mathbf{Z}, +)$ je zřejmě třída $T(0,0)$ (a samozřejmě také všechny jí rovné třídy, např. $T(1, 1)$, $T(3, 3)$, $T(9, 9)$ atd.).

Zbývá dokázat, že $(\mathbf{Z}, +)$ je struktura s opačnými prvky. Nechť tedy $T(x, y)$ je libovolný prvek ze $\mathbf{Z}$ a předpokládejme, že $T(\bar{x}, \bar{y})$ je prvek k němu opačný, tj.

$$T(x, y) + T(\bar{x}, \bar{y}) = T(0, 0).$$

Odtud užitím (5), (4) a (1) dostáváme vztah

$$x + \bar{x} = y + \bar{y}.$$

Chápeme-li tuto rovnost jako soustavu lineárních rovnic o neznámých $\bar{x}$ a $\bar{y}$, snadno nahlédneme, že jedním jejím řešením je dvojice přirozených čísel $\bar{x} = y$, $\bar{y} = x$. Tedy opačným prvkem k třídě $T(x, y)$ je třída $T(y, x)$ čili

$$(6) \qquad -T(x, y) = T(y, x).$$

Tím jsme vytvořili, a to pouze užitím vlastností přirozených čísel, strukturu $(\mathbf{Z}, +)$, která je grupou, a tudíž jsme splnili alespoň část úkolu, který jsme si v úvodu tohoto paragrafu vytkli. Požadovali jsme však také, aby množina $\mathbf{Z}$ vznikla doplněním množiny $\mathbf{N}$ o vhodné prvky, tj., aby platilo $\mathbf{N} \subseteq \mathbf{Z}$. Je však na první pohled zřejmé, že žádné přirozené číslo není třídou uspořádaných dvojic prvků z $\mathbf{N}$, a tedy není prvkem $\mathbf{Z}$, takže požadavek $\mathbf{N} \subseteq \mathbf{Z}$ není splněn. O tom, jak si poradit s tímto zdánlivě neřešitelným problémem, si řekneme v následujícím odstavci.

(c) Souvislost struktury $(\mathbf{N}, +)$ a $(\mathbf{Z}, +)$.

Základem našich úvah bude tato věta:

Věta 2. *V* $(\mathbf{Z}, +)$ *existuje podstruktura* $(\mathbf{Z}_0, +)$ *izomorfní s* $(\mathbf{N}, +)$.

Důkaz. Existenci struktury $(\mathbf{Z}_0, +)$ dokážeme tím, že ji zkonstruujeme. Za $\mathbf{Z}_0$ vezmeme množinu všech těch tříd $T(x, y) \in \mathbf{Z}$, do nichž patří dvojice tvaru $(z, 0)$, neboli

$$\mathbf{Z}_0 = \{T(z, 0);\ z \in \mathbf{N}\}.$$

Z množiny $\mathbf{Z}_0$ vytvoříme strukturu $(\mathbf{Z}_0, +)$ tak, že v ní definujeme operaci $+$ předpisem (5), tj. vlastně týmž způsobem jako v $\mathbf{Z}$, takže $(\mathbf{Z}_0, +)$ je podstrukturou struktury $(\mathbf{Z}, +)$.

K tomu, abychom dokázali, že $(\mathbf{N}, +)$ je izomorfní s $(\mathbf{Z}_0, +)$ musíme ověřit

(viz kap. II, § 4), že existuje vzájemně jednoznačné zobrazení φ množiny $\mathbf{N}$ na množinu $\mathbf{Z}_0$, které má vlastnost

$$(7) \qquad (\forall x, y \in \mathbf{N})\ \varphi(x + y) = \varphi(x) + \varphi(y).$$

Zobrazení φ definujme tímto předpisem:

$$(8) \qquad (\forall x \in \mathbf{N})\ \varphi(x) = T(x, 0).$$

Je ihned zřejmé, že φ je zobrazení $\mathbf{N}$ na $\mathbf{Z}_0$. Sporem ukážeme, že je zobrazením prostým. Nechť tedy $x, y \in \mathbf{N}$, $x \neq y$ a nechť $\varphi(x) = T(x, 0) = \varphi(y) = T(y, 0)$. Pak podle (4) musí platit $(x, 0) \approx (y, 0)$, a tedy podle (1) $x = y$, což je ve sporu s předpokladem $x \neq y$. Tedy musí být $T(x, 0) \neq T(y, 0)$, a tudíž φ je prosté. Zbývá ověřit platnost formule (7). Nechť x, y jsou libovolná přirozená čísla, pak postupně užitím (8), (5) a znovu (8) odvodíme

$$\varphi(x + y) = T(x + y, 0) = T(x + y, 0 + 0) =$$
$$= T(x, 0) + T(y, 0) = \varphi(x) + \varphi(y),$$

takže věta 2 je kompletně dokázána.

(d) Izomorfní struktury $(\mathbf{N}, +)$ a $(\mathbf{Z}_0, +)$ ztotožníme:

Libovolné přirozené číslo x a třídu $T(x, 0) \in \mathbf{Z}_0$, jež mu odpovídá v izomorfismu (8) budeme považovat za totožné, tj. položíme

$$(9) \qquad (\forall x \in \mathbf{N})\ x = T(x, 0).$$

Přijetím této úmluvy jsme docílili toho, že $\mathbf{N} \subseteq \mathbf{Z}$, a tedy náš úkol o vhodném rozšíření struktury $(\mathbf{N}, +)$ můžeme považovat za splněný.

Je však ještě zajímavé prozkoumat, jaké důsledky má přijetí úmluvy (9) nejen pro množinu $\mathbf{Z}_0$, ale pro celou množinu $\mathbf{Z}$. Jako východisko k vyšetření této otázky nám poslouží následující věta.

Věta 3. *Pro každou třídu* $T(x, y) \in \mathbf{Z}$ *lze nalézt právě jedno přirozené číslo* z *tak, že buď* $T(x, y) = T(z, 0)$, *nebo* $T(x, y) = T(0, z)$; *čili zapsáno formulí*

$$(\forall T(x, y) \in \mathbf{Z})\,(\exists! z \in \mathbf{N})\ T(x, y) = T(z, 0) \vee T(x, y) = T(0, z).$$

Důkaz. Nechť $T(x, y)$ je libovolná třída z množiny $\mathbf{Z}$. Poněvadž $x, y \in \mathbf{N}$, nastane pro ně podle věty 3g) z kap. V právě jedna z možností $x < y$, $x = y$, $y < x$. Jestliže $x = y$, je $T(x, y) = T(0, 0)$ a tvrzení věty je splněno (pro $z = 0$). Jestliže $x < y$, existuje podle definice relace $<$ prvek $z \in \mathbf{N}$ tak, že $x + z = y$, a tedy

$$T(x, y) = T(x, x + z) = T(x + 0, x + z) =$$
$$= T(x, x) + T(0, z) = T(0, 0) + T(0, z) = T(0, z).$$

V případě $y < x$ analogicky ověříme, že platí $T(x, y) = T(z, 0)$, kde je $z \in \mathbf{N}$ takové, že $x = y + z$. Jednoznačnost určení prvku z plyne z vlastnosti krácení ve struktuře $(\mathbf{N}, +)$.

Právě dokázané věty využijeme k rozšíření úmluvy (9) na celou množinu $\mathbf{Z}$. Nechť $T(x, y)$ je libovolná třída ze $\mathbf{Z}$, pak podle věty 3 buď

a) existuje $z \in \mathbf{N}$ takové, že $T(x, y) = T(z, 0)$; potom $T(x, y) \in \mathbf{Z}_0$ a podle (9) ji můžeme považovat za přirozené číslo z, tj. $T(x, y) = z$, nebo

b) existuje $z \in \mathbf{N}$ takové, že $T(x, y) = T(0, z)$; potom podle (6) je $T(x, y) = -T(z, 0)$, takže úmluva (9) nám dává možnost psát $T(x, y) = -z$.

Je tedy vidět, že pro označování prvků z množiny $\mathbf{Z}$ není třeba vymýšlet nějaký nový způsob, že plně vystačíme se značením zavedeným pro přirozená čísla: pro prvky ze $\mathbf{Z}_0$ užijeme téhož symbolu jako pro příslušné přirozené číslo a pro prvky ze $\mathbf{Z} - \mathbf{Z}_0$ před tento symbol připojíme znak „$-$".

Množinu $\mathbf{Z}$ nazveme – jak je obvyklé – množinou (všech) celých čísel a její prvky celá čísla. Grupa $(\mathbf{Z}, +)$ se nazývá aditivní grupa celých čísel.

Věta 3 nám umožňuje rozdělit celá čísla do tří skupin: Celá čísla $T(x, y)$, k nimž existuje nenulové přirozené číslo z tak, že $T(x, y) = T(z, 0) = z$, se nazývají kladná celá čísla a množinu všech těchto čísel označíme $\mathbf{Z}^+$, tedy

$$\mathbf{Z}^+ = \{T(z, 0) \in \mathbf{Z};\, z \in \mathbf{N} \wedge z \neq 0\}.$$

Každé $T(x, y) \in \mathbf{Z}$, k němuž existuje nenulové $z \in \mathbf{N}$ tak, že $T(x, y) = T(0, z) = -z$, se nazývá záporné celé číslo, přičemž označíme

$$\mathbf{Z}^- = \{T(0, z) \in \mathbf{Z};\, z \in \mathbf{N} \wedge z \neq 0\}.$$

Je zřejmé, že existuje jediné celé číslo $T(x, y)$, které není kladné, ani záporné, totiž číslo $T(x, y) = T(0, 0) = 0$.

Dalším snadným důsledkem věty 3 je skutečnost, že systém $\{\mathbf{Z}^+, \mathbf{Z}^-, \{0\}\}$ je rozkladem množiny $\mathbf{Z}$ (na disjunktní množiny). Tedy pro každé celé číslo z nastane právě jedna z možností: buď a) z je kladné ($z \in \mathbf{Z}^+$), nebo b) z je záporné ($z \in \mathbf{Z}^-$), nebo c) $z = 0$.

Z (6) ihned plyne, že opačný prvek k zápornému číslu (celému) je číslo kladné a opačný prvek ke kladnému číslu je číslo záporné, tj.

(10) $\qquad (\forall x \in \mathbf{Z}^-)\, -x \in \mathbf{Z}^+ \wedge (\forall x \in \mathbf{Z}^+)\, -x \in \mathbf{Z}^-.$

Z toho, že $(\mathbf{Z}, +)$ je komutativní grupa, plyne, že pro počítání s celými čísly můžeme pochopitelně užívat všech výsledků, jež jsme již dříve pro komutativní grupy odvodili. Uveďme z nich alespoň dva, jež budeme dále nejčastěji potřebovat.

(11) $\qquad (\forall x \in \mathbf{Z})\, -(-x) = x$

(12) $\qquad (\forall x, y \in \mathbf{Z})\, -(x + y) = (-x) + (-y)$

Z definice (5) sčítání v $\mathbf{Z}$ a z definice množin $\mathbf{Z}^+$ a $\mathbf{Z}^-$ ihned plynou tyto dvě vlastnosti:

(13a) $\qquad (\forall x, y \in \mathbf{Z}^+)\, x + y \in \mathbf{Z}^+,$

(13b) $\qquad (\forall x, y \in \mathbf{Z}^-)\, x + y \in \mathbf{Z}^-.$

Struktura $(\mathbf{Z}, +, \cdot)$. Na množině přirozených čísel máme vedle operace sčítání definováno též násobení. Proto se pokusíme i na množině $\mathbf{Z}$ definovat součin (označíme ho prozatím $\odot$), a to tak, aby $(\mathbf{N}, +, \cdot)$ byla podstrukturou struktury $(\mathbf{Z}, +, \odot)$. Operaci $\odot$ definujeme pomocí operace násobení v $\mathbf{N}$ tímto způsobem:

Definice. *Pro libovolná čísla $x, y \in \mathbf{Z}$ definujeme*

(14)
1. $x \odot y = x \cdot y$ *pro* $x, y \in \mathbf{N}$
2. $x \odot y = (-x) \cdot (-y)$ *pro* $x, y \in \mathbf{Z}^-$
3. $x \odot y = -(x \cdot (-y))$ *pro* $x \in \mathbf{N}$ *a* $y \in \mathbf{Z}^-$
4. $x \odot y = -((-x) \cdot y)$ *pro* $x \in \mathbf{Z}^-$ *a* $y \in \mathbf{N}$

Připomeňme výslovně, že právě zformulovaná definice je korektní. Jednak uvedené čtyři případy zahrnují skutečně všechny možnosti, jež pro celá čísla x, y mohou nastat, neboť množiny $\mathbf{N}$ a $\mathbf{Z}^-$ tvoří rozklad množiny $\mathbf{Z}$ na disjunktní třídy, jednak všechny výrazy na pravých stranách rovností v (14) jsou definovány, jak plyne z (10). Např. v bodě 2 $-x \in \mathbf{N}$ a $-y \in \mathbf{N}$, takže $(-x) \cdot (-y)$ je skutečně součin přirozených čísel.

Z definice (14) dále ihned plyne, že $(\mathbf{N}, +, \cdot)$ je podstruktura struktury $(\mathbf{Z}, +, \odot)$, neboť pro prvky z $\mathbf{N}$ se stačí omezit na bod 1 této definice a v tomto případě je operace „$\odot$" totožná s „$\cdot$".

Je užitečné uvědomit si ještě tento bezprostřední důsledek definice (14): pro libovolná celá čísla x, y součin

(15a) $\qquad x \odot y \in \mathbf{N}$, právě když obě čísla x, y patří do téže z množin $\mathbf{N}, \mathbf{Z}^-$,

(15b) $\qquad x \odot y \in \mathbf{Z}^-$, právě když čísla x, y nejsou prvky téže z množin $\mathbf{N}, \mathbf{Z}^-$.

Nejdůležitější vlastnosti operace $\odot$ shrneme do věty.

Věta 4. $(\mathbf{Z}, \odot)$ *je komutativní pologrupa s jednotkovým prvkem, v níž lze krátit každým nenulovým prvkem.*

Důkaz. Dokážeme jako ukázku práce s definicí (14) pouze komutativnost struktury $(\mathbf{Z}, \odot)$, důkazy zbývajících tvrzení věty přenecháváme čtenáři (viz cvičení 2).

Zvolme libovolně $x, y \in \mathbf{Z}$. Podle definice (14) musíme rozlišovat čtyři případy.

1. Jestliže $x \in \mathbf{N}$ a $y \in \mathbf{N}$, je naše tvrzení totožné s větou 2e) z kap. V.

2. Jestliže $x \in \mathbf{Z}^-$, $y \in \mathbf{Z}^-$, je podle bodu 2 z (14) $x \odot y = (-x)(-y)$, a tento

součin přirozených čísel je podle citované již věty 2e) roven $(-y)(-x)$, což opět podle bodu 2 z (14) dá $y \odot x$.

3. Jestliže $x \in \mathbf{N}$, $y \in \mathbf{Z}^-$, obdržíme postupně užitím bodu 3 z (14), věty 2e) z kap. V a bodu 4 z (14) tento výsledek:

$$x \odot y = -(x(-y)) = -((-y)x) = y \odot x.$$

4. Případ $x \in \mathbf{Z}^-$, $y \in \mathbf{N}$ je obdobný:

$$x \odot y = -((-x).y) = -(y.(-x)) = y \odot x.$$

Přejdeme nyní k vyšetřování vlastností struktury $(\mathbf{Z}, +, \odot)$. Při formulaci příslušných vět už budeme – jak je obvyklé – užívat pro operaci $\odot$ multiplikativního zápisu.

Věta 5. *Struktura* $(\mathbf{Z}, +, \cdot)$ *je (komutativní) obor integrity, který není těleso.*

Důkaz. K tomu, abychom dokázali, že $(\mathbf{Z}, +, \cdot)$ je okruh s jednotkovým prvkem, a s krácením nenulovými prvky, stačí díky větám 1 a 4 ověřit již jen $(+, \cdot)$-distributivnost. Při jejím důkazu budeme pro zamezení nejasnostem pro násobení v $\mathbf{Z}$ užívat ještě symbolu $\odot$. Máme tedy ověřit platnost formule

$$(\forall x, y, z \in \mathbf{Z})(x + y) \odot z = (x \odot z) + (y \odot z).$$

Vyšetříme jako ukázku pouze složitější případ $x \in \mathbf{N}$, $y, z \in \mathbf{Z}^-$ a ostatních 7 případů přenecháme čtenáři (viz cvičení 3).

Zvolme tedy libovolně $x \in \mathbf{N}$, $y, z \in \mathbf{Z}^-$ a předpokládejme, že (pro přirozená čísla) $x, -y$ platí

a) $-y \leqq x$. Pak podle definice $\leqq$ existuje $u \in \mathbf{N}$ tak, že $-y + u = x$, a tedy $u = x + y \in \mathbf{N}$. Potom podle bodu 3 z definice (14)

$$(x + y) \odot z = u \odot z = -(u(-z)).$$

Postupně podle (14), věty 2a) z kap. V a (12) obdržíme

$$\begin{aligned}(x \odot z) + (y \odot z) &= -(x(-z)) + (-y)(-z) = \\ &= -((-y + u)(-z)) + (-y)(-z) = -((-y)(-z) + u(-z)) + \\ &+ (-y)(-z) = -((-y)(-z) + (-(u(-z))) + (-y)(-z) = \\ &= -(u(-z)).\end{aligned}$$

Tedy v tomto případě dokazované tvrzení platí.

b) $x \leqq -y$. Pak existuje $v \in \mathbf{N}$ tak, že $x + v = -y$, a tedy $x + y = -v \in \mathbf{Z}^-$. Potom podle definice (14) a podle (11) je

$$(x + y) \odot z = (-(x + y))(-z) = v(-z).$$

Obdobně jako v případě a) získáme

$$\begin{aligned}(x \odot z) + (y \odot z) &= -(x(-z)) + (-y)(-z) = \\ &= -(x(-z)) + (x + v)(-z) = \\ &= -(x(-z)) + x(-z) + v(-z) = v(-z),\end{aligned}$$

čímž je i v tomto případě distributivnost dokázána.

Tedy $(\mathbf{Z}, +, \cdot)$ je okruh s krácením nenulovými prvky, a protože v okruhu lze krátit právě těmi (nenulovými) prvky, jež nejsou děliteli nuly (viz § 4, kap. II), je $(\mathbf{Z}, +, \cdot)$ obor integrity.

Zbývá dokázat, že $(\mathbf{Z}, +, \cdot)$ není tělesem, neboli že existuje alespoň jedno nenulové celé číslo, k němuž nelze v $\mathbf{Z}$ nalézt prvek inverzní; tedy že platí

$$(\exists x \in \mathbf{Z})(x \neq 0 \wedge (\forall y \in \mathbf{Z})\, xy \neq 1).$$

Položme $x = 2$ a předpokládejme, že existuje $y \in \mathbf{Z}$ tak, že platí $2.y = 1$. Kdyby $y \in \mathbf{Z}^-$, bylo by $2.y \in \mathbf{Z}^-$ neboli $1 \in \mathbf{Z}^-$, což neplatí. Tedy musí být $y \in \mathbf{N}$ a přitom $y \neq 0$ (jinak by podle věty 2c), kap. V bylo $2y = 0$), takže existuje $z \in \mathbf{N}$ takové, že $z' = y$. Tedy

$$2y = 2z' = 2(z + 1) = 2 + 2z = 1.$$

Protože $2z \in \mathbf{N}$, znamená poslední rovnost $2 \leqq 1$, takže dostáváme spor i v tomto případě, a tedy uvažované celé číslo y nemůže existovat. Tím je věta 5 dokázána.

Obsah věty 5 je zřejmě v souladu s tím, co si představujeme, že by mělo platit o operacích s celými čísly. Naše představa celých čísel však také zahrnuje skutečnost, že je lze srovnávat co do velikosti.

Uspořádání na celých číslech definujeme takto:

Definice.

$$(\forall x, y \in \mathbf{Z})\, x \prec y \Leftrightarrow y + (-x) \in \mathbf{Z}^+,$$

přičemž slovo $x \prec y$ *čteme „celé číslo* x *je menší než celé číslo* y*“.*

Souvislost mezi uspořádáním v $\mathbf{N}$ a v $\mathbf{Z}$ popisuje následující lemma.

Lemma 1. *Pro libovolná celá čísla* x, y *platí*

$$\begin{aligned}x \prec y \Leftrightarrow (x, y \in \mathbf{N} \wedge x < y) \vee (x \in \mathbf{Z}^- \wedge y \in \mathbf{N}) \vee \\ \vee (x, y \in \mathbf{Z}^- \wedge -y < -x).\end{aligned}$$

Důkaz rozdělíme na čtyři případy podle toho, jaká situace může nastat pro libovolně zvolená celá čísla x, y.

1. Nechť $x, y \in \mathbf{N}$; pak podle definice relace $<$ v $\mathbf{N}$ užitím vlastností grupy

$(\mathbf{Z}, +)$ a podle definice relace $\prec$ v $\mathbf{Z}$ postupně dostaneme

$$x < y \Leftrightarrow (\exists z \in \mathbf{Z}^+)\, y = x + z \Leftrightarrow (\exists z \in \mathbf{Z}^+)\, y + (-x) = z \Leftrightarrow \Leftrightarrow x \prec y.$$

2. Je-li $x \in \mathbf{Z}^-$ a $y \in \mathbf{N}$, je $-x \in \mathbf{Z}^+$, a tedy vždy platí $y + (-x) \in \mathbf{Z}^+$, takže $x \prec y$.

3. Je-li $x \in \mathbf{N}$ a $y \in \mathbf{Z}^-$, je $-x \in \mathbf{Z}^-$ nebo $-x = 0$, takže $y + (-x) \in \mathbf{Z}^-$, a tudíž v tomto případě nemůže nikdy nastat $x \prec y$.

4. Nechť $x, y \in \mathbf{Z}^-$, pak $-x \in \mathbf{N}$ a $-y \in \mathbf{N}$, a zřejmě

$$-y < -x \Leftrightarrow (\exists z \in \mathbf{Z}^+) - y + z = -x \Leftrightarrow \Leftrightarrow (\exists z \in \mathbf{Z}^+)\, y + (-x) = z \Leftrightarrow x \prec y.$$

Poněvadž další případ pro volbu čísel x a y nemůže nastat, je tím lemma dokázáno.

Z lemmatu 1 vyplývá, že relace $<$ je restrikcí relace $\prec$ na množinu $\mathbf{N}$. Tato skutečnost nám umožňuje obě relace označovat týmž znakem $<$, čehož budeme v dalším textu využívat.

V § 3 kap. V byl definován pojem uspořádaného polookruhu. Protože každý obor integrity i každé těleso je také polookruh s nulovým prvkem, můžeme podle zmíněné definice mluvit o uspořádaném oboru integrity (ev. tělese), popřípadě o archimedovsky uspořádaném oboru integrity (tělese).

Následující věta, týkající se struktury $(\mathbf{Z}, +, \cdot, <)$, nás ujistí, že i pokud jde o uspořádání, odpovídá námi zkonstruovaná struktura naší představě o celých číslech.

Věta 6. *Struktura $(\mathbf{Z}, +, \cdot, <)$ je archimedovsky uspořádaný obor integrity.*

Důkaz přenecháváme čtenáři (viz cvičení 4a), b), c), d), f)).

Další možnost, jak lze využít uspořádání struktury přirozených čísel k práci ve struktuře čísel celých, ukazuje následující zobrazení množiny $\mathbf{Z}$ na $\mathbf{N}$, které libovolnému celému číslu x přiřazuje přirozené číslo $|x|$ a které je definováno takto:

$$(\forall x \in \mathbf{Z})\, [(x \in \mathbf{N} \Rightarrow |x| = x) \wedge (x \in \mathbf{Z}^- \Rightarrow |x| = -x)].$$

Toto zobrazení se nazývá absolutní hodnota (v $\mathbf{Z}$). Jeho základní vlastnosti shrneme v následující větě.

Věta 7. *Pro absolutní hodnotu v $\mathbf{Z}$ platí:*

a) $(\forall x \in \mathbf{Z})\, |x| \in \mathbf{N}$;
b) $(\forall x \in \mathbf{Z})\, |x| = 0 \Leftrightarrow x = 0$;
c) $(\forall x \in \mathbf{Z})\, |x| = |-x|$;
d) $(\forall x \in \mathbf{Z}) - |x| \leqq x \leqq |x|$;

e) $(\forall a \in \mathbf{N})(\forall x \in \mathbf{Z}) - a \leqq x \leqq a \Rightarrow |x| \leqq a$;
f) $(\forall x, y \in \mathbf{Z})\, |x + y| \leqq |x| + |y|$;
g) $(\forall x, y \in \mathbf{Z})\, |xy| = |x| \,.\, |y|$.

Důkaz tvrzení a) až e) a g) přenecháváme čtenáři (viz cvičení 5). Zde na ukázku dokážeme tvrzení f) za předpokladu, že předcházející body a) až e) jsou již dokázány.

Nechť $x, y \in \mathbf{Z}$. Podle bodu d) této věty platí

$$-|x| \leqq x \leqq |x| \wedge -|y| \leqq y \leqq |y|.$$

Sečtením těchto nerovností dostaneme

$$-|x| + (-|y|) \leqq x + y \leqq |x| + |y|,$$

a protože podle (12) $-|x| + (-|y|) = -(|x| + |y|)$, obdržíme užitím bodu e) této věty nerovnost

$$|x + y| \leqq |x| + |y|.$$

Pro celá čísla odvodíme nyní ještě větu, jež je rozšířením věty 4 z kap. V, o dělení se zbytkem.

Věta 8. $(\forall x)(\forall y \neq 0)(\exists! u)(\exists! z)(x = yu + z \wedge 0 \leqq z < |y|)$.

Obdobně jako v případě přirozených čísel budeme i v oboru integrity $(\mathbf{Z}, +, \cdot)$ jednoznačně určené celé číslo u nazývat neúplný podíl a číslo z nejmenší nezáporný zbytek (po dělení čísla x číslem y).

Je-li tedy například $x = -190$, $y = -17$, je jejich neúplný podíl $u = 12$ a nejmenší nezáporný zbytek $z = 14$, neboť

$$-190 = (-17) \,.\, 12 + 14 \wedge 0 \leqq 14 < |-17|.$$

Důkaz provedeme pouze pro případ $x, y \in \mathbf{Z}^-$; zbývající tři případy přenecháme čtenáři (viz cvičení 6).

Nechť tedy x a y jsou libovolná čísla ze $\mathbf{Z}^-$, pak je $-x \in \mathbf{N}$, $-y \in \mathbf{N}$, a tedy podle věty 4, § 2, kap. V existují čísla $u', z' \in \mathbf{N}$ tak, že platí

$$-x = (-y) \,.\, u' + z' \wedge 0 \leqq z' < -y = |y|,$$

takže též

$$x = y \,.\, u' + (-z'). \tag{16}$$

Pokud $z' = 0$, je též $-z' = 0$ a můžeme položit $u = u'$ a $z = z' = 0$. Je-li $z' > 0$, přepíšeme (16) ve tvaru

$$x = yu' + y + (-y) + (-z') = y(u' + 1) + (-(y + z')).$$

Z $0 < z' < -y$ plyne $y < y + z' < 0$, a tedy podle definice uspořádání v **Z** dostáváme

$$0 < -(y + z') < -y = |y|.$$

Proto můžeme zvolit $u = u' + 1$ a $z = -(y + z')$.

Cvičení

1. Ukažte, že platí: aplikujeme-li konstrukci (K) na strukturu $(\mathbf{Z}, +)$, vytvoříme strukturu se $(\mathbf{Z}, +)$ izomorfní.
2. Dokažte, že struktura $(\mathbf{Z}, \cdot)$ (viz věta 1)
   a) je pologrupa s jednotkovým prvkem;
   b) je struktura s krácením nenulovým prvkem, tj., že platí
   $(\forall x, y, z \in \mathbf{Z})\, x \neq 0 \Rightarrow (xy = xz \Rightarrow y = z)$.
3. Ověřte, že struktura $(\mathbf{Z}, +, \cdot)$ je $(+, \cdot)$-distributivní.
4. Ukažte, že ve struktuře $(\mathbf{Z}, +, \cdot, <)$ platí:
   a) relace $<$ je tranzitivní;
   b) relace $<$ je trichotomická;
   c) $(\forall x, y, z \in \mathbf{Z})\, x < y \Rightarrow (x + z) < (y + z)$;
   d) $(\forall x, y, z \in \mathbf{Z})(0 < z \wedge x < y) \Rightarrow xz < yz$;
   e) $(\forall x, y \in \mathbf{Z})(0 < x \wedge 0 < y) \Rightarrow 0 < xy$;
   f) $(\forall x, y \in \mathbf{Z})\, [0 < y \Rightarrow (\exists n \in \mathbf{N})\, x < (n \times y)]$.
5. Dokažte tvrzení a), b), c), d), e) a g) z věty 7.
6. Proveďte důkaz věty 8 pro zbývající případy.

§ 2. Vnoření pologrupy do grupy

Postupu, pomocí něhož jsme v předcházejícím paragrafu vytvořili strukturu $(\mathbf{Z}, +)$, je možno užít i při sestrojování dalších číselných struktur, a proto ho v tomto paragrafu prozkoumáme z poněkud obecnějšího hlediska.

Nejprve si připomeňme, že zmíněným postupem vytvořená struktura $(\mathbf{Z}, +)$ neobsahovala výchozí strukturu $(\mathbf{N}, +)$, nýbrž pouze podstrukturu $(\mathbf{Z}_0, +)$ s $(\mathbf{N}, +)$ izomorfní. Tedy vlastně teprve po ztotožnění těchto izomorfních struktur můžeme $(\mathbf{N}, +)$ považovat za podstrukturu v $(\mathbf{Z}, +)$. Pro zjednodušení vyjadřování budeme tuto situaci popisovat krátce slovy: strukturu $(\mathbf{N}, +)$ lze izomorfně vnořit do $(\mathbf{Z}, +)$. Protože jde o důležitý pojem, vyslovíme ještě jeho definici v obecném tvaru.

Definice. *Říkáme, že strukturu* $(M, *)$ *lze izomorfně vnořit do struktury* $(\overline{M}, \circ)$, *právě když existuje v* $(\overline{M}, \circ)$ *podstruktura* $(M', \circ)$, *která je izomorfní s* $(M, *)$.

Skutečnost, že $(M, *)$ lze izomorfně vnořit do $(\overline{M}, \circ)$, budeme zapisovat tímto způsobem:

$$(M, *) \trianglelefteq (\overline{M}, \circ).$$

Pomocí právě vyslovené definice můžeme výsledek, k němuž jsme dospěli v předcházejícím paragrafu, to jest vybudování struktury $(\mathbf{Z}, +)$ ze struktury $(\mathbf{N}, +)$, zapsat $(\mathbf{N}, +) \trianglelefteq (\mathbf{Z}, +)$.

Dále nám půjde – jak již bylo řečeno – o zobecnění konstrukce z předchozího paragrafu. Budeme je realizovat ve dvou fázích. Nejprve vyslovíme tzv. větu o vnoření pologrupy do grupy, která je vlastně pouhým přeformulováním konstrukce z § 1.

Věta 1. *Nechť* $(H, *)$ *je komutativní pologrupa s krácením a s neutrálním prvkem, pak existuje komutativní grupa* $(G, \circ)$ *tak, že* $(H, *) \trianglelefteq (G, \circ)$ *(tj. taková, že lze do ní pologrupu* $(H, *)$ *izomorfně vnořit).*

Důkaz pouze nastíníme. Nechť je dána pologrupa $(H, *)$ splňující předpoklady věty. Existenci grupy G dokážeme tak, že ji sestrojíme pomocí konstrukce analogické konstrukci, již jsme ze struktury $(\mathbf{N}, +)$ vytvořili $(\mathbf{Z}, +)$. Pro snadnější porovnání obou postupů označíme jednotlivé kroky této konstrukce stejným způsobem, jako byly označeny v předcházejícím paragrafu.

Konstrukce (K) *(provedená na pologrupu $(H, *)$).*

(A) *Nejprve sestrojíme množinu G.*

(a) Utvoříme množinu $M = H \times H$ (všech uspořádaných dvojic prvků z H) a v ní definujeme relaci $\approx$ takto:

$$(\forall x, y, u, v \in H)\,(x, y) \approx (u, v) \Leftrightarrow x * v = y * u.$$

(b) O této relaci ukážeme, že je ekvivalencí v množině M.

(c) Rozklad množiny M podle ekvivalence $\approx$ označíme G, tj.

$$M/\approx\ = G = \{T(x, y)\}_{(x, y) \in M},$$

kde

$$T(x, y) = \square \approx (x, y) = \{(u, v) \in M;\ (u, v) \approx (x, y)\}.$$

(B) *Vytvoříme strukturu $(G, \circ)$ a ověříme požadované vlastnosti.*

(a) Operaci $\circ$ v G definujeme tímto způsobem:

$$(\forall T(x, y), T(u, v) \in G) \qquad T(x, y) \circ T(u, v) = T(x * u, y * v).$$

K důkazu věty 1 zbývá ověřit tyto její vlastnosti:

(b) Struktura $(G, \circ)$ je komutativní grupa.

(c) Struktura $(G, \circ)$ obsahuje podstrukturu $(G_0, \circ)$ izomorfní s pologrupou $(H, *)$.

Důkazy obou těchto tvrzení jsou zcela obdobné důkazům vět 1 a 2 z předchozího paragrafu a přenecháváme je proto čtenáři do cvičení. Zde ovšem G_0 bude množina všech těch tříd $T(x, y)$ z G, které obsahují alespoň jednu dvojici (u, e), kde e je neutrální prvek pologrupy H.

Platí tedy $(H, *) \lhd (G, \circ)$, čímž je důkaz věty o vnoření pologrupy do grupy dovršen.

Při budování číselných struktur nastanou však někdy případy, kdy nebude možné ve výchozí pologrupě krátit všemi jejími prvky. Pak nelze užít věty 1 a konstrukce (K), nýbrž jejich jistého zobecnění, které nyní popíšeme. Půjde o tzv. zobecněnou větu o vnoření pologrupy do grupy.

Věta 2. *Nechť $(H, *)$ je komutativní pologrupa s neutrálním prvkem a $(S, *)$ její podpologrupa taková, že v H lze krátit každým prvkem z S. Pak existuje komutativní pologrupa $(T, \circ)$ s neutrálním prvkem a její podgrupa $(G, \circ)$ tak, že*

$$(H, *) \lhd (T, \circ) \wedge (S, *) \lhd (G, \circ).$$

Povšimněme si nejprve, že věta 1 je speciálním případem věty 2. Je-li totiž pologrupa $(H, *)$ z věty 2 navíc struktura s krácením, můžeme položit $S = H$, a potom také $T = G$, takže $(T, \circ)$ je grupa.

Důkaz. Nechť jsou dány pologrupy $(H, *)$ a $(S, *)$ splňující předpoklady věty. Protože z vlastnosti neutrálního prvku e v H plyne

$$(\forall x, y \in H)\, x * e = y * e \Rightarrow x = y,$$

lze prvkem e krátit v H, a tedy můžeme předpokládat, že $e \in S$.

Existenci struktur $(T, \circ)$ a $(G, \circ)$ dokážeme tak, že je zkonstruujeme. Užijeme konstrukce, jež je zobecněním konstrukce (K) a kterou proto označíme (K′).

Konstrukce (K′) (*provedená na struktury $(H, *)$ a $(S, *)$*)

(A) *Nejprve sestrojíme množinu T.*

(a) Utvoříme množinu $M = H \times S$ (všech uspořádaných dvojic prvků z množiny H a S) a v M definujeme relaci $\approx$ tímto způsobem:

$$(\forall p, p' \in H)(\forall s, s' \in S)(p, s) \approx (p', s') \Leftrightarrow p * s' = p' * s.$$

(b) Ověření, že tato relace je ekvivalence v M, provede čtenář snadno sám.

(c) Rozklad množiny M podle ekvivalence $\approx$ je již hledanou množinou T, takže označíme

$$T = M/\approx\; = \{T(h, s)\}_{(h,s)\in M}.$$

Tedy prvky množiny T jsou třídy tohoto rozkladu, to jest podmnožiny množiny M. Připomeňme ještě jednou, že pro libovolný prvek $(h, s) \in M$ se definuje třída $T(h, s) \in T$, jejímž je prvek (h, s) reprezentantem, tímto způsobem:

(1) $$T(h, s) = \square \approx (h, s) = \{(x, y) \in M;\, (x, y) \approx (h, s)\},$$

a že táž třída může být zapsána i pomocí různých reprezentantů, přičemž lze ukázat, že (pro libovolné prvky (h, s), (h', s') z M) platí

(2) $$T(h, s) = T(h', s') \Leftrightarrow (h', s') \approx (h, s)$$

(B) *Vytvoříme struktury $(T, \circ)$ a $(G, \circ)$ a ověříme požadované vlastnosti.*

(a) Položíme

(3) $$(\forall T(h, s), T(h', s') \in T)\, T(h, s) \circ T(h', s') = T(h * h', s * s');$$

ověření, že tímto předpisem je skutečně definována operace v množině T, přenecháváme čtenáři. Tedy (3) definuje skutečně operaci v T, takže $(T, \circ)$ je struktura.

Dále ukážeme, že množina G všech těch tříd z T, které mají alespoň jednoho reprezentanta z množiny $S \times S$, tvoří podstrukturu v $(T, \circ)$. Je tedy

(4) $$G = \{T(x, y) \in T;\, (\exists(s, r) \in S \times S)\, T(x, y) = T(s, r)\}.$$

Musíme ověřit, že výsledek operace $\circ$, provedené na libovolné dva prvky z G, je opět prvek z G. Zvolme tedy libovolně $T(x, y)$, $T(x', y') \in G$. Potom díky definici (4) množiny G můžeme předpokládat, že $x, x' \in S$, takže také $x * x' \in S$, a tedy podle (1)

$$T(x, y) \circ T(x', y') = T(x * x', y * y') \in G,$$

což znamená, že $(G, \circ)$ je podstruktura v $(T, \circ)$.

Tím jsme pomocí konstrukce (K′) z $(H, *)$ a $(S, *)$ vytvořili jisté struktury $(T, \circ)$ a $(G, \circ)$.

(b) Ověříme, že $(T, \circ)$ je komutativní pologrupa s neutrálním prvkem a $(G, \circ)$ komutativní grupa.

Snadno lze nahlédnout, že $(T, \circ)$, a tedy i $(G, \circ)$, jsou komutativní a asociativní struktury.

Rovněž bez obtíží ukážeme, že třída $T(e, e)$, jež se podle (1) zřejmě skládá ze všech dvojic tvaru (s, s), kde $s \in S$, je neutrálním prvkem v T, a tedy i v G: zvolme libovolně $T(x, y) \in T$; pak podle (3)

$$T(x, y) \circ T(e, e) = T(x * e, y * e) = T(x, y).$$

Jestliže $T(u, v)$ je libovolný prvek z G, můžeme předpokládat, že $u \in S$, a potom také $T(v, u) \in G$. Avšak zřejmě

$$T(u, v) \circ T(v, u) = T(u * v, v * u) = T(e, e),$$

což znamená, že třída $T(v, u)$ je inverzním prvkem k $T(u, v)$, takže $(G, \circ)$ je též struktura s inverzními prvky, a tedy – vzhledem k předchozím výsledkům – Abelova grupa.

(c) Dále ukážeme, že $(H, *) \lhd (T, \circ)$, neboli že existuje v $(T, \circ)$ podstruktura $(H_0, \circ)$ izomorfní s $(H, *)$.

Za množinu H_0 zvolíme množinu všech těch tříd $T(h, s) \in T$, jež obsahují alespoň jednu dvojici tvaru (x, e), tj.

$$H_0 = \{T(h, s) \in T; (\exists x \in H)(x, e) \in T(h, s)\}.$$

Protože $e * e = e$, snadno nahlédneme, že formuli (3) můžeme považovat také (omezíme-li se pouze na třídy z H_0) za definici operace $\circ$ v H_0, takže $(H_0, \circ)$ je podstrukturou struktury $(T, \circ)$.

Zbývá ověřit, že $(H, *)$ je izomorfní s $(H_0, \circ)$. Definujme zobrazení F množiny H do H_0 tímto způsobem:

(5) $$(\forall x \in H)\, F(x) = T(x, e);$$

pak je ihned zřejmé, že F je zobrazení H na H_0. Protože pro libovolné prvky $x, y \in H$, $x \neq y$, musí být i třídy $T(x, e)$ a $T(y, e)$ různé (jinak by podle (2) platilo $(x, e) \approx (y, e)$ neboli $x * e = y * e$, a tedy $x = y$), je F prosté zobrazení. Ověříme ještě vlastnost homomorfismu, tj. platnost formule

(6) $$(\forall x, y \in H)\, F(x * y) = F(x) \circ F(y).$$

Zvolme libovolně prvky $x, y \in H$; užitím formule (6), vlastnosti neutrálního prvku, formule (3) a znovu (6) postupně obdržíme

$$F(x * y) = T(x * y, e) = T(x * y, e * e) = \\ = T(x, e) \circ T(y, e) = F(x) \circ F(y).$$

Ukázali jsme tedy, že platí $(H, *) \lhd (T, \circ)$ a obdobně lze dokázat $(S, *) \lhd (G, \circ)$. Tím je důkaz věty 2 dokončen.

Poznamenejme ještě, že izomorfismus (6) nám umožňuje přijmout úmluvu o ztotožnění odpovídajících si prvků množiny H a množiny H_0, tj. položit

(8) $$(\forall x \in H)\, T(x, e) = x.$$

Tato úmluva dovoluje zjednodušit i zápisy prvků z T, neboť libovolný prvek $T(h, s)$ z T lze vyjádřit pomocí (3) a (5) tímto způsobem:

(9) $$T(h, s) = T(h, e) \circ T(e, s) = T(h, e) \circ [T(s, e)]^{-1},$$

a tedy podle úmluvy (8) lze psát

$$T(h, s) = h \circ s^{-1}.$$

Symbol s^{-1} pochopitelně nesmíme chápat jako inverzní prvek k prvku s v $(H, *)$ – ten ani nemusí existovat – nýbrž jako inverzní prvek v $(G, \circ)$ k prvku přiřazenému izomorfismem (6) prvku $s \in H$ (což ostatně popisuje formule (9)).

Příklad 1. Užití věty 2 ukážeme na sestrojení struktury tzv. nezáporných desetinných čísel $\mathbf{D}^+$, jíž využijeme v pozdějším výkladu.

Za pologrupu $(H, *)$ vezměme pologrupu $(\mathbf{N}, \cdot)$, za S množinu všech přirozených čísel tvaru 10^n, kde $n \in \mathbf{N}$. Zřejmě $(S, \cdot)$ je podpologrupa v $(\mathbf{N}, \cdot)$, neboť evidentně platí

$$(\forall m, n \in \mathbf{N})\, 10^m \,.\, 10^n = 10^{m+n},$$

takže násobení v S je zúžením operace $\cdot$ struktury $(\mathbf{N}, \cdot)$ na množinu S.

Užitím konstrukce (K′) vytvoříme množinu $\mathbf{N} \times S$ všech dvojic $(a, 10^n)$, kde $a, n \in \mathbf{N}$, a na ní definujeme relaci $\approx$ tak, že pro libovolné dvojice $(a, 10^n)$, $(b, 10^m)$ z $\mathbf{N} \times S$

$$(a, 10^n) \approx (b, 10^m) \Leftrightarrow a \,.\, 10^m = b \,.\, 10^n.$$

Relace $\approx$ je ekvivalencí v $\mathbf{N} \times S$; rozklad této množiny podle $\approx$ označme $\mathbf{D}^+$. Ukázkami prvků z $\mathbf{D}^+$ jsou tedy např.

$$T(2, 10) = T(20, 100) = T(200, 1000),$$

nebo

$$T(3, 1) = T(30, 10) = T(300, 100).$$

V množině $\mathbf{D}^+$ definujeme podle konstrukce (K′) operaci $\cdot$ tímto způsobem:

$$(\forall T(a, b), T(c, d) \in \mathbf{D}^+)\, T(a, b) \,.\, T(c, d) = T(ac, bd).$$

Lze snadno nahlédnout, že $(\mathbf{D}^+, \cdot)$ je komutativní pologrupa s neutrálním prvkem, jímž je třída $T(1, 1)$.

V $(\mathbf{D}^+, \cdot)$ existuje podgrupa G, jež má za prvky právě ty třídy z $\mathbf{D}^+$, které obsahují alespoň jednu dvojici z množiny $S \times S$. Pro libovolnou třídu $T(a, b) \in G$ je $T(b, a)$ rovněž z G a platí

$$[T(a, b)]^{-1} = T(b, a),$$

neboť

$$T(a, b) \,.\, T(b, a) = T(ab, ab) = T(1, 1).$$

Množina všech těch tříd z $\mathbf{D}^+$, které obsahují alespoň jednu dvojici tvaru $(a, 1)$, vytváří v $(\mathbf{D}^+, \cdot)$ podstrukturu $(\overline{\mathbf{N}}, \cdot)$ izomorfní s $(\mathbf{N}, \cdot)$, takže $(\mathbf{N}, \cdot) \lhd (\mathbf{D}^+, \cdot)$ a příslušný izomorfismus F má tvar

$$(\forall T(a, 1) \in \overline{\mathbf{N}}) F(T(a, 1)) = a.$$

Ztotožníme-li v F odpovídající si prvky, máme dokonce $(\mathbf{N}, \cdot) \subseteq (\mathbf{D}^+, \cdot)$. Protože pro libovolný prvek $T(a, b) \in \mathbf{D}^+$ platí

$$T(a, b) = T(a, 1) \,.\, T(1, b) = T(a, 1) \,.\, [T(b, 1)]^{-1},$$

umožňuje nám ztotožnění množin $\overline{\mathbf{N}}$ a $\mathbf{N}$ psát místo $T(a, b)$ pouze $a \,.\, b^{-1}$ nebo a/b. Máme tedy možnost označovat třídy z $\mathbf{D}^+$ pomocí „podílů“ prvků z $\mathbf{N}$ a S. Tedy např. místo $T(2, 10)$ můžeme psát $2/10$ nebo $20/100$ atd. a třídu $T(3, 1)$ můžeme značit $3/1$ nebo $30/10$ atd.

Příklad 2. V této ukázce užijeme větu 2 na strukturu $(\mathbf{Z}, \cdot)$, tj. na multiplikativní pologrupu oboru integrity celých čísel a za pologrupu S zvolíme touž strukturu jako v předcházejícím příkladě, tj. množinu všech přirozených mocnin čísla 10 s operací násobení.

Prvky výsledné pologrupy budou třídy tvaru $T(a, 10^n)$, kde $n \in \mathbf{N}$ a – na rozdíl od předcházejího příkladu – a je tentokrát libovolné celé číslo. Je proto na místě nazvat množinu všech těchto prvků – označíme ji $\mathbf{D}$ – množinou desetinných čísel.

Věta 2 nám zaručuje, že $(\mathbf{D}, \cdot)$ je komutativní pologrupa s neutrálním prvkem, do níž lze izomorfně vnořit výchozí pologrupu $(\mathbf{Z}, \cdot)$. K desetinným číslům se ještě vrátíme v § 4.

Cvičení

1. Dokažte detailně větu 1. [Při práci můžete využít analogie s konstrukcí struktury $(\mathbf{Z}, +)$ z předchozího paragrafu.]

2. a) Přeformulujte větu 2 pro struktury $(\mathbf{N}, \cdot)$ a $(\mathbf{N} - \{0\}, \cdot)$.

b) Definujte na množině $\mathbf{N} \times (\mathbf{N} - \{0\})$ relaci $\approx$ tímto způsobem:

$$(\forall (a, b), (c, d) \in \mathbf{N} \times (\mathbf{N} - \{0\}))\, (a, b) \approx (c, d) \Leftrightarrow ad = bc$$

a ukažte, že je ekvivalencí.

c) Proveďte rozklad množiny $\mathbf{N} \times (\mathbf{N} - \{0\})$ podle $\approx$ (označte ho L) a na třídách rozkladu definujte operaci „$\cdot$“ takto:

$$(\forall T(a, b), T(c, d) \in L)\, T(a, b) \,.\, T(c, d) = T(ac, bd).$$

d) Ukažte, že $(L, \cdot)$ je komutativní pologrupa s neutrálním prvkem.

e) Najděte v $(L, \cdot)$ podstrukturu izomorfní s $(\mathbf{N}, \cdot)$, proveďte příslušné ztotožnění a všimněte si, že $(L, \cdot)$ je vlastně struktura všech nezáporných racionálních čísel.

3. Ukažte, že struktura $(\mathbf{D}^+, \cdot)$ z příkladu 1 je vlastní podstrukturou v $(L, \cdot)$ (viz předchozí cvičení).

§ 3. Čísla racionální

Další důležitou aplikaci věty o vnoření pologrupy do grupy uvidíme při konstrukci tělesa racionálních čísel $(\mathbf{Q}, +, \cdot)$. Vyjdeme od struktury $(\mathbf{Z}, \cdot)$; poněvadž je pologrupou s jednotkovým prvkem, v níž lze krátit pouze každým nenulovým prvkem, je třeba užít věty 2 (z předchozího paragrafu). Za pologrupu $(H, *)$ vezmeme pochopitelně $(\mathbf{Z}, \cdot)$ a za množinu S množinu $\mathbf{Z}_0 = \mathbf{Z} - \{0\}$. Předpoklady věty 2 jsou pak zřejmě splněny, a tedy podle ní existuje komutativní pologrupa s neutrálním prvkem $(\mathbf{Q}, \cdot)$ a její podgrupa, kterou označíme $(\mathbf{Q}_0, \cdot)$, tak, že platí

$$(\mathbf{Z}, \cdot) \lhd (\mathbf{Q}, \cdot) \wedge (\mathbf{Z}_0, \cdot) \lhd (\mathbf{Q}_0, \cdot).$$

Struktury $(\mathbf{Q}, \cdot)$ a $(\mathbf{Q}_0, \cdot)$ sestrojíme užitím konstrukce (K'); celý postup si zde stručně připomeneme.

(A) (a) Utvoříme množinu $M = \mathbf{Z} \times \mathbf{Z}_0$, na ní definujeme relaci $\approx$ známým způsobem: pro libovolné $p, r \in \mathbf{Z}$, $q, s \in \mathbf{Z}_0$

(1) $$(p, q) \approx (r, s) \Leftrightarrow ps = qr.$$

(b) Snadno ověříme, že relace $\approx$ je ekvivalence v množině M.

(c) Rozklad množiny M na třídy podle ekvivalence $\approx$ je již hledanou množinou $\mathbf{Q}$:

(2) $$\mathbf{Q} = M/\approx\, = \{T(p, q)\}_{(p,q) \in M}\,.$$

(B) Vytvoříme struktury $(\mathbf{Q}, \cdot)$ a $(\mathbf{Q}_0, \cdot)$ a ověříme, že mají požadované vlastnosti.

(a) V množině $\mathbf{Q}$ definujeme operaci „$\cdot$“ tímto předpisem:

(3) $$(\forall T(p, q), T(r, s) \in \mathbf{Q})\, T(p, q) \,.\, T(r, s) = T(pr, qs)$$

a ověříme, že jde skutečně o operaci.

Tedy $(\mathbf{Q}, \cdot)$ je struktura a snadno ukážeme, že $(\mathbf{Q}_0, \cdot)$, kde $\mathbf{Q}_0$ je množina všech těch tříd $T(p, q) \in \mathbf{Q}$, pro něž $p \in \mathbf{Z}_0$ neboli $p \neq 0$, je podstrukturou v $(\mathbf{Q}, \cdot)$.

(b) Snadno ověříme, že $(\mathbf{Q}, \cdot)$ je komutativní pologrupa s jednotkovým prvkem $T(1, 1)$ a že $(\mathbf{Q}_0, \cdot)$ je komutativní grupa, přičemž pro libovolnou třídu $T(p, q) \in \mathbf{Q}_0$ platí

(4) $$[T(p, q)]^{-1} = T(q, p).$$

(c) Dále ukážeme, že množina $\overline{\mathbf{Q}}$ skládající se ze všech těch tříd z $\mathbf{Q}$, které obsahují alespoň jednu dvojici tvaru $(p, 1)$ pro $p \in \mathbf{Z}$ a které tedy lze označit jako $T(p, 1)$, tvoří podpologrupu v $(\mathbf{Q}, \cdot)$ izomorfní s $(\mathbf{Z}, \cdot)$. Přitom příslušný izomorfismus F má tvar

(5) $$(\forall T(p, 1) \in \overline{\mathbf{Q}})\, F(T(p, 1)) = p.$$

Obdobně podstruktura $(\overline{\mathbf{Q}} \cap \mathbf{Q}_0, \cdot)$ struktury $(\mathbf{Q}_0, \cdot)$ je izomorfní s $(\mathbf{Z}_0, \cdot)$. Tedy skutečně platí

$$(\mathbf{Z}, \cdot) \lhd (\mathbf{Q}, \cdot) \wedge (\mathbf{Z}_0, \cdot) \lhd (\mathbf{Q}_0, \cdot).$$

Izomorfismus (5) nám dovoluje ztotožnit struktury $(\mathbf{Z}, \cdot)$ a $(\overline{\mathbf{Q}}, \cdot)$, což prakticky znamená, že přijmeme úmluvu, že třídu $T(p, 1)$ z $\overline{\mathbf{Q}}$ a její obraz p v homomorfismu F budeme považovat za týž objekt, což zapíšeme

(6) $\qquad (\forall T(p, 1) \in \overline{\mathbf{Q}})\, T(p, 1) = p.$

Tuto úmluvu lze však rozšířit i na prvky celé množiny $\mathbf{Q}$: Je-li $T(p, q) \in \mathbf{Q}$, je

$$T(p, q) = T(p, 1) \,.\, T(1, q) = T(p, 1) \,.\, [T(q, 1)]^{-1}.$$

Tedy užitím úmluvy (6) (a užitím obvyklého zápisu $1/q$ místo q^{-1}) dostáváme

(7) $\qquad T(p, q) = p \,.\, q^{-1} = p/q.$

V tomto smyslu lze tedy prvky množiny $\mathbf{Q}$ chápat jako podíly dvou celých čísel (přičemž číslo ve jmenovateli je ze $\mathbf{Z}_0$, tedy nenulové). Proto množinu $\mathbf{Q}$ nazveme množinou (všech) racionálních čísel a její prvky budeme nazývat racionální čísla. Přitom musíme mít stále na mysli, že týž prvek množiny $\mathbf{Q}$, to jest totéž racionální číslo, může být zapsáno různými způsoby ve tvaru podílu. Platí však díky (7) a (1)

(8) $\qquad p/q = r/s \Leftrightarrow ps = rq.$

Při zavedeném způsobu zápisu racionálních čísel nabude (3) „obvyklého" tvaru

(3′) $\qquad (\forall p/q, r/s \in \mathbf{Q})\, p/q \,.\, r/s = pr/qs$

a úmluva (6) přejde v

(6′) $\qquad (\forall p \in \mathbf{Z})\, p/1 = p.$

Skutečnost, že $(\mathbf{Q}, \cdot)$ je komutativní pologrupa s jednotkovým prvkem obsahující podgrupu $(\mathbf{Q}, \cdot)$, zaručuje řadu vlastností struktury $(\mathbf{Q}, \cdot)$, jež shrneme ve větu.

Věta 1. *Pro libovolné prvky p/q, r/s, $t/u \in \mathbf{Q}$ platí:*

a) $(p/q \,.\, r/s) \,.\, t/u = p/q \,.\, (r/s \,.\, t/u)$;
b) $p/q \,.\, r/s = r/s \,.\, p/q$;
c) $1/1 = 1$ *je jednotkový prvek v* $(\mathbf{Q}, \cdot)$;
d) $p/q \,.\, 0/1 = 0/1 = 0$;
e) *je-li $p/q \neq 0$, platí*
$\quad p/q \,.\, r/s = p/q \,.\, t/u \Rightarrow r/s = t/u$;
f) *je-li $p/q \neq 0$, existuje v $(\mathbf{Q}, \cdot)$ k němu inverzní prvek $(p/q)^{-1}$ a platí*

$$(p/q)^{-1} = q/p.$$

V množině racionálních čísel $\mathbf{Q}$ zavedeme ještě operaci sčítání tímto předpisem:

(9) $\qquad (\forall p/q, r/s \in \mathbf{Q})\, p/q + r/s = (ps + qr)/(qs).$

Je ovšem třeba ukázat – obdobně jako u násobení racionálních čísel – že výsledek závisí pouze na daných číslech a nikoli na jejich zápisu ve tvaru podílu. Snadné ověření provede čtenář jako cvičení (viz cvičení 1).

Formule (9) tudíž definuje operaci $+$ v $\mathbf{Q}$. Můžeme proto hovořit o struktuře $(\mathbf{Q}, +, \cdot)$ a pro ni odvodíme několik dalších vlastností, jež opět shrneme do jediné věty.

Věta 2. *Pro libovolné prvky p/q, r/s, $t/u \in \mathbf{Q}$ platí:*

a) $(p/q + r/s) + t/u = p/q + (r/s + t/u)$;
b) $p/q + r/s = r/s + p/q$;
c) $p/q + 0/1 = p/q$, *takže* $0/1 = 0$ *je nulovým prvkem struktury* $(\mathbf{Q}, +, \cdot)$;
d) $p/q + (-p)/q = 0$, *což znamená, že opačný prvek k číslu p/q je $(-p)/q$*;
e) $(p/q + r/s) \,.\, t/u = (p/q \,.\, t/u) + (r/s \,.\, t/u)$.

Důkaz přenecháváme čtenáři (viz cvičení 2).

Pro další úvahy je užitečné si uvědomit, že každé racionální číslo lze zapsat ve tvaru podílu tak, že „jmenovatel" je kladný, tj., že platí

$$(\forall p/q \in \mathbf{Q})\, (\exists p_0/q_0 \in \mathbf{Q})\, (p/q = p_0 q_0 \wedge 0 < q_0).$$

Tato skutečnost nám dovoluje přijmout úmluvu, že při zápisech racionálních čísel ve tvaru p/q budeme předpokládat, že q je kladné. Tato úmluva nám bude užitečná zvláště v následující partii, kde se budeme zabývat uspořádáním racionálních čísel.

V množině $\mathbf{Q}$ zavedeme relaci „$<$" tímto způsobem:

(10) $\qquad (\forall p/q, r/s \in \mathbf{Q})\, p/q < r/s \Leftrightarrow ps < qr,$

přičemž předpokládáme (což nebudeme v dalším výslovně zdůrazňovat), že ve smyslu naší úmluvy je $0 < q$ a $0 < s$.

Aby zavedená relace byla skutečně relací v množině racionálních čísel $\mathbf{Q}$, musíme opět ověřit, že pro

(11) $\qquad p/q = p'/q' \wedge r/s = r'/s'$

platí

$$p/q < r/s \Leftrightarrow p'/s' < r'/s',$$

což si čtenář dokáže samostatně jako cvičení 3.

Jestliže v (11) uvažujeme p/q a r/s celá, tj. položíme-li $q = s = 1$, vidíme, že relace $<$ v $\mathbf{Z}$ je zúžením relace $<$ v $\mathbf{Q}$, a proto není na závadu, že obě relace označujeme týmž symbolem.

Vlastnosti relace $<$ v $\mathbf{Q}$ shrneme opět do jedné věty.

Věta 3. *Pro libovolné prvky p/q, r/s, t/u struktury* $\mathbb{Q}$ *platí:*

a) $(p/q < r/s \wedge r/s < t/u) \Rightarrow p/q < t/u$;

b) *nastane právě jeden z případů*

$$p/q < r/s, \quad p/q = r/s, \quad r/s < p/q;$$

c) $p/q < r/s \Rightarrow p/q + t/u < r/s + t/u$;

d) $(0 < p/q \wedge 0 < r/s) \Rightarrow 0 < p/q \,.\, r/s$;

e) $(p/q < r/s \wedge 0 < t/u) \Rightarrow p/q \cdot t/u < r/s \cdot t/u$;

f) $0 < p/q \Rightarrow (\exists n \in \mathbf{N})\, r/s < n \times (p/q)$;

g) $p/q < r/s \Rightarrow (\exists v/w \in \mathbb{Q})\, p/q < v/w < r/s$.

Důkaz. Na ukázku dokážeme pouze tvrzení g); ostatní tvrzení přenecháváme čtenáři jako cvičení (viz cvičení 4).

Jsou-li p/q a r/s libovolná racionální čísla taková, že $pq < r/s$, je

(12) $$ps < rq.$$

Zvolíme-li

$$v/w = 1/2 \,.\, (p/q + r/s) = (ps + rq)/2qs,$$

plyne z (12)

$$2pqs < pqs + rqq \wedge pss + rqs < 2rqs,$$

takže podle definice uspořádání v $\mathbb{Q}$ platí

$$p/q < v/w \wedge v/w < r/s.$$

Poznamenejme ještě, že z právě dokázaného tvrzení g) věty 3 plyne, že mezi libovolnými dvěma různými racionálními čísly existuje nekonečně mnoho racionálních čísel.

Uspořádaná množina M, s relací uspořádání U, která má vlastnost g) z věty 3, tj. pro niž platí

$$(\forall x, y \in M)\, xUy \Rightarrow (\exists z \in M)(xUz \wedge zUy),$$

se nazývá hustě uspořádaná množina.

Shrneme-li výsledky vět 1 až 3, dostáváme následující tvrzení:

Věta 4. *Struktura* $(\mathbb{Q}, +, \cdot, <)$ *tvoří archimédovsky a hustě uspořádané (komutativní) těleso.*

Cvičení

1. Ověřte, že sčítání definované na množině $\mathbb{Q}$ předpisem (9) má tuto vlastnost: pro libovolné prvky

$$p/q,\ p'/q',\ r/s,\ r'/s' \in \mathbb{Q}$$

platí

$$(p/q = p'/q' \wedge r/s = r'/s') \Rightarrow (ps + qr)/qs = (p's' + q'r')/q's'.$$

2. Dokažte větu 2.

3. Ukažte, že předpis (10) definuje skutečně relaci v množině $\mathbb{Q}$.

4. Dokažte tvrzení a) až f) věty 3.

§ 4. Rozvoje racionálních čísel v pozičních soustavách

Zápisy racionálních čísel ve tvaru podílu p/q, kterých jsme užívali v předcházejícím paragrafu, nejsou vždy vhodné pro konkrétní počítání s racionálními čísly.

Ukážeme, že postup užitý v kapitole VI pro vyjádření přirozených čísel v pozičních číselných soustavách, lze vhodným způsobem zobecnit i pro čísla racionální. Východiskem bude pro nás následující tvrzení.

Věta 1. *Každé racionální číslo p/q je součtem celého čísla c a racionálního čísla p_0/q, pro něž platí $0 \leqq p_0/q < 1$ (a přitom čísla c a p_0 jsou jednoznačně určena).*

Snadný důkaz přenecháváme čtenáři (viz cvičení 1).

Poněvadž každé celé číslo umíme vyjádřit v poziční číselné soustavě o libovolném základu z (> 1), umožňuje nám věta 1 zaměřit se pouze na nezáporná racionální čísla p/q menší než 1, tj. (vzhledem k tomu, že předpokládáme $q > 0$) taková, že $0 \leqq p < q$.

Východiskem k vyjádření racionálních čísel v poziční číselné soustavě o základu $z > 1$ bude pro nás následující věta.

Věta 2. *Nechť $p/q \in \mathbb{Q}$ je racionální číslo takové, že*

(1) $$0 \leqq p/q < 1$$

a nechť $z \in \mathbf{N}$, $z > 1$. Pak existují jednoznačně určená přirozená čísla s (neúplný podíl) a r (zbytek) tak, že platí

(2) $$pz = sq + r \wedge 0 \leqq r < q \wedge 0 \leqq s < z.$$

Důkaz. Nechť jsou dána čísla p, q a z splňující předpoklady věty. Protože pz a q jsou přirozená čísla a $q \neq 0$, existují podle věty o dělení se zbytkem pro přirozená