5. Okruh celých čísel

5.1. Definice. Nechť $\mathcal{G} = (G, \cdot)$, $\mathcal{H} = (H, \cdot)$ jsou grupoidy. Řekneme, že grupoid $\mathcal{G}$ *lze vnořit* do grupoidu $\mathcal{H}$, jestliže existuje vnoření (tj. injektivní homomorfismus) f grupoidu $\mathcal{G}$ do grupoidu $\mathcal{H}$.

Vyřešíme nyní otázku, kdy komutativní grupoid lze vnořit do nějaké grupy. (Nekomutativní případ přesahuje rámec tohoto textu.)

5.2. Věta. *Nechť $\mathcal{G} = (G, \cdot)$ je komutativní grupoid. Pak následující výroky jsou ekvivalentní:*

(a) *Grupoid $\mathcal{G}$ je asociativní a platí v něm zákon o krácení.*

(b) *Grupoid $\mathcal{G}$ lze vnořit do nějaké grupy.*

Důkaz. Nejdříve ukážeme implikaci „(b) $\Longrightarrow$ (a)". Nechť tedy existuje grupa $\mathcal{H} = (H, \cdot)$ a vnoření f grupoidu $\mathcal{G}$ do grupoidu $\mathcal{H}$. Pak pro libovolná $a, b, c \in G$ můžeme psát: $f(a \cdot (b \cdot c)) = f(a) \cdot f(b \cdot c) = f(a) \cdot (f(b) \cdot f(c)) = (f(a) \cdot f(b)) \cdot f(c) = f(a \cdot b) \cdot f(c) = f((a \cdot b) \cdot c)$ a z injektivnosti zobrazení f plyne $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. Grupoid $\mathcal{G}$ je tudíž asociativní. Nechť dále platí $a \cdot c = b \cdot c$. Pak $f(a) \cdot f(c) = f(a \cdot c) = f(b \cdot c) = f(b) \cdot f(c)$ a jelikož v grupě platí zákon o krácení, dostáváme $f(a) = f(b)$, z čehož plyne $a = b$. Platí výrok (a).

Nyní dokazujeme implikaci „(a) $\Longrightarrow$ (b)". Předpokládejme tedy, že grupoid $\mathcal{G}$ je asociativní a platí v něm zákon o krácení. Prvek $\alpha = [\, a, b \,] \in G \times G$ nazveme *zlomkem grupoidu* $\mathcal{G}$ a na množině $G \times G$ všech zlomků grupoidu $\mathcal{G}$ definujeme relaci $\sim$ následující podmínkou: pro $\alpha = [\, a, b \,] \in G \times G$ a $\beta = [\, c, d \,] \in G \times G$ položme $\alpha \sim \beta$, jestliže $a \cdot d = b \cdot c$.

Snadno se nahlédne, že relace $\sim$ je reflexivní a symetrická. Sami si dokažte, že její tranzitivnost plyne ze zákona o krácení. Zlomky $\alpha, \beta \in G \times G, \alpha \sim \beta$ nazýváme ekvivalentní. Rozklad na $G \times G$ příslušný relaci $\sim$ označme Γ. Prvek z Γ je pak třída ekvivalentních zlomků grupoidu $\mathcal{G}$.

Na množině Γ budeme definovat operaci $\circ$. Pro $A, B \in \Gamma$ nechť $\alpha = [a, b] \in A$, $\beta = [c, d] \in B$ a nechť $C \in \Gamma$ je třída určená podmínkou $[\, a \cdot c, b \cdot d \,] \in C$. Jestliže $\alpha_1 = [\, a_1, b_1 \,] \in A$, $\beta_1 = [\, c_1, d_1 \,] \in B$, pak $\alpha \sim \alpha_1$, $\beta \sim \beta_1$, tudíž $a \cdot b_1 = a_1 \cdot b$, $c \cdot d_1 = c_1 \cdot d$. Odtud plyne $a \cdot c \cdot b_1 \cdot d_1 = a_1 \cdot c_1 \cdot b \cdot d$, tedy $[a \cdot c, b \cdot d] \sim [a_1 \cdot c_1, b_1 \cdot d_1]$, tudíž $[\, a_1 \cdot c_1, b_1 \cdot d_1 \,] \in C$. Třída C nezávisí na volbě reprezentantů α, β tříd A, B, a je tedy jednoznačně určena třídami A, B. Můžeme pak položit $A \circ B = C$. Tím je definována operace $\circ$ na množině Γ.

Snadno se ověří, že $(\Gamma, \circ)$ je komutativní grupa. Jednotkovým prvkem je třída $E = \{[\, g, g \,] \mid g \in G\}$ a pro $A \in \Gamma$ je $A^{-1} = \{[\, b, a \,] \mid [\, a, b \,] \in A\}$.

Pro $g \in G$ je $A_g = \{[\, g \cdot x, x \,] \mid x \in G\}$ prvek grupy $(\Gamma, \circ)$. Nyní definujme zobrazení $\psi : G \to \Gamma$ vztahem $\psi(g) = A_g$ pro $g \in G$, o kterém se snadno přesvědčíme, že je vnořením grupoidu $\mathcal{G}$ do grupy $(\Gamma, \circ)$. Pro libovolné $g, h \in G$ totiž platí $[\, g \cdot g, g \,] \in A_g$, $[\, h \cdot h, h \,] \in A_h$, odkud $[\, (g \cdot h) \cdot (g \cdot h), g \cdot h \,] \in A_g \circ A_h$. Současně $[\, (g \cdot h) \cdot (g \cdot h), g \cdot h \,] \in A_{g \cdot h}$, a tedy $A_g \circ A_h = A_{g \cdot h}$. Dokázali jsme, že ψ je

homomorfismus. Sami si dokažte, opět s využitím zákona o krácení, že zobrazení ψ je prosté.

Věta je dokázána.

5.3. Definice. Grupa $(\Gamma, \circ)$ konstruovaná v důkazu věty 5.2 se nazývá *podílová grupa grupoidu* $\mathcal{G}$. Vnoření ψ se nazývá *kanonické vnoření grupoidu* $\mathcal{G}$ *do jeho podílové grupy*.

Jelikož není nebezpečí nedorozumění, často označujeme operaci $\circ$ na Γ stejným symbolem jako operaci na grupoidu $\mathcal{G}$. Užíváme-li aditivní zápis operace, mluvíme o *rozdílové grupě* (místo podílové) a místo názvu zlomek se užívá název *rozdíl*.

Často se prvek $g \in G$ identifikuje se svým obrazem $\psi(g) = \{[\, g \cdot x, x \,] \mid x \in G\}$. Pologrupa $(G, \cdot)$ je potom podgrupoid své podílové grupy $(\Gamma, \cdot)$.

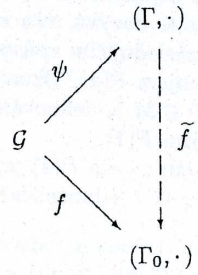
5.4. Poznámka. Jestliže pro $\alpha = [\, a, b \,]$, $\beta = [\, c, d \,] \in G \times G$ definujeme $\alpha \cdot \beta = [\, a \cdot c, b \cdot d \,]$, pak ekvivalence $\sim$ na $G \times G$ definovaná v důkazu věty 5.2 je kongruence na grupoidu $(G \times G, \cdot)$ a rozklad Γ je vytvořující rozklad na tomto grupoidu. Podílová grupa $(\Gamma, \cdot)$ je pak faktorgrupoid grupoidu $(G \times G, \cdot)$.

Všimněme si ještě, že pro $[\, a, b \,] \in A \in \Gamma$ platí $A = \psi(a) \cdot \psi(b)^{-1}$.

Mezi grupami, do kterých se dá uvažovaný grupoid vnořit, má podílová grupa význačné postavení charakterizované následující větou.

5.5. Věta. *Nechť $(\Gamma, \cdot)$ je podílová grupa asociativního a komutativního grupoidu $\mathcal{G} = (G, \cdot)$, ve kterém platí zákon o krácení. Nechť ψ je kanonické vnoření grupoidu $\mathcal{G}$ do grupoidu $(\Gamma, \cdot)$ a nechť f je homomorfismus grupoidu $\mathcal{G}$ do nějaké grupy $(\Gamma_0, \cdot)$. Pak existuje právě jeden homomorfismus $\tilde{f}$ grupy $(\Gamma, \cdot)$ do grupy $(\Gamma_0, \cdot)$ tak, že $\tilde{f} \circ \psi = f$. Jestliže f je vnoření, pak $\tilde{f}$ je taktéž vnoření.*

Můžeme pak říci, že diagram na obrázku 5 komutuje.



Obr. 5.

Důkaz. Ukážeme nejdříve, že pro $x, y \in G$ platí $f(x) \cdot f(y) = f(y) \cdot f(x)$ a $f(x) \cdot f(y)^{-1} = f(y)^{-1} \cdot f(x)$. Skutečně z $x \cdot y = y \cdot x$ plyne $f(x) \cdot f(y) = f(y) \cdot f(x)$, z čehož dostáváme taktéž $f(y)^{-1} \cdot f(x) = f(x) \cdot f(y)^{-1}$.

Nechť $A \in \Gamma$ je libovolné. Pro $\alpha = [\, a, b \,] \in A$, $\alpha_1 = [\, a_1, b_1 \,] \in A$ máme $\alpha \sim \alpha_1$, tudíž $b_1 \cdot a = a_1 \cdot b$, odkud plyne $f(b_1) \cdot f(a) = f(a_1) \cdot f(b)$, z čehož dostáváme

$f(a)\cdot f(b)^{-1} = f(b_1)^{-1}\cdot f(a_1) = f(a_1)\cdot f(b_1)^{-1}$. Hodnota $f(a)\cdot f(b)^{-1}$ závisí jen na třídě A a můžeme položit $\widetilde{f}(A) = f(a)\cdot f(b)^{-1}$. Pak $\widetilde{f}$ je zobrazení Γ do Γ_0.

Buď $A, B \in \Gamma$, $\alpha = [\,a,b\,] \in A$, $\beta = [\,c,d\,] \in B$. Pak $\widetilde{f}(A) = f(a)\cdot f(b)^{-1}$, $\widetilde{f}(B) = f(c)\cdot f(d)^{-1}$, a protože $[\,a\cdot c, b\cdot d\,] \in A\cdot B$, platí $\widetilde{f}(A\cdot B) = f(a\cdot c)\cdot$ $\cdot f(b\cdot d)^{-1} = f(a)\cdot f(c)\cdot [f(b)\cdot f(d)]^{-1} = f(a)\cdot f(c)\cdot [f(d)\cdot f(b)]^{-1} = f(a)\cdot f(c)\cdot$ $\cdot f(b)^{-1}\cdot f(d)^{-1} = f(a)\cdot f(b)^{-1}\cdot f(c)\cdot f(d)^{-1} = \widetilde{f}(A)\cdot\widetilde{f}(B)$. Zobrazení $\widetilde{f}$ je tudíž homomorfismus grupy $(\Gamma,\cdot)$ do $(\Gamma_0,\cdot)$.

Nechť $g \in G$. Pak $\psi(g) = \{[\,g\cdot x, x\,] \mid x \in G\}$, odkud plyne (položíme-li $x = g$) $(\widetilde{f}\circ\psi)(g) = f(g\cdot g)\cdot f(g)^{-1} = f(g)\cdot f(g)\cdot f(g)^{-1} = f(g)$. Tedy $\widetilde{f}\circ\psi = f$.

Buď $\widetilde{f}_1$ homomorfismus grupy $(\Gamma,\cdot)$ do $(\Gamma_0,\cdot)$ takový, že $\widetilde{f}_1\circ\psi = f$. Buď $A \in \Gamma, \alpha = [\,a,b\,] \in A$. Pak $\widetilde{f}(A) = f(a)\cdot f(b)^{-1} = \widetilde{f}_1(\psi(a))\cdot\widetilde{f}_1(\psi(b))^{-1} =$ $= \widetilde{f}_1(\psi(a))\cdot\widetilde{f}_1(\psi(b)^{-1}) = \widetilde{f}_1(\psi(a)\cdot\psi(b)^{-1}) = \widetilde{f}_1(A)$ (podle 5.4). Tudíž $\widetilde{f} = \widetilde{f}_1$.

Buď f injekce, $A, B \in \Gamma$, $\widetilde{f}(A) = \widetilde{f}(B)$, $[\,a,b\,] \in A$, $[\,c,d\,] \in B$. Potom $f(a)\cdot f(b)^{-1} = f(c)\cdot f(d)^{-1}$, tedy $f(b)^{-1}\cdot f(a) = f(c)\cdot f(d)^{-1}$. Odtud plyne $f(a)\cdot f(d) = f(b)\cdot f(c)$, a tedy $f(a\cdot d) = f(b\cdot c)$, z čehož díky tomu, že f je injekce, dostáváme $a\cdot d = b\cdot c$, $A = B$. Zobrazení $\widetilde{f}$ je tedy též injekce.

Věta je dokázána.

5.6. Poznámka. Věta 5.5 skutečně charakterizuje podílovou grupu, neboť lze dokázat i opačnou implikaci. Přesněji platí: *Nechť $f : G \to H$ je vnoření komutativního grupoidu $\mathcal{G} = (G,\cdot)$ do grupy $(H,\cdot)$ takové, že ke každému vnoření g grupoidu $\mathcal{G}$ do libovolné grupy $(H_0,\cdot)$ existuje jediné vnoření h grupy $(H,\cdot)$ do grupy $(H_0,\cdot)$ s vlastností $h\circ f = g$. Potom $(H,\cdot)$ je izomorfní podílové grupě grupoidu $\mathcal{G}$.*

5.7. Definice. Rozdílová grupa pologrupy $(\mathbb{N},+)$ se nazývá *aditivní grupa celých čísel* a značí se $(\mathbb{Z},+)$. Prvek množiny $\mathbb{Z}$ se nazývá *celé číslo*. Celé číslo je tedy třída ekvivalentních rozdílů $[\,a,b\,] \in \mathbb{N}\times\mathbb{N}$ pologrupy $(\mathbb{N},+)$.

Přirozené číslo $n \in \mathbb{N}$ identifikujeme s jeho obrazem v $\mathbb{Z}$ při kanonickém vnoření, tudíž $n = \{[\,n+x, x\,] \mid x \in \mathbb{N}\}$. Množina $\mathbb{N}$ je pak podmnožina $\mathbb{Z}$ a pologrupa $(\mathbb{N},+)$ je podgrupoid grupy $(\mathbb{Z},+)$. Připomeňme, že nulovým prvkem této grupy je třída $\{[\,x,x\,] \mid x \in \mathbb{N}\}$, která se označuje symbolem 0 a nazývá se *číslo nula* nebo jen *nula*. Pro $z \in \mathbb{Z}$ je $-z = \{[\,b,a\,] \mid [\,a,b\,] \in z\}$.

5.8. Definice. Na množině $\mathbb{Z}$ definujeme operaci *násobení* následujícím způsobem. Pro $\alpha,\beta \in \mathbb{Z}$, $[\,a,b\,] \in \alpha$, $[\,c,d\,] \in \beta$ klademe $\alpha\cdot\beta = \gamma$, kde $\gamma \in \mathbb{Z}$ je třída určená podmínkou $[\,ac+bd, ad+bc\,] \in \gamma$.

Jestliže $[u,v] \in \alpha, [r,s] \in \beta$ jsou jiní reprezentanti tříd α,β, pak $[a,b] \sim [u,v]$, $[\,c,d\,] \sim [\,r,s\,]$, tudíž $a+v = u+b$, $c+s = d+r$, odkud plyne $ca+cv = cu+cb$, $db+du = da+dv$, $uc+us = ud+ur$, $vd+vr = vc+vs$. Sečtením a užitím zákona o odečítání 4.7 dostaneme $ac+bd+us+vr = ad+bc+ur+sv$, což znamená, že rozdíly $[\,ac+bd, ad+bc\,]$ a $[\,ur+sv, us+vr\,]$ jsou ekvivalentní. Třída γ nezávisí tudíž na volbě reprezentantů tříd α,β. Definice operace násobení je tudíž korektní.

Zřejmě pro přirozená čísla α,β je součin $\alpha\cdot\beta$ roven dříve definovanému součinu na $\mathbb{N}$. Stejně jako na množině přirozených čísel při zápisu operace násobení často vynecháváme symbol $\cdot$, píšeme tedy $\alpha\beta$ místo $\alpha\cdot\beta$.

5.9. Tvrzení. *Grupoid $(\mathbb{Z},\cdot)$ je komutativní, asociativní a má jednotkový prvek, který je roven přirozenému číslu 1. Pro $\alpha,\beta,\gamma \in \mathbb{Z}, \gamma \neq 0$ platí*

$$\alpha\cdot\gamma = \beta\cdot\gamma \Longrightarrow \alpha = \beta$$

(tzv. omezený zákon o krácení).

Důkaz. Platnost komutativního zákona plyne ihned z definice.

Buď $\alpha,\beta,\gamma \in \mathbb{Z}, [\,a,b\,] \in \alpha, [\,c,d\,] \in \beta, [\,e,f\,] \in \gamma$.

Pak $[\,ac+bd, ad+bc\,] \in \alpha\cdot\beta$, $[\,ce+df, cf+de\,] \in \beta\cdot\gamma$. Tedy

$$[\,(ac+bd)e+(ad+bc)f, (ac+bd)f+(ad+bc)e\,] \in (\alpha\cdot\beta)\cdot\gamma,$$
$$[\,(ce+df)a+(cf+de)b, (ce+df)b+(cf+de)a\,] \in \alpha\cdot(\beta\cdot\gamma).$$

Jelikož se oba tyto rozdíly rovnají, platí $(\alpha\cdot\beta)\cdot\gamma = \alpha\cdot(\beta\cdot\gamma)$.

Nechť $x \in \mathbb{N}$. Pak $[\,1+x, x\,] \in 1$, tudíž $[\,a(1+x)+bx, b(1+x)+ax\,] \in 1\cdot\alpha$. Jelikož $[\,a(1+x)+bx, b(1+x)+ax\,] \sim [\,a,b\,]$, platí $1\cdot\alpha = \alpha$.

Nechť $\gamma \neq 0$ a $\alpha\cdot\gamma = \beta\cdot\gamma$. Pak $[\,ae+bf, af+be\,] \sim [\,ce+df, cf+de\,]$, tudíž $ae+bf+cf+de = af+be+ce+df$, odkud plyne

$$(a+d)e+(b+c)f = (b+c)e+(a+d)f \quad (*).$$

Jelikož $\gamma \neq 0$, platí $e \neq f$, a pak $e < f$ nebo $f < e$. Existuje tudíž $n \in \mathbb{N}$ tak, že $f = e+n$ nebo $e = f+n$. Dosazením do rovnosti $(*)$ dostaneme v obou případech pomocí zákona o odečítání 4.7 rovnost $n(b+c) = n(a+d)$, z čehož užitím 4.25 (b) plyne $b+c = a+d$, tedy $[\,a,b\,] \sim [\,c,d\,]$ a $\alpha = \beta$.

Tvrzení je tím dokázáno.

Sami si dokažte, že operace $+$ a $\cdot$ na $\mathbb{Z}$ jsou svázány distributivním zákonem, z čehož pak podle 5.9 plyne:

5.10. Věta. *Trojice $(\mathbb{Z},+,\cdot)$ je obor integrity, jehož jednotkový prvek je roven přirozenému číslu 1.*

5.11. Definice. Pro celá čísla α,β nechť $[\,a,b\,] \in \alpha, [\,c,d\,] \in \beta$. Položme $\alpha \leq \beta$, jestliže $a+d \leq b+c$.

Vztah $\alpha \leq \beta$ nezávisí na volbě reprezentantů tříd α,β: pokud $[\,u,v\,] \in \alpha$, $[\,r,s\,] \in \beta$, pak $[\,a,b\,] \sim [\,u,v\,], [\,c,d\,] \sim [\,r,s\,]$, tudíž $a+v = b+u$, $d+r = c+s$, odkud dostaneme sečtením $a+d+r+v = b+c+u+s$. Je-li $a+d = b+c$, pak $u+s = r+v$. Jestliže $a+d < b+c$, pak existuje přirozené číslo n tak, že platí $a+d+n = b+c$, tedy $r+v = u+s+n$, odkud plyne $u+s < r+v$. Ověřili jsme, že z $a+d \leq b+c$ plyne $u+s \leq r+v$; analogicky je možné ověřit opačnou implikaci. Výše uvedená definice relace $\leq$ je proto korektní.

Tím je definována na množině $\mathbb{Z}$ relace $\leq$, která zřejmě pro přirozená čísla souhlasí s dříve definovanou relací $\leq$ na množině $\mathbb{N}$. Pro celá čísla $\alpha, \beta \in \mathbb{Z}$ klademe $\alpha < \beta$, jestliže $\alpha \leq \beta$ a $\alpha \neq \beta$. O číslu α řekneme, že je *kladné* (resp. *záporné*), jestliže $0 < \alpha$ (resp. $\alpha < 0$). V opačném případě hovoříme o čísle *nekladném* (resp. *nezáporném*).

5.12. Věta. *Relace $\leq$ na množině $\mathbb{Z}$ je lineární uspořádání.*

Důkaz. Zřejmě je relace $\leq$ reflexivní. Nechť $\alpha, \beta, \gamma \in \mathbb{Z}$, $[a, b] \in \alpha$, $[c, d] \in \beta$, $[e, f] \in \gamma$.

Jestliže $\alpha \leq \beta$, $\beta \leq \alpha$, pak platí $a+d \leq b+c$, $b+c \leq a+d$, tudíž $a+d = b+c$, odkud plyne $[a, b] \sim [c, d]$, a tedy $\alpha = \beta$. Relace je antisymetrická.

Nechť $\alpha \leq \beta$, $\beta \leq \gamma$, potom $a+d \leq b+c$, $c+f \leq e+d$. Sečtením těchto nerovností (podle 4.12 (b), (d)) dostaneme $a+f \leq b+e$, tudíž $\alpha \leq \gamma$. Relace $\leq$ je tranzitivní.

Platí $a+d \leq b+c$ nebo $b+c \leq a+d$. V prvním případě dostaneme $\alpha \leq \beta$ a ve druhém $\beta \leq \alpha$. Relace $\leq$ je úplná.

Věta je tímto dokázána.

5.13. Tvrzení. *Při identifikaci provedené v 5.7 platí*

$\{z \in \mathbb{Z} \mid 0 < z\} = \mathbb{N}$,

$\{z \in \mathbb{Z} \mid z < 0\} = \{-n \mid n \in \mathbb{N}\}$.

Důkaz. Nechť $z \in \mathbb{N}$. Pak $[z+1, 1] \in z$, $[1, 1] \in 0$. Jelikož $1+1 < z+1+1$, platí $0 < z$.

Nechť $z \in \mathbb{Z}$, $0 < z$. Buď $[a, b] \in z$. Jelikož $[b, b] \in 0$, platí $b+b < a+b$, tudíž existuje $n \in \mathbb{N}$ tak, že $b+b+n = a+b$, odkud plyne $[a, b] \sim [n+b, b]$, tudíž $z = n \in \mathbb{N}$.

Dostáváme pak $\{z \in \mathbb{Z} \mid 0 < z\} = \mathbb{N}$.

Nechť existuje $n \in \mathbb{N}$ tak, že $z = -n$. Jelikož $[1, n+1] \in z$, $[1, 1] \in 0$ a $1+1 < 1+1+n$, pak platí $z < 0$.

Buď $z \in \mathbb{Z}$, $z < 0$, $[a, b] \in z$. Pak $a+b < b+b$, tudíž existuje přirozené číslo n tak, že $a+b+n = b+b$, odkud plyne $[a, b] \sim [b, b+n]$, tudíž $z = -n$.

Dostáváme pak $\{z \in \mathbb{Z} \mid z < 0\} = \{-n \mid n \in \mathbb{N}\}$.

5.14. Tvrzení. *Pro přirozené číslo $n \in \mathbb{N}$ položme $f(n) = -n$. Pak f je bijekce množiny $\mathbb{N}$ na množinu $\{-n \mid n \in \mathbb{N}\}$ s vlastností: $a, b \in \mathbb{N}$, $a \leq b \Longrightarrow f(b) \leq f(a)$.*

Důkaz. Pro $a, b \in \mathbb{N}$, $a < b$ platí nerovnost $a+a+a < a+b+a$. Jelikož $[a, a+a] \in -a$, $[a, a+b] \in -b$, pak $-b < -a$, tedy $f(b) < f(a)$. Odtud se již snadno dokáže, že f je bijekce splňující uvedenou podmínku.

5.15. Poznámka. Nechť $(P, \leq)$, $(Q, \leq)$ jsou lineárně uspořádané množiny, f bijekce P na Q. Zobrazení f se nazývá *antiizomorfismus uspořádané množiny* $(P, \leq)$ na $(Q, \leq)$, jestliže platí: $a, b \in P$, $a \leq b \Longrightarrow f(b) \leq f(a)$. Zobrazení f z 5.14 je tudíž antiizomorfismus uspořádané množiny $(\mathbb{N}, \leq)$ na uspořádanou množinu $(\{-n \mid n \in \mathbb{N}\}, \leq)$.

5.16. Věta. *Nechť $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Pak platí*

(a) $\alpha < \beta \Longleftrightarrow \alpha+\gamma < \beta+\gamma$,

(b) $\alpha \leq \beta \Longleftrightarrow \alpha+\gamma \leq \beta+\gamma$,

(c) *jestliže $\alpha < \beta, \gamma < \delta$ nebo $\alpha \leq \beta, \gamma < \delta$ nebo $\alpha < \beta, \gamma \leq \delta$, potom $\alpha+\gamma < \beta+\delta$,*

(d) $\alpha \leq \beta, \gamma \leq \delta \Longrightarrow \alpha+\gamma \leq \beta+\delta$,

(e) *pro $0 < \gamma$ platí: $\alpha < \beta \Longleftrightarrow \alpha \cdot \gamma < \beta \cdot \gamma$, $\alpha \leq \beta \Longleftrightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$,*

(f) *pro $\gamma < 0$ platí: $\alpha < \beta \Longleftrightarrow \beta \cdot \gamma < \alpha \cdot \gamma$, $\alpha \leq \beta \Longleftrightarrow \beta \cdot \gamma \leq \alpha \cdot \gamma$.*

Důkaz. Nechť $[a, b] \in \alpha$, $[c, d] \in \beta$, $[e, f] \in \gamma$.

Jestliže $\alpha < \beta$, pak $a+d < b+c$ a z 4.12 (a) plyne $a+e+d+f < b+f+c+e$. Jelikož $[a+e, b+f] \in \alpha+\gamma$, $[c+e, d+f] \in \beta+\gamma$, pak $\alpha+\gamma < \beta+\gamma$.

Je-li $\alpha+\gamma < \beta+\gamma$, potom podle předchozího $\alpha = (\alpha+\gamma)+(-\gamma) < (\beta+\gamma)+(-\gamma) = \beta$. Platí tudíž (a), odkud se snadno odvodí výroky (b), (c), (d).

Nechť $0 < \gamma$. Pak $f+f < e+f$ a z 4.12 (a) dostáváme $f < e$, tedy existuje $n \in \mathbb{N}$ tak, že $f+n = e$. Nerovnost $\alpha < \beta$ platí právě tehdy, když $a+d < b+c$, což nastane podle 4.25 (a) právě tehdy, když $(a+d)n < (b+c)n$. Tato nerovnost je ekvivalentní s nerovností $(a+d)e+(b+c)f < (b+c)e+(a+d)f$, která platí, právě když $\alpha \cdot \gamma < \beta \cdot \gamma$. Odtud pak plyne druhá ekvivalence ve výroku (e). Výrok (f) plyne z (e) a z tvrzení 5.14.

5.17. Definice. Pro celé číslo $\alpha \in \mathbb{Z}$ položíme

$$|\alpha| = \begin{cases} \alpha, & \text{pro } \alpha \geq 0, \\ -\alpha, & \text{pro } \alpha < 0, \end{cases}$$

$$\operatorname{sgn} \alpha = \begin{cases} 1, & \text{pro } \alpha > 0, \\ 0, & \text{pro } \alpha = 0, \\ -1, & \text{pro } \alpha < 0. \end{cases}$$

Číslo $|\alpha|$ se nazývá *absolutní hodnota čísla* α a zřejmě $|\alpha| \geq 0$. Číslo $\operatorname{sgn} \alpha$ se nazývá *znaménko (signum) čísla* α.

Zřejmě platí:

5.18. Tvrzení. *Pro $\alpha, \beta \in \mathbb{Z}$ platí $|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$, $|\alpha| = \alpha \cdot \operatorname{sgn} \alpha$, $\alpha = |\alpha| \cdot \operatorname{sgn} \alpha$.*

5.19. Věta (o dělení dvou celých čísel se zbytkem). *Nechť α, β jsou celá čísla, $\beta \neq 0$. Pak existují celá čísla γ, ϱ tak, že platí: $\alpha = \beta \cdot \gamma + \varrho$, $0 \leq \varrho < |\beta|$. Čísla γ, ϱ s těmito vlastnostmi jsou určena jednoznačně.*

Důkaz. Položme $\mathcal{M} = \{\alpha - \beta \cdot x \mid x \in \mathbb{Z}, \alpha - \beta \cdot x \geq 0\}$. Ukážeme, že $\alpha - \beta \cdot (-\operatorname{sgn} \beta) \cdot |\alpha| \in \mathcal{M}$. Skutečně $\alpha - \beta \cdot (-\operatorname{sgn} \beta) \cdot |\alpha| = \alpha + |\beta| \cdot |\alpha| \geq \alpha + |\alpha| \geq 0$, neboť $|\beta| \geq 1$. Tedy $\mathcal{M} \neq \emptyset$ a podle 4.15 má množina $\mathcal{M}$ nejmenší prvek ϱ. Pak existuje $\gamma \in \mathbb{Z}$ takové, že $\alpha - \beta\gamma = \varrho$, tedy $\alpha = \beta\gamma + \varrho$. Pokud $|\beta| \leq \varrho$, pak $0 \leq \varrho - |\beta| = \alpha - \beta(\gamma + \operatorname{sgn} \beta)$ a tudíž $\varrho - |\beta| \in \mathcal{M}$, což je spor, neboť ϱ byl nejmenší prvek $\mathcal{M}$. Odtud plyne $\varrho < |\beta|$.

Ukažme nyní jednoznačnost čísel γ, ϱ. Buďte $\gamma, \gamma_1, \varrho, \varrho_1 \in \mathbb{Z}$, $\alpha = \beta\gamma + \varrho = \beta\gamma_1 + \varrho_1$, $0 \leq \varrho < |\beta|$, $0 \leq \varrho_1 < |\beta|$, pak $\beta(\gamma - \gamma_1) = \varrho_1 - \varrho$. Vzhledem k $-|\beta| < -\varrho \leq 0$ máme $-|\beta| < \varrho_1 - \varrho < |\beta|$, tzn. $|\varrho_1 - \varrho| < |\beta|$. Odtud plyne $|\beta| > |\beta(\gamma - \gamma_1)| = |\beta| \cdot |\gamma - \gamma_1|$, což vzhledem k $|\beta| > 0$ dává $|\gamma - \gamma_1| < 1$. Tedy $\gamma = \gamma_1$, z čehož plyne také $\varrho = \varrho_1$.

Věta je dokázána.

5.20. Definice. Číslo γ z věty 5.19 se nazývá *(neúplný) podíl po dělení* čísla α číslem β a číslo ϱ se nazývá *zbytek po dělení* čísla α číslem β.

Jestliže zbytek po dělení čísla α číslem β je roven 0, říkáme, že číslo β *dělí* číslo α a píšeme $\beta \mid \alpha$. Číslo β se pak nazývá *dělitel* čísla α a číslo α *násobek* čísla β.

Každé číslo α má dělitele $1, -1, \alpha, -\alpha$. Tito dělitelé se nazývají *nevlastní dělitelé* čísla α, ostatní dělitelé se nazývají *vlastní dělitelé* čísla α. Zřejmě číslo 1 má pouze dva nevlastní dělitele. Jestliže celé číslo $p > 1$ nemá vlastní dělitele, nazývá se *prvočíslo*. Prvočísla jsou $2, 3, 5, 7, \ldots$. Dělitel celého čísla α, který je prvočíslem, se nazývá *prvočinitel* čísla α.

Z věty 5.19 o dělení dvou celých čísel se zbytkem se dá odvodit následující věta o jednoznačnosti rozkladu celého čísla na prvočinitele. Důkaz této věty lze nalézt např. v [4, věta 2.3. v kap. 3].

5.21. Základní věta aritmetiky celých čísel. *Každé celé číslo $m \neq 0$ lze jednoznačně, až na pořadí, psát ve tvaru $m = \varepsilon p_1^{a_1} \ldots p_k^{a_k}$, kde $p_1, \ldots, p_k$ jsou navzájem různá prvočísla, $a_1, \ldots, a_k$ přirozená čísla, $\varepsilon \in \{1, -1\}$ a $k \geq 0$ celé číslo.*

5.22. Poznámka. Výrazy typu $p_1^{a_1} \ldots p_k^{a_k}$, $\alpha_1 + \cdots + \alpha_k$ a pod. se definují rekurentně. Pro $k = 0$ rozumíme výrazem $\varepsilon p_1^{a_1} \ldots p_k^{a_k}$ číslo ε.

5.23. Definice. Pro celé číslo $m \neq 0$ se tvar čísla m v 5.21 nazývá *kanonický rozklad čísla m na prvočinitele*. Z 5.21 pak plyne, že množina prvočinitelů m je rovna množině $\{p_1, \ldots, p_k\}$.

Buď p prvočíslo. Jestliže p je prvočinitel čísla m, položme $v_p(m) = a_i$, kde $p = p_i$. Není-li p prvočinitel čísla m (tj. p nedělí m), položíme $v_p(m) = 0$. Hodnota $v_p(m)$ se nazývá *exponent čísla m příslušný prvočíslu p*.

Je tedy v_p zobrazení množiny celých nenulových čísel na množinu celých nezáporných čísel.

Pro celá nenulová čísla a, b a prvočíslo p platí $v_p(a \cdot b) = v_p(a) + v_p(b)$.

Dále pro $a, b \in \mathbb{Z}, a \neq 0 \neq b$ platí: $a = \pm b$ právě tehdy, když $v_p(a) = v_p(b)$ pro každé prvočíslo p.

Celé nenulové číslo m budeme často vyjadřovat ve tvaru tzv. *formálně nekonečného součinu*:

$$m = \varepsilon \prod_{p \in \mathcal{P}} p^{v_p(m)},$$

kde $\varepsilon \in \{1, -1\}$ a $\mathcal{P}$ je množina všech prvočísel. Uvědomte si, že všichni činitelé v tomto součinu s výjimkou konečně mnoha se rovnají jedné.