6. Těleso racionálních čísel

6.1. Definice. Nechť $\mathcal{R} = (R, +, \cdot)$, $\mathcal{S} = (S, +, \cdot)$ jsou okruhy. *Vnořením okruhu $\mathcal{R}$ do okruhu $\mathcal{S}$* rozumíme injektivní homomorfismus okruhu $\mathcal{R}$ do okruhu $\mathcal{S}$, tj. injektivní zobrazení f množiny R do množiny S takové, že pro libovolná $a, b \in R$ platí:

$$f(a+b) = f(a) + f(b), \quad f(a \cdot b) = f(a) \cdot f(b).$$

Jestliže existuje vnoření okruhu $\mathcal{R}$ do okruhu $\mathcal{S}$, řekneme, že *okruh $\mathcal{R}$ lze vnořit do okruhu $\mathcal{S}$* nebo že *okruh $\mathcal{R}$ je vnořen do okruhu $\mathcal{S}$*.

Vyřešme nyní otázku, kdy lze komutativní okruh vnořit do tělesa.

6.2. Věta. *Nechť $\mathcal{R} = (R, +, \cdot)$ je komutativní okruh. Pak následující výroky jsou ekvivalentní:*

(a) *V okruhu $\mathcal{R}$ platí omezený zákon o krácení, tj. pro libovolnou trojici $x, y, z \in R$, $x \neq 0$ takovou, že $x \cdot y = x \cdot z$, platí $y = z$.*

(b) *Okruh $\mathcal{R}$ lze vnořit do tělesa.*

Důkaz. Budeme postupovat jako v důkaze věty 5.2.

Nechť platí (b). Pak existuje těleso $\mathcal{T} = (T, +, \cdot)$ a vnoření $f : R \to T$. Buďte dále $x, y, z \in R, x \neq 0$ taková, že $x \cdot y = x \cdot z$. Pak $f(x) \cdot f(y) = f(x) \cdot f(z)$, $f(x) \neq 0$, tudíž $f(y) = f(z)$, odkud plyne rovnost $y = z$.

Předpokládejme nyní naopak, že v okruhu $\mathcal{R}$ platí omezený zákon o krácení. Jelikož nulový okruh lze vnořit do každého tělesa, můžeme předpokládat, že okruh $\mathcal{R}$ je nenulový.

Prvek $\alpha = [\, a, b \,] \in R \times (R - \{0\})$ nazveme *zlomkem okruhu $\mathcal{R}$*. Na množině všech zlomků $R \times (R - \{0\})$ okruhu $\mathcal{R}$ definujeme relaci $\sim$ následujícím způsobem: pro $\alpha = [\, a, b \,], \beta = [\, c, d \,] \in R \times (R - \{0\})$ položme

$$\alpha \sim \beta \iff a \cdot d = b \cdot c.$$

Promyslete si sami, že z komutativity násobení a z platnosti omezeného zákona o krácení plyne, že relace $\sim$ je ekvivalence na množině $R \times (R - \{0\})$. Rozklad příslušný této ekvivalenci označme T. Zlomky $\alpha, \beta \in R \times (R - \{0\})$ takové, že $\alpha \sim \beta$, nazveme *ekvivalentní*. Pro $A, B \in T$ nechť $[\, a, b \,] \in A, [\, c, d \,] \in B$ a nechť $C, D \in T$ jsou určeny podmínkami $[\, ad + bc, bd \,] \in C, [\, ac, bd \,] \in D$. Snadno se ukáže, že třídy C, D nezávisí na volbě reprezentantů tříd A a B. Skutečně, je-li též $[\, a', b' \,] \in A$, $[\, c', d' \,] \in B$, pak platí $a \cdot b' = a' \cdot b$, $c \cdot d' = c' \cdot d$, odkud plyne $(a \cdot c) \cdot (b' \cdot d') = (a' \cdot c') \cdot (b \cdot d)$, $(a \cdot d + b \cdot c) \cdot (b' \cdot d') = (a' \cdot d' + b' \cdot c') \cdot (b \cdot d)$, tedy i $[\, a' \cdot d' + b' \cdot c', b' \cdot d' \,] \in C$, $[\, a' \cdot c', b' \cdot d' \,] \in D$. Můžeme proto položit

$$A + B = C, \quad A \cdot B = D.$$

Tím jsou na množině T definovány operace $+$ a $\cdot$ a snadno se zjistí, že $\mathcal{T} = (T, +, \cdot)$ je těleso. Jednotkovým prvkem tohoto tělesa je třída $E = \{[\, r, r \,] \mid r \in R - \{0\}\}$

a nulovým prvkem je třída $\{[\,0,r\,] \mid r \in R - \{0\}\}$. Pro $A \in \mathcal{T}$ je opačným prvkem třída $-A = \{[\,-a,b\,] \mid [\,a,b\,] \in A\}$. Inverzním prvkem pro $A \in \mathcal{T}$, $A \neq 0$ je třída $A^{-1} = \{[\,b,a\,] \mid [\,a,b\,] \in A\}$.

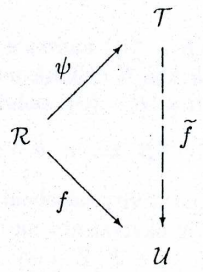
Pro $r \in R$ je množina $A_r = \{[\,r \cdot x, x\,] \mid x \in R - \{0\}\}$ prvkem rozkladu T. Promyslete si sami, že zobrazení $\psi : R \to T$ definované vztahem $\psi(r) = A_r$ pro libovolné $r \in R$ je vnořením okruhu $\mathcal{R}$ do tělesa $\mathcal{T}$ (pro důkaz injektivity ψ je třeba využít omezeného zákona o krácení). Věta je tím dokázána.

6.3. Definice. Pro nenulový komutativní okruh $\mathcal{R}$ nazveme těleso $\mathcal{T}$ konstruované podle důkazu věty 6.2 *podílové těleso okruhu* $\mathcal{R}$. Uvedené vnoření ψ nazveme *kanonické vnoření okruhu* $\mathcal{R}$ *do jeho podílového tělesa*. Pro $[\,a,b\,] \in A \in T$ zřejmě platí: $A = \psi(a) \cdot \psi(b)^{-1}$. Prvek r z okruhu $\mathcal{R}$ se ztotožňuje se svým obrazem $\psi(r)$ v podílovém tělese. Na základě tohoto ztotožnění můžeme považovat okruh $\mathcal{R}$ za podokruh jeho podílového tělesa $\mathcal{T}$.

Podílové těleso má význačné postavení mezi tělesy, do kterých lze okruh vnořit. Tato vlastnost je charakterizována následující větou.

6.4. Věta. *Nechť $\mathcal{T}$ je podílové těleso nenulového komutativního okruhu $\mathcal{R}$ s omezeným zákonem o krácení a nechť ψ je kanonické vnoření $\mathcal{R}$ do $\mathcal{T}$. Buď f vnoření okruhu $\mathcal{R}$ do nějakého tělesa $\mathcal{U}$. Pak existuje jediné vnoření $\tilde{f}$ tělesa $\mathcal{T}$ do tělesa $\mathcal{U}$ takové, že $\tilde{f} \circ \psi = f$.*

Můžeme říci, že diagram na obrázku 6 komutuje.



Obr. 6.

Důkaz. Nechť $\mathcal{R} = (R,+,\cdot), \mathcal{T} = (T,+,\cdot), \mathcal{U} = (U,+,\cdot)$.

Protože homomorfismus f je prostý, a protože $f(0) = 0$, existuje pro libovolné $x \in R$, $x \neq 0$ inverze prvku $f(x)$ v tělese $\mathcal{U}$.

Buď $A \in T$, $[\,a,b\,]$, $[\,c,d\,] \in A$. Potom $a \cdot d = b \cdot c$, odkud plyne $f(a) \cdot f(d) = f(b) \cdot f(c)$, tudíž $f(a) \cdot f(b)^{-1} = f(b)^{-1} \cdot f(a) = f(c) \cdot f(d)^{-1}$. Můžeme proto korektně definovat zobrazení $\tilde{f}$ množiny T do množiny U vztahem

$$\tilde{f}(A) = f(a) \cdot f(b)^{-1}.$$

Promyslete si sami, že z toho, že f je vnoření okruhu $\mathcal{R}$ do tělesa $\mathcal{U}$ plyne, že $\tilde{f}$ je vnořením tělesa $\mathcal{T}$ do tělesa $\mathcal{U}$ a platí: $\tilde{f} \circ \psi = f$.

Dokážeme, že $\tilde{f}$ je jediné vnoření s požadovanou vlastností. Nechť g je vnoření tělesa $\mathcal{T}$ do tělesa $\mathcal{U}$ takové, že platí: $g \circ \psi = f$. Buď $[\,a,b\,] \in A \in T$. Potom $\tilde{f}(A) = f(a) \cdot f(b)^{-1} = g(\psi(a)) \cdot [g(\psi(b))]^{-1} = g(\psi(a) \cdot \psi(b)^{-1}) = g(A)$. Dostáváme pak $\tilde{f} = g$ a věta je dokázána.

6.5. Poznámka. Podobně jako v případě grup podmínka v předchozí větě skutečně charakterizuje podílové těleso, neboť platí následující: *Buď f vnoření komutativního okruhu $\mathcal{R}$ do tělesa $\mathcal{T}$ takové, že ke každému vnoření g okruhu $\mathcal{R}$ do tělesa $\mathcal{U}$ existuje vnoření $\tilde{g}$ tělesa $\mathcal{T}$ do tělesa $\mathcal{U}$ s vlastností $\tilde{g} \circ f = g$. Potom $\mathcal{T}$ je izomorfní podílovému tělesu okruhu $\mathcal{R}$.*

6.6. Definice. Podílové těleso okruhu celých čísel $(\mathbb{Z},+,\cdot)$ se nazývá *těleso racionálních čísel* a značí se $(\mathbb{Q},+,\cdot)$. Prvek tělesa $(\mathbb{Q},+,\cdot)$ se nazývá *racionální číslo*.

6.7. Poznámka. Můžeme tudíž říci, že racionální číslo je třídou ekvivalentních zlomků okruhu celých čísel. Celé číslo $z \in \mathbb{Z}$ se identifikuje se svým obrazem v $\mathbb{Q}$ při kanonickém vnoření, tedy celé číslo se považuje za číslo racionální: $\mathbb{Z} \subseteq \mathbb{Q}$. Okruh celých čísel je pak podokruhem tělesa racionálních čísel.

Pro $A \in \mathbb{Q}, [\,a,b\,] \in A$ dostáváme

$$A = a \cdot b^{-1} = \frac{a}{b}.$$

Každé racionální číslo lze tudíž psát ve tvaru $\frac{a}{b}$, kde $a,b \in \mathbb{Z}, b \neq 0$.

Těleso racionálních čísel se často značí pouze symbolem $\mathbb{Q}$.

6.8. Definice. Nechť $A,B \in \mathbb{Q}$ jsou libovolné a $[\,a,b\,] \in A, [\,c,d\,] \in B$. Jelikož $[\,a,b\,] \sim [\,-a,-b\,]$ a $[\,c,d\,] \sim [\,-c,-d\,]$, můžeme předpokládat, že $b > 0, d > 0$. Položíme nyní

$$A \leq B \iff a \cdot d \leq b \cdot c.$$

Uvedená definice nezávisí na volbě reprezentantů tříd A,B. Skutečně, je-li též $[\,k,l\,] \in A, [\,m,n\,] \in B, l > 0, n > 0$, pak $k \cdot b = a \cdot l, m \cdot d = c \cdot n$. Z $a \cdot d \leq b \cdot c$ pak vynásobením číslem $l \cdot n > 0$ podle 5.16 (e) plyne $l \cdot n \cdot a \cdot d \leq l \cdot n \cdot b \cdot c$ a dosazením dostaneme $k \cdot n \cdot b \cdot d \leq l \cdot m \cdot b \cdot d$. Opět dle 5.16 (e) máme $k \cdot n \leq l \cdot m$, neboť $b \cdot d > 0$.

Tím je tedy definována relace $\leq$ na množině $\mathbb{Q}$.

6.9. Věta. *Relace $\leq$ na množině $\mathbb{Q}$ je lineární uspořádání. Pro celá čísla je tato relace rovna dříve definované relaci $\leq$ na množině $\mathbb{Z}$.*

Důkaz. Reflexivita relace $\leq$ je zřejmá.

Buďte $A,B,C \in \mathbb{Q}$, $[\,a,b\,] \in A$, $[\,c,d\,] \in B$, $[\,e,f\,] \in C$, kde $b > 0, d > 0, f > 0$.

Jestliže $A \leq B$ a $B \leq A$, pak $ad \leq bc, bc \leq ad$, tedy $ad = bc$, odkud plyne $[\,a,b\,] \sim [\,c,d\,]$. Pak $A = B$ a relace $\leq$ je tudíž antisymetrická.

Závěrem tohoto odstavce si provedeme úplnou diskusi řešení binomické rovnice v okruhu celých čísel a tělese racionálních čísel.

6.19. Tvrzení. *Nechť $\mathcal{R} = (R, +, \cdot)$ je okruh celých čísel nebo těleso racionálních čísel, n přirozené číslo, $\alpha \in R, \alpha < 0$.*

Je-li n sudé číslo, pak binomická rovnice $x^n = \alpha$ nemá žádné řešení v okruhu $\mathcal{R}$.

Je-li n liché číslo, pak $\beta \in R$ je řešením binomické rovnice $x^n = \alpha$ v $\mathcal{R}$ právě tehdy, když $-\beta$ je řešením binomické rovnice $x^n = -\alpha$ v okruhu $\mathcal{R}$.

Důkaz. Nechť n je sudé, tedy $n = 2m$, kde m je přirozené číslo. Jestliže existuje $\beta \in R$ takové, že $\beta^n = \alpha$, pak $\gamma^2 = \alpha$, kde $\gamma = \beta^m \in R$. Podle 6.10 (e), (f) je pak $0 \leq \gamma^2 = \alpha$, což je spor. Tudíž binomická rovnice $x^n = \alpha$ nemá v $\mathcal{R}$ řešení.

Nechť n je liché a $\beta \in R$. Je-li β řešení rovnice $x^n = \alpha$, pak $\beta^n = \alpha$ a jelikož $(-1)^n = -1$, dostáváme $(-\beta)^n = -\alpha$. Tedy $-\beta$ je řešení rovnice $x^n = -\alpha$.

Je-li $-\beta$ řešením rovnice $x^n = -\alpha$, pak $-\alpha = (-\beta)^n = (-1)^n\beta^n = -\beta^n$, tudíž $\beta^n = \alpha$ a β je řešením rovnice $x^n = \alpha$. Tvrzení je tím dokázáno.

6.20. Poznámka. Podle 6.18 a 6.19 se můžeme v okruhu celých čísel a tělese racionálních čísel omezit jen na binomické rovnice s „kladnou pravou stranou". Diskuse řešení těchto rovnic je provedena v následující větě.

6.21. Věta. *Nechť $\mathcal{R} = (R, +, \cdot)$ je okruh celých čísel nebo těleso racionálních čísel, n přirozené číslo, $\alpha \in R, \alpha > 0$. Binomická rovnice $x^n = \alpha$ je řešitelná v $\mathcal{R}$ právě tehdy, když $n \mid v_p(a)$ pro každé prvočíslo p. V tomto případě má rovnice $x^n = \alpha$ právě jedno řešení β s vlastností $\beta > 0$. Toto β je rovno číslu*

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

kde $m(p) = \frac{1}{n} v_p(\alpha)$.

Je-li n liché, pak číslo β je jediným řešením rovnice $x^n = \alpha$.

Je-li n sudé, pak rovnice $x^n = \alpha$ má právě dvě řešení β a $-\beta$.

Důkaz. Předpokládejme nejprve, že $\beta \in R$ je řešením rovnice $x^n = \alpha$. Pak

$$\prod_{p \in \mathcal{P}} p^{v_p(\alpha)} = \alpha = \beta^n = \pm \prod_{p \in \mathcal{P}} p^{n v_p(\beta)}$$

a z jednoznačnosti vyjádření racionálního čísla pomocí formálně nekonečného součinu (věta 6.16) pak plyne $v_p(\alpha) = n v_p(\beta)$, tedy $n \mid v_p(\alpha)$ pro každé prvočíslo p. Uvědomme si, že opět podle 6.16 je touto podmínkou číslo β až na znaménko jednoznačně určeno.

Předpokládejme nyní naopak, že pro každé prvočíslo p platí $n \mid v_p(\alpha)$. Položíme $m(p) = \frac{1}{n} v_p(\alpha)$ a $\beta = \prod_{p \in \mathcal{P}} p^{m(p)}$. Pak $\beta \in R, \beta > 0, \beta^n = \alpha$, a tedy β je řešením rovnice $x^n = \alpha$.

Je-li n sudé, pak zřejmě $(-\beta)^n = \beta^n = \alpha$. Nechť $\gamma \in R, \gamma < 0, \gamma^n = \alpha$. Je-li n sudé, pak $-\gamma > 0, (-\gamma)^n = \alpha$, tudíž $-\gamma = \beta$ a $\gamma = -\beta$. Je-li n liché, pak $\gamma^n < 0$, což je spor. Věta je tím dokázána.

6.22. Příklad. Nechť n je přirozené číslo větší než 1. Jelikož pro každé prvočíslo p je $v_p(p) = 1$ a $n \nmid 1$, nemá binomická rovnice $x^n = p$ v okruhu celých čísel ani tělese racionálních čísel žádné řešení.

6.23. Cvičení.

1) Lze okruh $(\mathbb{Z}_6, +, \cdot)$, resp. $(\mathbb{Z}_7, +, \cdot)$, vnořit do tělesa? Pokud ano, popište podílové těleso. Pokud ne, zdůvodněte, proč podílové těleso zkonstruovat nelze.

2) Uvažme okruhy $\mathbb{Z}[x]$ (resp. $\mathbb{Q}[x]$) polynomů s celočíselnými (resp. racionálními) koeficienty. Tvoří $\mathbb{Z}[x]$ nebo $\mathbb{Q}[x]$ těleso? Popište jejich podílová tělesa.

3) Dokažte, že v okruhu $\mathcal{R} = (R, +, \cdot)$ platí omezený zákon o krácení právě tehdy, když $\mathcal{R}$ neobsahuje dělitele nuly, tj. když pro každé $x, y \in R$ z toho, že $x \cdot y = 0$, plyne $x = 0$ nebo $y = 0$.

4) Ve větě 6.4 jsme na rozdíl od věty 5.5 požadovali navíc injektivitu zobrazení f. Promyslete si, proč bez této podmínky nelze větu dokázat. Zkonstruujte neinjektivní homomorfismus f z okruhu $\mathbb{Z}$ do vhodného tělesa $\mathcal{T}$ a dokažte, že neexistuje $\tilde{f} : \mathbb{Q} \to \mathcal{T}$ požadovaných vlastností.

5) Dokažte tvrzení uvedené v poznámce 6.5.

6) a) V definici 6.8 relace $\leq$ na množině $\mathbb{Q}$ jsme předpokládali $b > 0$, $d > 0$. Rozmyslete si, co je na následujícím textu, kde jsou tyto podmínky vypuštěny, špatně. Na množině $\mathbb{Q}$ pro $[a, b] \in A, [c, d] \in B$ zavedeme relaci $\lhd$ podmínkou

$$A \lhd B \iff a \cdot d \leq b \cdot c.$$

b) Na množině $\mathbb{Q}$ budeme definovat relaci $\lhd$ podmínkou: $A \lhd B$ právě tehdy, když existují reprezentanti $[a, b] \in A, [c, d] \in B$ tak, že $a \cdot d \leq b \cdot c$. Jaké vlastnosti relace $\lhd$ splňuje? (Je to relace reflexivní, symetrická, antisymetrická, tranzitivní, úplná?)

7) Označme $M = \{\alpha \in \mathbb{Q} \mid 0 < \alpha \leq 1 \vee 2 < \alpha \leq 3\}$. Rozhodněte, zda $(M, \leq)$ a $(M \cup \{2\}, \leq)$ jsou hustě uspořádané množiny, kde $\leq$ je uspořádání racionálních čísel (přesněji jeho zúžení na dané množiny).

8) Nechť $(M, \leq)$ je konečná lineárně uspořádaná množina. Dokažte, že $(M, \leq)$ není hustě uspořádaná.

9) Nechť $A = \{\frac{m}{2^n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$. Dokažte, že $(A, \leq)$, kde $\leq$ je uspořádání racionálních čísel, je hustě uspořádaná množina.

10) Buď p prvočíslo a α, β libovolná racionální čísla, taková, že $\alpha \neq 0$, $\beta \neq 0$, $\alpha + \beta \neq 0$. Dokažte, že pak platí $v_p(\alpha + \beta) \geq \min\{v_p(\alpha), v_p(\beta)\}$.

Nechť $A \leq B$, $B \leq C$. Pak $ad \leq bc$, $cf \leq ed$, odkud podle 5.16 (e) dostáváme $adf \leq bcf, bcf \leq bed$ a tudíž $adf \leq bed$. Odtud opět podle 5.16 (e) dostáváme $af \leq be$, tudíž $A \leq C$. Relace $\leq$ je tranzitivní.

Z 5.12 plyne, že buď $ad \leq bc$ nebo $bc \leq ad$. V prvním případě dostaneme $A \leq B$, v druhém $B \leq A$. Relace $\leq$ je tedy lineárním uspořádáním na $\mathbb{Q}$.

Nechť jsou $A, B \in \mathbb{Z}$. Pak pro libovolné $x \in \mathbb{Z}$, $x > 0$ platí $[\, ax, x \,] \in A = a$, $[\, bx, x \,] \in B = b$. Podle 5.16 (e) je $a \leq b$ v původně definované relaci $\leq$ na $\mathbb{Z}$, právě když $ax^2 \leq bx^2$, tudíž právě když $A \leq B$. Věta je tím dokázána.

6.10. Věta. *Nechť $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$. Pak platí:*

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

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

(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: $\alpha < \beta \iff \alpha \cdot \gamma < \beta \cdot \gamma$, $\alpha \leq \beta \iff \alpha \cdot \gamma \leq \beta \cdot \gamma$,*

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

Důkaz. Nechť $[\, a, b \,] \in \alpha, [\, c, d \,] \in \beta, [\, e, f \,] \in \gamma, b > 0, d > 0, f > 0$. V průběhu důkazu užijeme několikrát větu 5.16, promyslete si sami kdy. Nejprve dokážeme platnost výroku (a).

Jestliže $\alpha < \beta$, pak $ad < bc$. Dále $[\, af + be, bf \,] \in \alpha + \gamma$, $[\, cf + ed, df \,] \in \beta + \gamma$. Platí $(af + be)fd = af^2d + befd < bf^2c + befd = bf(cf + ed)$, tudíž $\alpha + \gamma < \beta + \gamma$.

Naopak, jestliže platí $\alpha + \gamma < \beta + \gamma$, pak podle předešlého dostáváme nerovnost $\alpha = \alpha + \gamma + (-\gamma) < \beta + \gamma + (-\gamma) = \beta$.

Platí tedy (a). Odtud se snadno odvodí platnost výroků (b), (c) a (d).

Nyní dokážeme platnost výroku (e). Nechť $0 < \gamma$. Jelikož $[\, 0, 1 \,] \in 0$, platí, že $0 \cdot f < 1 \cdot e$, tedy $e > 0$.

Je-li $\alpha < \beta$, pak $ad < bc$, tudíž $adef < bcef$, odkud plyne $\alpha \cdot \gamma < \beta \cdot \gamma$.

Naopak předpokládejme, že $\alpha \cdot \gamma < \beta \cdot \gamma$. Jelikož $[\, f, e \,] \in \gamma^{-1}$, je $0 < \gamma^{-1}$ a podle předešlého tedy $\alpha = (\alpha \cdot \gamma) \cdot \gamma^{-1} < (\beta \cdot \gamma) \cdot \gamma^{-1} = \beta$.

Platnost ekvivalence $\alpha \leq \beta \iff \alpha \cdot \gamma \leq \beta \cdot \gamma$ pak již z předešlého zřejmě vyplývá. Platí tedy výrok (e).

Výrok (f) se snadno odvodí z implikace $\gamma < 0 \Longrightarrow 0 < -\gamma$, která plyne například z (a). Věta je tím dokázána.

6.11. Definice. Lineárně uspořádaná množina $(M, \leq)$ se nazývá *hustě uspořádaná*, jestliže má alespoň dva prvky a platí:

$$m_1 \in M, m_2 \in M, m_1 < m_2 \Longrightarrow \exists\, m \in M : m_1 < m < m_2.$$

6.12. Tvrzení. *Množina racionálních čísel $(\mathbb{Q}, \leq)$ je hustě uspořádaná.*

Důkaz. Nechť $[\, a, b \,] \in \alpha \in \mathbb{Q}$, $[\, c, d \,] \in \beta \in \mathbb{Q}$, $b > 0$, $d > 0$, $\alpha < \beta$. Pak $ad < bc$, odkud plyne $ad + 1 \leq bc$, tudíž $2ad + 1 < 2ad + 2 \leq 2bc$. Nechť $\gamma \in \mathbb{Q}$,

$[\, 2ad + 1, 2bd \,] \in \gamma$. Jelikož $2abd < 2abd + b$, je $\alpha < \gamma$. Obdobně $(2ad + 1)d < 2bcd$, tudíž $\gamma < \beta$. Tvrzení je tím dokázáno.

6.13. Příklad. Množina celých čísel $(\mathbb{Z}, \leq)$ není hustě uspořádaná, neboť např. pro $m_1 = 1$ a $m_2 = 2$ neexistuje $m \in \mathbb{Z}$ takové, aby $1 < m < 2$.

6.14. Tvrzení. *Pro každé číslo $\varrho \in \mathbb{Q}$ existuje přirozené číslo n takové, že $-n < \varrho < n$.*

Důkaz. Nechť $[\, a, b \,] \in \varrho, b > 0$. Položme $n = |a| + 1$. Pak n je přirozené číslo a platí $bn \geq n > |a| \geq a$, odkud plyne $\varrho < n$, neboť $[\, n, 1 \,] \in n$. Z nerovnosti $|a| < bn$ dostáváme $-bn < -|a| \leq a$. Protože $[\, -n, 1 \,] \in -n$, je $-n < \varrho$.

6.15. Definice. Nechť p je prvočíslo, $[\, a, b \,] \in \varrho \in \mathbb{Q}$, $\varrho \neq 0$. Pak definujeme *exponent čísla ϱ příslušný prvočíslu p* takto:

$$v_p(\varrho) = v_p(a) - v_p(b).$$

Tato definice je korektní, neboť pokud $[\, c, d \,] \in \varrho$, pak $a \neq 0 \neq c$, $a \cdot d = b \cdot c$. Podle 5.23 tudíž $v_p(a) + v_p(d) = v_p(b) + v_p(c)$, odkud $v_p(a) - v_p(b) = v_p(c) - v_p(d)$. Číslo $v_p(a) - v_p(b)$ nezávisí na volbě reprezentanta $[\, a, b \,]$ racionálního čísla ϱ.

Potom v_p je zobrazení množiny nenulových racionálních čísel na množinu celých čísel.

Pro nenulová racionální čísla α, β a prvočíslo p pak zřejmě platí:

$$v_p(\alpha \cdot \beta) = v_p(\alpha) + v_p(\beta).$$

Dále pro $\alpha, \beta \in \mathbb{Q}, \alpha \neq 0 \neq \beta$ máme: $\alpha = \pm\beta$ právě tehdy, když $v_p(\alpha) = v_p(\beta)$ pro každé prvočíslo p.

Ze základní věty aritmetiky celých čísel 5.21 se snadno odvodí následující věta.

6.16. Věta. *Každé nenulové racionální číslo α lze jednoznačně psát ve tvaru formálně nekonečného součinu*

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

kde $\varepsilon = \in \{1, -1\}$, $\mathcal{P}$ je množina všech prvočísel, $v_p(\alpha) \neq 0$ jen pro konečně mnoho prvočísel p.

6.17. Definice. Nechť $\mathcal{R} = (R, +, \cdot)$ je okruh, $a \in R$ a n přirozené číslo. *Binomickou rovnicí n-tého stupně* v okruhu $\mathcal{R}$ rozumíme rovnici tvaru:

$$x^n = a.$$

Zřejmě platí následující tvrzení:

6.18. Tvrzení. *Pro obor integrity $\mathcal{R}$ má binomická rovnice $x^n = 0$, kde n je přirozené číslo, právě jedno řešení $x = 0$.*