9. Podílová tělesa

O prvku a komutativního okruhu $R = R(+,\cdot,-,\mathbf{0},\mathbf{1})$ řekneme, že je *dělitel nuly*, jestliže $a \neq \mathbf{0}$ a existuje $b \in R$, $b \neq \mathbf{0}$ takové, že $ab = \mathbf{0}$. Okruh $R = R(+,\cdot,-,\mathbf{0},\mathbf{1})$, který je komutativní, není triviální a je bez dělitelů nuly, se nazývá *obor integrity.* Všimněte si, že netriviální komutativní okruh R je oborem integrity právě když $R^{\#} = R \backslash \{\mathbf{0}\}$ je podmonoid $R(\cdot,\mathbf{1})$.

Je-li R obor integrity a $a,b,c \in R^{\#}$, tak z $ab = ac$ plyne $a(b-c) = 0$, odkud $b - c = 0$, a tedy $b = c$. To znamená, že $R^{\#}(\cdot,\mathbf{1})$ je komutativní monoid s krácením.

9.1 Lemma. *Konečný obor integrity je komutativní těleso.*

Důkaz. Ať R je konečný obor integrity a $a \in R$, $a \neq \mathbf{0}$. Zobrazení $x \mapsto ax$ je injektivní, a protože R je konečné, je to permutace R. Proto existuje $b \in R$, že $ab = \mathbf{1}$. $\square$

Buď nyní $R = R(+,\cdot,-,0,1)$ obor integrity. Na množině $F = R \times R^{\#}$ budeme definovat algebru $F = F(+,\cdot,-,\mathbf{0},\mathbf{1})$. Pro přehlednost budeme uspořádané dvojice $(a,b) \in R \times R^{\#} = F$ zapisovat $\frac{a}{b}$. Buď $a,c \in R$ a $b,d \in R^{\#}$. Definujeme

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad+bc}{bd}, \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}, \\ -\frac{a}{b} &= \frac{-a}{b}, \\ \mathbf{0} &= \frac{0}{1}, \\ \mathbf{1} &= \frac{1}{1}. \end{aligned}$$

9.2 Lemma. *$F(+,\mathbf{0})$ a $F(\cdot,\mathbf{1})$ jsou komutativní monidy.*

Důkaz. Komutativita je zřejmá přímo z definice. Buď $a \in R$ a $b \in R^{\#}$. Pak $\frac{a}{b} + \frac{0}{1} = \frac{a\cdot 1 + b \cdot 0}{b \cdot 1} = \frac{a}{b}$ a $\frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}$, takže $\mathbf{0}$ a $\mathbf{1}$ jsou neutrálními prvky. Pro násobení asociativita plyne rovněž okamžitě z definice. Ověřme asociativitu sčítání. Buď $a,c,e \in R$ a $b,d,f \in R^{\#}$. Pak $(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{adf+bcf+bde}{bdf} = \frac{a}{b} + \frac{cf+de}{df} = \frac{a}{b} + (\frac{c}{d} + \frac{e}{f})$. $\square$

Na F definujeme ekvivalenci $\sim$ tak, že $\frac{a}{b} \sim \frac{c}{d}$ právě když $ad = bc$.

9.3 Lemma. *$\sim$ je kongruence F.*

Důkaz. Nejprve je třeba ověřit, že $\sim$ je vskutku ekvivalence. Reflexivita a symetrie je jasná. Ať $\frac{a}{b} \sim \frac{c}{d}$ a $\frac{c}{d} \sim \frac{e}{f}$. Pak $acf = ade = bce$, čili $af = be$. Nyní je třeba ověřit, že $\sim$ je kongruence. Buď $\frac{a}{b} \sim \frac{c}{d}$. Pak jistě $-\frac{a}{b} \sim -\frac{c}{d}$. Buď ještě $\frac{e}{f} \sim \frac{g}{h}$. Pak $\frac{a}{b} + \frac{e}{f} = \frac{af+be}{bf}$ a $\frac{c}{d} + \frac{g}{h} = \frac{ch+dg}{dh}$. Ovšem $afdh + bedh = adfh + bdeh = bcfh + bdfg = bfch + bfdg$, takže $\frac{a}{b} + \frac{e}{f} \sim \frac{c}{d} + \frac{g}{h}$. Podobně z $adeh = bcfg$ plyne $\frac{a}{b} \cdot \frac{e}{f} \sim \frac{c}{d} \cdot \frac{g}{h}$. $\square$

Očividně platí

9.4 Lemma. *Buď $a \in R^{\#}$. Potom $\frac{0}{a} \sim \mathbf{0}$ a $\frac{a}{a} \sim \mathbf{1}$.*

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

9.5 Lemma. *$F/\sim$ je komutativní okruh.*

Důkaz. Podle 9.2 stačí ověřit, že unární minus poskytuje opačné prvky, a ověřit distributivní zákon. Buď $a \in R$ a $b \in R^{\#}$. Pak $\frac{a}{b} + (-\frac{a}{b}) = \frac{ab-ab}{bb} \sim \mathbf{0}$. Buď ještě $c, e \in R$ a $d, f \in R^{\#}$. Pak $\frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{acf+ade}{bdf} \sim \frac{abcf+abde}{bbdf} = \frac{ac}{bd} + \frac{ae}{bf}$. $\square$

Z 9.4 dostáváme:

9.6 Lemma. *Buď $a, b \in R^{\#}$. Pak $\frac{a}{b} \cdot \frac{b}{a} \sim \mathbf{1}$.*

Formálně správnější (ale méně přehledné) by bylo v předchozím textu místo $\frac{a}{b}$ psát (a, b). Představme si, že jsme zvolili tento formálně korektnější postup a nyní definujeme $\frac{a}{b} = [(a, b)]_{\sim}$. Čili od této chvíle zlomkem $\frac{a}{b}$ označujeme celou ekvivalenční třídu $\sim$. (Koneckonců v tomto významu zlomky používáme běžně – to, že $\frac{2}{6} = \frac{1}{3}$ překvapí jen málokoho.)

Z 9.5 a 9.6 plyne, že $T = F/\sim$ je komutativní těleso. Toto těleso se nazývá *podílovým tělesem* oboru integrity R. Je tvořeno všemi zlomky $\frac{a}{b}$, kde $a \in R$ a $b \in R^{\#}$.

9.7 Tvrzení. *Buď R obor integrity a T jeho podílové těleso. Definujme zobrazení $\sigma : R \to T$ tak, že $\sigma(r) = \frac{r}{1}$. Platí, že σ je injektivní homomorfismus okruhů.*

Důkaz. Zjevně $\frac{r}{1} + \frac{s}{1} = \frac{r+s}{1}$, $\frac{r}{1} \cdot \frac{s}{1} = \frac{rs}{1}$ atd., takže σ je homomorfismus. Přitom $\frac{r}{1} = \frac{s}{1}$ právě když $r = s$, a proto je σ prosté. $\square$

Ztotožníme-li, jak je obvyklé, každý prvek $r \in R$ s $\frac{r}{1} \in T$, plyne z 9.7, že můžeme R považovat za podmnožinu (a tedy podokruh) T.

9.8 Tvrzení. *Ať je R obor integrity, U těleso a $\sigma : R \to U$ injektivní homomorfismus okruhů. Potom existuje jediný homomorfismus $\psi : T \to U$, kde T je podílové těleso R, takový, že $\psi(a) = \sigma(a)$ pro každé $a \in R$. Přitom $\psi(\frac{a}{b}) = \sigma(a)(\sigma(b))^{-1}$ pro všechna $\frac{a}{b} \in T$.*

Důkaz. Protože $\mathbf{1} = \psi(\mathbf{1}) = \psi(\frac{b}{b}) = \psi(b \cdot \frac{1}{b}) = \sigma(b) \cdot \psi(\frac{1}{b})$, musí být $\psi(\frac{1}{b}) = (\sigma(b))^{-1}$ pro každé $b \in R^{\#}$, a tedy $\psi(\frac{a}{b}) = \psi(a \cdot \frac{1}{b}) = \sigma(a)(\sigma(b)^{-1})$ pro každé $\frac{a}{b} \in T$. Pro libovolná $a, b \in R^{\#}$ je $\sigma(a)\sigma(b) = \sigma(ab) = \sigma(ba) = \sigma(b)\sigma(a)$, a proto i $\sigma(b)\sigma(a)^{-1} = \sigma(a)^{-1}\sigma(b)$. Tudíž pro $\frac{a}{b} = \frac{c}{d}$ (a tedy $ad = bc$), dostáváme $\sigma(a)\sigma(b)^{-1} = \sigma(b)^{-1}\sigma(a) = \sigma(c)\sigma(d)^{-1}$. Tím je dokázána korektnost a jednoznačnost definice ψ. Zbývá ověřit, že ψ je homomorfismus. Zjevně $\psi(\mathbf{0}) = \mathbf{0}$, $\psi(\mathbf{1}) = \mathbf{1}$, $\psi(-\frac{a}{b}) = -\psi(\frac{a}{b})$, $\psi(\frac{a}{b} \cdot \frac{c}{d}) = \psi(\frac{a}{b})\psi(\frac{c}{d})$, a konečně $\psi(\frac{a}{b} + \frac{c}{d}) = \psi(\frac{ad+bc}{bd}) = \sigma(ad+bc)\sigma(bd)^{-1} = \sigma(a)\sigma(b)^{-1} + \sigma(c)\sigma(d)^{-1} = \psi(\frac{a}{b}) + \psi(\frac{c}{d})$. $\square$

9.9 Tvrzení. *Buď $\sigma : R \simeq S$ izomorfismus oborů integrity. Buď T podílové těleso R a U podílové těleso S. Potom $\psi : T \to U$, $\psi(\frac{a}{b}) = \frac{\sigma(a)}{\sigma(b)}$ pro každé $\frac{a}{b} \in T$ je také izomorfismus.*

Důkaz. Protože $S \subseteq U$, je ψ podle 9.8 korektně definováno. Současně k $\sigma^{-1} : S \simeq R$ existuje homorfismus $\kappa : U \to T$ takový, že $\kappa(\frac{c}{d}) = \frac{\sigma^{-1}(c)}{\sigma^{-1}(d)}$ pro všechna $\frac{c}{d} \in U$. Ovšem $\kappa\psi(\frac{a}{b}) = \frac{a}{b}$ a $\psi\kappa(\frac{c}{d}) = \frac{c}{d}$, takže ψ je bijektivní. $\square$

9.10 Tvrzení. *Buď U těleso, $R \subseteq U$ obor integrity a T podílové těleso R. Buď V podtěleso U generované R. Potom $\sigma : T \to V$, kde $\sigma(\frac{a}{b}) = ab^{-1}$ pro každé $\frac{a}{b} \in T$, je izomorfismus.*

Důkaz. To, že $\sigma : T \to V$ je injektivní homomorfismus, plyne z 9.8 a 7.12. Přitom $\sigma(T) \subseteq V$ je těleso, takže musí být i $V \subseteq \sigma(T)$. $\square$

9.11 Důsledek. *Buď T podílové těleso $\mathbb{Z}$ a $\sigma : T \to \mathbb{Q}$ homomorfismus, kde $\sigma(\frac{a}{b}) = ab^{-1}$ pro každé $\frac{a}{b} \in T$. Pak σ je izomorfismus.*

Poznámka. V teoretické aritmetice se postupně logicky budují jednotlivé číselné obory. Racionální čísla se odvozují z celých čísel konstrukcí, jež není ničím jiným leč definicí podílového tělesa. Z tohoto hlediska je Důsledek 9.11 vlastně definicí racionálních čísel.

9.12 Důsledek. *Buď U komutativní těleso a T jeho podílové těleso. Pak $U = T$.*

Důkaz. Podle 9.7 je $\sigma : U \to T$, $\sigma(a) = \frac{a}{1}$ injektivní homomorfismus. Pro každé $\frac{a}{b} \in T$ je $\frac{a}{b} = \frac{ab^{-1}}{1} = \sigma(ab^{-1})$, takže σ je dokonce izomorfismus. Přitom ztožňujeme a a $\frac{a}{1}$. $\square$

9.13 Tvrzení. *Buď R obor integrity. Pak $\operatorname{char} R = 0$ nebo $\operatorname{char} R = p > 0$ je prvočíslo.*

Důkaz. Předpokládejme, že platí $\operatorname{char} R > 0$. Potom je prvookruh R izomorfní $\mathbb{Z}_n$, kde $n = \operatorname{char} R$. Podle 9.1 a 8.8 platí, že $\mathbb{Z}_n$ je obor integrity právě když n je prvočíslo. $\square$

9.14 Tvrzení. *Buďte T těleso a P jeho prvotěleso. Je-li $\operatorname{char} T > 0$, tak P je rovno prvookruhu R. Je-li T charakteristiky nula, tak $\frac{a}{b} \to (a\mathbf{1}_T)\cdot(b\mathbf{1}_T)^{-1}$ je izomorfismus $\mathbb{Q}$ a P.*

Důkaz. Pro nenulovou charakteristiku tvrzení plyne z 8.8 a 9.13. Je-li $\operatorname{char} T = 0$, je $a \to a\mathbf{1}_T$ izomorfismus $\mathbb{Z}$ a prvookruhu $S \subseteq P$. Prvotěleso P obsahuje prvookruh, takže naň můžeme nahlížet jako na těleso generované prvookruhem S. Podle 9.10 je P izomorfní podílovému okruhu S, a ten je podle 9.9 izomorfní podílovému okruhu $\mathbb{Z}$. Ovšem podle 9.11 je podílový okruh $\mathbb{Z}$ izomorfní okruhu racionálních čísel $\mathbb{Q}$. $\square$