Konstrukce podílového tělesa $Q(R)$ oboru integrity R

Motivace. Víme, že každý podokruh tělesa je oborem integrity. Ukažme, že i naopak každý obor integrity je podokruhem vhodného tělesa. Nechť dále R je libovolný, ale pevně zvolený obor integrity.

Věta. Na množině $R \times R^*$ definujeme relaci $\equiv$ předpisem

$$(a, b) \equiv (c, d) \quad \Longleftrightarrow \quad a \cdot d = b \cdot c$$

pro libovolné $a, c \in R$, $b, d \in R^*$. Pak $\equiv$ je relace ekvivalence.

Označení. Označme $Q(R)$ rozklad příslušný ekvivalenci $\equiv$, tedy $Q(R) = (R \times R^*)/\equiv$. Pro libovolné $(a, b) \in R \times R^*$ označme $\frac{a}{b} \in Q(R)$ třídu obsahující (a, b), pro každé $a, c \in R$, $b, d \in R^*$ tedy platí

$$\frac{a}{b} = \frac{c}{d} \quad \Longleftrightarrow \quad a \cdot d = b \cdot c.$$

Věta. Na $Q(R)$ lze definovat operace $+$ a $\cdot$ takto: pro každé $a, c \in R$, $b, d \in R^*$ definujeme

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

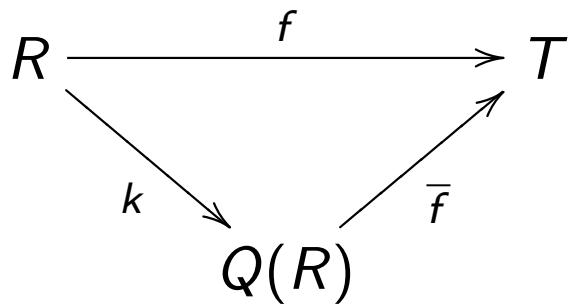
Pak $(Q(R), +, \cdot)$ je těleso a zobrazení $k : R \to Q(R)$, určené předpisem $k(a) = \frac{a}{1}$, je vnoření (tj. injektivní homomorfismus okruhů).

Konstrukce podílového tělesa $Q(R)$ oboru integrity R

Máme vnoření $k : R \to Q(R)$, $k(a) = \frac{a}{1}$ pro každé $a \in R$.

Příklad. $Q(\mathbb{Z}) = \mathbb{Q}$.

Věta. *Nechť $f : R \to T$ je vnoření oboru integrity R do tělesa T. Pak předpis $\overline{f}(\frac{a}{b}) = f(a) \cdot f(b)^{-1}$ pro libovolné $a, b \in R$, $b \neq 0$ dává homomorfismus $\overline{f} : Q(R) \to T$ takový, že $\overline{f} \circ k = f$.*



Navíc platí, že $\overline{f}$ je jediný takový homomorfismus a že $\overline{f}$ je také vnoření, a tedy $Q(R)$ je izomorfní se svým obrazem v homomorfismu $\overline{f}$, tj. $Q(R) \cong \{f(a) \cdot f(b)^{-1}; a, b \in R,\ b \neq 0\}$.

Příklad. $\mathbb{Z}[i] = \{x + i \cdot y; x, y \in \mathbb{Z}\}$ je obor integrity, inkluze dává jeho vnoření do $\mathbb{C}$, tj. máme injektivní homomorfismus $f : \mathbb{Z}[i] \to \mathbb{C}$, kde $f(\alpha) = \alpha$ pro $\alpha \in \mathbb{Z}[i]$. Proto $Q(\mathbb{Z}[i]) \cong \{\alpha \cdot \beta^{-1}; \alpha, \beta \in \mathbb{Z}[i],\ \beta \neq 0\} = \{x + i \cdot y; x, y \in \mathbb{Q}\} = \mathbb{Q}[i]$. Výpočet.

Příklad. Podobně $Q(\mathbb{Z}[\sqrt{p}]) \cong \mathbb{Q}[\sqrt{p}]$ pro libovolné prvočíslo p.

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvek b **dělí** prvek a, neboli že prvek a **je dělitelný** prvkem b, píšeme $b \mid a$, jestliže existuje prvek $q \in R$ takový, že $a = q \cdot b$.
V opačném případě říkáme, že prvek b **nedělí** prvek a, neboli že prvek a **není dělitelný** prvkem b, píšeme $b \nmid a$.

Věta. *Nechť R je komutativní okruh, pak platí*

- $\forall a \in R : \ 1 \mid a, \ a \mid a;$
- $\forall a, b, c \in R : \ a \mid b, \ b \mid c \implies a \mid c;$ *Důkaz.*
- $\forall a, b, c \in R : \ a \mid b, \ a \mid c \implies a \mid b + c;$
- $\forall a \in R : \ a \in R^\times \iff a \mid 1;$
- $\forall a, b \in R : \ a \in R^\times, \ b \mid a \implies b \in R^\times;$
- $\forall a, b \in R : \ a \in R^\times \implies a \mid b.$

Důsledek. *Nechť R je komutativní okruh, $a_1, \ldots, a_n, b \in R$, $u_1, \ldots, u_n \in R$ libovolné. Jestliže $b \mid a_i$ pro každé $i = 1, \ldots, n$, pak $b \mid \sum_{i=1}^{n} u_i \cdot a_i$.*

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvky a, b jsou **asociované**, píšeme $a \sim b$, jestliže $a \mid b$ a současně $b \mid a$.

Věta. *Nechť R je komutativní okruh. Relace asociovanosti $\sim$ je relací ekvivalence na množině R.*

Věta. *Nechť R je obor integrity, $a, b \in R$. Pak platí $a \sim b$, právě když existuje jednotka $c \in R^\times$ tak, že $a = c \cdot b$.* Důkaz.

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $c \mid a$, $c \mid b$, se nazývá **společný dělitel** prvků a, b. Libovolný prvek $d \in R$ se nazývá **největší společný dělitel** prvků a, b, jestliže

- $d \mid a$, $d \mid b$,
- $\forall c \in R: \ c \mid a, c \mid b \implies c \mid d$.

Tedy největší společný dělitel prvků a, b je takový jejich společný dělitel, který je dělitelný každým jejich společným dělitelem.

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $a \mid c$, $b \mid c$, se nazývá **společný násobek** prvků a, b. Libovolný prvek $d \in R$ se nazývá **nejmenší společný násobek** prvků a, b, jestliže

- $a \mid d$, $b \mid d$,
- $\forall c \in R : \ a \mid c, b \mid c \implies d \mid c$.

Tedy nejmenší společný násobek prvků a, b je takový jejich společný násobek, který dělí každý jejich společný násobek.

Poznámka. Předchozí definice mírně pozměňují dříve definované pojmy „největší společný dělitel“ a „nejmenší společný násobek“ v $\mathbb{Z}$. Definovali jsme je totiž pomocí uspořádání podle velikosti, které v obecném okruhu nemáme k dispozici. Dále budeme tyto pojmy používat podle nové definice, avšak zavedené označení (m, n) a $[m, n]$ ponecháme. Tedy (m, n) značí *nezáporný* největší společný dělitel čísel $m, n \in \mathbb{Z}$. Podobně $[m, n]$ značí jejich *nezáporný* nejmenší společný násobek.

Dělitelnost v komutativních okruzích

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Největší společný dělitel prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost. Také nejmenší společný násobek prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost.*

Definice. Nechť R je komutativní okruh, $a \in R$. Řekneme, že a je **ireducibilní** prvek okruhu R, jestliže $a \neq 0$, $a \notin R^\times$ a pro každé $b, c \in R$ takové, že $a = b \cdot c$, platí $b \in R^\times$ a $c \sim a$ anebo $c \in R^\times$ a $b \sim a$.

Příklad. Ireducibilními prvky okruhu $\mathbb{Z}$ jsou právě prvočísla a čísla k nim opačná.

Příklad. Je-li T těleso, pak v T neexistují žádné ireducibilní prvky.

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Je-li a ireducibilní prvek okruhu R a $b \sim a$, pak je také b ireducibilní.*

Okruhy s jednoznačným rozkladem

Definice. Řekneme, že R je **okruh s jednoznačným rozkladem**, jestliže

- R je obor integrity,
- každé $a \in R$, $a \neq 0$, $a \notin R^\times$, lze rozložit na součin několika ireducibilních prvků, přičemž tento součin je jednoznačný až na pořadí a asociovanost.

Příklad. Víme, že $\mathbb{Z}$ je okruh s jednoznačným rozkladem, například rozklady $6 = 2 \cdot 3 = 3 \cdot 2 = (-2) \cdot (-3) = (-3) \cdot (-2)$ se liší jen pořadím a asociovaností.

Příklad. Každé těleso je okruh s jednoznačným rozkladem, neboť neobsahuje žádný prvek, který by byl nenulový a nebyl jednotka.

Příklad. V okruhu $\mathbb{Z}[i]$ je možné dokázat větu o dělení se zbytkem (aby se dalo říct, že zbytek je „menší“ než číslo, kterým se dělilo, je třeba nějak měřit velikost zbytku; v tomto případě to lze udělat pomocí absolutní hodnoty). Stejnou úvahou jako v $\mathbb{Z}$, tedy pomocí Euklidova algoritmu a Bezoutovy rovnosti lze pak ukázat, že $\mathbb{Z}[i]$ je okruh s jednoznačným rozkladem.

Polynomy nad libovolným okruhem R

Poznámka. Abychom nemuseli definovat, co je to výraz a kdy jsou si dva výrazy rovny, nezavedeme polynom jako výraz určitého tvaru, ale pomocí posloupnosti koeficientů. To lze udělat nad libovolným okruhem R.

Definice. Nechť R je okruh. **Polynomem** nad okruhem R rozumíme nekonečnou posloupnost $f = (f_0, f_1, f_2, \dots)$, kde $f_i \in R$ pro každé $i = 0, 1, 2, \dots$ a platí, že množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná. Prvky $f_0, f_1, f_2, \dots$ nazýváme **koeficienty** polynomu f. Množinu všech polynomů nad okruhem R označujeme symbolem $R[x]$.

Dohoda. Koeficienty polynomu f budeme automaticky označovat symboly $f_0, f_1, f_2, \dots$.

Věta. *Nechť R je okruh. Na množině $R[x]$ definujeme operace $+$, $\cdot$ vztahy*

$$(f + g)_i = f_i + g_i, \qquad (f \cdot g)_i = \sum_{k=0}^{i} f_k g_{i-k}$$

pro každé $f, g \in R[x]$, $i \in \mathbb{Z}$, $i \geq 0$. Pak $(R[x], +, \cdot)$ je okruh. Je-li R komutativní, pak $R[x]$ je také komutativní.

Polynomy nad libovolným okruhem R

Definice. Okruh $R[x]$ se nazývá **okruh polynomů** nad okruhem R.

Věta. *Nechť R je okruh. Zobrazení $k : R \to R[x]$ určené předpisem $k(a) = (a, 0, 0, \dots)$ je vnoření.*

Ztotožnění. Polynomy tvaru $(a, 0, 0, \dots)$ se nazývají **konstatntní**. Předchozí věta nám umožňuje ztotožnit $a \in R$ s konstantním polynomem $(a, 0, 0, \dots)$. Tím se okruh R stává podokruhem okruhu $R[x]$. Polynom $0 = (0, 0, 0, \dots)$ se nazývá **nulový**, ostatní polynomy se nazývají **nenulové**.

Definice. Nechť f je nenulový polynom nad okruhem R. Největší $n \geq 0$ takové, že $f_n \neq 0$, se nazývá **stupeň** polynomu f, značíme $\mathrm{st}(f)$. (Takové n existuje, vždyť množina $\{i \in \mathbb{N} \cup \{0\};\ f_i \neq 0\}$ je konečná.) Koeficient f_n se pak nazývá **vedoucí koeficient** polynomu f. Stupeň nulového polynomu klademe roven $-\infty$, jeho vedoucí koeficient nedefinujeme.

Příklad. Polynomy stupně 0 jsou právě nenulové konstantní polynomy.

Polynomy nad libovolným okruhem R

Definice. Polynomy stupně 1 se nazývají **lineární**, polynomy stupně 2 **kvadratické**, polynomy stupně 3 **kubické**. Lineární polynom $(0, 1, 0, 0, \dots)$ budeme označovat symbolem x.

Příklad. Zřejmě $x^2 = (0, 0, 1, 0, 0, \dots)$, $x^3 = (0, 0, 0, 1, 0, \dots)$ atd.

Věta. Nechť R je okruh a $f \in R[x]$ nenulový polynom stupně n. Pak platí $f = f_n \cdot x^n + \cdots + f_1 \cdot x + f_0$, kde koeficienty f_i polynomu f chápeme jako konstantní polynomy a operace $+$ a $\cdot$ jsou operace v okruhu $R[x]$.

Poznámka. Přestože jsme polynomy nedefinovali jako výrazy, předchozí věta nám umožňuje s nimi tak pracovat.

Dohoda. V následující větě budeme potřebovat tyto vztahy pro počítání s nekonečnem: $-\infty < n$,
$(-\infty) + (-\infty) = (-\infty) + n = n + (-\infty) = -\infty$
pro libovolné $n \in \mathbb{Z}$, $n \geq 0$.

Polynomy nad libovolným okruhem R

Věta. *Nechť R je okruh a $f, g \in R[x]$. Pak platí*

- $\mathrm{st}(f+g) \leq \max\{\mathrm{st}(f), \mathrm{st}(g)\}$,
- $\mathrm{st}(f \cdot g) \leq \mathrm{st}(f) + \mathrm{st}(g)$, Důkaz.
- *jestliže $f \neq 0$, $g \neq 0$ a alespoň jeden z vedoucích koeficientů polynomů f a g není dělitel nuly, pak* $\mathrm{st}(f \cdot g) = \mathrm{st}(f) + \mathrm{st}(g)$.

Věta. *Je-li R obor integrity, pak také $R[x]$ je obor integrity.*

Věta. *Nechť R je obor integrity. Pak $(R[x])^\times = R^\times$, tedy polynom f je jednotkou okruhu $R[x]$, právě když je konstantní a současně je jednotkou okruhu R.* Důkaz.

Důsledek. *Pro žádný okruh R není $R[x]$ těleso.*

Příklad. Jestliže R není obor integrity, mohou existovat i nekonstatní jednotky okruhu $R[x]$, například v $\mathbb{Z}_9[x]$ platí $([3]_9 \cdot x + [1]_9) \cdot ([6]_9 \cdot x + [1]_9) = [1]_9$.