Charakteristika okruhu

Definice. Nechť R je okruh. Nejmenší přirozené číslo n takové, že $n1 = 0$, se nazývá **charakteristika** okruhu R. Pokud takové n neexistuje (tedy pro všechna $k \in \mathbb{N}$ platí $k1 \neq 0$), řekneme, že charakteristika okruhu R je nula. Charakteristiku okruhu R značíme $\operatorname{char} R$.

Věta. *Nechť R je obor integrity. Pak pro libovolný $a \in R^*$ platí:*

- *pokud* $\operatorname{char} R = 0$, *pak pro každé* $k \in \mathbb{N}$ *je* $ka \neq 0$;
- *pokud* $\operatorname{char} R = p > 0$, *pak řád prvku a v grupě $(R, +)$ je p.*

Důkaz.

Důsledek. *Je-li R obor integrity, pak všechny nenulové prvky grupy $(R, +)$ mají stejný řád.*

Důsledek. *Je-li R konečné těleso, $p = \operatorname{char} R$, pak grupa $(R, +)$ je izomorfní s grupou $(\mathbb{Z}_p, +) \times \cdots \times (\mathbb{Z}_p, +)$, počet prvků konečného tělesa R je tedy mocninou jeho prvočíselné charakteristiky p.*

Homomorfismus okruhů

Definice. Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy, $f : R \to S$ zobrazení. Řekneme, že f je **homomorfismus** okruhu R do okruhu S, jestliže

- pro každé $a, b \in R$ platí $f(a + b) = f(a) + f(b)$,
- pro každé $a, b \in R$ platí $f(a \cdot b) = f(a) \cdot f(b)$,
- $f(1) = 1$.

Injektivní homomorfismus se nazývá **vnoření**, bijektivní **izomorfismus**. O okruzích R, S řekneme, že jsou izomorfní, píšeme $R \cong S$, existuje-li alespoň jeden izomorfismus $R \to S$.

Příklad. Pro libovolné $m \in \mathbb{N}$ je zobrazení $\pi : \mathbb{Z} \to \mathbb{Z}_m$, určené předpisem $\pi(a) = [a]_m$ pro libovolné $a \in \mathbb{Z}$, homomorfismus okruhu $(\mathbb{Z}, +, \cdot)$ celých čísel do okruhu $(\mathbb{Z}_m, +, \cdot)$ zbytkových tříd modulo m.

Věta. Jsou-li $f : R \to S$ a $g : S \to T$ homomorfismy okruhů, pak také $g \circ f : R \to T$ je homomorfismem okruhů.

Homomorfismus okruhů, jeho jádro

Věta. *Nechť $f : R \to S$ je izomorfismus okruhů. Pak i inverzní zobrazení $f^{-1} : S \to R$ je izomorfismus okruhů.*

Důsledek. *Pro libovolné okruhy R, S, T platí: $R \cong R$; z $R \cong S$ plyne $S \cong R$; a konečně z $R \cong S$ a $S \cong T$ plyne $R \cong T$.*

Poznámka. Zapomeneme-li v okruhu R, jak se násobí, zůstane nám aditivní grupa $(R, +)$. Každý homomorfismus okruhů $f : R \to S$ je také homomorfismem aditivních grup, je tedy $f(0) = 0$, pro každé $a \in R$ platí $f(-a) = -f(a)$, a máme jeho jádro:

Definice. Nechť $f : R \to S$ je homomorfismus okruhů. Množina $\ker f = \{a \in R;\ f(a) = 0\}$ se nazývá **jádro homomorfismu** f.

Věta. *Homomorfismus okruhů $f : R \to S$ je injektivní, právě když $\ker f = \{0\}$.*

Příklad. Zobrazení $f : \mathbb{C} \to M_{2,2}(\mathbb{R})$, kde $f(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ pro libovolné $a, b \in \mathbb{R}$, je vnoření tělesa $\mathbb{C}$ komplexních čísel do okruhu $M_{2,2}(\mathbb{R})$ matic typu 2×2. Ověření.

Binomická věta

Věta (binomická). Nechť R je komutativní okruh, pak pro každé $a, b \in R$ a každé $n \in \mathbb{N}$ platí

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} \cdot b^i,$$

kde $\binom{n}{i} = \frac{n!}{(n-i)!i!}$ značí obvyklý binomický koeficient.

Důkaz. indukcí vůči n: I. krok: případ $n = 1$ je zřejmý.
II. krok: předpokládejme, že pro nějaké $n \in \mathbb{N}$ už bylo dokázáno, dokážeme tvrzení pro $n+1$. Víme tedy
$(a+b)^n = a^n + \binom{n}{1} a^{n-1} \cdot b + \binom{n}{2} a^{n-2} \cdot b^2 + \cdots + \binom{n}{n-1} a \cdot b^{n-1} + b^n.$
Vynásobením (užíváme komutativitu okruhu)
$(a+b)^n \cdot a = a^{n+1} + \binom{n}{1} a^n \cdot b + \binom{n}{2} a^{n-1} \cdot b^2 + \cdots + \binom{n}{n} a \cdot b^n,$
$(a+b)^n \cdot b = \binom{n}{0} a^n \cdot b + \binom{n}{1} a^{n-1} \cdot b^2 + \cdots + \binom{n}{n-1} a \cdot b^n + b^{n+1}.$
Sečtením a užitím $\binom{n}{i+1} + \binom{n}{i} = \binom{n+1}{i+1}$ dostaneme
$(a+b)^{n+1} =$
$a^{n+1} + \binom{n+1}{1} a^n \cdot b + \binom{n+1}{2} a^{n-1} \cdot b^2 + \cdots + \binom{n+1}{n} a \cdot b^n + b^{n+1},$
což se mělo dokázat. Proč binomická věta platí jen v komutativních okruzích?

Umocnění na charakteristiku v oboru integrity

Věta. *Pro libovolné prvočíslo p a libovolné $i \in \{1, 2, \ldots, p-1\}$ platí $p \mid \binom{p}{i}$.*

Důkaz. Platí $p \mid p! = \binom{p}{i} \cdot i! \cdot (p-i)!$. Současně $p \nmid i! \cdot (p-i)!$.

Věta. *Nechť R je obor integrity charakteristiky* $\operatorname{char} R = p > 0$. *Pak pro každé $a, b \in R$ platí*

$$(a+b)^p = a^p + b^p.$$

Důsledek. *Nechť R je obor integrity charakteristiky* $\operatorname{char} R = p > 0$. *Pak zobrazení $f : R \to R$, kde $f(r) = r^p$, je injektivní homomorfismus okruhů.* Důkaz.

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

- $0, 1 \in H$,
- pro každé $a \in H$ platí $-a \in H$,
- pro každé $a, b \in H$ platí $a + b$, $a \cdot b \in H$.

Poznámka. Největším podokruhem okruhu R (vzhledem k $\subseteq$) je celý okruh R, nejmenším podokruhem je $\{n1;\ n \in \mathbb{Z}\}$. Část zdůvodnění.

Věta. *Nechť H je podokruh okruhu $(R, +, \cdot)$. Pak $+$ a $\cdot$ určují operace na množině H, přičemž H je okruh vzhledem k těmto operacem. Je-li okruh R komutativní, pak je i okruh H komutativní. Je-li R obor integrity, pak je i H obor integrity.*

Důsledek. *Každý podokruh tělesa je oborem integrity.*

Příklad. Podokruh tělesa nemusí být těleso: vždyť $\mathbb{Z}$ je podokruhem $\mathbb{Q}$.

Věta. *Jestliže H je podokruh okruhu R a K je podokruh okruhu H, pak je K také podokruh okruhu R.*

Podokruh okruhu generovaný podmnožinou okruhu

Věta. *Nechť R je okruh, I neprázdná množina taková, že pro každé $i \in I$ je dán podokruh H_i okruhu R. Pak průnik $\bigcap_{i\in I} H_i$ všech těchto podokruhů je opět podokruhem okruhu R.*

Definice. Nechť M je podmnožina okruhu R. Symbolem $\langle M\rangle$ označíme průnik všech podokruhů okruhu R, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M\rangle$ podokruhem okruhu R obsahující množinu M; evidentně je nejmenší s touto vlastností. Podokruh $\langle M\rangle$ nazýváme **podokruh generovaný množinou** M, množinu M nazýváme **množina generátorů podokruhu** $\langle M\rangle$.

Poznámka. Zřejmě $\langle R\rangle = R$, $\langle\emptyset\rangle = \{n1;\ n \in \mathbb{Z}\}$.

Označení. Je-li $M = H \cup \{a\}$, kde H je podokruh okruhu R a $a \in R$, píšeme též $H[a]$ místo $\langle M\rangle$.

Věta. *Nechť H je podokruh komutativního okruhu R a $a \in R$. Pak* $H[a] = \{h_0 + h_1 a + h_2 a^2 + \cdots + h_n a^n;\ n \in \mathbb{N},\ h_0, h_1, \ldots, h_n \in H\}$.

Důkaz.

Součin okruhů

Věta. *Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy. Definujme na kartézském součinu $R \times S$ nové operace $+$ a $\cdot$ po složkách, tj.*

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2),$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

pro libovolné $r_1, r_2 \in R$ a $s_1, s_2 \in S$. Pak $(R \times S, +, \cdot)$ je okruh s nulou $(0, 0)$ a jedničkou $(1, 1)$. Navíc platí $(R \times S)^\times = R^\times \times S^\times$.

Definice. Výše popsaný okruh $(R \times S, +, \cdot)$ se nazývá **součin okruhů** $(R, +, \cdot)$ a $(S, +, \cdot)$. Zobrazení $p_1 : R \times S \to R$ a $p_2 : R \times S \to S$ určená předpisy $p_1((r, s)) = r$, $p_2((r, s)) = s$ pro libovolné $(r, s) \in R \times S$ se nazývají **projekce** (ze součinu).

Věta. *Nechť $(R \times S, +, \cdot)$ je součin okruhů $(R, +, \cdot)$ a $(S, +, \cdot)$. Pak obě projekce p_1 a p_2 jsou surjektivní homomorfismy okruhů.*

Čínská zbytková věta

Věta (Čínská zbytková). *Nechť* $m, n \in \mathbb{N}$ *a zobrazení* $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ *je určeno předpisem* $f([a]_{mn}) = ([a]_m, [a]_n)$ *pro libovolné* $a \in \mathbb{Z}$. *Pak* f *je homomorfismus okruhů.* Část důkazu. *Je-li navíc* $(m, n) = 1$, *je* f *izomorfismus, a tedy* $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

Důsledek. *Je-li* $(m, n) = 1$, *pak* $\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$, *a tedy* $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Důsledek. *Je-li* $(m, n) = 1$, *pak pro každé* $a, b \in \mathbb{Z}$ *existuje* $c \in \mathbb{Z}$ *tak, že*

$$c \equiv a \pmod{n},$$
$$c \equiv b \pmod{m}.$$