Okruhy a tělesa

Budeme se zabývat strukturami se dvěma binárními operacemi. Mějme tedy množinu R, na níž jsou zadány dvě binární operace $+$ a $\cdot$. Takovou strukturu zapisujeme jako trojici $(R, +, \cdot)$. Předpokládejme navíc, že tato struktura splňuje následující podmínky:

$(R, +)$ je komutativní grupa,

$(R, \cdot)$ je monoid,

platí následující **distributivní** zákony:
pro každá $a, b, c \in R$ je splněno

$$a \cdot (b + c) = a{\cdot}b + a{\cdot}c \quad \text{a} \quad (a + b) \cdot c = a{\cdot}c + b{\cdot}c.$$

Pak struktura $(R, +, \cdot)$ se nazývá **okruh**. Operace $+$, resp. $\cdot$ se pak nazývají sčítání, resp. násobení. Neutrální prvek grupy $(R, +)$ se potom nazývá **nulový prvek** daného okruhu a označuje se symbolem 0. Inverzní prvek k prvku $a \in R$ v grupě $(R, +)$ se nazývá **opačný prvek** k prvku a a označuje se symbolem $-a$. Pro libovolné dva prvky $a, b \in R$ budeme symbolem $a - b$ označovat prvek $a + (-b)$. Neutrální prvek monoidu $(R, \cdot)$ se nazývá **jednotkový prvek** daného okruhu a označuje se symbolem 1.

Příklady. Trojice $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, kde $+$ a $\cdot$ jsou obvyklé operace sčítání a násobení v rámci číselných množin, jsou okruhy.

Pro libovolné $n \in \mathbb{N}$ trojice $(\mathbb{Z}_n, +, \cdot)$, kde $+$ a $\cdot$ jsou operace sčítání a násobení zbytkových tříd podle modulu n, je okruh.

Tvrzení. Buď $(R, +, \cdot)$ okruh. Pak pro libovolná $a, b, c \in R$ platí

$$a \cdot 0 = 0 \cdot a = 0,$$

$$a \cdot (-b) = (-a) \cdot b = -(a \cdot b),$$

$$a \cdot (b - c) = a{\cdot}b - a{\cdot}c \quad \text{a} \quad (a - b) \cdot c = a{\cdot}c - b{\cdot}c.$$

Důkaz. Poněvadž $0+0=0$, dostáváme $a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$. Přičtením prvku $-(a\cdot 0)$ k oběma stranám této rovnosti obdržíme $0 = a\cdot 0$. Obdobně se zjistí, že $0 = 0\cdot a$.

Poněvadž $b+(-b)=0$ a $a\cdot 0 = 0$ podle předchozího, dostáváme $0 = a\cdot 0 = a\cdot(b+(-b)) = a\cdot b + a\cdot(-b)$. Přičtením prvku $-(a\cdot b)$ k oběma stranám této rovnosti obdržíme $-(a\cdot b) = a\cdot(-b)$. Obdobně se zjistí, že $-(a\cdot b) = (-a)\cdot b$.

Nakonec $a\cdot(b-c) = a\cdot(b+(-c)) = a\cdot b + a\cdot(-c) = a\cdot b + (-a\cdot c) = a\cdot b - a\cdot c$ podle předchozího. Obdobně se zjistí, že $(a-b)\cdot c = a\cdot c - b\cdot c$.

Buď $R = \{e\}$ jednoprvková množina, na níž jsou definovány binární operace $+$ a $\cdot$ jediným možným způsobem, totiž tak, že $e+e=e$ a $e\cdot e = e$. Pak $(R,+,\cdot)$ je okruh, který se nazývá **triviální okruh**. Platí v něm $0=e$ a $1=e$, takže $0=1$. Ve skutečnosti pro libovolný okruh $(R,+,\cdot)$ platí, že $(R,+,\cdot)$ je triviální okruh právě tehdy, když $0=1$. Skutečně, je-li $0=1$, pak pro libovolný prvek $a\in R$ platí, že $a = a\cdot 1 = a\cdot 0 = 0$, takže $R=\{0\}$ a $(R,+,\cdot)$ je tedy triviální okruh.

Buď $(R,+,\cdot)$ okruh. Je-li operace $\cdot$ na R komutativní, tedy je-li $(R,\cdot)$ komutativní monoid, pak $(R,+,\cdot)$ se nazývá **komutativní** okruh. Všechny doposud uvedené příklady okruhů byly komutativní okruhy.

Buď $(R,+,\cdot)$ okruh. Platí-li pro nějaké dva prvky $a,b\in R$, že $a\neq 0$, $b\neq 0$, avšak $a\cdot b = 0$, pak prvky a,b se nazývají **dělitelé nuly** v okruhu $(R,+,\cdot)$. Neobsahuje-li okruh $(R,+,\cdot)$ žádné dělitele nuly, znamená to, že množina $R-\{0\}$ je uzavřená vzhledem k operaci $\cdot$. Je-li navíc okruh $(R,+,\cdot)$ netriviální, znamená to, že $(R-\{0\},\cdot)$ je monoid. Netriviální komutativní okruh $(R,+,\cdot)$ neobsahující žádné dělitele nuly se nazývá **obor integrity**.

Příklady. Všechny výše uvedené číselné okruhy $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ jsou obory integrity.

Okruh zbytkových tříd $(\mathbb{Z}_n, +, \cdot)$, kde $n \in \mathbb{N}$, je oborem integrity právě tehdy, když n je prvočíslo.

Tvrzení. Netriviální komutativní okruh $(R, +, \cdot)$ je obor integrity právě tehdy, když splňuje následující zákon o **krácení**:

$$(\,\forall a \in R - \{0\}\,)(\,\forall b, c \in R\,)(\,a \cdot b = a \cdot c \implies b = c\,).$$

Důkaz. Jsou-li $a \in R - \{0\}$ a $b, c \in R$ taková, že $a \cdot b = a \cdot c$, pak $0 = a \cdot b - a \cdot c = a \cdot (b - c)$. Je-li nyní $(R, +, \cdot)$ obor integrity, neobsahuje žádné dělitele nuly, takže $b - c = 0$, a tedy $b = c$.

Je-li naopak $(R, +, \cdot)$ netriviální komutativní okruh, v němž platí zákon o krácení, pak pro libovolné prvky $a, b \in R$ takové, že $a \neq 0$ a $a \cdot b = 0$ platí $a \cdot b = 0 = a \cdot 0$, takže $b = 0$. Neobsahuje tedy okruh $(R, +, \cdot)$ žádné dělitele nuly, čili jde o obor integrity.

Buď $(R, +, \cdot)$ netriviální okruh. Pak každý prvek $a \in R$, který je invertibilním prvkem monoidu $(R, \cdot)$, se nazývá **jednotka** okruhu $(R, +, \cdot)$ a prvek k němu inverzní se značí symbolem a^{-1}. Jednou z obecně mnoha jednotek okruhu $(R, +, \cdot)$ je jeho jednotkový prvek 1. Podle posledního důsledku z kapitoly o grupách množina všech jednotek okruhu $(R, +, \cdot)$ je uzavřená vzhledem k operaci $\cdot$ a tvoří vzhledem k této operaci grupu.

Netriviální komutativní okruh $(R, +, \cdot)$, jehož všechny nenulové prvky jsou jednotkami, se nazývá **těleso**. Jinak řečeno, netriviální komutativní okruh $(R, +, \cdot)$ je tělesem, jestliže množina $R - \{0\}$ je uzavřená vzhledem k operaci $\cdot$ a přitom $(R - \{0\}, \cdot)$ tvoří grupu. Je jasné, že každé těleso je oborem integrity.

Příklady. Okruhy $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ a $(\mathbb{C}, +, \cdot)$ všech racionálních, reálných a komplexních čísel jsou tělesa.

Pro každé prvočíslo p je okruh zbytkových tříd $(\mathbb{Z}_p, +, \cdot)$ tělesem. Plyne to z poslední věty v kapitole o zbytkových třídách.

Věta. Každý konečný obor integrity je těleso.

Důkaz. Nechť $(R, +, \cdot)$ je konečný obor integrity. Pak je to netriviální komutativní okruh. Vezměmě libovolný prvek $a \in R-\{0\}$. Pak množina $\{a\cdot r \mid r \in R\}$ má týž počet prvků jako R, neboť v $(R,+,\cdot)$ platí zákon o krácení. Takže $R = \{a\cdot r \mid r \in R\}$. Poněvadž $1 \in R$, existuje tedy prvek $b \in R$ takový, že $a \cdot b = 1$. Je tedy každý prvek $a \in R - \{0\}$ jednotkou okruhu $(R,+,\cdot)$, takže $(R,+,\cdot)$ je těleso.

Nechť $(R,+,\cdot)$ je okruh s nulovým prvkem 0 a s jednotkovým prvkem 1 a nechť $S \subseteq R$ je podmnožina splňující následující tři podmínky:

$$(\forall a,b \in S)(a+b \in S \ \ \& \ \ a\cdot b \in S),$$
$$0,1 \in S,$$
$$(\forall a \in S)(-a \in S).$$

Pak říkáme, že S je **podokruh** okruhu $(R,+,\cdot)$. Potom totiž množina S je uzavřená vzhledem k operacím $+$ a $\cdot$ a přitom trojice $(S,+,\cdot)$ je opět okruh.

Je-li $(R,+,\cdot)$ těleso a je-li $S \subseteq R$ podokruh tohoto tělesa takový, že je splněna ještě následující podmínka:

$$(\forall a \in S-\{0\})(a^{-1} \in S),$$

pak říkáme, že S je **podtěleso** tělesa $(R,+,\cdot)$. Potom totiž trojice $(S,+,\cdot)$ je sama tělesem.

Příklady. Množina $\mathbb{Z}$ všech celých čísel je podokruhem těles $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ i $(\mathbb{C},+,\cdot)$. Množina $\mathbb{Q}$ všech racionálních čísel je podtělesem těles $(\mathbb{R},+,\cdot)$ i $(\mathbb{C},+,\cdot)$.

Nechť $(R,+,\cdot)$ a $(S,\#,*)$ jsou dva okruhy s jednotkovými prvky 1 a $\mathbb{1}$ a nechť $f : R \to S$ je zobrazení. Řekneme, že f je **homomorfismus** okruhu $(R,+,\cdot)$ do okruhu $(S,\#,*)$, jsou-li splněny následující podmínky:

$$(\forall a,b \in R)(f(a+b) = f(a) \,\#\, f(b)),$$

$$(\forall a, b \in R)(f(a \cdot b) = f(a) * f(b)),$$
$$f(1) = \mathbb{1}.$$

Poněvadž pak f je homomorfismem grupy $(R, +)$ do grupy $(S, +)$, podle prvního tvrzení v kapitole o homomorfismech grup potom platí rovněž podmínky

$$f(0) = \mathbb{0} \quad \text{a} \quad (\forall a \in R)(f(-a) = -f(a)),$$

kde 0, resp. $\mathbb{0}$ jsou nulové prvky v okruzích $(R, +, \cdot)$, resp. $(S, \#, *)$.

Příklady. Pro libovolné $n \in \mathbb{N}$ je zobrazení $h : \mathbb{Z} \to \mathbb{Z}_n$ dané pro každé $a \in \mathbb{Z}$ předpisem $h(a) = [a]_n$ homomorfismem okruhu $(\mathbb{Z}, +, \cdot)$ do okruhu $(\mathbb{Z}_n, +, \cdot)$.

Zobrazení $^{-} : \mathbb{C} \to \mathbb{C}$ přiřazující každému komplexnímu číslu $z \in \mathbb{C}$ číslo $\bar{z}$ k němu komplexně sdružené je homomorfismem okruhu $(\mathbb{C}, +, \cdot)$ do něj samotného.

Pro skládání okruhových homomorfismů platí analogické tvrzení jako pro skládání homomorfismů grup. Žádáme-li, aby homomorfismus okruhu $(R, +, \cdot)$ do okruhu $(S, \#, *)$ byl současně bijekcí množiny R na množinu S, dostáváme pojem izomorfismu těchto dvou okruhů a mluvíme o izomorfních okruzích. Inverzní zobrazení k takovému izomorfismu je pak rovněž izomorfismem. Obdobnou argumentací jako v kapitole o podgrupách a homomorfismech grup lze dokázat rovněž následující fakt.

Tvrzení. Nechť $(R, +, \cdot)$ a $(S, \#, *)$ jsou okruhy a nechť $f : R \to S$ je homomorfismus okruhu $(R, +, \cdot)$ do okruhu $(S, \#, *)$. Pak obraz $f(R)$ při tomto homomorfismu je podokruh okruhu $(S, \#, *)$.

Poznámka. V takové situaci pak trojice $(f(R), \#, *)$ sama je okruhem. Je-li zmíněný homomorfismus f navíc prostým zobrazením množiny R do množiny S, jde o bijekci množiny R na množinu $f(R)$, a tedy o izomorfismus okruhu $(R, +, \cdot)$ s okruhem $(f(R), \#, *)$, který sám je podokruhem okruhu $(S, \#, *)$.