# 1. Okruhy

## 1.1. Okruh

▶ 1.1.1. Definice. Řekneme, že algebra $R = (M, +, \cdot)$ je okruh (angl. ring), pokud platí:

**(1)** algebra $(M, +)$ je Abelova grupa; nazýváme ji aditivní grupa okruhu $R$ a značíme $R_+$;

**(2)** algebra $(M, \cdot)$ je grupoid; nazýváme jej multiplikativní grupoid okruhu $R$ a značíme $R_\bullet$;

**(3)** distributivní zákon, tj.

$$(\forall a, b, c \in M)(a(b + c) = (ab) + (ac) \ \wedge \ (b + c)a = (ba) + (ca)).$$

▶ 1.1.2. Poznámka. Někdy se v literatuře očekává od okruhu ještě asociativita.

▶ 1.1.3. Příklad. $Z = (\mathbb{Z}, +, \cdot)$ je okruh celých čísel.

▶ 1.1.4. Poznámka. Jak jsme zvyklí, má operace násobení větší prioritu než operace sčítání, tj. $ab + c := (ab) + c$.

▶ 1.1.5. Definice. $E = (\{0\}, +, \cdot)$ je triviální okruh.

▶ 1.1.6. Definice. Řekneme, že okruh $R$ je asociativní, resp. je komutativní, resp. má jednotku, má-li stejnou vlastnost i multiplikativní grupoid $R_\bullet$.

▶ 1.1.7. Příklad.

**(1)** Okruh $Z = (\mathbb{Z}, +, \cdot)$ je asociativní, komutativní a má jednotku.

**(2)** Okruh $(\mathbb{C}^{n,n}, +, \cdot)$ je asociativní, má jednotku (jednotkovou matici), ale není komutativní.

**(3)** Vektorový prostor $(V, +)$ s vektorovým součinem $\times$ tvoří okruh $(V, +, \times)$, který není ani asociativní, ani komutativní.

▶ 1.1.8. Definice. Zerový okruh je okruh $R = (M, +, \cdot)$, kde $(\forall a, b \in M)(ab := 0)$.

▶ 1.1.9. Definice. Definujeme rozdíl prvků, $(\forall a, b \in M)(a - b := a + (-b))$.

▶ 1.1.10. Věta. Buď $R = (M, +, \cdot)$ okruh, nechť $a, b \in M$. Potom platí:

**(1)** $c(a - b) = ca - cb$; $(a - b)c = ac - bc$;

**(2)** $0 \cdot a = a \cdot 0 = 0$;

**(3)** $(-a)b = a(-b) = -(ab)$;

**(4)** $(-a)(-b) = ab$.

◦ *Důkaz.* Všechno je podobné, ukážeme první dvě.

**(1)** $c(a-b) = c(a-b) + cb - cb = c(a-b+b) - cb = ca - cb$.

**(2)** $0 \cdot a = (b-b)a = ba - ba = 0$.

□

► 1.1.11. DEFINICE. Číselný okruh je libovolný okruh s přirozenými číselnými operacemi a s nosičem, který je číselnou množinou.

► 1.1.12. DEFINICE. Dělitelé nuly jsou libovolné $a, b \in R^\bullet$ takové, že $a, b \neq 0$, ale $ab = 0$. Okruhem bez dělitelů nuly rozumíme okruh, ve kterém neexistují dělitelé nuly.

► 1.1.13. PŘÍKLAD. Např. $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$.

► 1.1.14. VĚTA. Číselné okruhy jsou bez dělitelů nuly, tj. pro $a, b \in R^\bullet$ platí, že

$$(ab = 0 \Rightarrow (a = 0 \vee b = 0)).$$

► 1.1.15. DEFINICE. Oborem integrity rozumíme asociativní a komutativní okruh bez dělitelů nuly.

► 1.1.16. DEFINICE. Buď $R = (M, +, \cdot)$ okruh. Formálním polynomem nad okruhem $R$ rozumíme libovolnou nekonečnou posloupnost $(a_n)_{n=0}^\infty$ prvků z $M$, v níž je konečný počet prvků nenulových.

Takové $n \in \mathbb{N}_0$, že $a_n \neq 0$ a $(\forall i > n)(a_i = 0)$, nazveme stupeň polynomu. Pro nulový polynom $\theta = 0\,0\,0\,0\ldots$ nedefinujeme stupeň.

Posloupnost $(a_n)_{n=0}^\infty$ označíme $\sum a_n x^n$ nebo $a_0 + a_1 x + a_2 x^2 + \ldots + a_s x^s$, kde $s$ je stupeň polynomu. Jde o formální zápis, nikoli sumu. Množinu všech polynomů nad okruhem $R$ označíme $R[x]^\bullet$.

► 1.1.17. POZNÁMKA. Skalní algebraici říkají $x$ neurčitá (nejedná se o proměnnou).

► 1.1.18. DEFINICE. Mějme okruh $R$ a polynomy $P = \sum a_i x^i$, $Q = \sum b_i x^i$. Potom definujeme součet polynomů jako $P + Q := \sum (a_i + b_i) x^i$ a součin polynomů jako $PQ := \sum c_k x^k$, kde $c_k := \sum_{i=0}^k a_i b_{k-i}$.

► 1.1.19. POZNÁMKA. Součet i součin polynomů jsou opět polynomy a operace jsou přirozené, jaké známe z analýzy.

► 1.1.20. DEFINICE. $R[x] = (R[x]^\bullet, +, \cdot)$ nazveme okruh polynomů nad okruhem $R$.

► 1.1.21. LEMMA. Pokud okruh $R$ je asociativní, resp. je komutativní, resp. má jednotku, má odpovídající vlastnost i $R[x]$. Jednotkou v okruhu polynomů je $1x^0 = 1\,0\,0\,0\ldots$.

► 1.1.22. LEMMA. Nemá-li okruh $R$ dělitele nuly, nemá je ani okruh $R[x]$.

◦ *Důkaz.* Mějme $P, Q \in R[x] \setminus \{\theta\}$, $P = \sum a_i x^i$, $Q = \sum b_i x^i$ a nechť stupeň $P$ je $p$ a $Q$ je $q$. Mějme součin $PQ = \sum c_k x^k$, pak je speciálně $c_{p+q} = \sum_0^{p+q} a_i b_{p+q-i}$. Pro $i > p$ je $a_i = 0$ a pro $i < p$ je $p + q - i > q$ a $b_i = 0$. Tedy $c_{p+q} = a_p b_q$, a neboť oba jsou nenulové a $R$ nemá dělitele nuly, je $c_{p+q} \neq 0$, a tedy $PQ \neq \theta$. □

► 1.1.23. Definice. Mějme $x_1, \ldots, x_n$ soubor neučitých. Pak definujeme $R[x_1, \ldots, x_n]$ indukcí jako $R[x_1, \ldots, x_n] := (R[x_1, \ldots, x_{n-1}])[x_n]$.

► 1.1.24. Věta. Buď $R$ obor integrity, pak také $R[x_1, \ldots, x_n]$ je obor integrity.

◦ *Důkaz.* Důkaz provedeme snadno indukcí podle $n$ s využitím předchozího lemmatu. □

## • 1.2. Těleso

► 1.2.1. Definice. Okruh $R = (M, +, \cdot)$ je <u>těleso</u>, pokud platí, že algebra $(M \setminus \{0\}, \cdot)$ je grupa. Grupu $(M \setminus \{0\}, \cdot)$ nazýváme <u>multiplikativní grupa</u> tělesa a značíme $T_*$. Těleso značíme $T$, a je-li $T_*$ Abelova, řekneme, že těleso $T$ je <u>komutativní</u>.

► 1.2.2. Lemma. Těleso vždy obsahuje alespoň 2 prvky, a to nulu a jednotku.

► 1.2.3. Definice. Definujeme <u>triviální těleso</u> $F = (\{0, 1\}, +, \cdot)$. Operace na triviálním tělese se definují pomocí <u>Cayleyových tabulek</u>:

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

► 1.2.4. Definice. Základní číselná tělesa:

**(1)** $Q := (\mathbb{Q}, +, \cdot)$;

**(2)** $R := (\mathbb{R}, +, \cdot)$;

**(3)** $C := (\mathbb{C}, +, \cdot)$.

► 1.2.5. Poznámka. Okruh celých čísel $Z = (\mathbb{Z}, +, \cdot)$ není tělesem!

► 1.2.6. Příklad. Položme $M = \left\{a + \sqrt{2}b \;\middle|\; a, b \in \mathbb{Q}\right\}$, pak $(M, +, \cdot)$ je těleso takové, že $\mathbb{Q} \subsetneq M \subsetneq \mathbb{R}$. Jediné zajímavé je ukázat přítomnost inverzního prvku: $(a + \sqrt{2}b)^{-1} = \frac{a - \sqrt{2}b}{a^2 - 2b^2}$.
Obecně lze definovat $\mathbb{Q}_{\sqrt{n}} = ((\mathbb{Q} + \sqrt{n}\mathbb{Q}), +, \cdot)$ pro libovolné $n \in \mathbb{N}$.

► 1.2.7. Věta.

**(1)** Těleso nemá dělitele nuly.

**(2)** Komutativní těleso je obor integrity.

◦ *Důkaz.*

**(1)** Nenulové prvky tělesa tvoří grupu, tedy jsou uzavřené vůči násobení, a tedy nemůže $ab = 0$.

**(2)** Těleso je vždy asociativní, tedy je-li i komutativní, je oborem integrity z definice.

□

► 1.2.8. Definice. Buďte $R = (M, +, \cdot)$ okruh a $T = (N, +, \cdot)$ těleso.

**(1)** Řekneme, že $A \subseteq M$, $A \neq \emptyset$ je uzavřená v okruhu $R$, platí-li

$$(\forall a, b \in A)(ab \in A \ \wedge \ a - b \in A).$$

Algebru $Q = (A, +, \cdot)$ nazveme podokruh okruhu $R$ a značíme $Q \Subset R$.

**(2)** Řekneme, že $B \subseteq N$, $B \neq \emptyset$ je uzavřená v tělese $T$, platí-li

$$\big(\forall a, b \in B\big)\big(b \neq 0 \Rightarrow (ab^{-1} \in B \ \wedge \ a - b \in B)\big).$$

Algebru $U = (B, +, \cdot)$ nazveme podtěleso tělesa $T$ a značíme $U \Subset T$. Těleso $T$ nazýváme nadtěleso tělesa $U$ a relaci $\Subset$ rozšířením těles.

► 1.2.9. Příklad.

**(1)** Označme $S = \{2k \mid k \in \mathbb{Z}\}$. Pak platí (pro okruhy) $(S, +, \cdot) \Subset_O (\mathbb{Z}, +, \cdot) \Subset_O (\mathbb{Q}, +, \cdot)$.

**(2)** Pro tělesa platí $(\mathbb{Q}, +, \cdot) \Subset_T (\mathbb{R}, +, \cdot) \Subset_T (\mathbb{C}, +, \cdot)$.

► 1.2.10. Věta. Buďte $R = (M, +, \cdot)$ okruh, resp. těleso a nechť $Q_i \Subset R, i \in I$ je systém podokruhů, resp. podtěles. Pak $\bigcap_{i \in I} G_i$ je podokruh, resp. podtěleso $R$.

► 1.2.11. Definice. Buďte $R = (M, +, \cdot)$ okruh, $A \subseteq M$. Pak $\langle A \rangle := \bigcap \{Q \Subset R \mid A \subseteq Q\}$ nazýváme podokruh generovaný množinou $A$.

► 1.2.12. Lemma.

$$\langle A \rangle^\bullet = \{k_1 \times a_{11} \dots a_{1m_1} + \dots + k_n \times a_{n1} \dots a_{nm_n} \mid n \in \mathbb{N}_0, m_i \in \mathbb{N}, k_i \in \mathbb{Z}, a_{ij} \in A\}$$

◦ *Důkaz.* Množina obsahuje $A$, nelze nic vyjmout a je uzavřená v $R$. □

► 1.2.13. Definice. Buďte $R = (M, +, \cdot)$ okruh a nechť $Q_i \Subset R, i \in I$ je systém podokruhů. Pak definujeme součet podokruhů jako $\sum_{i \in I} Q_i := \big\langle \bigcup_{i \in I} Q_i^\bullet \big\rangle$

## • 1.3. Kongruence

► 1.3.1. Definice. Buď $R = (M, +, \cdot)$ okruh a $\equiv$ ekvivalence na $M$. Řekneme, že $\equiv$ je kongruence na okruhu $R$, platí-li:

$$(\forall a, b, c, d \in M)\big((a \equiv b \ \wedge \ c \equiv d) \Rightarrow (a + c \equiv b + d \ \wedge \ ac \equiv bd)\big).$$

► 1.3.2. Definice. Buď $\equiv$ kongruence na okruhu $R$. Pak $R/\equiv := (M/\equiv, +, \cdot)$ s operacemi $T_a + T_b := T_{a+b}$ a $T_{ab} := T_a T_b$ nazýváme faktorokruh okruhu $R$ podle kongruence $\equiv$.

► 1.3.3. Lemma. Buď $\equiv$ kongruence na okruhu $R$. Pak faktorokruh $R/\equiv$ je okruh.

► 1.3.4. Věta. Je-li okruh $R$ asociativní, resp. komutativní, resp. má jednotku, potom má tutéž vlastnost i faktorokruh $R/\equiv$.

► 1.3.5. Poznámka. Neplatí obecně, že faktorokruh tělesa je tělesem (nepřenáší se vlastnost nemíti dělitele nuly).

► 1.3.6. Definice. Nechť $Q \Subset R$ je okruh a jeho podokruh. Pak definujeme ekvivalenci $\equiv_Q$ na $R$ tak, že $a \equiv_Q b \Leftrightarrow a - b \in Q$.

► 1.3.7. Poznámka. $R_+$ je Abelova, tedy $\equiv_Q$ je kongruence na grupě $R_+$, ne však kongruence na okruhu $R$.

► 1.3.8. Definice. Podokruh $I$ okruhu $R$ nazýváme ideál v $R$ a značíme $I \lhd R$, platí-li, že

$$(\forall a \in I^\bullet)(\forall r \in R^\bullet)(ra \in I^\bullet \ \wedge \ ar \in I^\bullet).$$

► 1.3.9. Poznámka.

**(1)** Při ověřování, že $I$ je ideál, je nejprve nutno ověřit, že je podokruhem, a pak teprve definující podmínku ideálu.

**(2)** Definující vlastnost ideálu je silnější než uzavřenost vůči násobení, tedy stačí ověřit tuto podmínku a uzavřenost vůči sčítání.

► 1.3.10. Věta. Ekvivalence $\equiv$ na $R$ je kongruencí právě tehdy, je-li ekvivalencí indukovanou ideálem, tj. $(\exists I \lhd R)((\equiv) = (\equiv_I))$.

◦ *Důkaz.*

**(⇐)** Vezměme třídu $T_0$ kongruence $\equiv$ a ukážeme, že $I = (T_0, +, \cdot)$ je hledaný ideál.

Platí $a \equiv 0$ a $b \equiv 0$, tedy $a - b \equiv 0$, a tedy $a - b \in T_0$. Dále $a \equiv 0$ a $r \equiv r$, tedy $ar \equiv 0$ a $ra \equiv 0$, a tedy $ar, ra \in T_0$.

Z grup víme, že $(\equiv) = (\equiv_{T_0})$, což jsme chtěli ukázat.

**(⇒)** Mějme $I \lhd R$. Pak $a \equiv_I b \Leftrightarrow a - b \in I^\bullet$. Ekvivalence $\equiv_I$ je kongruencí na $R_+$, tedy zbývá ukázat druhá podmínka, tj. že $ac \equiv_I bd$, pokud $a \equiv_I b$ a $c \equiv_I d$. Platí $ac - bd = ac - ad + ad - bd = a(c - d) + (a - b)d$, a neboť $(c - d), (a - b) \in I$ a ideál je uzavřený na násobení všemi prvky $R$ a na sčítání, je i $a(c - d) + (a - b)d \in I$.

□

► 1.3.11. Příklad. Mějme okruh celých čísel $Z = (\mathbb{Z}, +, \cdot)$. Pak pro libovolné $m \in \mathbb{N}_0$ definujeme $\equiv_m$ jako $a \equiv_m b \Leftrightarrow (\exists s \in \mathbb{Z})(a - b = sm)$. Pak $I_m := \{sm \mid s \in \mathbb{Z}\}$ je ideál a $I_m$ jsou všechny ideály na $Z$.

Zjevně splývá $Z / \equiv_m$ a $Z / I_m$. Budeme proto používat společnou značku $Z_m$ a název okruh zbytkových tříd modulo $m$.

► 1.3.12. Věta. Nechť $m \in \mathbb{N}$ (tedy $m \neq 0$). Pak v jedné třídě $Z_m$ leží 2 čísla $a, b$ právě tehdy, dávají-li stejný zbytek po dělení $m$. Okruh zbytkových tříd $Z_m$ má řád $m$.

► 1.3.13. Věta. Buďte $R$ okruh s jednotkou, $I \lhd R$ a nechť $1 \in I^\bullet$. Pak $I = R$.

○ *Důkaz.* Mějme libovolné $r \in R^\bullet$ a $1 \in I^\bullet$. Pak nutně $r \cdot 1 \in I$, a tedy $R^\bullet \subseteq I^\bullet$. Opačná inkluze plyne z definice ideálu. □

► 1.3.14. Věta. Buď $R$ okruh. Pak:

**(1)** $R \lhd R$;

**(2)** $E \lhd R$.

► 1.3.15. Definice.

**(1)** Ideál $I \lhd R$ nazveme netriviální, pokud $I \neq R$ a $I \neq E$.

**(2)** Okruh $R$ označujeme jednoduchý, pokud nemá netriviální ideály.

## • 1.4. Jednoduché okruhy

► 1.4.1. Věta. Nechť $R$ je okruh a $I \lhd R$. Pak $I_+ \lhd R_+$. (Tedy je-li $I$ ideál, pak je i normální podgrupou aditivní grupy $R_+$.)

► 1.4.2. Věta.

**(1)** Okruh $R$ prvočíselného řádu $p$ je jednoduchý.

**(2)** Libovolné těleso $T$ je jednoduchý okruh.

○ *Důkaz.*

**(1)** Pokud by $R$ měl netriviální ideál, pak by $R_+$ měla netriviální normální podgrupu, ale z prvočíselnosti řádu víme, že taková normální podgrupa neexistuje.

**(2)** Mějme libovolný ideál $I \lhd T$. Ukážeme, že $I \neq E \Rightarrow I = T$, tedy existují pouze triviální ideály. Ideál je nenulový, tedy $(\exists a \in I^\bullet \setminus \{0\})$. Pak $a^{-1} \in T$, tedy $aa^{-1} = 1 \in I^\bullet$, a tedy $I = T$.

□

► 1.4.3. Poznámka. Lze definovat jednostranné ideály, ale z důkazu je vidět, že těleso nemá ani jednostranné ideály.

► 1.4.4. Věta. Průnik i součet libovolného systému ideálů v okruhu $R$ je ideál v $R$.

◦ *Důkaz.* Mějme systém $I_\alpha \lhd R$ pro $\alpha \in J$. Označme $A = \bigcap I_\alpha$ a $B = \sum I_\alpha$

**(průnik)** Průnik je podokruhem, tedy stačí ukázat definiční podmínku ideálu. Mějme libovolné $a \in A$ a $r \in R^\bullet$. Pak $(\forall \alpha \in J)(a \in I_\alpha)$, tedy $(\forall \alpha \in J)(ar \in I_\alpha)$, tedy $ar \in A$.

**(součet)** Součet je podokruhem, tedy opět stačí ukázat definiční podmínku ideálu. Mějme libovolné $a \in B$ a $r \in R^\bullet$. Pak $a$ je tvaru $a = k_1 \times a_{11} \dots a_{1n_1} + \dots + k_m \times a_{m1} \dots a_{mn_m}$, kde $k_i \in \mathbb{Z}$ a $a_{i\ell} \in \bigcup I_\alpha$. Tedy zvláště $a_{i1} \in I^\bullet_{\alpha_i}$ ($\alpha_i$ vybere příslušný ideál). Pak součin $a_{i1}a_{i2} \dots a_{in_i}$ je tvaru $a_{i1}r_i$ pro nějaké $r_i \in R^\bullet$, tedy neboť $I_\alpha$ je ideál, je $a_{i1}r_i \in I_\alpha$ a také $b_i = k_i \times a_{i1}r_i \in I_\alpha$. Potom $a = b_1 + \dots + b_m$. Pro libovolné $r \in R^\bullet$ je $ra = rb_1 + \dots + rb_m$ a platí $(\forall i)(rb_i \in I_{\alpha_i})$. Ale $I_{\alpha_i} \subseteq \bigcup I_\alpha \subseteq \langle \bigcup I_\alpha \rangle = B$. Z uzavřenosti $B$ na součty je $ra \in B$ a podobným způsobem ukážeme, že $ar \in B$.

□

► 1.4.5. Definice. Buď $R = (M, +, \cdot)$ okruh. Hlavním ideálem generovaným prvkem $a \in M$ (značíme $I_a$) rozumíme nejmenší ideál v $R$ obsahující prvek $a$.

► 1.4.6. Poznámka. Definice je korektní, neboť každý prvek leží v nějakém ideálu (přinejhorším $a \in R \lhd R$), a existuje nejmenší, neboť průnik systémem ideálů obsahujících $a$ je ideál obsahující $a$ a je nutně nejmenší:

$$I_a = \bigcap_{\substack{J \lhd R \\ a \in J}} J.$$

► 1.4.7. Lemma. Nechť $R$ je asociativní a komutativní okruh, $a \in R$ a označme $J_a := \{ra \mid r \in R^\bullet\}$. Pak $J_a$ je ideál a platí:

**(1)** Má-li $R$ jednotku, je $I_a = J_a$ (tedy $J_a$ je hlavní ideál generovaný $a$).

**(2)** Nemá-li $R$ jednotku, je $I_a = \langle J_a \cup \{a\} \rangle = \{ra + k \times a \mid r \in R^\bullet, k \in \mathbb{Z}\}$.

◦ *Důkaz.* Mějme libovolné $b = ra \in J_a$, kde $r \in R$ a $a \in J_a$ a libovolné $q \in R$. Pak $bq = qb = qra \in R^\bullet a = J^\bullet_a$, tedy $J_a$ splňuje definiční vlastnost ideálu. V hlavním ideálu generovaném $a$ leží všechny součiny tvaru $ra$, tedy nutně $J_a \subseteq I_a$. Pokud navíc existuje jednotka, je $a = 1a \in J_a$, a tedy $J_a = I_a$. Pokud jednotka neexistuje, je nutné $J_a$ rozšířit o násobky $a$. □

► 1.4.8. Definice. Asociativní a komutativní okruh nazveme okruhem hlavních ideálů, je-li v něm každý ideál hlavní.

► 1.4.9. Příklad. Ukážeme, že $Z = (\mathbb{Z}, +, \cdot)$ je okruh hlavních ideálů. Ideály $I_m = \{sm \mid s \in \mathbb{Z}\}$ jsou hlavní. Vezměme si libovolný ideál $I \lhd Z$, pak víme, že $I_+$ je normální podgrupa $Z_+$. Ale $Z_+$ je cyklická, tedy i $I_+$ je cyklická, a tedy existuje generátor $m$ takový, že $I = I_+ = \langle m \rangle = \{k \times m \mid k \in \mathbb{Z}\} = \{sm \mid s \in \mathbb{Z}\}$. Tedy $I = I_m$ a je hlavní.

## 1.5. Homomorfismy

▶ 1.5.1. Definice. Buďte $R_1$, $R_2$ okruhy, $R_i = (M_i, +, \cdot)$. Řekneme, že $h : M_1 \to M_2$ je homomorfismus okruhů, pokud platí:

$$(\forall x, y \in M_1)\big(h(x+y) = h(x) + h(y) \ \wedge \ h(xy) = h(x)h(y)\big).$$

(Tedy $h$ je homomorfismus na okruhu, pokud je homomorfismem na aditivním i multiplikativním grupoidu.)

Značíme $h : R_1 \to R_2$.

▶ 1.5.2. Definice. Podobně, jako na grupách, definujeme na okruzích monomorfismus, epimorfismus, izomorfismus, endomorfismus, automorfismus.

▶ 1.5.3. Definice. Okruhy $R_1$ a $R_2$ jsou izomorfní (značíme $R_1 \cong R_2$), pokud existuje izomorfismus $h : R_1 \to R_2$.

▶ 1.5.4. Lemma. $h(R_1) \Subset R_2$.

▶ 1.5.5. Věta. Je-li $R_1$ asociativní, resp. komutativní, resp s jednotkou, pak tutéž vlastnost má i $h(R_1)$.

▶ 1.5.6. Poznámka. Nepřenáší se vlastnost nemíti dělitele nuly a býti tělesem.

▶ 1.5.7. Definice. Jádrem homomorfismu $h : R_1 \to R_2$ rozumíme množinu $\ker h := h^{-1}(\{0\}) = \{x \in R_1^\bullet \mid h(x) = 0\}$.

▶ 1.5.8. Lemma. Nechť $h$ je homomorfismus. Pak

**(1)** $\ker h \lhd R_1$;

**(2)** $h$ je monomorfní (prostý) právě tehdy, když $\ker h = \{0\}$.

▶ 1.5.9. Věta. Podokruh okruhu $R$ je ideál právě tehdy, je-li jádrem nějakého homomorfismu definovaného na $R$.

▶ 1.5.10. Věta (o homomorfismu okruhů). Buďte $R_1$, $R_2$ okruhy a nechť $h : R_1 \to R_2$ je homomorfismus. Potom $h(R_1) \cong R_1 \,/\, \ker h$.

▶ 1.5.11. Věta. Buďte $R_1$, $R_2$ okruhy, $h : R_1 \to R_2$ monomorfismus. Je-li $R_1$ bez dělitele nuly, resp. tělesem, pak má odpovídající vlastnost i podokruh $h(R_1)$ okruhu $R_2$.

## 1.6. Podílová tělesa

▶ 1.6.1. Věta. Nechť $m \geq 2$. Okruh $Z_m$ je okruhem s děliteli nuly pro $m$ složené a je komutativním tělesem pro $m$ prvočíselné.

◦ *Důkaz.*

**(1)** Mějme $m = uv$ takové, že $u, v < m$. Pak $T_0 = T_m = T_u T_v$ a $T_u, T_v$ jsou dělitelé nuly.

**(2)** Mějme $m \in \mathbb{P}$ a nechť $k$ je takové, že $0 < k < m$. Pak, neboť $\delta(k, m) = 1$, existují $u, v \in \mathbb{Z}$ taková, že $uk + vm = 1$, z čehož $T_u T_k = T_1 - T_v T_m = T_1$, a tedy $T_u = T_k^{-1}$.

□

► 1.6.2. Lemma. Buď $R$ okruh. Potom $R$ je bez dělitelů nuly právě tehdy, lze-li v jeho multiplikativním grupoidu $R_\bullet$ krátit nenulovým prvkem, tj.

$$(\forall a, b, c \in R^\bullet, c \neq 0)\big((ac = bc \vee ca = cb) \Rightarrow a = b\big).$$

◦ *Důkaz.*

(⇒) Platí $0 = ac - bc = (a - b)c$. Neboť $c \neq 0$ a $R$ je bez dělitelů nuly, je $a - b = 0$, a tedy $a = b$. Krácení zleva se ukáže obdobně.

(⇐) Nechť $ab = 0 = 0 \cdot b$ nebo $ba = 0 = b \cdot 0$. Tedy pro $b \neq 0$ je $a = 0$, což znamená, že nejsou oba nenulové.

□

► 1.6.3. Poznámka. Má-li se okruh $R$ vnořit do tělesa, nutně nesmí mít dělitele nuly.

► 1.6.4. Lemma. Nechť okruh $R_1$ lze izomorfně vnořit do okruhu $R_2$ a nechť $R_1^\bullet \cap R_2^\bullet = \emptyset$. Pak existuje okruh $Q$ takový, že $R_1 \Subset Q$ a $Q \cong R_2$.

◦ *Důkaz.* Definujme $Q^\bullet = (R_2^\bullet \setminus h(R_1)) \cup R_1^\bullet$ a definujme zobrazení $g : Q^\bullet \to R_2^\bullet$ následovně:

$$g(x) = \begin{cases} h(x) \text{ pro } x \in R_1^\bullet \\ x \text{ jinak} \end{cases}.$$

Zjevně $g$ je bijekce. To nám umožňuje definovat $Q = (Q^\bullet, \oplus, \odot)$ s operacemi $a \oplus b := g^{-1}(g(a) + g(b))$ a $a \odot b := g^{-1}(g(a) \cdot g(b))$. Pak $g(a \oplus b) = g(a) + g(b)$ a $g(a \odot b) = g(a) \cdot g(b)$, tedy $g$ je homomorfismus, a tedy izomorfismus.

Celkově tedy máme, že $Q \cong R_2$ a $R_1 \Subset Q$. □

► 1.6.5. Věta. Libovolný obor integrity $R$ lze vnořit do komutativního tělesa.

◦ *Důkaz.* Je-li $R = E$, pak jej lze vnořit do triviálního tělesa $F$. Tedy předpokládejme $R \neq E$.

Definujme množinu $M := \{\langle a, b\rangle \mid a, b \in R^\bullet, b \neq 0\}$. Dále definujeme $\equiv$ jako $\langle a, b\rangle \equiv \langle c, d\rangle \Leftrightarrow ad = bc$ a ukážeme, že je ekvivalencí. Reflexivita a symetrie je zřejmá, ukážeme transitivitu. Nechť $ad = bc$ a $cf = de$. Pak $adf = bcf = bed$ a z předchozího lemmatu, z nenulovosti $d$ a z komutativity vidíme, že $af = be$.

Vezměme faktor-množinu $M / \equiv$ a označujme $\frac{a}{b}$ třídu $M / \equiv$ obsahující prvek $\langle a, b\rangle$, tedy $\langle a, b\rangle \in \frac{a}{b} \in M / \equiv$. „Zlomky“ se chovají přirozeně: $\frac{a}{b} = \frac{c}{d} \Leftrightarrow \langle a, b\rangle \equiv \langle c, d\rangle \Leftrightarrow ad = bc$. Lze také krátit nenulovým prvkem: $\frac{ae}{be} = \frac{a}{b}$.

Definujeme okruh $U_R := (M / \equiv, \oplus, \odot)$ jako $\frac{a}{b} \oplus \frac{c}{d} := \frac{ad+bc}{bd}$ a $\frac{a}{b} \odot \frac{c}{d} := \frac{ac}{bd}$. Neboť $R$ neobsahuje dělitele nuly, nemáme ve jmenovateli nulu. Zbývá ukázat korektnost definice: Mějme $\frac{a'}{b'} = \frac{a}{b}$, tj. $a'b = ab'$, a $\frac{c'}{d'} = \frac{c}{d}$, tj. $c'd = cd'$.

Ukážeme, že $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$, tj. $bd(a'd' + b'c') \stackrel{?}{=} b'd'(ad + bc)$, tj. $bda'd' + bdb'c' \stackrel{?}{=} b'd'ad + b'd'bc$, tj. $(a'b)dd' + (c'd)bb' \stackrel{?}{=} (ab')dd' + (cd')bb'$, ale $a'b = ab'$ a $c'd = cd'$, tedy rovnost platí. Podobně lze rozepsat operaci $\odot$. □

Dále definujeme $h : R \to U_R$ jako $h(x) = \frac{xa}{a}$ pro $a \neq 0$ (nezávislost na výběru $a$ je zřejmá). Ukážeme, že $h$ je monomorfismus. Platí $h(x + y) = \frac{(x+y)a}{a} = \frac{xa+ya}{a} = \frac{(xa)a+(ya)a}{aa} = \frac{xa}{a} \oplus \frac{ya}{a}$ a $h(x) \odot h(y) = \frac{xa}{a} \odot \frac{ya}{a} = \frac{xaya}{aa} = \frac{xya}{a}$. Nechť $h(x) = 0$, tj. $ax = 0$, ale $a \neq 0$ a nejsou dělitelé nuly, tedy $x = 0$ a $h$ je prosté.

Celkově tedy máme $R \cong h(R) \Subset U_R$ a podle předchozího lemmatu existuje těleso $T_R$ takové, že $R \Subset T_R \cong U_R$.

► 1.6.6. Definice. Okruh $U_R$ z předchozí věty nazveme <u>těleso zlomků</u>.

► 1.6.7. Poznámka.

**(1)** Každý zlomek tvaru $\frac{0}{b}$ je nulou.

**(2)** Každý zlomek tvaru $\frac{a}{a}$ je jednotkou.

**(3)** Platí $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$.

**(4)** Pro $a \neq 0$ je $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

**(5)** $U_R$ je obor integrity s jednotkou, tedy těleso.

► 1.6.8. Definice. Těleso $T_R$ z předchozí věty nazveme <u>podílové těleso</u> oboru itegrity $R$.

► 1.6.9. Lemma. Buďte $R_1$, $R_2$ obory integrity a $T_1$, $T_2$ jejich podílová tělesa. Pak $R_1 \cong R_2 \Rightarrow T_1 \cong T_2$.

◦ *Důkaz.* Existuje izomorfismus $h : R_1 \to R_2$ a definujme izomorfismus $\bar{h} : U_1 \to U_2$ jako $\bar{h}\left(\frac{a}{b}\right) = \frac{h(a)}{h(b)}$. Je třeba triviálně ukázat, že obraz nezavisí na reprezentantu $\frac{a}{b}$, že $h(b) \neq 0$ a že $\bar{h}$ je izomorfismus. Tedy máme $T_1 \cong U_1 \cong U_2 \cong T_2$. □

► 1.6.10. Lemma. Těleso $T_R$ je nejmenší těleso obsahující obor integrity $R$.

◦ *Důkaz.* Nechť $S$ je libovolné těleso a $R \Subset S$. Definujeme $h : U_R \to S$ jako $h\left(\frac{a}{b}\right) = ab^{-1}$, což můžeme, protože $a$, $b$ jsou prvky tělesa a $b \neq 0$. Opět definice nezávisí na reprezentantu.

Ukážeme, že zobrazení $h$ je homomorfismus. $h\left(\frac{a}{b} \oplus \frac{c}{d}\right) = h\left(\frac{ad+bc}{bd}\right) = (ad + bc)(bd)^{-1} = add^{-1}b^{-1} + bcd^{-1}b^{-1} = ab^{-1} + cd^{-1} = h\left(\frac{a}{b}\right) + h\left(\frac{c}{d}\right)$. Zachování součinu se ověří podobně. Opomněli jsme ověřit, že prvky inverzní k prvkům z oboru integrity komutují. Tedy nechť $xy = yx$, pak $y = x^{-1}yx$, a tedy $yx^{-1} = x^{-1}y$. Opět $h\left(\frac{a}{b}\right) = 0 \Leftrightarrow ab^{-1} = 0 \Leftrightarrow a = 0$, tedy $h$ je prosté.

Celkově dostáváme, že $T_R \cong U_R \cong h(U_R) \Subset S$. □

► 1.6.11. Důsledek. Podílové těleso komutativního tělesa $T$ (jako oboru integrity) je izomorfní s $T$.

## 1.7. Charakteristika tělesa

► 1.7.1. Poznámka. Řád jednotky 1 jako prvku aditivní grupy $T_+$ tělesa $T$ je nejmenší přirozené číslo $n \in \mathbb{N}$ takové, že $n \times 1 = \underbrace{1 + \cdots + 1}_{n\text{-krát}} = 0$. Pokud $(\forall n \in \mathbb{N})(n \times 1 \neq 0)$, má jednotka nekonečný řád.

► 1.7.2. Lemma. Jednotka má v $T_+$ řád nekonečný nebo prvočíselný.

○ *Důkaz.* Lemma dokážeme sporem. Nechť $n = uv$ a $u, v < n$. Pak $(u \times 1) \cdot (v \times 1) = (1 + \ldots + 1)(1 + \ldots + 1) = (uv) \times 1 = n \times 1 = 0$, tedy $u \times 1$ a $v \times 1$ jsou dělitelé nuly, což je spor. □

► 1.7.3. Definice. Řekneme, že těleso $T$ má charakteristiku (značíme $ch\ T$) $p \in \mathbb{P}$, resp. 0, má-li jednotka v $T_+$ řád $p$, resp. nekonečný.

► 1.7.4. Důsledek.

**(1)** Všechna číselná tělesa (např. $Q$, $R$, $C$) mají charakteristiku 0.

**(2)** Každé konečné těleso má nenulovou charakteristiku.

**(3)** Těleso zbytkových tříd $Z_p$ má charakteristiku $p$.

► 1.7.5. Věta. Buď $T$ těleso charakteristiky $p$, resp. 0. Pak libovolný prvek $a \in T^\bullet$, $a \neq 0$ má v $T_+$ řád $p$, resp. nekonečný.

○ *Důkaz.* Platí $n \times a = a + \ldots + a = 1a + \ldots + 1a = (1 + \cdots + 1)a = (n \times 1)a$. Tedy $n \times a = 0 \Leftrightarrow n \times 1 = 0$, což jsme chtěli ukázat. □

## 1.8. Prvotěleso

► 1.8.1. Definice. Prvotělesem tělesa $T$ rozumíme jeho nejmenší podtěleso (průnik všech jeho podtěles). Prvotěleso značíme $P_T$.

► 1.8.2. Věta. Buď $T$ těleso charakteristiky $p$, resp. 0. Potom prvotěleso $T$ je izomorfní s tělesem zbytkových tříd $Z_p$, resp. s tělesem racionálních čísel $Q$.

○ *Důkaz.* Označme $P_T$ prvotěleso tělesa $T$. Pak nutně $1 \in P_T$. Definuji $S := \{k \times 1 \mid k \in \mathbb{Z}\}$ a nutně $S \subseteq P_T$. Platí $(k \times 1) - (\ell \times 1) = (k - \ell) \times 1 \in S$ a $(\ell \times 1)(k \times 1) = \ell k \times 1 \in S$, tedy $S$ je podokruh okruhu $T$.

Definujeme $h : Z \to S$ jako $h(k) = k \times 1$. Snadno ukážeme, že $h$ je epimorfismus. Podle věty o homomorfismu je $h(Z) = S \cong Z / \ker h$.

Zkoumejme následující 2 možné případy:

($\mathrm{ch}\, T = p \in \mathbb{P}$) Pak $\ker h = \{k \in \mathbb{Z} \mid k \times 1 = 0\} = I_p$. Tedy $S \cong Z / I_p = Z_p$, a protože $p$ je prvočíslo, je $Z_p$ těleso. Z izomorfie $S$ je také tělesem a platí $S \subset P_T$, a neboť $S$ je těleso a $P_T$ je nejmenší podtěleso, platí $S = P_T$ a $P_T \cong Z_p$.

(ch $T = 0$) Pak $k \times 1 = 0 \Leftrightarrow k = 0$ a $\ker h = E = \{0\}$. A tedy $S \cong Z/E \cong Z$, ale $Z$ není tělesem, je pouze oborem integrity, tedy i $S$ je oborem integrity a existují podílová tělesa $T_S$ a $T_Z$, která jsou izomorfní. Vezměme $U_S$ a definujme $g : U_S \to T$ jako $g\left(\frac{a}{b}\right) = ab^{-1}$. O tomto zobrazení jsme již dříve ukázali, že je monomorfismus, tedy $U_S \cong g(U_S) \Subset T$ (podtělesem). Ukážeme, že $g(U_S) = P_T$.

(⊆) $P_T$ je nejmenší podtěleso, tedy $P_T \subseteq g(U_S)$.

(⊇) Mějme libovolné $y \in g(U_S)$, $y = ab^{-1}$, kde $a, b \in S \subseteq P_T$. Ale $P_T$ je těleso, tedy $y \in P_T$.

Tedy celkově máme $P_T = g(U_S) \cong U_S \cong T_S \cong T_Z = Q$.

□

► 1.8.3. Poznámka.

**(1)** Okruh $Z$ nemá dělitele nuly, ale $Z_m$ pro $m$ složené mají dělitele nuly. To dává protipříklad k domněnce, že obecný homomorfismus zachová vlastnost nemíti dělitele nuly.

**(2)** Nechť $T$ je jednoduchý okruh, tj. jediné jeho ideály jsou $E$ a $T$. Ale všechny ideály jsou jádra všech homomorfismů. Tedy buď $\ker h = E$ a $h$ je monomorfismus, nebo $\ker h = T$ a $h(T) = \{0\}$, což zjevně není tělesem. To dává protipříklad k domněnce, že obecný homomorfismus zachovává tělesovost.