1 Základné definície

Definícia 1. *Okruh* $(R, +, \cdot)$ je množina R spolu s dvoma binárnymi operáciami $+$ a $\cdot$ taká, že $(R, +)$ je komutatívna grupa, operácia $\cdot$ je asociatívna a platia distributívne zákony

$$a.(b+c) = a.b + a.c$$
$$(b+c).a = b.a + c.a$$

Ak je navyše operácia $\cdot$ komutatívna, hovoríme o *komutatívnom okruhu* a ak má neutrálny prvok, hovoríme o *okruhu s jednotkou.*

Teleso je okruh, v ktorom je každý prvok rôzny od 0 invertibilný (existuje k nemu inverzný prvok vzhľadom na operáciu $\cdot$). Komutatívne teleso nazývame *pole.*

Okruh bez deliteľov nuly je taký okruh, v ktorom platí

$$a.b = 0 \qquad \Rightarrow a = 0 \vee b = 0.$$

Obor integrity je komutatívny okruh s jednotkou bez deliteľov nuly.

Definícia 2. Neprázdnu podmnožinu I okruhu A nazývame *ideálom* okruhu A, ak

(i) $x, y \in I \Rightarrow x - y \in I$,

(ii) $x \in I, a \in A \Rightarrow ax \in I, xa \in I$.

I je *vlastný ideál,* ak $I \neq A$.

Veta 1. *Ak I je ideál okruhu A, tak množina A/I všetkých tried aditívnej grupy A podľa podgrupy I s operáciami*

$$(a+I) + (b+I) = (a+b) + I$$
$$(a+I)(b+I) = ab + I$$

tvorí okruh. Tento okruh nazývame faktorový okruh *A podľa I. Ak A je komutatívny, resp. obsahuje jednotku, tak aj A/I je komutatívny, resp. obsahuje jednotku.*

Definícia 3. Ideál I okruhu A nazývame *prvoideál*, ak

$$\forall a, b \in A : ab \in I \Rightarrow a \in I \vee b \in I.$$

Ideál I okruhu A nazývame *maximálny*, ak $I \neq A$ a ak pre každý ideál J $I \subset J \subset A$ implikuje $J = I$ alebo $J = A$.

Každý maximálny ideál je prvoideál.

Veta 2. *Faktorový okruh A/I komutatívneho okruhu A s jednotkou je poľom práve vtedy, keď I je maximálny ideál.*

Faktorový okruh A/I komutatívneho okruhu A s jednotkou je oborom integrity práve vtedy, keď I je vlastný prvoideál.

Definícia 4. Hovoríme, že prvok $x \in A$ generuje ideál I komutatívneho okruhu A s jednotkou, ak $I = xA = \{xa; a \in A\}$.

Ideál I okruhu A nazývame *hlavným ideálom,* ak je generovaný niektorým prvkom $x \in A$.

Komutatívny okruh A nazývame *okruh hlavných ideálov*, ak každý ideál okruhu A je hlavný.

Ideál generovaný prvkom x sa zvykne označovať aj ako (x).

Príkladom okruhu, ktorý nie je okruhom hlavných ideálov, je okruh $Z[x]$ všetkých polynómov s celočíselnými koeficientami. Ak totiž v tomto okruhu vezmeme ako ideál I ideál generovaný polynómami 2 a x, tak dostaneme všetky polynómy, ktorých absolútny koeficient je párny. Tento ideál nemôže byť generovaný jediným polynómom.

Veta 3. *V okruhu hlavných ideálov je každý prvoideál maximálny.*

2 Okruhy

1. Zistite, či v nasledujúcich príkladoch ide o (komutatívny) okruh, či má jednotku, či je to obor integrity, teleso, pole.
   a) $(2\mathbb{Z}, +, \cdot)$,
   b) matice 2×2 s obvyklým sčitovaním a násobením matíc,
   c) $Q_n = \{\frac{p}{q}; p \in \mathbb{Z}, q \in \mathbb{Z}, n \mid q\}$, kde $n \in \mathbb{Z}$ je pevne zvolené prirodzené číslo (opäť obvyklý súčet a súčin),
   d) $C(a, b) =$ reálne funkcie spojité na intervale $\langle a, b\rangle$ (zvyčajné sčitovanie a násobenie funkcií),
   e) Nech $D \subseteq \mathbb{R}$ a $M = \{f : \mathbb{R} \to \mathbb{R}; f(x) = 0$ pre všetky $x \in D\}$ (zvyčajné sčitovanie a násobenie funkcií)

2. Nech p je prvočíslo. Potom množina $\{\frac{m}{n}; m, n \in \mathbb{Z}, p \nmid n\}$ s obvyklým sčítaním a násobením tvorí okruh. Ku ktorým prvkom z tohto okruhu existuje inverzný prvok vzhľadom na násobenie?

3. Nech R je obor integrity. Potom:
   a) Pre ľubovoľné $a \neq 0$ platí $ax = ay \Rightarrow x = y$.
   b) Ak $a \in R$ a $a \neq 0$, tak zobrazenie $x \mapsto ax$ je injektívne.
   c) Každý konečný obor integrity je pole.

4. Nech R je okruh. Prvok $x \in R$ sa volá *nilpotentný,* ak existuje $n \in \mathbb{N}$, $n > 0$, také, že $x^n = 0$. Dokážte, že ak x je nilpotentný, tak $1 + x$ aj $1 - x$ majú inverzné prvky vzhľadom na násobenie.

5. Ukážte, že matice typu $n \times n$ s obvyklým sčitovaním a násobením matíc tvoria okruh.

6. Ak m je nepárne, má 2 inverzný prvok v okruhu $\mathbb{Z}_m$? Má ho, ak m je párne?

7. Nech X je neprázdna množina. Potom $(\mathcal{P}(X), \triangle, \cap)$ tvorí okruh. (Znak $\triangle$ označuje symetrickú diferenciu). Všimnite si, že v tomto okruhu pre všetky prvky $x^2 = 1$. Takéto okruhy sa nazývajú *Booleove.*

8. Nech $(R, +, \cdot)$ je okruh s jednotkou. Dokážte, že pre operácie $\oplus$, $\odot$ definované ako $x \oplus y = x + y - 1$ a $x \odot y = x + y - xy$ je $(R, \oplus, \odot)$ okruh s jednotkou. Nájdite jednotku a nulu v tomto okruhu. Overte ďalej, že ak definujeme $x' = 1 - x$, tak $(x.y)' = x' \odot y'$. Všimnite si, že v okruhu z úlohy 7 posledná rovnosť vyjadruje jedno z de Morganových pravidiel.

9. Je $(\mathbb{R} \setminus \{0\}, \cdot, *)$, kde $\cdot$ označuje obvyklé násobenie a $a * b = 1$ pre všetky $a, b \in \mathbb{R}$, okruh?

10. Ukážte, že $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ s obvyklým sčitovaním a násobením je komutatívny okruh s 1.

11. Nech $(G, *)$ je komutatívna grupa. Ako $\mathrm{End}(G)$ označme množinu všetkých endomorfizmov grupy G. (Endomorfizmus je homomorfizmus $G \to G$.) Dokážte, že $(\mathrm{End}(G), *, \circ)$ je okruh. Je komutatívny, má jednotku? (Pre endomorfizmy $f, g \in \mathrm{End}(G)$ definujeme $f * g$ ako $x(f * g) = (xf) * (xg)$.)

12. Nech P je množina všetkých polynómov s reálnymi koeficientmi. Je $(P, +, \circ)$ komutatívny okruh s jednotkou?

13. Ako $Z[X]$ označme množinu všetkých polynómov s celočíselnými koeficientami. Dokážte, že $Z[X]$ s obvyklým násobením a sčitovaním tvorí okruh.

14. Je $Z \times Z$ (s obvyklým násobením a sčitovaním) okruh? Je komutatívny, má jednotku?

3 Ideály, faktorové okruhy

1. Ak F je pole, tak jediné ideály F sú $\{0\}$ a F.

2. Ak I a J sú ideály okruhu R, tak aj $I \cap J$ a $I + J = \{a + b; a \in I, b \in J\}$ sú ideály okruhu R.

3. Ak I a J sú ideály okruhu R, tak definujeme IJ ako množinu všetkých konečných súčtov $\sum_{k=1}^{n} a_k b_k$, kde $a_k \in I$, $b_k \in J$. Dokážte, že IJ je tiež ideál okruhu R.

4. Nech $Z[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$. Ukážte, že $Z[\sqrt{2}]$ (s obvyklým sčitovaním a násobením) je okruh, ale nie je pole.

5. Ak M_1, M_2 sú ideály okruhu R také, že $M_1 + M_2 = R$, tak $M_1^2 + M_2^2 = R$. (Pod označením M_1^2 tu rozumieme $M_1 M_1$ v zmysle súčinu 2 ideálov definovaného v úlohe **??**)

6. Nech R je komutatívny okruh a M, L sú ideály v okruhu R.
   a) Ukážte, že $M.L \subseteq M \cap L$
   b) Nájdite príklad, pre ktorý $ML \neq M \cap L$.

7. Nech R je okruh všetkých spojitých funkcií na intervale $\langle 0, 1\rangle$. Ukážte, že pre ľubovoľné pevne zvolené $x \in \langle 0, 1\rangle$ je $\{f \in R; f(x) = 0\}$ ideál okruhu R. Dokážte, že je to maximálny ideál. (Hint: Na dôkaz, že tento ideál je maximálny sa dá použiť veta o faktorovom izomorfizme.)

4 Polia

1. Ktoré z uvedených množín tvoria vzhľadom na obvyklé sčitovanie a násobenie pole?
   a) $F = \{a + ib; a \in R, b \in R, b \geq 0\}$
   b) $F = \{a + ib; a \in Q, b \in Q\}$
   c) $F = \{a + ib; a \in Z, b \in Z\}$
   d) $F = \{a + b\sqrt{5}; a \in Q, b \in Q\}$
   e) $F = \{a + \sqrt{3}ib; a \in Q, b \in Q\}$
   f) $F = \{a + \frac{b}{\sqrt{2}}; a \in Q, b \in Q\}$
   g) $F = \{a + b\sqrt[3]{5}; a \in Q, b \in Q\}$
   h) $F = \{a + b\sqrt{4} + c\sqrt[3]{4}; a \in Q, b \in Q\}$

2. *Automorfizmom* poľa F nazývame ľubovoľný izomorfizmus $\varphi\colon F \to F$. Nech φ je automorfizmus poľa $\mathbb{R}$. Potom:
a) Platí $\varphi(a) = a$ pre všetky $a \in \mathbb{Q}$. b) Ak $a \geq 0$, tak $\varphi(a) \geq 0$. c) Zobrazenie φ zachováva usporiadanie (čiže $a \geq b \Rightarrow \varphi(a) \geq \varphi(b)$). d) Jediný automorfizmus poľa $\mathbb{R}$ je identita.

3. Dokážte, že jediné automorfizmy poľa $\mathbb{C}$ komplexných čísel, ktoré zobrazujú $\mathbb{R}$ do $\mathbb{R}$, sú identita $x+yi \mapsto x+yi$ a kongjugácia $x+yi \mapsto x-yi$ (inak: prvé zobrazenie zobrazuje z na z a druhé z na komplexne združené číslo $\overline{z}$).

4. Zistite pre aké n je $\mathbb{Z}_n$ obor integrity? Kedy to je pole?

5. Nech R je okruh a $F \subseteq R$ je množina všetkých prvkov R, ktoré majú inverzný prvok vzhľadom na násobenie. Ukážte, že potom F s násobením je grupa. Musí byť F pole?

6. Nájdite prvok $x \in \mathbb{Z}_{34}$ taký, že všetky invertibilné prvky $\mathbb{Z}_{34}$ sú mocninami x. Nájdite prvok $x \in Z_{23}$ taký, že všetky nenulové prvky Z_{23} sú jeho mocninami.