

## Cvičenie 8

### Okruhy, ideály, faktorizácia

**Na pripomenutie:** Veta o izomorfizme platí pre okruhy v rovnakom znení ako pre grupy (iba normálne podgrupy sa nahradia ideálmi).

Ak Nech  $R$  je komutatívny okruh s jednotkou a  $I$  je ideál v  $R$ , tak:

$R/I$  je pole práve vtedy, keď  $I$  je maximálny ideál,

$R/I$  je oborom integrity práve vtedy, keď  $I$  je vlastný prvoideál.

Každý maximálny ideál je prvoideál.

1. Nech  $F$  je pole a  $I \neq \emptyset$ . Nech Dokážte, že v okruhu  $F^I$  je každý ideál tvaru  $M_p = \{f \in F^I; f(p) = 0\}$ , kde  $p$  je nejaký prvok z  $I$ , maximálny. (Hint: Je faktorový okruh poľom?)
2. Ak pre každé  $n \in \mathbb{N}$  je  $I_n$  ideál v okruhu  $R$  a navyše platí  $I_n \subseteq I_{n+1}$ , tak aj zjednotenie  $\bigcup_{i=1}^{\infty} I_i$  je ideál v  $R$ .
3. Okruh  $R$  sa volá boolovský okruh, ak pre každé  $a \in R$  platí  $a^2 = a$ . Dokážte, že každý boolovský okruh je komutatívny. (Boolovským okruhom je napríklad okruh  $(P(X), \Delta, \cap)$  z minulého cvičenia.)
4. Nech  $R$  je komutatívny okruh s jednotkou. Dokážte, že v ňom platí binomická veta

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} \times a^k b^{n-k}.$$

5. Nech  $R$  je ľubovoľný okruh a  $a \in R$ . Potom množina  $\{ax; x \in R\}$  je ideál v  $R$ . Tento ideál označujeme  $(a)$  a takéto ideály nazývame hlavné.
6. Zistite, s akými okruhmi sú izomorfné okruhy  $\mathbb{Z}_{60}/(15)$ ,  $\mathbb{Z}_{60}/(20)$ ,  $\mathbb{Z}_{60}/(12)$ .
7. Zistite, či dané ideály v okruhu  $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$  (s obvyklým sčítaním a násobením komplexných čísel) sú maximálne ideály/prvoideály. (Hint: Na zodpovedanie tejto otázky by možno stačilo zistiť počet tried rozkladu. Samozrejme, možné sú aj úplne iné riešenia.)
  - a)  $(1 + i) = \{(1 + i)z; z \in \mathbb{C}\}$
  - b)  $(2) = \{2z; z \in \mathbb{C}\}$
  - c\*)  $(2 + i) = \{(2 + i)z; z \in \mathbb{C}\}$
8. Ak  $I_1, I_2$  sú ideály v okruhu  $(R, +, \cdot)$ , tak aj
  - a)  $I_1 + I_2 = \{a + b; a \in I_1, b \in I_2\}$  je ideál v  $R$ .
  - b)  $I_1 \cdot I_2 = \{a_1 b_1 + \dots + a_n b_n; n \in \mathbb{N}, a_i, b_i \in R\}$  je ideál v  $R$ .
9. Nech  $(G, *)$  je cyklická grupa,  $a$  je jej generátor, t.j.  $G = [a]$ . Ak definujeme operáciu  $\cdot$  ako  $a^k \cdot a^l = a^{k \cdot l}$  (pre ľubovoľné  $k, l \in \mathbb{Z}$ ), tak  $(G, *, \cdot)$  je okruh. Viete povedať (v závislosti od rádu generátora  $a$ ) s akým okruhom je tento okruh izomorfný?