# Domácí úkol č.4 - Galoisova tělesa

1. Je dáno těleso $\mathbb{Z}_{37}$.

   a) Najděte primitivní prvek tohoto tělesa.

   b) Najděte všechny prvky řádu 6 v tomto tělese.

   c) Najděte všechny kořeny polynomu $x^8 - 1$ v tomto tělese.

2. Je dáno těleso $A = \mathbb{Z}_2[x]/x^6 + x + 1$.

   a) Ověřte, že okruh $A$ skutečně tvoří těleso. Popište jeho prvky ve tvaru polynomů v proměnné $\alpha$ a napište přepisovací pravidla potřebná pro násobení.

   b) Ověřte, že $\alpha$ je primitivním prvkem tělesa $A$.

   c) Najděte všechny prvky řádu tři v tělese $A$ a také všechny kořeny polynomu $x^3 - 1$ v $A$.

   d) Najděte všechny kořeny polynomu $q(x) = x^6 + x + 1$ v tělese $A$.

3. Je dáno těleso $B = \mathbb{Z}_5[x]/x^2 + x + 1$.

   a) Ověřte, že okruh $B$ tvoří těleso. Napište jeho prvky ve tvaru polynomů v proměnné $\alpha$ a napište přepisovací pravidla pro násobení. Kolik prvků má toto těleso?

   b) Ověřte, že $\alpha + 2$ je primitivní prvek tělesa $B$. Kolik je zde primitivních prvků?

   c) Řešte rovnici $x^9 = 1$ v tělese $B$.

   d) Najděte minimální polynom pro prvek $\alpha$ a minimální polynom pro prvek $\alpha + 2$.

   e) Najděte všechny kořeny polynomu $t(x) = x^3 + x^2 + 4x + 2$ v tělese $B$, prozradíme-li, že prvek $\alpha + 1$ je jeho kořenem (ověřte si to).

4. Je dán okruh $K = \mathbb{Z}_5[x]/x^2 + 1 = \mathbb{Z}_5[i]$ komplexních čísel nad $\mathbb{Z}_5$.

   a) Ověřte, že okruh $K$ netvoří těleso.

   b) Dokažte, že grupa $K^*$ invertibilních prvků v okruhu $K$ není cyklická.

**Výsledky**

1. a) primitivní prvek je např. 2, neboť $r(2) = 36$

   b) prvky řádu 6 jsou dva, a to 11 a 27

   c) kořeny jsou v podgrupě $< 2^9 >= \{\pm 1, \pm 6\}$

2. a) $x^6 + x + 1$ je ireducibilní nad $\mathbb{Z}_2$, neboť nemá kořen a není dělitelný ireducibilními polynomy stupně 2 a 3, tedy $A$ je těleso

   $A = \{\sum_{i=0}^{5} a_i \alpha^i, a_i \in \mathbb{Z}_2, \alpha^6 = \alpha + 1, \ldots, \alpha^{10} = \alpha^5 + \alpha^4\}$

   b) $\alpha^9 \neq 1$ a $\alpha^{21} \neq 1$, tedy $r(\alpha) = 63$

   c) prvky řádu 3 jsou dva $\alpha^{21} = \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$ a $\alpha^{42} = \alpha^5 + \alpha^4 + \alpha^3 + \alpha$, kořeny polynomu $x^3 - 1$ jsou v podgrupě $< \alpha^{21} >= \{\alpha^{21}, \alpha^{42}, 1\}$

   d) kořeny jsou $\alpha$, $\alpha^2$, $\alpha^4$, $\alpha^8 = \alpha^3 + \alpha^2$, $\alpha^{16} = \alpha^4 + \alpha + 1$ a $\alpha^{32} = \alpha^3 + 1$

3. a) $x^2 + x + 1$ je ireducibilní nad $\mathbb{Z}_5$, neboť nemá kořen v $\mathbb{Z}_5$, tedy $B$ je těleso

   $B = \{a\alpha + b, a, b \in \mathbb{Z}_5, \alpha^2 = -\alpha - 1\}$, $|B| = 5^2 = 25$

   b) $\alpha + 2$ je primitivní prvek, neboť $r(\alpha + 2) = 24$, celkem jich je $\varphi(24) = 8$

   c) Řešení jsou tři ($\gcd(9, 24) = 3$) a leží v podgrupě $\langle \alpha \rangle = \{\alpha, 4\alpha + 4, 1\}$.

   d) $m_\alpha(x) = x^2 + x + 1$, pomocí něhož bylo vytvořeno těleso $B$,

   $m_{\alpha+2}(x) = (x - (\alpha + 2))(x - (4\alpha + 1)) = x^2 + 2x + 3$

   e) kořeny jsou $(\alpha + 1)$, $(\alpha + 1)^5 = 4\alpha$, 3

4. a) $x^2 + 1$ není ireducibilní nad $\mathbb{Z}_5$, neboť má kořeny 2 a 3 v $\mathbb{Z}_5$, tedy rozkládá se na $x^2 + 1 = (x + 2)(x + 3)$.

   b) $K^* = \{a, ai, a(i + 1), a(i + 4), a \in \mathbb{Z}_5^*\}$, celkem 16 prvků. Maximální řád prvku v $K^*$ je však 4.