Algebra — cvičení 12

(příklady cihlovou barvou jsme dělali on-line, na doma jsou ty ostatní bez hvězdiček)

deg m_{a,T} = [T(a) : T]

Minimální polynomy a tělesová rozšíření

1. Nalezněte minimální polynomy $m_{a,T}$ následujících prvků $a \in S$ nad T:

   (a) $a = -1 + i$, $S = \mathbb{C}$, $T = \mathbb{Q}$, (x+1)^2+1 = x^2 + 2x + 2

   (b) $a = \sqrt{2}i$, $S = \mathbb{C}$, $T = \mathbb{Q}(i)$,

   x^4-6 ... ireducibilní nad Q (Eisenstein pro 2 nebo 3 + Gaussovo lemma)

   (c) $a = \sqrt[4]{6}$, $S = \mathbb{R}$, $T = \mathbb{Q}$,

   (d) $a = \sqrt[4]{2}$, $S = \mathbb{R}$, $T = \mathbb{Q}(\sqrt{2})$,

   (e) $a = \sqrt{2} + \sqrt{5}$, $S = \mathbb{R}$, $T = \mathbb{Q}$,

   (f) $a = \sqrt{2} + \sqrt{5}$, $S = \mathbb{R}$, $T = \mathbb{Q}(\sqrt{2})$, (x - sqrt(2))^2 - 5 = x^2 - 2xsqrt(2) - 3

   (g) $a = \sqrt{2} + \sqrt{5}$, $S = \mathbb{R}$, $T = \mathbb{R}$,

   (h)* $a = \sqrt{2}$, $S = \mathbb{R}$, $T = \mathbb{Q}(\sqrt{2} + \sqrt{5})$,

   (i)* $a = t^3$, $S = \mathbb{Z}_2(t)$, $T = \mathbb{Z}_2(t + t^2)$ (čili t je proměnná a $T = \mathbb{Z}_2(b)$ pro $b = t + t^2 \in \mathbb{Z}_2[t] \subsetneq S$).

2. Nalezněte nějakou bázi $T(a)$ nad T v případech (a), (c) a (e) v úloze 1 a určete stupeň rozšíření $T(a) \geq T$. Q(-1+i) = Q(i) (1, i) vždy bude báze tvaru (1, a, a^2, ..., a^{n-1}), kde [T(a) : T] = n

3. Určete stupeň rozšíření $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}]$ a nalezněte nějakou bázi $\mathbb{Q}(\sqrt[3]{3})$ nad $\mathbb{Q}$. Je $\mathbb{Q}(\sqrt[3]{3})$ rozkladové nadtěleso nějakého polynomu z $\mathbb{Q}[x]$?

4. Víte-li, že $m_{\sqrt{2}+i,\mathbb{Q}} = x^4 - 2x^2 + 9$, nalezněte $m_{\sqrt{2}+i+1,\mathbb{Q}}$ (a rozmyslete si, že je to skutečně on)!

5. Kterému známému okruhu je izomorfní faktorokruh $\mathbb{Q}[x]/(x^2 + a)$, pro

   (a) $a = 2$,

   (b) $a = -4$?

6. Nechť $a \in S$ je algebraický nad T (kde $T \leq S$) a nechť $b \in S$ splňuje $m_{a,T}(b) = 0$. Rozmyslete si, že pak $m_{a,T} = m_{b,T}$.

7. Nechť $T \leq S$ jsou tělesa taková, že $[S : T]$ je prvočíslo. Dokažte, že pak $S = T(a)$ pro *libovolný* prvek $a \in S \setminus T$.

8.* Nechť T je těleso a a algebraický prvek nad T takový, že $[T(a) : T]$ je lichý. Dokažte, že $T(a) = T(a^2)$.

9.* Nechť a, b jsou algebraické prvky nad T takové, že jejich minimální polynomy $m_{a,T}$, $m_{b,T}$ mají nesoudělné stupně. Dokažte, že pak $m_{a,T} = m_{a,T(b)}$ a $m_{b,T} = m_{b,T(a)}$.

10.* Dokažte, že $\mathbb{Q}(\sqrt{2} + \sqrt[3]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

11.* Není těžké ukázat, že zobrazení

$$f : \mathbb{Q}[\sqrt{3}] \to \left\{ \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}; \qquad a + b\sqrt{3} \mapsto \begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$$

   je izomorfismus okruhů (a dokonce těles). Vymyslete, jak vám může f pomoci k výpočtu minimálních polynomů prvků z $\mathbb{Q}(\sqrt{3})$ nad $\mathbb{Q}$.

12.* Užitím 2. věty o izomorfismu pro okruhy dokažte, že pro prvočíslo p platí $\mathbb{Z}_p[x]/(x^2 + 1) \cong \mathbb{Z}[i]/(p)$. Na základě toho identifikujte, která prvočísla jsou ireducibilními prvky v $\mathbb{Z}[i]$. Nakonec pro p, jež ireducibilní nejsou, ukažte, že existují $a, b \in \mathbb{Z}$ splňující $a^2 + b^2 = p$.