13. Algebrou za lepší svět

Minimální polynomy a tělesová rozšíření

1. Nalezněte minimální polynomy $m_{a,\mathbf{T}}$ následujících prvků $a \in \mathbf{S}$ nad $\mathbf{T}$ a příslušné stupně tělesových rozšíření $T(a) \geq \mathbf{T}$:

a	$\mathbf{S}$	$\mathbf{T}$	$m_{a,\mathbf{T}}$	$[\mathbf{T}(a) : \mathbf{T}]$
$\sqrt[4]{6}$	$\mathbb{R}$	$\mathbb{Q}$	$[x^4 - 6]$	[4]
$-1 + i$	$\mathbb{C}$	$\mathbb{Q}$	$[x^2 + 2x + 2]$	[2]
$\sqrt{2}i$	$\mathbb{C}$	$\mathbb{Q}(i)$	$[x^2 + 2]$	[2]
$\sqrt[4]{2}$	$\mathbb{R}$	$\mathbb{Q}(\sqrt{2})$	$[x^2 - \sqrt{2}]$	[2]
$\sqrt{2} + \sqrt{5}$	$\mathbb{R}$	$\mathbb{Q}$	$[x^4 - 14x^2 + 9]$	[4]
$\sqrt{2} + \sqrt{5}$	$\mathbb{R}$	$\mathbb{Q}(\sqrt{2})$	$[(x - \sqrt{2})^2 - 5 = x^2 - 2\sqrt{2}x - 3]$	[2]
$\sqrt{2} + \sqrt{5}$	$\mathbb{R}$	$\mathbb{R}$	$[x - \sqrt{2} - \sqrt{5}]$	[1]

2. Nalezněte nějaké báze $\mathbf{T}(a)$ nad $\mathbf{T}$ v předchozím příkladě pro $a = -1 + i$, resp. $\sqrt[4]{6}$, $\sqrt{2} + \sqrt{5}$

   [vždy lze využít první řádek důkazu Tvrzení 22.3]

3. Určete stupeň rozšíření $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}]$ a nalezněte nějakou bázi $\mathbb{Q}(\sqrt[3]{3})$ nad $\mathbb{Q}$.

   [$[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$, báze např, $\{1, \sqrt[3]{3}, \sqrt[3]{9}\}$]

4. Připomeňme značení $\zeta_n = e^{2\pi i/n}$.

   (a) Spočtěte minimální polynom $m_{a,\mathbb{Q}}$ pro prvky

   (i) ζ_3 $[x^2 + x + 1]$

   (ii) ζ_5 $[x^4 + x^3 + x^2 + x + 1$; ireducibilita se ověří pomocí př. 16 z pátého cvičení, tj. skrze substituci $x \mapsto x + 1$ a následně Eisensteinovým kritériem]

   (iii) $\zeta_7 + \zeta_7^{-1}$. $[x^3 + x^2 - 2x - 1$; pro prvek ζ_7 platí $1 + \zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 + \zeta_7^6 = 0$. Dál si z rovnosti $\zeta_7^7 = 1$ můžeme všinout, že $\zeta_7^6 = \zeta_7^{-1}, \zeta_7^5 = \zeta_7^{-2}$ a $\zeta_7^4 = \zeta_7^{-3}$. Dohromady tedy $1 + (\zeta_7 + \zeta_7^{-1}) + (\zeta_7^2 + \zeta_7^{-2}) + (\zeta_7^3 + \zeta_7^{-3}) = 0$. Dál si stačí všimnout, že každý z prvků $\zeta_7^k + \zeta_7^{-k}$ jde vyjádřit jako polynomiální kombinaci prvku $\zeta_7 + \zeta_7^{-1}$, speciálně: $\zeta_7^2 + \zeta_7^{-2} = (\zeta_7 + \zeta_7^{-1})^2 - 2$, a $\zeta_7^3 + \zeta_7^{-3} = (\zeta_7 + \zeta_7^{-1})^3 - 3(\zeta_7 + \zeta_7^{-1})$. Dohromady dostáváme $\zeta_7 + \zeta_7^{-1})^3 + (\zeta_7 + \zeta_7^{-1})^2 - 2(\zeta_7 + \zeta_7^{-1}) - 1 = 0$. Jen si je potřeba rozmyslet, že tohle už opravdu dává minimální polynom.]

   (b) Spočtěte dimenzi a najděte nějakou bázi vektorového prostoru $\mathbb{Q}(\zeta_n)_\mathbb{Q}$ pro n rovno

   (i) 5 [4; báze $\{(\zeta_5)^i \mid i = 0, \ldots, 3\}$] (ii) 6 [2; báze $\{1, \zeta_6\}$] (iii) 8. [4; báze $\{(\zeta_8)^i \mid i = 0, \ldots, 3\}$ (ohledně ireducibility polynomu $x^4 + 1$ opět viz páté cvičení, př. 17)]

5. 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).

   $[(x-1)^4 - 2(x-1)^2 + 9 = x^4 - 4x^3 + 4x^2 + 8]$

6. Určete stupeň rozšíření nejmenšího kořenového nadtělesa polynomu $x^5 - 3x + 3$ nad tělesem $\mathbb{Q}$. [jelikož je polynom dle Eisensteinova kritéria nerozložitelný, je minimálním polynomem libovolného svého kořene a, tedy $[\mathbb{Q}(a) : \mathbb{Q}] = 5$]

7. Spočtěte stupeň rozšíření rozkladového nadtělesa polynomu $x^4 + x^3 + 2x^2 + x + 1$ nad tělesem $\mathbb{Q}$. [Polynom se rozkládá na $(x^2 + 1)(x^2 + x + 1)$, má tudíž kořeny $\pm i$, $\frac{1}{2}(1 \pm \sqrt{3}i)$, a tedy jeho rozkladovým nadtělesem je $\mathbb{Q}(\sqrt{3}, i)$; platí $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = 2 \cdot 2 = 4$ (je třeba si uvědomit, že polynom $x^2 + x + 1$ je nad $\mathbb{Q}(i)$ stále nerozložitelný)]

8. Spočtěte stupeň rozšíření $[\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}]$. [6; $[\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$, druhý činitel je zjevně roven dvěma a stačí si uvědomit, že žádný z kořenů polynomu $x^3 - 3$ neleží v $\mathbb{Q}(\sqrt{3})$]

9. Dokažte, že $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$. [První rovnost, konkrétně vztah „$\supseteq$“, plyne například z inkluze „$\subseteq$“ a faktu, že jde o rozšíření stejného stupně, což dokážeme stejně jako v předchozím příkladu. Pro důkaz „$\subseteq$“ v druhé rovnosti je možné spočítat (nechat si spočítat) mocniny prvku $(\sqrt{2} + \sqrt[3]{2})^i$ pro $0 \leq i \leq 5$, výsledky zapsat jako vektory v bázi a $\{\sqrt[6]{2^i} \mid 0 \leq i \leq 5\}$ a rozhodnout o jejich lineární (ne)závislosti.]

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

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

A pro odvážné několik zábavných příkladů navíc:

12. Nalezněte minimální polynomy $m_{a,T}$ následujících prvků $a \in S$ nad T:
    (a) $a = \sqrt{2}$, $S = \mathbb{R}$, $T = \mathbb{Q}(\sqrt{2} + \sqrt{5})$, [$x - \sqrt{2}$]
    (b) $a = t^3$, $S = \mathbb{Z}_2(t)$, $T = \mathbb{Z}_2(t + t^2)$ (podtěleso $\mathbb{Z}_2(t)$). [$x^2 + (t^2 + t + 1)x + (t^2 + t)^3$]
    (c) Najděte minimální polynom čísla $\cos\left(\frac{2\pi}{5}\right)$ nad racionálními čísly. [$4x^2 + 2x - 1$ (Nejprve využijme Moivreovu větu $\cos(5x) = \cos^5(x) - 10\cos^3(x)\sin^2(x) + 5\cos(x)\sin^4(x)$, pak substituce $x \mapsto \frac{2\pi}{5}$ a rozložme na činitele nad $\mathbb{R}$.)]

13. Nechť $\mathbf{T}$ je těleso a a algebraický prvek nad $\mathbf{T}$ takový, že $[\mathbf{T}(a) : \mathbf{T}]$ je lichý. Dokažte, že $\mathbf{T}(a) = \mathbf{T}(a^2)$.

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

15. Kterému známému okruhu je izomorfní faktorokruh $\mathbb{Q}[x]/(x^2 + a)$, pro
    (a) $a = 2$ [$\mathbb{Q}(\sqrt{-2}) = \mathbb{Q}(\sqrt{2}i)$]
    (b) $a = -4$? [$\mathbb{Q} \times \mathbb{Q}$]