2. cvičení

Výsledky úloh 1 a 2 jsou na konci druhé strany.

☼ **Úloha 1.** Pro daný polynom $f \in \Bbbk[x]$ nalezněte (a vhodně popište) těleso $\mathbb{K}$ rozšiřující $\Bbbk$, ve kterém bude mít f kořen, a rozložte f v $\mathbb{K}[x]$ na ireducibilní polynomy. Pokud možno usilujte o to, aby bylo $\mathbb{K}$ „co nejmenší“.

(a) $\Bbbk = \mathbb{R}$, $f = x^2 + 2x + 2$,
(b) $\Bbbk = \mathbb{Q}$, $f = x^3 - 3$,
(c) $\Bbbk = \mathbb{Q}$, $f = x^4 - 5x^2 + 6$,
(d) $\Bbbk = \mathbb{Z}_2$, $f = x^2 + x + 1$,
(e) $\Bbbk = \mathbb{Z}_7$, $f = x^2 + x + 1$,
(f) $\Bbbk = \mathbb{Z}_3$, $f = x^4 + 1$,
⋕ (g) $\Bbbk = \mathbb{Q}(t)$ (podílové těleso oboru polynomů $\mathbb{Q}[t]$), $f = x^2 + t$,
⋕ (h) $\Bbbk = \mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$, $f = x^2 + x + \alpha$ (zkuste zde $\mathbb{K}$ „vyjádřit“ ve tvaru $\mathbb{Z}_2[\beta]/(g)$ pro $g \in \mathbb{Z}_2[\beta]$ ireducibiliní a nahlédnout, jaké podmnožině $\mathbb{K}$ odpovídá $\Bbbk$).

Definice. Buď $\Bbbk \leq \mathbb{K}$ rozšíření těles, $a \in \mathbb{K}$ algebraický nad $\Bbbk$. Pak *minimální polynom* $m_{a,\Bbbk} \in \Bbbk[x]$ *prvku* a *nad* $\Bbbk$ je monický polynom nejmenšího kladného stupně takový, že $m_{a,\Bbbk}(a) = 0$.

Úloha 2. Nalezněte minimální polynomy $m_{x,\Bbbk}$ následujících prvků $x \in \mathbb{K}$ nad $\Bbbk$:

(a) $x = -1 + i$, $\mathbb{K} = \mathbb{C}$, $\Bbbk = \mathbb{Q}$
(b) $x = \sqrt{2}i$, $\mathbb{K} = \mathbb{C}$, $\Bbbk = \mathbb{Q}(i)$,
(c) $x = \sqrt[4]{2}$, $\mathbb{K} = \mathbb{R}$, $\Bbbk = \mathbb{Q}(\sqrt{2})$,
(d) $x = \sqrt{2} + \sqrt{3}$, $\mathbb{K} = \mathbb{R}$, $\Bbbk = \mathbb{Q}$,
(e) $x = \sqrt{2} + \sqrt{3}$, $\mathbb{K} = \mathbb{R}$, $\Bbbk = \mathbb{Q}(\sqrt{2})$,
⋆ (f) $x = \sqrt{2}$, $\mathbb{K} = \mathbb{R}$, $\Bbbk = \mathbb{Q}(\sqrt{2} + \sqrt{3})$,
⋆ (g) $x = t^3$, $\mathbb{K} = \mathbb{Z}_2(t)$, $\Bbbk = \mathbb{Z}_2(t + t^2)$ (podtěleso $\mathbb{Z}_2(t)$),

(Nápověda: Obecný přístup je zhruba takovýto – píšeme si mocniny $x^0, x^1, x^2, \ldots$ tak dlouho, dokud nedostaneme lineárně závislé prvky nad $\Bbbk$. Koeficienty lineární kombinace, která dá nulový prvek, jsou přesně koeficienty minimálního polynomu (pokud nejvyšší mocnině x dáme koeficient 1).)

Úloha 3. Dokažte, že pro každé $q \in \mathbb{Q}$ je $\sin(q\pi)$ algebraické číslo. (Nápověda: Pomocí komplexního sdružení lze dokázat, že komplexní číslo je algebraické právě tehdy, když je algebraická jeho reálná i imaginární část. Pro čísla tvaru $\exp(q\pi i)$ to pak už není těžké dokázat.)

⋆ **Úloha 4.** Dokažte, že množina algebraických čísel je

(a) hustá v $\mathbb{C}$ s běžnou metrikou,
(b) spočetná.

(Nápověda: Pro (a) stačí například ukázat, že všechny prvky $\mathbb{Q}(i)$ jsou algebraické. Ad (b): $\mathbb{Q}[x]$ je spočetná množina a každý nenulový polynom má jen konečně mnoho kořenů.)

⋆ **Úloha 5.** Z prvního domácího úkolu v ZS „víme“, že zobrazení

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

je isomorfismus okruhů (a dokonce těles). Vymyslete, jak si vypomoct f k výpočtu minimálních polynomů prvků $\mathbb{Q}(\sqrt{3})$ nad $\mathbb{Q}$.

⋆⋆ **Úloha 6.** „Elementárně“ pomocí symetrických polynomů dokažte, že algebraická čísla tvoří podtěleso $\mathbb{C}$.[1] (Nápověda: Pro $x, y \in \overline{\mathbb{Q}}$ potřebujeme ukázat, že $xy \in \overline{\mathbb{Q}}$, $x + y \in \overline{\mathbb{Q}}$ a pro $x \neq 0$ i $x^{-1} \in \overline{\mathbb{Q}}$. To poslední se udělá snadno přechodem k „převrácenému“ polynomu, pro součet a součin je potřeba vymyslet, jak ze dvou polynomů v $\mathbb{Q}[x]$ vyrobit jeden polynom, jehož kořeny budou součty, resp. součiny kořenů oněch dvou polynomů – a tento polynom bude stále v $\mathbb{Q}[x]$.)

Výsledky 1. **(a)** $\mathbb{K} = \mathbb{C}$, $f = (x + 1 - i)(x + 1 + i)$; **(b)** $\mathbb{K} = \mathbb{Q}(\sqrt[3]{3})$, $f = (x - \sqrt[3]{3})(x^2 + x\sqrt[3]{3} + \sqrt[3]{9})$; **(c)** $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, $f = (x^2 - 3)(x + \sqrt{2})(x - \sqrt{2})$ (nebo podobně se $\sqrt{3}$); **(d)** $\mathbb{K} = \mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$, $f = (x + \alpha)(x + \alpha + 1)$; **(e)** $\mathbb{K} = \mathbb{Z}_7$, $f = (x + 3)(x + 5)$; **(f)** např. $\mathbb{K} = \mathbb{Z}_3[\alpha]/(\alpha^2 + \alpha + 2)$, $f = (x - \alpha)(x + 2 - \alpha)(x - 1 - \alpha)(x + \alpha)$ (je totiž $f = (x^2 + x + 2)(x^2 + 2x + 2)$); **(g)** $\mathbb{K} = \mathbb{Q}(\sqrt{-t})$, $f = (x + \sqrt{-t})(x - \sqrt{t})$; **(h)** např. $\mathbb{K} = \mathbb{Z}_2[\beta]/(\beta^4 + \beta + 1)$, v tomto tělese je buď $\alpha = \beta^2 + \beta + 1$, pak $f = x^2 + x + (\beta^2 + \beta + 1) = (x + \beta^2)(x + \beta^2 + 1)$, nebo $\alpha = \beta^2 + \beta$, pak $f = x^2 + x + (\beta^2 + \beta) = (x + \beta)(x + \beta + 1)$.[2] Každopádně při této reprezentaci $\mathbb{K}$ je $\Bbbk = \{0, 1, \beta^2 + \beta, \beta^2 + \beta + 1\}$.

Výsledky 2. **(a)** $x^2 + 2x + 2$; **(b)** $x^2 + 2$; **(c)** $x^2 - \sqrt{2}$; **(d)** $x^4 - 10x^2 + 1$; **(e)** $x^2 - 2\sqrt{2}x - 1$; **(f)** $x - \sqrt{2}$ (protože $\sqrt{2} = \frac{1}{2}\big((\sqrt{2} + \sqrt{3})^3 - 9(\sqrt{2} + \sqrt{3})\big)$); **(g)** $x^2 + (1 + (t + t^2))x + (t + t^2)^3$.

[1] Na přednášce se to (doufám) dokáže efektivně.

[2] V zadání ze cvičení je rozklad f v tomto bodě špatně.