Algebra — cvičení 12, řešení

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

(b) $a = \sqrt{2}i$, $S = \mathbb{C}$, $T = \mathbb{Q}(i)$: Jelikož $\sqrt{2}i \notin \mathbb{Q}(i)$, nemůže mít minimální polynom stupeň 1. Je proto $m_{a,T} = x^2 + 2$.

(d) $a = \sqrt[4]{2}$, $S = \mathbb{R}$, $T = \mathbb{Q}(\sqrt{2})$: Víme-li, že $\sqrt[4]{2} \notin \mathbb{Q}(\sqrt{2})$, je jasné, že $m_{a,T} = x^2 - \sqrt{2}$. Že platí $\sqrt[4]{2} \notin \mathbb{Q}(\sqrt{2})$, plyne kromě snadného výpočtu také z toho, že $\deg m_{a,T} = [T(a) : T] = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})]$ a $4 = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = [T(a) : T][T : \mathbb{Q}] = [T(a) : T] \cdot 2$, kde první rovnost plyne z toho, že $m_{\sqrt[4]{2},\mathbb{Q}} = x^4 - 2$ a poslední z $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.

(e) $a = \sqrt{2} + \sqrt{5}$, $S = \mathbb{R}$, $T = \mathbb{Q}$: Nejprve nalezneme kandidáta na minimální polynom, tj. nějaký polynom, který má jistě a za kořen. To bude určitě případ polynomu $(x-\sqrt{2})^2-5 = x^2-2\sqrt{2}x-3 =: g$, který má za kořeny $\sqrt{2}\pm\sqrt{5}$. Problém je, že nemá racionální koeficienty; z on-line cvičení ovšem víme, že $m_{a,\mathbb{Q}(\sqrt{2})} = g$. Platí

$$g(x) = 0 \iff x^2 - 3 = 2\sqrt{2}x \implies (x^2-3)^2 = 8x^2 \iff x^4 - 14x^2 + 9 = 0.$$

Poslední polynom (4. stupně) je naším kandidátem, označme ho f. Snadno vidíme, že jeho kořeny jsou právě všechny tvaru $\pm\sqrt{2}\pm\sqrt{5}$. Jeho rozkladové nadtěleso je proto rovno $U = \mathbb{Q}(\sqrt{2},\sqrt{5})$, které má stupeň 4 nad $\mathbb{Q}$ (to plyne mimo jiného z $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$). Jelikož víme, že $\deg m_{a,T} = [\mathbb{Q}(a) : \mathbb{Q}]$, k prokázání ireducibility polynomu f stačí, když ověříme, že $\mathbb{Q}(\sqrt{2},\sqrt{5}) = \mathbb{Q}(a)$; netriviální je jen inkluze $\subseteq$. To plyne bezprostředně ze vztahu $\sqrt{2} = a^3/6 - 11a/6$, který dává $\sqrt{2} \in \mathbb{Q}(a)$. Následně pak ihned $\sqrt{5} = a - \sqrt{2} \in \mathbb{Q}(a)$.

(g) $a = \sqrt{2} + \sqrt{5}$, $S = \mathbb{R}$, $T = \mathbb{R}$: Triviálně $x - (\sqrt{2} + \sqrt{5})$.

(h*) $a = \sqrt{2}$, $S = \mathbb{R}$, $T = \mathbb{Q}(\sqrt{2}+\sqrt{5})$: Ihned z řešení části (e) máme, že hledaným polynomem je $x - \sqrt{2}$.

(i*) $a = t^3$, $S = \mathbb{Z}_2(t)$, $T = \mathbb{Z}_2(t + t^2)$): Předně zopakujme, že $\mathbb{Z}_2(t)$ je podílové těleso oboru $\mathbb{Z}_2[t]$. Pro konkrétní prvek $b = t^2 + t \in \mathbb{Z}_2(t)$ pak uvažujeme nejmenší podtěleso tělesa $\mathbb{Z}_2(t)$ obsahující prvek b (a těleso $\mathbb{Z}_2$); to se standardně značí $\mathbb{Z}_2(b)$.

Jak víte ze zimního semestru, $\mathbb{Z}_2(b)$ je podílové těleso oboru $\mathbb{Z}_2[b] = \{f(b);\ f \in \mathbb{Z}_2[x]\}$, to jest

$$\mathbb{Z}_2(b) = \left\{ \frac{f(b)}{g(b)};\ f, g \in \mathbb{Z}_2[x], g(b) \neq 0 \right\}.$$

Jelikož $f(b)$ je pro $f \in \mathbb{Z}_2[x]$ vždy polynom sudého stupně v proměnné t, jsou i všechny prvky z $\mathbb{Z}_2[t] \cap \mathbb{Z}_2(b)$ polynomy sudého stupně v t. Mimo jiné tedy $a = t^3 \notin \mathbb{Z}_2(b)$ a hledaný minimální polynom má stupeň alespoň 2.

Na druhou stranu t^6 už je polynom sudého stupně v t, což dává tušit, že by hledaný minimální polynom mohl mít stupeň 2, tj. mohl by být tvaru $x^2 + dx + c$ pro vhodná $d, c \in \mathbb{Z}_2(b)$. Hledáme tedy taková d, c, že $t^6 = dt^3 + c$. Pokud by d, c existovala již v $\mathbb{Z}_2[b]$, bylo by dt^3 lichého stupně, a tedy c musí v sobě obsahovat t^6. Vyzkoušíme proto $c = (t^2+t)^3 = (t^2+t)(t^4+t^2) = t^6 + t^5 + t^4 + t^3$. Takže $dt^3 = t^5 + t^4 + t^3$ a stačí položit $d = t^2 + t + 1 \in \mathbb{Z}_2(b)$. Dostali jsme $m_{t^3,\mathbb{Z}_2(t^2+t)}(x) = x^2 + (t^2+t+1)x + (t^2+t)^3$.

2. Nalezněte nějakou bázi $T(a)$ nad T v případech (c) a (e) v úloze **1.** a určete stupeň rozšíření $T(a) \geq T$. V případě (c) máme například $(1, \sqrt[4]{6}, \sqrt[4]{36}, \sqrt[4]{216})$ jako bázi prostoru $\mathbb{Q}(\sqrt[4]{6})$ nad $\mathbb{Q}$. V případě (e) lze vzít $(1, \sqrt{2}, \sqrt{5}, \sqrt{10})$.

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 $\mathbb{Q}[x]$?

Máme $m_{\sqrt[3]{3},\mathbb{Q}} = x^3 - 3$, takže je hledaný stupeň rozšíření roven 3. Bází je například $(1, \sqrt[3]{3}, \sqrt[3]{9})$. Těleso $\mathbb{Q}(\sqrt[3]{3})$ rozhodně není rozkladové nadtěleso polynomu $x^3 - 3$, který se nerozkládá ani nad

$\mathbb{R}$ na lineární činitele. Negativní odpověď na zadanou obecnější otázku plyne z lemmatu 25.4. Lze dokazovat i sporem s využitím Tvrzení 24.5 (3), kde se za U zvolí rozkladové nadtěleso polynomu x^3-3, což je $\mathbb{Q}(\sqrt[3]{3}, \mathrm{e}^{\frac{2\pi i}{3}})$; je potřeba ale vědět, že $\mathrm{Gal}(U/\mathbb{Q}) \cong \mathbf{S}_3$ (a že $\mathbf{S}_3$ nemá dvouprvkovou normální podgrupu).

4. Víte-li, že $m_{\sqrt{2}+i,\mathbb{Q}} = x^4 - 2x^2 + 9$, nalezněte $m_{\sqrt{2}+i+1,\mathbb{Q}}$. Řešením je $(x-1)^4 - 2(x-1)^2 + 9 = x^4 - 4x^3 + 4x^2 + 8$. Stačí uvážit, že lineární substituce zachovává ireducibilitu polynomu (což jsme již měli na jednom z dávno minulých cvičení).

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

(a) $a = 2$,
(b) $a = -4$?

(a). Stačí uvažovat dosazovací homomorfismus $d : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{-2})$, kde $d(f) = f(\sqrt{-2})$. Ten je jistě surjektivní. V jeho jádru jsou právě všechny polynomy $g \in \mathbb{Q}[x]$ takové, že $g(\sqrt{-2}) = 0$, tj. takové, že v $\mathbb{Q}[x]$ platí $m_{\sqrt{-2},\mathbb{Q}} \mid g$. Máme ovšem $m_{\sqrt{-2},\mathbb{Q}} = x^2 + 2$. Jádro je tedy ideál generovaný polynomem x^2+2 a zbývá užít 1. větu o izomorfismu pro okruhy.

(b). Polynom $x^2 - 4$ není nad $\mathbb{Q}$ ireducibilní, neboť $x^2 - 4 = (x+2)(x-2)$. Nelze tedy postupovat analogicky jako v případě (a). Ledaže místo jednoho dosazovacího homomorfismu budeme uvažovat dva (nebo jeden dvojitý). Definujeme totiž $d : \mathbb{Q}[x] \to \mathbb{Q}^2$ vztahem $d(f) = (f(-2), f(2))$. Jelikož se operace v $\mathbb{Q}^2$ provádějí po složkách, je nasnadě, že se opět jedná o okruhový homomorfismus.

V jeho jádru jsou právě všechny polynomy $g \in \mathbb{Q}[x]$ takové, že $(g(-2), g(2)) = (0,0)$. Jinak řečeno takové, že $x+2 \mid g$ a zároveň $x-2 \mid g$ platí v $\mathbb{Q}[x]$. Jelikož jsou $x+2$ a $x-2$ nesoudělné a $\mathbb{Q}[x]$ je Gaussův obor, jde právě o všechna g, pro něž $x^2 - 4 \mid g$. Je proto $\mathrm{Ker}\, d = (x^2-4)$.

Abychom mohli uzavřít 1. větou o izomorfismu, stačí ještě ověřit, že $\mathrm{Im}\, d = \mathbb{Q}^2$. K tomu je potřeba pro libovolná racionální čísla a, b najít $g \in \mathbb{Q}[x]$ tak, aby $(g(-2), g(2)) = (a,b)$. To je snadné. A že to skutečně lze, plyne, ne náhodou, z věty o interpolaci, která je variantou ČZV pro polynomy.

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

Plyne ihned ze vztahu $p = [S:T] = [S:T(a)][T(a):T]$, kde p je zadané prvočíslo. Z $a \in S \setminus T$ totiž máme $[T(a):T] \geq 2$. Nutně proto $[S:T(a)] = 1$, a tedy $S = T(a)$.

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

Stačí použít, že $T \leq T(a^2) \leq T(a)$ a $[T(a):T] = [T(a):T(a^2)][T(a^2):T]$. Jelikož je $[T(a):T]$ liché a platí $[T(a):T(a^2)] \leq 2$, protože $x^2 - a^2 \in T(a^2)[x]$ má a za kořen, musí být nutně $[T(a):T(a^2)] = 1$, což je ekvivalentní s $T(a) = T(a^2)$.

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 $m_{b,T} = m_{b,T(a)}$.

Označme $s = \deg m_{a,T}$ a $t = \deg m_{b,T}$. Máme

$$[T(a,b):T] = \begin{cases} [T(a,b):T(a)][T(a):T] = [T(a,b):T(a)] \cdot s \\ [T(a,b):T(b)][T(b):T] = [T(a,b):T(b)] \cdot t. \end{cases}$$

Z nesoudělnosti s a t dostáváme $st \mid [T(a,b) : T]$. Z triviálních nerovností $\deg m_{a,T(b)} \leq s$ a $\deg m_{b,T(a)} \leq t$ obdržíme naopak $[T(a,b) : T] \leq st$. Dohromady proto $[T(a,b) : T] = st$, a tedy $\deg m_{a,T(b)} = [T(a,b) : T(b)] = s$ a $\deg m_{b,T(a)} = t$, z čehož ihned plyne kýžená rovnost minimálních polynomů.

10. Dokažte, že $\mathbb{Q}(\sqrt{2}+\sqrt[3]{2}) = \mathbb{Q}(\sqrt{2},\sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$. Pro každé $n \in \mathbb{N}$ je $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$; ireducibilita plyne z Eisensteinova kritéria pro 2 a z Gaussova lemmatu. Triviálně máme $\mathbb{Q}(\sqrt{2},\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[6]{2})$, přičemž $\mathbb{Q}(\sqrt[6]{2})$ je šestirozměrný vektorový prostor nad $\mathbb{Q}$. Z předchozí úlohy ale víme, že $[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$, a proto platí $\mathbb{Q}(\sqrt{2},\sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

Zbývá dokázat první rovnost, k čemuž stačí ukázat, že $\deg m_{\sqrt{2}+\sqrt[3]{2},\mathbb{Q}} \geq 6$ (druhá nerovnost plyne z triviální inkluze $\mathbb{Q}(\sqrt{2}+\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt[3]{2})$). K tomu uvažujme rozkladové nadtěleso S polynomu $x^6 - 2$ nad $\mathbb{Q}$ (to je, mimochodem, ostře větší než $\mathbb{Q}(\sqrt[6]{2})$).

Podle Tvrzení 24.5(2) existuje $\varphi' \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2}))$ posílající $\sqrt{2}$ na $-\sqrt{2}$. Tento φ' rozšíříme Lemmatem 24.4 do nějakého $\varphi \in \mathrm{Gal}(S/\mathbb{Q}(\sqrt[3]{2}))$. Analogicky existují $\psi_1, \psi_2 \in \mathrm{Gal}(S/\mathbb{Q}(\sqrt{2}))$ takové, že $\psi_k(\sqrt[3]{2}) = \sqrt[3]{2}\mathrm{e}^{\frac{2k\pi i}{3}}$ pro $k = 1, 2$.

Podle Tvrzení 24.1 musí $\mathbb{Q}$-automorfismy φ, ψ_1, ψ_2 permutovat kořeny polynomu $m_{\sqrt{2}+\sqrt[3]{2},\mathbb{Q}}$. To ale znamená, že $m_{\sqrt{2}+\sqrt[3]{2},\mathbb{Q}}$ má za kořeny přinejmenším všech 6 prvků $(-1)^m\sqrt{2}+\sqrt[3]{2}\mathrm{e}^{\frac{2k\pi i}{3}}$, kde $m = 1, 2$ a $k = 0, 1, 2$. Není těžké si uvědomit, že se jedná o 6 různých prvků. Proto $\deg m_{\sqrt{2}+\sqrt[3]{2},\mathbb{Q}} \geq 6$.

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

Pokud $b = 0$, pomoc od f rozhodně nepotřebujeme. Předpokládejme proto dále, že $b \neq 0$. Víme, že minimální polynom prvku $a + b\sqrt{3}$ je potom stupně 2. Zároveň z Hamiltonovy–Cayleyho věty z lineární algebry plyne, že při dosazení matice z $\mathrm{Im}(f)$ do jejího charakteristického polynomu, obdržíme 0. Hledaným minimálním polynomem proto bude charakteristický polynom $(a - x)^2 - 3b^2 = x^2 - 2ax + a^2 - 3b^2$.

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 $a^2 + b^2 = p$.

V $\mathbb{Z}[x]$ máme hlavní ideály $(p), (x^2+1)$ a jejich součet $I = (p, x^2+1)$. Druhá věta o izomorfismu říká jednak, že $\mathbb{Z}[x]/I \cong \frac{\mathbb{Z}[x]/(p)}{I/(p)}$, a jednak, že $\mathbb{Z}[x]/I \cong \frac{\mathbb{Z}[x]/(x^2+1)}{I/(x^2+1)}$. Z předchozích cvičení a přednášky víme, že $\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]$, resp. $\mathbb{Z}[x]/(p) \cong \mathbb{Z}_p[x]$. Tyto izomorfismy pošlou ideál $I/(x^2+1)$ faktorokruhu $\mathbb{Z}[x]/(x^2+1)$ na ideál $p\mathbb{Z}[i]$ okruhu $\mathbb{Z}[i]$, resp. ideál $I/(p)$ faktorokruhu $\mathbb{Z}[x]/(p)$ na ideál $(x^2+1)\mathbb{Z}_p[x]$ okruhu $\mathbb{Z}_p[x]$. Dohromady pak dostáváme

$$\mathbb{Z}[i]/(p) \cong \frac{\mathbb{Z}[x]/(x^2+1)}{I/(x^2+1)} \cong \mathbb{Z}[x]/I \cong \frac{\mathbb{Z}[x]/(p)}{I/(p)} \cong \mathbb{Z}_p[x]/(x^2+1).$$

Tyto faktorokruhy jsou dle tvrzení z přednášky tělesy právě tehdy, když je (p) maximální ideál v oboru $\mathbb{Z}[i]$ (tj. p je ireducibilní prvek v eukleidovském oboru $\mathbb{Z}[i]$), ekvivalentně (x^2+1) je maximální ideál v oboru $\mathbb{Z}_p[x]$ (tj. x^2+1 je ireducibilní prvek v eukleidovském oboru $\mathbb{Z}_p[x]$). Zřejmě je x^2+1 ireducibilní v $\mathbb{Z}_p[x]$ právě tehdy, když x^2+1 nemá kořen v $\mathbb{Z}_p$, tj. v $\mathbb{Z}_p$ neexistuje druhá odmocnina prvku -1. Pro $p = 2$ je $x^2+1 = (x+1)^2$, a tedy 2 není ireducibilní prvek v $\mathbb{Z}[i]$ a inkriminovaný faktorokruh není tělesem. Buď dále $p > 2$.

V tom případě je -1 prvek řádu 2 v grupě $\mathbb{Z}_p^*$. Prvek -1 má proto druhou odmocninu v $\mathbb{Z}_p$ právě tehdy, když v $\mathbb{Z}_p^*$ existuje prvek řádu 4: připomeňme, že z cykličnosti grupy $\mathbb{Z}_p^*$ plyne, že v ní

existuje právě jeden prvek řádu 2, a sice -1; je-li $a \in \mathbb{Z}_p^*$ řádu 4, pak tedy nutně $a^2 = -1$. Jelikož v konečných cyklických grupách platí i obrácená implikace Lagrangeovy věty, dostáváme, že $\mathbb{Z}_p^*$ obsahuje prvek řádu 4 právě tehdy, když $|\mathbb{Z}_p^*|$ je násobkem 4, tj. právě tehdy, když $p \equiv 1 \pmod 4$.

Je-li tedy p liché prvočíslo, pak $p \equiv 1 \pmod 4$ právě tehdy, když p není ireducibilním prvkem v eukleidovském oboru $\mathbb{Z}[i]$. Pro taková neireducibilní p tedy existuje v $\mathbb{Z}[i]$ nějaký netriviální rozklad tvaru $p = (a + bi)(c + di)$, kde ovšem nutně $a^2 + b^2 = \nu(a + bi) = \nu(c + di) = p$.