13 Minimální polynom – Napoleon Galoisovy teorie

Řešení
verze ze dne 13. května 2025.

Cíle cvičení: Dnes budeme počítat minimální polynomy prvků nad tělesem, což se ukáže být ve své podstatě lineárně algebraickou úlohou. Dobře si přitom rozmyslíme lineárně algebraické důsledky našich výpočtů, především ten, který říká, že stupeň minimálního polynomu je právě stupněm rozšíření daného prvkem, tedy dimenzí rozšíření chápaného jako vektorový prostor nad rozšiřovaným tělesem.

Úlohy, které bychom určitě měli umět řešit:

Úloha 13.1. Spočítejte minimální polynom $m_{a,\mathbb{Q}}$ nad tělesem $\mathbb{Q}$ a stupeň rozšíření $[\mathbb{Q}(a):\mathbb{Q}]$ pro komplexní prvky a s hodnotou (a) $\sqrt[3]{2}$, (b) $-1+i$, (c) $\sqrt[4]{6}$, (d) ζ_3, (e) $\sqrt{2}+\sqrt{5}$.

Řešení. (a) Prvek $\sqrt[3]{2}$ je zjevně kořenem monického polynomu $x^3-2\in\mathbb{Q}[x]$, o němž už jsme dříve a mnoha způsoby dokázali, že je ireducibilní v $\mathbb{Q}[x]$, tedy podle tvrzení 22.1 a 22.3 máme

$$m_{\sqrt[3]{2},\mathbb{Q}} = x^3-2 \quad \text{a} \quad [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = \deg m_{\sqrt[3]{2},\mathbb{Q}} = 3.$$

(b) Úvahou o komplexně sdružených kořenech s využitím tvrzení 22.1 a 22.3 nahlédneme, že

$$m_{i-1,\mathbb{Q}} = (x+1+i)\cdot(x+1-i) = x^2+2x+2,$$

je monický polynom ireducibilní v $\mathbb{Q}[x]$, a proto $[\mathbb{Q}(-1+i):\mathbb{Q}] = \deg m_{i-1,\mathbb{Q}} = 2$.

(c) Vidíme, že $\sqrt[4]{6}$ je kořenem monického polynomu x^4-6, který je díky Eisensteinovu kritériu ireducibilní v $\mathbb{Z}[x]$, a tedy (věta 8.5) i v $\mathbb{Q}[x]$. Stejným argumentem jako v předchozích dvou úlohách zjišťujeme, že

$$m_{\sqrt[4]{6},\mathbb{Q}} = x^4-6 \quad \text{a} \quad [\mathbb{Q}(\sqrt[4]{6}):\mathbb{Q}] = \deg m_{\sqrt[4]{6},\mathbb{Q}} = 4.$$

(d) Tentokrát je prvek ζ_3 zjevně kořenem polynomu $x^3-1=(x-1)(x^2+x+1)$, tudíž je kořenem monického ireducibilního polynomu x^2+x+1, standardním argumentem dostáváme

$$m_{\zeta_3,\mathbb{Q}} = x^2+x+1 \quad \text{a} \quad [\mathbb{Q}(\zeta_3):\mathbb{Q}] = 2.$$

(e) Nejprve najdeme netriviální racionální koeficienty a_i, pro které $\sum_{j\geq 0} a_j(\sqrt{2}+\sqrt{5})^j = 0$, tedy koeficienty polynomu, jehož je prvek $\sqrt{2}+\sqrt{5}$ kořenem. Zřejmě $(\sqrt{2}+\sqrt{5})^0 = 1$, $(\sqrt{2}+\sqrt{5})^1 = \sqrt{2}+\sqrt{5}$ a spočítáme-li

$$(\sqrt{2}+\sqrt{5})^2 = 7+2\sqrt{10}, \quad (\sqrt{2}+\sqrt{5})^4 = (7+2\sqrt{10})^2 = 89+28\sqrt{10},$$

vidíme, že k nalezení netriviální racionální lineární kombinace stačí vzít sudé mocniny 1, $7+2\sqrt{10}$ a $89+28\sqrt{10}$. Řešíme rovnici, která je z lineárně algebraického pohledu vektorová

$$a_0 + a_2(7+2\sqrt{10}) + a_4(89+28\sqrt{10}) = 0.$$

Rozdělíme ji na racionální a iracionální část v souřadnicích vzhledem k bázi $(1,\sqrt{10})$ podprostoru, v němž všechny hodnoty (tedy vektory) leží, a dostaneme homogenní soustavu dvou lineárních rovnic ve třech neznámých nad tělesem $\mathbb{Q}$:

$$\begin{aligned} a_0 + 7a_2 + 89a_4 &= 0,\\ 2a_2 + 28a_4 &= 0 \end{aligned}$$

pro niž snadno najdeme netriviální řešení $a_0=9$, $a_2=-14$, $a_4=1$. Zjistili jsme, že

$$(\sqrt{2}+\sqrt{5})^4 - 14(\sqrt{2}+\sqrt{5})^2 + 9 = 0,$$

tedy $\sqrt{2}+\sqrt{5}$ je kořenem monického polynomu $x^4-14x^2+9\in\mathbb{Q}[x]$.

Dále se může naše argumentace odvíjet vícero směry:

(1) přímo dokážeme, že nalezený polynom je ireducibilní,

(2) dokážeme, že $\big(1, \sqrt{2}, \sqrt{5}, \sqrt{10}\big)$ je lineárně nezávislá posloupnost nad $\mathbb{Q}$, což spolu s výpočty výše ukáže lineární nezávislost prvků $(\sqrt{2}+\sqrt{5})^0, \dots, (\sqrt{2}+\sqrt{5})^3$ nad $\mathbb{Q}$ a tedy neexistenci polynomu nižšího stupně s kořenem $\sqrt{2}+\sqrt{5}$,

(3) dokážeme, že musí platit $[\mathbb{Q}(\sqrt{2}+\sqrt{5}) : \mathbb{Q}] \geq 4$, tedy hledaný minimální polynom bude mít stupeň alespoň 4, tedy to bude ten nalezený.

(1) Nalezený polynom můžeme snadno rozložit na kořenové činitele

$$x^4 - 14x^2 + 9 = (x^2 - 7 - 2\sqrt{10})(x^2 - 7 + 2\sqrt{10}) = (x - \sqrt{2} - \sqrt{5})(x + \sqrt{2} + \sqrt{5})(x - \sqrt{2} + \sqrt{5})(x + \sqrt{2} - \sqrt{5}),$$

odkud snadno vidíme, že nemá racionální kořeny. Dále snadno spočítáme, že součiny dvou kořenových činitelů jsou jednoho z tvarů

$$x^2 - 7 \pm 2\sqrt{10}, \qquad x^2 \pm 2\sqrt{5}x \pm 3, \qquad x^2 \pm 2\sqrt{2}x \pm 3,$$

tudíž nejde o polynomy s racionálními koeficienty. To znamená, že je polynom $x^4 - 14x^2 + 9$ nutně ireducibilní v $\mathbb{Q}[x]$, tedy

$$m_{\sqrt{2}+\sqrt{5},\mathbb{Q}} = x^4 - 14x^2 + 9 \quad \text{a} \quad [\mathbb{Q}(\sqrt{2}+\sqrt{5}) : \mathbb{Q}] = 4.$$

(2) Pro důkaz lineární nezávislosti $\big(1, \sqrt{2}, \sqrt{5}, \sqrt{10}\big)$ nad $\mathbb{Q}$ uvažme pro $a, b, c, d \in \mathbb{Q}$ rovnost

$$a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10} = 0,$$

kterou můžeme přepsat na

$$\underbrace{(a + b\sqrt{2})}_{\in \mathbb{Q}(\sqrt{2})} + \underbrace{(c + d\sqrt{2})}_{\in \mathbb{Q}(\sqrt{2})}\sqrt{5} = 0. \qquad (\spadesuit)$$

Nahlédněme, že $(1, \sqrt{5})$ je lineárně nezávislá nad $\mathbb{Q}(\sqrt{2})$: na to stačí ukázat, že $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$. Pokud by to nebyla pravda, tedy by platilo

$$\sqrt{5} = k + l\sqrt{2}$$

pro nějaká $k, l \in \mathbb{Q}$, pak umocněním na druhou snadno dostaneme spor s $\sqrt{2}, \sqrt{5} \notin \mathbb{Q}$. Ze $(\spadesuit)$ tedy máme

$$a + b\sqrt{2} = 0 \quad \text{a} \quad c + d\sqrt{2} = 0,$$

což ovšem vzhledem k $\sqrt{2} \notin \mathbb{Q}$ nutně znamená $a = b = c = d = 0$.

(3) Jelikož racionální lineární kombinací $\sqrt{2} + \sqrt{5}$ a

$$(\sqrt{2} + \sqrt{5})^3 = 2\sqrt{2} + 3 \cdot 2 \cdot \sqrt{5} + 3 \cdot 5 \cdot \sqrt{2} + 5\sqrt{5} = 17\sqrt{2} + 11\sqrt{5}$$

můžeme dostat jak $\sqrt{2}$, tak $\sqrt{5}$, platí inkluze těles $\mathbb{Q}(\sqrt{2}, \sqrt{5}) \leq \mathbb{Q}(\sqrt{2}+\sqrt{5})$, přičemž opačná inkluze je zřejmá, jde tedy o totéž těleso. Pro stupeň rozšíření dle tvrzení 22.5 platí

$$[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}],$$

přičemž $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Nyní stačí ukázat, že $[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})] > 1$, aby byl výsledný stupeň rozšíření alespoň 4 a námi nalezený polynom byl minimální. Ovšem $[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})] = 1$ je ekvivalentní s $\sqrt{5} \in \mathbb{Q}(\sqrt{2})$, což můžeme vyloučit výpočtem podobným jako v postupu (2).

Úloha 13.2. Najděte nějaké báze rozšíření $\mathbb{Q}(a)$ tělesa $\mathbb{Q}$ pro hodnoty a z předchozího příkladu.

Řešení. Stačí využít důkaz Tvrzení 22.3, který říká, že bázi $\mathbb{Q}(\alpha)$ tvoří posloupnost $(1, \alpha, \dots, \alpha^{n-1})$ pro $n = \deg m_{\alpha,\mathbb{Q}}$. Tedy pro konkrétní hodnoty α máme následující báze:

(a) $\big(1, \sqrt[3]{2}, \sqrt[3]{4}\big)$,

(b) $(1, -1+i)$,

(c) $\left(1, \sqrt[4]{6}, \sqrt{6}, \sqrt[4]{6}\sqrt{6}\right)$

(d) $(1, \zeta_3)$,

(e) $\left(1, \sqrt{2}+\sqrt{5}, 7+2\sqrt{10}, 17\sqrt{2}+11\sqrt{5}\right)$; alternativně můžeme využít, že $\mathbb{Q}(\sqrt{2}+\sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$, a za bázi vzít $\left(1, \sqrt{2}, \sqrt{5}, \sqrt{10}\right)$.

Úloha 13.3. Spočítejte minimální polynom (a) prvku $\sqrt{2}i$ nad tělesem $\mathbb{Q}(i)$, (b) prvku $\sqrt[4]{2}$ nad tělesem $\mathbb{Q}(\sqrt{2})$, (c) prvku $\sqrt{2}$ nad tělesem $\mathbb{Q}(\sqrt{2}+\sqrt{5})$.

Řešení. (a) Protože $(\sqrt{2}i)^2 = -2$, okamžitě vidíme, že $\sqrt{2}i$ je kořenem monického polynomu $x^2+2 \in \mathbb{Q}(i)[x]$. Dále $\sqrt{2}i \notin \mathbb{Q}(i)$ (důkaz se provede standardním umocněním $\sqrt{2}i = a+bi$ na druhou), tudíž polynom nerozložíme v $\mathbb{Q}(i)[x]$ na kořenové činitele a jedná se už nutně o minimální polynom $m_{a,\mathbb{Q}(i)} = x^2+2$. Můžeme si rovněž všimnout, že je to minimální polynom téhož prvku i nad tělesem $\mathbb{Q}$, tedy $m_{a,\mathbb{Q}} = m_{a,\mathbb{Q}(i)}$.

(b) Protože $\sqrt{2} = (\sqrt[4]{2})^2$, vidíme, že $\sqrt[4]{2}$ je kořenem monického polynomu $x^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$. Protože je polynom x^4-2 díky Eisensteinovu kritériu ireducibilní nad $\mathbb{Z}$, a proto (věta 8.5) i nad $\mathbb{Q}$, jde o minimální polynom $\sqrt[4]{2}$ nad $\mathbb{Q}$, z čehož plyne díky tvrzení 22.3, že

$$[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = \deg x^4 - 2 = 4.$$

Rovněž víme, že $m_{\sqrt{2},\mathbb{Q}} = x^2-2$ a $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg m_{\sqrt{2},\mathbb{Q}} = 2$, což s využitím tvrzení 22.5 znamená, že

$$\deg m_{\sqrt[4]{2},\mathbb{Q}(\sqrt{2})} = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = \frac{[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]} = \frac{4}{2} = 2.$$

Protože $m_{\sqrt[4]{2},\mathbb{Q}(\sqrt{2})}$ dělí $x^2-\sqrt{2}$ podle tvrzení 22.3, je polynom $x^2-\sqrt{2}$ hledaným minimálním polynomem.

Alternativně zde stačilo opět ukázat, že $\sqrt[4]{2} \notin \mathbb{Q}(\sqrt{2})$, což lze provést prostým umocněním na druhou ($k, l \in \mathbb{Q}$):

$$\sqrt[4]{2} = k + l\sqrt{2} \;\Rightarrow\; \sqrt{2} = 2kl\sqrt{2} + k^2 + 2l^2 \;\Rightarrow\; k^2 + 2l^2 = 0 \;\Rightarrow\; k = l = 0,$$

spor.

(c) Jelikož (jak jsme ukázali v řešení úlohy 13.1) platí $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{5})$, je minimálním polynomem přímo $x - \sqrt{2}$.

Úloha 13.4. Určete stupeň rozšíření všech kořenových nadtěles polynomu $x^5 - 3x + 3$ nad $\mathbb{Q}$.

Řešení. Jelikož je polynom dle Eisensteinova kritéria (volbou $p=3$) a věty 8.5 nerozložitelný v $\mathbb{Q}[x]$, je minimálním polynomem libovolného svého kořene a, tedy $[\mathbb{Q}(a) : \mathbb{Q}] = \deg(x^5 - 3x + 3) = 5$.

Úloha 13.5. Spočtěte stupeň rozšíření $[\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}]$.

Řešení. Nejprve uvážíme, že díky znalosti minimálních polynomů známe stupně rozšíření

$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = \deg(x^2-3) = 2, \quad [\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = \deg(x^3-3) = 3.$$

Dále si uvědomíme, že $m_{\sqrt[3]{3},\mathbb{Q}(\sqrt{3})}$ dělí $m_{\sqrt[3]{3},\mathbb{Q}} = x^3-3$, proto

$$[\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = \deg(m_{\sqrt[3]{3},\mathbb{Q}(\sqrt{3})}) \le \deg(m_{\sqrt[3]{3},\mathbb{Q}}) = \deg(x^3-3) = [\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3.$$

Nyní několikrát využijeme tvrzení 22.5:

$$[\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \le 3 \cdot 2 = 6,$$

$$[\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] \cdot 2,$$

$$[\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}(\sqrt[3]{3})] \cdot [\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}(\sqrt[3]{3})] \cdot 3,$$

proto $6 \mid [\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}] \le 6$. To znamená, že $[\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}] = 6$.

Nakonec ještě pár příkladů pro nadšené dobrovolníky:

Úloha 13.6. Víte-li, že $m_{\sqrt{2}+i,\mathbb{Q}} = x^4 - 2x^2 + 9$, najděte $m_{\sqrt{2}+i+1,\mathbb{Q}}$.

Řešení. Snadno uvážíme, že je-li α kořenem ireducibilního polynomu $m \in T[x]$ a $b \in T$, pak $\alpha + b$ je kořenem ireducibilního polynomu $m(x-b) \in T[x]$. V našem případě to znamená, že

$$m_{\sqrt{2}+i+1,\mathbb{Q}} = (x-1)^4 - 2(x-1)^2 + 9 = x^4 - 4x^3 + 4x^2 + 8$$

je hledaný minimální polynom.

Úloha 13.7. Spočítejte minimální polynom

(a) prvku $\sqrt{2} + \sqrt{5}$ nad tělesem $\mathbb{Q}(\sqrt{2})$,

(b) prvku $\sqrt{2} + \sqrt{5}$ nad tělesem $\mathbb{R}$,

(c) prvku ζ_5 nad tělesem $\mathbb{Q}$,

⋆ (d) prvku $\zeta_7 + \zeta_7^{-1}$ nad tělesem $\mathbb{Q}$.

Řešení. (a) Zde si stačí všimnout, že pro $\alpha = \sqrt{2} + \sqrt{5}$ platí, že $(\alpha - \sqrt{2})^2 = (\sqrt{5})^2 = 5 \in \mathbb{Q}(\sqrt{2})$. Což znamená, že je α kořenem polynomu

$$(x - \sqrt{2})^2 - 5 = x^2 - 2\sqrt{2}x - 3 \in \mathbb{Q}(\sqrt{2})[x].$$

Protože z 13.1(e) plyne, že $\sqrt{2} + \sqrt{5} \notin \mathbb{Q}(\sqrt{2})$, jedná se o hledaný minimální polynom.

Mohli jsme rovněž standardně hledat minimální netriviální lineární kombinaci mocnin prvků

$$1 = (\sqrt{2} + \sqrt{5})^0, \quad \sqrt{2} + \sqrt{5}, \quad 7 + (2\sqrt{2}) \cdot \sqrt{5} = (\sqrt{2} + \sqrt{5})^2$$

nad tělesem $\mathbb{Q}(\sqrt{2})$, což by vedlo na řešení homogenní soustavy nad tělesem $\mathbb{Q}(\sqrt{2})$, kde rovnice dostaneme pro jednotlivé souřadnice vzhledem k bázi $1, \sqrt{5}$ vektorového prostoru $(\mathbb{Q}(\sqrt{2}))(\sqrt{5})$ nad tělesem $\mathbb{Q}(\sqrt{2})$. Snadno bychom zjistili, že $1 \cdot (7 + (2\sqrt{2}) \cdot \sqrt{5}) - 2\sqrt{2} \cdot (\sqrt{2} + \sqrt{5}) - 3$, což by opět dalo, že $\sqrt{2} + \sqrt{5}$ je kořenem monického polynomu $x^2 - 2\sqrt{2}x - 3$, který je ireducibilní v $\mathbb{Q}(\sqrt{2})[x]$.

(b) Vzhledem k tomu, že prvek $\sqrt{2} + \sqrt{5}$ je reálné číslo, je hledaným minimálním polynomem kořenový činitel $x - \sqrt{2} - \sqrt{5}$.

(c) Všimneme si, že ζ_5 je kořenem polynomu $m = \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$. Protože je polynom $\hat{m} = m(x+1) = \frac{x+1^5-1}{x} = x^4 + 5x^3 + 10x^2 + 10x + 5$ ireducibilní v $\mathbb{Z}[x]$ díky Eisensteinovu kritériu, je tamtéž ireducibilní i polynom $m = \hat{m}(x-1)$, a tudíž je to díky tvrzení 8.5(2) ireducibilní polynom v $\mathbb{Q}[x]$. Zjistili jsme, že $x^4 + x^3 + x^2 + x + 1$ je minimální polynom prvku ζ_5 nad $\mathbb{Q}$.

(d) Nejprve uvážíme, že 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 všimnout, že $\zeta_7^6 = \zeta_7^{-1}, \zeta_7^5 = \zeta_7^{-2}$ a $\zeta_7^4 = \zeta_7^{-3}$, a proto

$$1 + (\zeta_7 + \zeta_7^{-1}) + (\zeta_7^2 + \zeta_7^{-2}) + (\zeta_7^3 + \zeta_7^{-3}) = 0.$$

Nyní nahlédneme, že každý z prvků $\zeta_7^k + \zeta_7^{-k}$ jde vyjádřit jako polynomiální kombinaci prvku $\zeta_7 + \zeta_7^{-1}$, speciálně:

$$\zeta_7^2 + \zeta_7^{-2} = (\zeta_7 + \zeta_7^{-1})^2 - 2, \text{ a } \zeta_7^3 + \zeta_7^{-3} = (\zeta_7 + \zeta_7^{-1})^3 - 3(\zeta_7 + \zeta_7^{-1})$$

Dohromady dostáváme

$$(\zeta_7 + \zeta_7^{-1})^3 + (\zeta_7 + \zeta_7^{-1})^2 - 2(\zeta_7 + \zeta_7^{-1}) - 1 = 0$$

Konečně, všimneme-li si, že $(x^3 + x^2 - 2x - 1) \mod 2 = x^3 + x^2 + 1$ je v $\mathbb{Z}_2[x]$ ireducibilní polynom, musí být původní monický polynom ireducibilní v $Z[x]$, tudíž

$$m_{\zeta_7+\zeta_7^{-1},\mathbb{Q}} = x^3 + x^2 - 2x - 1$$

je hledaný minimální polynom.

Úloha 13.8. Nechť $a \in S$ je algebraický prvek nad tělesem T, kde T je podtěleso tělesa S, a nechť $b \in S$ splňuje $m_{a,T}(b) = 0$. Dokažte, že $m_{a,T} = m_{b,T}$.

Řešení. Protože je podle tvrzení 22.1(2) $m_{a,T}$ ireducibilní polynom, který je dělitelný rovněž ireducibilním polynomem $m_{b,T}$, jsou oba polynomy asociované a monické, tudíž se sobě budou rovnat.

⋆ **Úloha 13.9.** 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 $m_{b,T} = m_{b,T(a)}$. (Nápověda: Uvažte vícenásobná rozšíření $T \leq T(a) \leq T(a,b)$ a $T \leq T(b) \leq T(a,b)$.)

Řešení. Podobně jako v úloze 13.5 si všimneme, že $m_{a,T(b)} \mid m_{a,T}$ a $m_{b,T(a)} \mid m_{b,T}$, a proto

$$[T(a,b) : T(b)] = \deg(m_{a,T(b)}) \leq \deg(m_{a,T}) = [T(a) : T],$$

$$[T(a,b) : T(a)] = \deg(m_{b,T(a)}) \leq \deg(m_{b,T}) = [T(b) : T].$$

Dále

$$[T(a,b) : T] = [T(a,b) : T(a)] \cdot [T(a) : T] = [T(a,b) : T(b)] \cdot [T(b) : T],$$

z čehož plyne, že $\deg(m_{a,T}) = [T(a) : T]$ stejně jako $\deg(m_{b,T}) = [T(b) : T]$ dělí $[T(a,b) : T]$. Protože se jedná o nesoudělné hodnoty, dostáváme

$$[T(a) : T] \cdot [T(b) : T] \mid [T(a,b) : T] \leq [T(a) : T] \cdot [T(b) : T],$$

proto $[T(a,b) : T] = [T(a) : T] \cdot [T(b) : T]$ a

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

$$\deg(m_{b,T(a)}) = [T(a,b) : T(a)] = [T(b) : T] = \deg(m_{b,T}).$$

Z rovnosti stupně a dělitelnosti už dostáváme, že $m_{a,T} = m_{a,T(b)}$ a $m_{b,T} = m_{b,T(a)}$.

Úloha 13.10. Spočtěte stupeň rozšíření rozkladového nadtělesa polynomu $x^4 + x^3 + 2x^2 + x + 1$ nad tělesem $\mathbb{Q}$.

Řešení. Nejprve si všimneme, že se polynom rozkládá na $(x^2 + 1)(x^2 + x + 1)$ a má tudíž jistě kořeny $\pm i, \frac{1}{2}(1 \pm \sqrt{3}i)$. To znamená, že jeho rozkladovým nadtělesem je $\mathbb{Q}(\sqrt{3}, i)$. Uvážíme, že kořeny $\frac{1}{2}(1 \pm \sqrt{3}i)$ polynomu $x^2 + x + 1$ neleží v $\mathbb{Q}(i)$, proto je tento polynom nerozložitelný nad $\mathbb{Q}(i)$, jedná se o minimální polynom obou kořenů. Proto platí, že

$$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(i)] = \big[\mathbb{Q}(\tfrac{1}{2}(1 + \sqrt{3}i), i) : \mathbb{Q}(i)\big] = \deg(x^2 + x + 1) = 2.$$

Nyní stačí využít tvrzení 22.5, abychom dostali

$$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Úloha 13.11. Dokažte, že $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2}) = \mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$.

Řešení. Nejprve dokážeme první z rovností. První inkluze $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \leq \mathbb{Q}(\sqrt[6]{2})$ plyne z pozorování $\sqrt{2} = \sqrt[6]{2}^3$ a $\sqrt[3]{2} = \sqrt[6]{2}^2$. Pro obrácenou inkluzi si podobně jako v 13.5 všimneme, že

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(x^2 - 2) = 2, \quad \mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^3 - 2) = 3 \quad \text{a} \quad [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = \deg(x^6 - 2) = 6$$

a dále, že podle tvrzení 22.5 máme

$$2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] \quad \text{a} \quad 3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}].$$

Protože $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \leq \mathbb{Q}(\sqrt[6]{2})$, tedy $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ je podprostor šestidimenzionálního racionálního vektorového prostoru $\mathbb{Q}(\sqrt[6]{2})$ a dimenze $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ je dělitelná čísly 2 a 3, je dimenze, tedy stupeň rozšíření $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$ roven šesti a proto $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

V důkazu druhé rovnosti okamžitě vidíme, že platí inkluze $\mathbb{Q}(\sqrt[6]{2}) \geq \mathbb{Q}(\sqrt{2}+\sqrt[3]{2})$, neboť $\sqrt{2}+\sqrt[3]{2} \in \mathbb{Q}(\sqrt[6]{2})$. Na ověření druhé inkluze si stačí uvědomit, že pro $\alpha = \sqrt[6]{2}$ je posloupnost $(\alpha^i \mid j = 0, \ldots, 5)$ báze prostoru $\mathbb{Q}(\sqrt[6]{2})$ nad tělesem $\mathbb{Q}$ a nahlédnout, že čtveřice vektorů v tomto prostoru

$$1,\ \alpha^2(\alpha+1) = \sqrt{2}+\sqrt[3]{2},\ 2\alpha^5+\alpha^4+2 = \alpha^4(\alpha+1)^2 = (\sqrt{2}+\sqrt[3]{2})^2,\ 2(\alpha^3+3\alpha^2+3\alpha+1) = (\sqrt{2}+\sqrt[3]{2})^3$$

je v tomto vektorovém prostoru lineárně nezávislá. To totiž znamená, že

$$4 \leq [\mathbb{Q}(\sqrt{2}+\sqrt[3]{2}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6,$$

a proto nutně $[\mathbb{Q}(\sqrt{2}+\sqrt[3]{2}) : \mathbb{Q}] = 6$. Tedy $\mathbb{Q}(\sqrt{2}+\sqrt[3]{2})$ je šestidimenzionální podprostor prostoru $\mathbb{Q}(\sqrt[6]{2})$ a musejí se tudíž rovnat.

Úloha 13.12. Nechť $T \leq S$ jsou tělesa taková, že $[S : T]$ je prvočíslo. Dokažte, že pak $S = T(a)$ pro libovolný prvek $a \in S \setminus T$. (Nápověda: Uvažte vícenásobné rozšíření $T \leq T(a) \leq S$.)

Řešení. Z tvrzení 22.5 plyne, že $[S : T] = [S : T(a)] \cdot [T(a) : T]$. Protože $[T(a) : T] > 1$ a je to vlastní dělitel prvočísla $[S : T]$, platí, že $[S : T] = [T(a) : T]$, a proto $S = T(a)$.

⋆ **Úloha 13.13.** Nechť T je těleso a a algebraický prvek nad T takový, že $[T(a) : T]$ je lichý. Dokažte, že $T(a) = T(a^2)$. (Nápověda: Uvažte vícenásobné rozšíření $T \leq T(a^2) \leq T(a)$.)

Řešení. Těleso $T(a^2)$ je jistě podtělesem tělesa $T(a)$. Protože $x^2 - a^2 \in T(a^2)[x]$ má za kořen a, platí, že

$$[T(a) : T(a^2)] = \deg m_{a,T(a^2)} \leq \deg x^2 - a^2 = 2.$$

Navíc dle tvrzení 22.5 je $[T(a) : T] = [T(a) : T(a^2)] \cdot [T(a^2) : T]$, a to je liché, což znamená, že $[T(a) : T(a^2)] = 1$, tedy $T(a) = T(a^2)$.