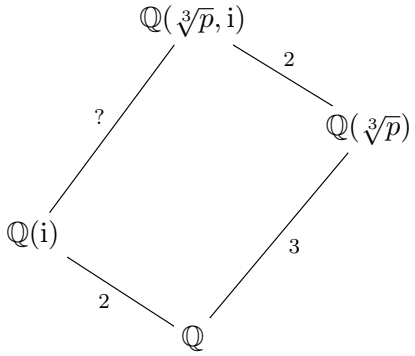
1 Galoisova teorie

Příklad 1.1. Buď $F = \mathbb{Q}(\mathrm{i})$. Ukažte, že pro libovolné prvočíslo p je polynom $x^3 - p$ ireducibilní nad F.

Řešení. Polynom $x^3 - p$ je ireducibilní nad F právě tehdy, když

$$[F(\sqrt[3]{p}) \colon F] = [\mathbb{Q}(\sqrt[3]{p}, \mathrm{i}) \colon \mathbb{Q}(\mathrm{i})] = 3.$$

Polynom $x^2 + 1$ je ireducibilní nad $\mathbb{Q}(\sqrt[3]{p})$, vždyť $\mathbb{Q}(\sqrt[3]{p}) \subseteq \mathbb{R}$, tedy $[\mathbb{Q}(\sqrt[3]{p}, \mathrm{i}) \colon \mathbb{Q}(\sqrt[3]{p})] = 2$. Z diagramu



již snadno odvodíme, že $[\mathbb{Q}(\sqrt[3]{p}, \mathrm{i}) \colon \mathbb{Q}(\mathrm{i})] = 3$. ◇

Příklad 1.2. Buď F těleso charakteristiky $\operatorname{char} F \neq 2$. Nechť a, b jsou prvky tělesa F, přičemž b není druhou mocninou prvku z F. Dokažte, že $a^2 - b$ je druhou mocninou prvku z F právě tehdy, když v tělese F existují prvky m, n splňující

$$\sqrt{a + \sqrt{b}} = \sqrt{m} + \sqrt{n}.$$

Řešení. „⇒:“ Předpokládejme, že existuje $c \in F$ takové, že

$$a^2 - b = c^2.$$

Pak $b = a^2 - b^2$. Položme

$$m = \frac{a - c}{2} \qquad n = \frac{a + c}{2}.$$

Odtud dostáváme

$$(\sqrt{m} + \sqrt{n})^2 = m + n + 2\sqrt{mn} = a + 2 \cdot \sqrt{\frac{a^2 - c^2}{4}} = a + \sqrt{b}.$$

„⇐:“ Nyní předpokládejme, že existují $m, n \in F$ tak, že

$$a + \sqrt{b} = m + n + 2\sqrt{mn}.$$

Pak platí

$$2\sqrt{mn} = a + \sqrt{b} - m - n = a - m - n + \sqrt{b},$$
$$4mn = (a - m - n)^2 + b + 2(a - m - n)\sqrt{b}.$$

Protože b není čtverec, tak musí platit $a - m - n = 0$, tedy $a = m + n$. Pak $4mn = b$ a platí

$$a^2 - b = (m + n)^2 - 4mn = (m - n)^2.$$ ◇

Nechť K/F je konečné rozšíření těles. Buď $\alpha \in K$ libovolný prvek. Pak zobrazení $\Psi_\alpha \colon K \to K$ dané předpisem

$$\Psi_\alpha(\beta) = \alpha \cdot \beta$$

je lineární transformace vektorového prostoru, tj. pro všechna $\beta, \gamma \in K$ a každé $a \in F$ platí

$$\Psi_\alpha(\beta + \gamma) = \Psi_\alpha(\beta) + \Psi_\alpha(\gamma),$$
$$\Psi_\alpha(a\beta) = a \cdot \Psi_\alpha(\beta).$$

Zvolme bázi K nad F a uvažme matici A_α lineární transformace Ψ_α v této bázi. Polynom

$$f_\alpha(x) = \det(x \cdot E - A_\alpha)$$

se nazývá *charakteristický polynom* Ψ_α, přičemž jeho definice nezávisí na volbě báze. Vskutku, je-li B_α matice $\Psi_\alpha(x)$ v jiné bázi, pak

$$B_\alpha = R^{-1} A_\alpha R,$$

kde R je vhodná regulární matice, a platí

$$\det(x \cdot E - B_\alpha) = \det(x \cdot E - R^{-1} A_\alpha R) = \det\big(R^{-1}(x \cdot E - A_\alpha)R\big) = \det(x \cdot E - A_\alpha).$$

Označme $m_\alpha(x)$ minimlní polynom prvku α nad F. Následující tvrzení dává do vztahu polynom m_α a polynom $f_\alpha(x)$.

Tvrzení 1.3. *Platí*

$$f_\alpha = m_\alpha^{[K\colon F(\alpha)]}.$$

Důkaz. Označme $d = [F(\alpha)\colon F]$, pak bází $F(\alpha)/F$ je $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$. Zvolme $\beta_1, \beta_2, \ldots, \beta_r$ bázi rozšíření $K/F(\alpha)$, tj. $r = [K\colon F(\alpha)]$. Víme, že

$$\alpha^i \beta_j \qquad \text{pro } 0 \le i < d, 1 \le j \le r$$

je báze K/F a platí

$$\Psi_\alpha(\alpha^i \beta_j) = \alpha^{i+1} \beta_j.$$

Je-li $i = d - 1$, pak nemáme prvek báze. Minimální polynom m_α prvku α nad F je tvaru

$$m_\alpha(x) = x^d - c_{d-1}x^{d-1} - \ldots - c_1 x - c_0$$

pro vhodná $c_i \in F$. Pak platí

$$\alpha^d = c_{d-1}\alpha^{d-1} + \cdots + c_1\alpha + c_0,$$

a tedy

$$\Psi_\alpha(\alpha^{d-1}\beta_j) = \alpha^d \beta_j = c_{d-1}\alpha^{d-1}\beta_j + \cdots + c_1\alpha\beta_j + c_0\beta_j.$$

Matice A_α má r bloků na diagonále (jinde 0) a tyto bloky jsou tvaru

$$B = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ c_0 & c_1 & c_2 & c_3 & \cdots & c_{d-2} & c_{d-1} \end{pmatrix}$$

Pak $f_\alpha(x) = \det(x \cdot E - B)^r$. Stačí dokázat následující lemma:

Lemma 1.4. *Platí*

$$\begin{vmatrix} x & -1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & x & -1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & x & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & -1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & x & -1 \\ -c_0 & -c_1 & -c_2 & -c_3 & \cdots & -c_{d-2} & x-c_{d-1} \end{vmatrix} = x^d - c_{d-1}x^{d-1} - \cdots - c_1 x - c_0$$

Důkaz. Lemma dokážeme indukcí vzhledem k d.

(i) $d = 1$. Zřejmé.

(ii) $d > 1$, předpokládejme, že pro $d-1$ tvrzení platí. Rozvoj podle prvního sloupce nám dá

$$x \underbrace{(x^{d-1} - c_{d-1}x^{d-2} - \cdots - c_2 x - c_1)}_{\text{indukční předpoklad}} + (-1)^{d+1} \cdot (-c_0) \cdot (-1)^{d-1} =$$
$$= x^d - c_{d-1}x^{d-1} - \cdots - c_1 x - c_0. \qquad \square$$

Tím je důkaz tvrzení hotov. $\square$

Je-li $\alpha \neq 0$, pak A_α je regulární, protože pro libovolné $\alpha \in K$ platí

$$0 = \det(A_\alpha) = f_\alpha(0) \Leftrightarrow m_\alpha(0) \Leftrightarrow \alpha = 0.$$

Příklad 1.5. Pro každé z čísel $\sqrt[3]{2}$ a $1 + \sqrt[3]{2} + \sqrt[3]{4}$ nalezněte kubický polynom, jehož je toto číslo kořenem.

Řešení. Uvažme těleso $\mathbb{Q}(\sqrt[3]{2})$ a zafixujme bázi $1, \sqrt[3]{2}, \sqrt[3]{4}$. Násobení číslem $\sqrt[3]{2}$ má v bázi $1, \sqrt[3]{2}, \sqrt[3]{4}$ matici

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$$

Charakteristický polynom pak je

$$\begin{vmatrix} x & -1 & 0 \\ 0 & x & -1 \\ -2 & 0 & x \end{vmatrix} = x^3 - 2.$$

Násobení číslem $1 + \sqrt[3]{2} + \sqrt[3]{4}$ má v bázi $1, \sqrt[3]{2}, \sqrt[3]{4}$ matici

$$\begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 1 \\ 2 & 2 & 1 \end{pmatrix}$$

Charakteristický polynom pak je

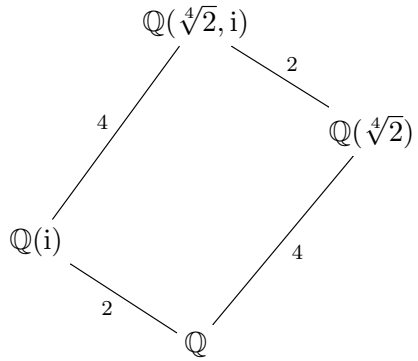
$$\begin{vmatrix} x-1 & -1 & -1 \\ -2 & x-1 & -1 \\ -2 & -2 & x-1 \end{vmatrix} = \begin{vmatrix} x-1 & -1 & -1 \\ -2 & x-1 & -1 \\ 0 & -x-1 & x \end{vmatrix} = (x-1) \cdot (x^2 - 2x - 1) + 2 \cdot (-2x - 1) =$$
$$= x^3 - 3x^2 - 3x - 1. \qquad \diamond$$

2 Rozkladová tělesa

Definice 2.1. Rozšíření K tělesa F se nazývá rozkladové těleso polynomu $f \in F[x]$, jestliže se polynom f rozkládá na lineární činitele nad K, ale už se nerozkládá nad M, kde $M \subsetneq K$ je libovolné podtěleso.

Příklad 2.2. Určete rozkladové těleso a jeho stupeň nad $\mathbb{Q}$ pro polynom $x^4 - 2$.

Řešení. Rozkladové těleso polynomu $x^4 - 2$ nad $\mathbb{Q}$ je $K = \mathbb{Q}(\sqrt[4]{2}, \mathrm{i})$. Z diagramu



pak snadno odvodíme, že $[\mathbb{Q}(\sqrt[4]{2}, \mathrm{i}) : \mathbb{Q}] = 8$. ◇

Příklad 2.3. Určete rozkladové těleso a jeho stupeň nad $\mathbb{Q}$ pro polynom $x^4 + 2$.

Řešení. Rozkladové těleso polynomu $x^4 + 2$ nad $\mathbb{Q}$ je $L = \mathbb{Q}(\alpha, \mathrm{i})$, kde $\alpha = \sqrt[4]{2}\left(\frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt{2}}{2}\right)$. Snadno se vidí, že $(\frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt{2}}{2})$ leží v K, a proto $L \subseteq K$. Dále platí

$$(1 - \mathrm{i})\alpha = \alpha - \mathrm{i}\alpha = \sqrt[4]{2}\left(\frac{\sqrt{2}}{2} + \mathrm{i}\frac{\sqrt{2}}{2}\right) + \sqrt[4]{2}\left(\frac{\sqrt{2}}{2} - \mathrm{i}\frac{\sqrt{2}}{2}\right) = \sqrt[4]{2} \cdot \sqrt{2} = \frac{2}{\sqrt[4]{2}},$$

tedy

$$\sqrt[4]{2} = \frac{2}{(1 - \mathrm{i})\alpha} \in L,$$

a proto $K = L$. ◇

Příklad 2.4. Určete rozkladové těleso a jeho stupeň nad $\mathbb{Q}$ pro polynom $x^4 + x^2 + 1$.

Řešení. Polynom $x^4 + x^2 + 1$ se nad $\mathbb{Q}$ rozkládá na součin

$$x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1).$$

Oba polynomy maj diskriminant $D = -3$, tedy rozkladovým tělesem polynomu $x^4 + x^2 + 1$ je těleso $\mathbb{Q}(\mathrm{i}\sqrt{3})$. ◇

Příklad 2.5. Určete rozkladové těleso a jeho stupeň nad $\mathbb{Q}$ pro polynom $x^6 - 4$.

Řešení. Polynom $x^6 - 4$ se nad $\mathbb{Q}$ rozkládá na součin

$$x^6 - 4 = (x^3 - 2)(x^3 + 2).$$

Pro libovolné $\alpha \in \mathbb{R}$ platí

$$\alpha^3 = 2 \Leftrightarrow (-\alpha)^3 = -2.$$

Stačí tedy uvažovat rozkladové těleso polynomu $x^3 - 2$ a tím je těleso $\mathbb{Q}(\mathrm{i}\sqrt{3}, \sqrt[3]{2})$. ◇

Definice 2.6. Buď K těleso. Nechť $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ je libovolný nekonstantní polynom. Označme $\alpha_1, \alpha_2, \ldots, \alpha_n$ kořeny polynomu f v $\overline{K}$. Výraz

$$D(f) = a_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

se nazývá *diskriminant polynomu* f.

Poznámka 2.1. Pro kubický polynom $f(x) = ax^3 + bx^2 + cx + d$ je diskriminant tvaru

$$D(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

Věta 2.7. *Nechť $f(x) \in \mathbb{Q}[x]$ je libovolný kubický polynom. Dále nechť $\alpha \in \overline{\mathbb{Q}}$ je jeho kořen. Pak rozkladovým tělesem polynomu f je těleso*

$$\mathbb{Q}(\alpha, \sqrt{D}),$$

kde D je diskriminant polynomu f.

Důkaz. Označme K rozkladové těleso polynomu f. Zřejmě $\mathbb{Q}(\alpha, \sqrt{D}) \subseteq K$. Označme β, γ zbylé dva kořeny polynomu f. Budeme hotovi, pokud ukážeme, že β a γ leží v $\mathbb{Q}(\alpha, \sqrt{D})$. Protože α leží v $\mathbb{Q}(\alpha, \sqrt{D})$, má polynom $(x - \beta)(x - \gamma)$ koeficienty z $\mathbb{Q}(\alpha, \sqrt{D})$, tedy $\gamma + \beta$ a $\gamma\beta$ leží v $\mathbb{Q}(\alpha, \sqrt{D})$. Označíme-li a vedoucí koeficient polynomu f, pak platí

$$\mathbb{Q}(\alpha, \sqrt{D}) \ni \sqrt{D} = a^2(\alpha - \beta)(\beta - \gamma)(\alpha - \gamma) = \underbrace{a^2\big(\alpha^2 + (\beta + \gamma)\alpha + \beta\gamma\big)}_{\in \mathbb{Q}(\alpha, \sqrt{D})}(\beta - \gamma),$$

a tedy $\beta - \gamma \in \mathbb{Q}(\alpha, \sqrt{D})$. Tím je důkaz hotov. □

Příklad 2.8. Rozhodněte, zda se jedná o normální rozšíření:

1. $\mathbb{Q}(\alpha)/\mathbb{Q}$, kde α je kořen polynomu $x^3 - 3x + 1$.
2. $\mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{4})/\mathbb{Q}$