14 Galois a jeho grupy

Řešení
verze ze dne 20. května 2025.

Cíle cvičení: Jako velký zlatý hřebík našeho algebraického snažení si zkusíme pro některá rozkladová nadtělesa spočítat jejich Galoisovy grupy. Ačkoli to zpravidla není nijak snadná úloha, máme síly na to, abychom Galoisovu grupu spočítali aspoň pro rozkladová nadtělesa polynomů malého stupně. Zásadním se ukáže zjištění, že Galoisovu grupu můžeme hledat jako podgrupu grupy permutací kořenů rozkládaného polynomu.

Úlohy, které bychom určitě měli umět řešit:

Úloha 14.1. Je-li U rozkladové nadtěleso polynomu $p = x^3 - 2$ nad tělesem $\mathbb{Q}$, ukažte, že

(a) $U = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$,

(b) $[U : \mathbb{Q}] = 6$,

(c) $\mathrm{Gal}(U/\mathbb{Q}) \cong \mathbf{S}_3$.

Řešení. (a) Nejprve uvážíme rozklad polynomu $x^3 - 2$ na kořenové činitele v $\mathbb{C}$

$$p = x^3 - 2 = \big(x - \sqrt[3]{2}\big)\big(x - \sqrt[3]{2}\,\omega\big)\big(x - \sqrt[3]{2}\,\overline{\omega}\big),$$

kde $\omega = e^{2\pi i/3}$, z definice rozkladového nadtělesa tedy je $U = \mathbb{Q}\big(\sqrt[3]{2}, \sqrt[3]{2}\,\omega, \sqrt[3]{2}\,\overline{\omega}\big)$. Platí dále $\overline{\omega} = -1-\omega = \omega^{-1} = \omega^2 = e^{-2\pi i/3}$, odkud dostáváme $U \leq \mathbb{Q}\big(\sqrt[3]{2}, \omega\big)$. Jelikož $\sqrt[3]{2}\,\omega \in U$ a $(\sqrt[3]{2})^{-1} \in U$, máme

$$\omega = \sqrt[3]{2}\,\omega \cdot (\sqrt[3]{2})^{-1} \in U,$$

tedy $\mathbb{Q}\big(\sqrt[3]{2}, \omega\big) \leq U$. V souhrnu dostáváme rovnost $U = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$.

(b) Spočítáme stupeň rozšíření pomocí tvrzení 22.5, které říká, že $[U : \mathbb{Q}] = [U : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$ pro každé $\alpha \in U$. Položíme $\alpha = \sqrt[3]{2}$ a nejprve standardním argumentem nahlédneme, že

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

neboť víme, že je polynom $x^3 - 2$ nad $\mathbb{Q}$ ireducibilní. Dále si všimneme, že minimální polynom prvku ω nad tělesem $\mathbb{Q}(\sqrt[3]{2})$ dělí polynom $x^3 - 1 = (x-1)(x^2+x+1)$ a tudíž i x^2+x+1. Protože kořeny polynomu $x^2 + x + 1$ nejsou reálné, dostáváme, že $m_{\omega,\mathbb{Q}(\sqrt[3]{2})} = x^2 + x + 1$, a proto

$$[U : \mathbb{Q}(\sqrt[3]{2})] = [(\mathbb{Q}(\sqrt[3]{2}))(\omega) : \mathbb{Q}(\sqrt[3]{2})] = \deg m_{\omega,\mathbb{Q}(\sqrt[3]{2})} = \deg(x^2 + x + 1) = 2$$

Ukázali jsme, že $[U : \mathbb{Q}] = [U : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$.

(c) Protože je polynom $x^3 - 2$ nad tělesem racionálních čísel ireducibilní, plyne z tvrzení 25.2(1), že je grupa $\mathrm{Gal}(U/\mathbb{Q})$ izomorfní podgrupě grupy permutací všech kořenů polynomu $x^3 - 2$, tedy grupy izomorfní $\mathbf{S}_3$. Nyní použijeme tvrzení 25.2 a Lagrangeovy věty, abychom ukázali, že je $\mathrm{Gal}(U/\mathbb{Q})$ řádu 6, tedy už musí být symetrické grupě $\mathbf{S}_3$ izomorfní.

Na přednášce jsme si uvědomili snadné pozorování, že zobrazení komplexního sdružení $\overline{\mathrm{id}}$ je prvek $\mathrm{Gal}(U/\mathbb{Q})$ a tvrzení 25.2(2) nám zaručuje existenci prvků $\varphi_1, \varphi_2 \in \mathrm{Gal}(U/\mathbb{Q})$ splňujících podmínku

$$\varphi_1(\sqrt[3]{2}) = \sqrt[3]{2}\,\omega, \qquad \varphi_2(\sqrt[3]{2}) = \sqrt[3]{2}\,\overline{\omega}$$

To tedy znamená, že Galoisova grupa $\mathrm{Gal}(U/\mathbb{Q})$, která je izomorfní nějaké podgrupě šestiprvkové grupy $\mathbf{S}_3$, obsahuje alespoň čtyři různé prvky $\mathrm{id}, \overline{\mathrm{id}}, \varphi_1, \varphi_2$, tedy nám Lagrangeova věta říká, že

$$4 \leq |\mathrm{Gal}(U/\mathbb{Q})| \mid |\mathbf{S}_3| = 6,$$

tudíž dostáváme izomorfismus $\mathrm{Gal}(U/\mathbb{Q}) \cong \mathbf{S}_3$.

Úloha 14.2. Spočítejte Galoisovu grupu $\mathrm{Gal}(U/\mathbb{Q})$, je-li U rozkladové nadtěleso polynomu

(a) $x^4 + 4x^2 + 2$,

(b) $x^4 - 2$.

Řešení. (a) Nejprve provedeme substituci $y = x^2$ a standardním postupem najdeme komplexní kořeny $-2 \pm \sqrt{2}$ polynomu $y^2 + 4y + 2$. Nyní vidíme, že $\pm i\sqrt{2 \pm \sqrt{2}}$ představuje všechny kořeny polynomu $x^4 + 4x^2 + 2$. Dále si všimněme, že

$$\sqrt{2} = -\left(i\sqrt{2+\sqrt{2}}\right)^2 - 2 \in \mathbb{Q}\left(i\sqrt{2+\sqrt{2}}\right),$$

$$i\sqrt{2-\sqrt{2}} = \frac{-\sqrt{2}}{i\sqrt{2+\sqrt{2}}}\frac{\sqrt{2-\sqrt{2}}}{\sqrt{2-\sqrt{2}}} = \frac{-\sqrt{2}}{i\sqrt{2+\sqrt{2}}} \in \mathbb{Q}\left(i\sqrt{2+\sqrt{2}}\right),$$

čímž jsme dokázali, že $U = \mathbb{Q}(i\sqrt{2+\sqrt{2}})$ a každý $\mathbb{Q}$-automorfismus tělesa U je určen obrazem prvku $i\sqrt{2+\sqrt{2}}$ na kterýkoli z kořenů kořenů $\pm i\sqrt{2 \pm \sqrt{2}}$, tedy $|\mathrm{Gal}(U/\mathbb{Q})| \leq 4$. S pomocí Eisensteinova kritéria standardně nahlédneme, že je polynom $x^4 + 4x^2 + 2$ ireducibilní nad tělesem $\mathbb{Q}$, což podle tvrzení 25.2(2) již znamená, že Galoisova grupa $\mathrm{Gal}(U/\mathbb{Q})$ je izomorfní čtyřprvkové podgrupě grupy $\mathbf{S}_4$. Nyní uvážíme automorfismus $\varphi \in \mathrm{Gal}(U/\mathbb{Q})$ určený podmínkou

$$\varphi\left(i\sqrt{2+\sqrt{2}}\right) = i\sqrt{2-\sqrt{2}},$$

pak z vlastností homomorfismu a vyjádření $\sqrt{2}$ a $i\sqrt{2-\sqrt{2}}$ spočtených výše, že

$$\varphi(\sqrt{2}) = \varphi\left(-\left(i\sqrt{2+\sqrt{2}}\right)^2 - 2\right) = -\varphi\left(i\sqrt{2+\sqrt{2}}\right)^2 - 2 = -\left(i\sqrt{2-\sqrt{2}}\right)^2 - 2 = -\sqrt{2},$$

$$\varphi\left(i\sqrt{2-\sqrt{2}}\right) = \varphi\left(-\frac{\sqrt{2}}{i\sqrt{2+\sqrt{2}}}\right) = \frac{-\varphi(\sqrt{2})}{\varphi(i\sqrt{2+\sqrt{2}})} = \frac{-\sqrt{2}}{i\sqrt{2-\sqrt{2}}} = -i\sqrt{2+\sqrt{2}}.$$

To znamená, že

$$\varphi^2\left(i\sqrt{2+\sqrt{2}}\right) = \varphi\left(i\sqrt{2-\sqrt{2}}\right) = -i\sqrt{2+\sqrt{2}} \neq \mathrm{id}\left(i\sqrt{2+\sqrt{2}}\right),$$

tedy φ je prvek grupy $\mathrm{Gal}(U/\mathbb{Q})$ řádu většího než 2, tudíž je podle Lagrangeovy věty nutně řádu 4, grupa $\mathrm{Gal}(U/\mathbb{Q})$ je cyklická a platí

$$\mathrm{Gal}(U/\mathbb{Q}) = \langle\varphi\rangle \cong \mathbb{Z}_4.$$

(b) Obdobně jako v úloze 14.1 nejprve zjistíme, že $U = \mathbb{Q}(\sqrt[4]{2}, i)$. Protože $\mathbb{Q}(i)$ je rozkladové nadtěleso polynomu $x^2 + 1$ na tělesem $\mathbb{Q}$, říká nám lemma 25.5, že $\mathrm{Gal}(U/\mathbb{Q}(i))$ je normální podgrupa $\mathrm{Gal}(U/\mathbb{Q})$ a navíc platí, že

$$\mathrm{Gal}(U/\mathbb{Q}) \,/\, \mathrm{Gal}(U/\mathbb{Q}(i)) \cong \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}).$$

Z rozkladu

$$x^4 - 2 = \left(x - \sqrt[4]{2}\right)\left(x - i\sqrt[4]{2}\right)\left(x + \sqrt[4]{2}\right)\left(x + i\sqrt[4]{2}\right)$$

vidíme, že kořenové činitele ani jejich součiny stupně dva nemají koeficienty v tělese $\mathbb{Q}(i)$, tedy $x^4 - 2$ je ireducibilní polynom nad tělesem $\mathbb{Q}(i)$, tedy také minimálním polynomem $\sqrt[4]{2}$ nad $\mathbb{Q}(i)$. Proto z tvrzení 22.3 máme

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

Všimněme si, že je rozkladové nadtěleso U polynomu x^4-2 chápaného nad tělesem $\mathbb{Q}(i)$ zároveň kořenovým nadtělesem pro kterýkoli z jeho kořenů, tedy například $U = (\mathbb{Q}(i))(\sqrt[4]{2})$ (obecně rozkladové nadtěleso izomorfní kopie kořenových nadtěles jen obsahuje). Proto je každý $\mathbb{Q}(i)$-automorfismus $\mathrm{Gal}(U/\mathbb{Q}(i))$ určený obrazem kořenu $\sqrt[4]{2}$, který se podle věty 25.1 musí nutně zobrazit na jeden ze čtyř kořenů polynomu x^4-2, což znamená, že $|\mathrm{Gal}(U/\mathbb{Q}(i))| \leq 4$. Nechť $\varphi \in \mathrm{Gal}(U/\mathbb{Q}(i))$ je automorfismus určený podmínkou $\varphi(\sqrt[4]{2}) = \sqrt[4]{2}i$, který existuje podle tvrzení 25.2. Pak snadno z vlastností $\mathbb{Q}(i)$-automorfismů spočítáme, že

$$\varphi^2(\sqrt[4]{2}) = \varphi(\sqrt[4]{2}i) = \varphi(\sqrt[4]{2})i = -\sqrt[4]{2}, \quad \varphi^3(\sqrt[4]{2}) = \varphi(-\sqrt[4]{2}) = -\varphi(\sqrt[4]{2}) = -\sqrt[4]{2}i,$$

jedná se o prvek Galoisovy grupy $\mathrm{Gal}(U/\mathbb{Q}(i))$, který tvoří čtyřcyklus na kořenech, tedy je to prvek řádu 4. Tudíž $\mathrm{Gal}(U/\mathbb{Q}(i))$ je nutně cyklická grupa řádu 4.

Dále si uvědomíme, že

$$\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{\mathrm{id}, \overline{\mathrm{id}}\} \cong \mathbb{Z}_2,$$

tudíž

$$\mathrm{Gal}(U/\mathbb{Q}) = \mathrm{Gal}(U/\mathbb{Q}(i)) \cup \overline{\mathrm{id}}\,\mathrm{Gal}(U/\mathbb{Q}(i)) = \{\mathrm{id}, \varphi, \varphi^2, \varphi^3, \overline{\mathrm{id}}, \overline{\varphi}, \overline{\varphi^2}, \overline{\varphi^3}\}.$$

Nyní si označíme kořeny polynomu x^4-2

$$\mathbf{1} = \sqrt[4]{2}, \quad \mathbf{2} = i\sqrt[4]{2}, \quad \mathbf{3} = -\sqrt[4]{2}, \quad \mathbf{4} = -i\sqrt[4]{2}$$

a přepíšeme si jednotlivé automorfismy $\mathrm{Gal}(U/\mathbb{Q})$ jako permutace kořenů

$$\{\mathrm{id}, \varphi, \varphi^2, \varphi^3, \overline{\mathrm{id}}, \overline{\varphi}, \overline{\varphi^2}, \overline{\varphi^3}\} \cong \{\mathrm{id}, (\mathbf{1234}), (\mathbf{13})(\mathbf{24}), (\mathbf{1432}), (\mathbf{24}), (\mathbf{14})(\mathbf{23}), (\mathbf{13}), (\mathbf{12})(\mathbf{34})\} \leq \mathbf{S}_4.$$

Nyní už snadno nahlédneme, že permutační podgrupa izomorfní $\mathrm{Gal}(U/\mathbb{Q})$ je izomorfní grupě $\mathbf{D}_8$ symetrií čtverce, kde hodnoty $\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}$ označují jeho vrcholy proti směru hodinových ručiček.

A teď něco pro pro potěšení, protože máme Galoise rádi:

Úloha 14.3. Pro $p > 2$ prvočíslo, polynom $\Phi_p = \frac{x^p-1}{x-1} = \sum_{j=0}^{p-1} x^j$ a rozkladové nadtěleso U polynomu Φ_p nad tělesem $\mathbb{Q}$ dokažte, že

(a) $U = \mathbb{Q}[\zeta_p]$,

(b) $[U : \mathbb{Q}] = p-1$,

(c) $\mathrm{Gal}(U/\mathbb{Q}) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$,

Řešení. (a) Protože ζ_p^a jsou pro $a \in \mathbb{Z}_p$ právě všechny kořeny polynomu x^p-1, dostáváme, že

$$\frac{x^p-1}{x-1} = \prod_{a \in \mathbb{Z}_p^*} (x - \zeta_p^a).$$

Protože všechny mocniny ζ_p^a už leží v tělese $\mathbb{Q}(\zeta_p)$, jedná se nejen o kořenové nadtěleso, nýbrž i rozkladové nadtěleso polynomu Φ_p nad tělesem $\mathbb{Q}$.

(b) Vzpomeneme-li si, že jsme v 5. sérii v úloze 5.14(c) ukázali, že je polynom Φ_p ireducibilní nad $\mathbb{Q}$ (nebo ireducibilitu znovu dokážeme substitucí $x \to x+1$ a využitím Eisensteinova kritéria), vidíme, že se jedná o minimální polynom prvku ζ_p nad $\mathbb{Q}$, a proto díky (a) a tvrzení 22.3 dostáváme

$$[U : \mathbb{Q}] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg(\Phi_p) = \deg\left(\sum_{j=0}^{p-1} x^j\right) = p-1.$$

(c) Podle tvrzení 25.2(1) a části (a) víme, že každé zobrazení kořenu ζ_p na kterýkoli kořen ζ_p^a pro $a \in \mathbb{Z}_p^*$ lze rozšířit na $\mathbb{Q}$-automorfismus $\rho_a \in \mathrm{Gal}(U/\mathbb{Q})$. Navíc obraz ζ_p už jednoznačně automorfismus určuje,

tedy jsme zkonstruovali bijekci $\mathbb{Z}_p^* \to \mathrm{Gal}(U/\mathbb{Q})$. Zbývá dokázat, že se jedná o grupový homomorfismus. Zvolíme-li $a, b \in \mathbb{Z}_p^*$, pak

$$(\rho_a \circ \rho_b)(\zeta_p) = \rho_a(\rho_b(\zeta_p)) = \rho_a(\zeta_p)^b) = \zeta_p^{ab} = \rho_{ab}(\zeta_p).$$

To znamená, že $\rho_a \circ \rho_b = \rho_{ab}$, a proto je zkonstruovaná bijekce izomorfismus.

Úloha 14.4. Explicitně popište všechny prvky Galoisovy grupy $\mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q})$ z předchozí úlohy. Jak vypadají její prvky řádu 2?

Řešení. Protože umíme pro jednotlivé prvky ρ_a Galoisovy grupy spočítat jejich hodnotu na bázi $M = (\zeta_p^j \mid j \in \mathbb{Z}_p)$, tedy $f_j(\zeta_p^a) = \zeta_p^{ja}$ a víme, že jde rovněž o lineární zobrazení vektorového prostoru U nad tělesem $\mathbb{Q}$ do sebe, snadno určíme chování f_a na libovolném prvku se souřadnicemi $(t_j)_{j=0}^{p-1}$ vzhledem k bázi M:

$$f_a\left(\sum_{j=0}^{p-1} t_j \zeta_p^j\right) = \sum_{j=0}^{p-1} t_j \zeta_p^{ja}.$$

Prvek řádu dva bude potom díky izomorfismu z předchozí úlohy obrazem jediného prvku řádu dva v grupě $\mathbb{Z}_p^*$, což je $-1 = p-1$, tedy

$$f_{p-1}\left(\sum_{j=0}^{p-1} t_j \zeta_p^j\right) = \sum_{j=0}^{p-1} t_j \zeta_p^{j(p-1)} = \sum_{j=0}^{p-1} t_j \zeta_p^{-j}.$$

Úloha 14.5. Nechť p je prvočíslo, n přirozené číslo a $\mathbb{F}_{p^n}$ konečné těleso velikosti p^n, označme $\mathbb{F}_p$ jeho p-prvkové podtěleso (tj. prvotěleso) a definujte zobrazení $f_p\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ předpisem $f_p(a) = a^p$. Dokažte, že

(a) $f_p \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$,

(b) $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle f_p \rangle$ je cyklická grupa řádu n,

⋆ (c) $\{a \in \mathbb{F}_{p^n} \mid f_p^d(a) = a\}$ je podtěleso tělesa $\mathbb{F}_{p^n}$ řádu p^d pro každé $d \mid n$.

Řešení. (a) Nejprve si uvědomíme, že z malé Fermatovy věty plyne, že $f_p(a) = a^p = a$ pro všechny prvky z podtělesa $\mathbb{F}_p \cong \mathbb{Z}_p$. Dále zvolíme $a, b \in \mathbb{F}_{p^n}$ a počítáme:

$$f_p(a \cdot b) = (ab)^p = a^p \cdot b^p = f_p(a) \cdot f_p(b), \quad f(1) = 1^p = 1,$$

$$f_p(a+b) = (a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} = a^p + b^p = f_p(a) + f_p(b),$$

kde jsme využili pozorování, že p dělí $\binom{p}{i}$ pro všechna $i = 1, \ldots, p-1$, a proto jsou všechny členy $\binom{p}{i} a^i b^{p-i}$ v tělese charakteristiky p nulové.

(b) Z přednášky víme, že je multiplikativní grupa $\mathbb{F}_{p^n}^*$ cyklická, tedy v ní najdeme prvek α řádu $p^n - 1$, pro který zřejmě platí, že $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$. Zároveň si snadno uvědomíme, že

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg(m_{\alpha,\mathbb{F}_p})$$

pro minimální polynom $m_{\alpha,\mathbb{F}_p}$ prvku α. Tudíž každý automorfismus tělesa $\mathbb{F}_p(\alpha)$ je jednoznačně určen obrazem generátoru α, což musí být rovněž kořen polynomu $m_{\alpha,\mathbb{F}_p}$. Máme tedy nejvýše n prvků Galoisovy grupy $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Na druhou stranu z předchozí úlohy víme, že $f_p \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ a také f_p^k jsou $\mathbb{F}_p$-automorfismy pro všechna $k \in \mathbb{N}$. Zbývá si uvědomit, že $f_p^n = \mathrm{id}$ a že $f_p^k(\alpha) = \alpha^{p^k}$ jsou různé prvky pro všechna $k = 0, \ldots, n-1$, neboť řád prvku α je $p^n - 1$. To znamená, že

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \{f_p^k \mid k = 0, \ldots, n-1\} = \langle f_p \rangle$$

je cyklická grupa právě řádu n.

(c) Nejprve uvážíme, že pokud $n = kd$, pak

$$p^n - 1 = (p^d - 1) \sum_{i=0}^{d-1} p^{id},$$

tedy pro $s = \sum_{i=0}^{d-1} p^{ik}$ máme $(p^n - 1) = s(p^d - 1)$. Obdobným argumentem dostáváme, že

$$(x^{p^n} - x) = x(x^{p^d-1} - 1) \sum_{i=0}^{s-1} x^{i(p^d-1)}.$$

Tím jsme dokázali, že polynom $x^{p^d} - x$ dělí polynom $x^{p^n} - x$.

Nyní si všimneme, že za Lagrangeovy věty plyne, že pro každé $u \in \mathbb{F}_{p^n}^*$ platí, že $u^{p^n-1} = 1$, tudíž jsou všechny prvky tělesa $\mathbb{F}_{p^n}$ kořeny polynomu $x^{p^n} - x$, což nutně znamená, že

$$x^{p^n} - x = \prod_{a \in \mathbb{F}} (x - a).$$

Dále si všimneme, že množina

$$U_d = \{a \in \mathbb{F}_{p^n} \mid f_p^d(a) = a\} = \{a \in \mathbb{F}_{p^n} \mid a^{p^d} - a = 0\}$$

obsahuje právě všechny kořeny polynomu $x^{p^d} - x$. Protože tento polynom dělí polynom $x^{p^n} - x$, který se v tělese $\mathbb{F}_{p^n}$ rozkládá na různé kořenové činitele, obsahuje množina právě p^d prvků.

Zbývá ukázat, že je množina opravdu podtělesem. K tomu využijeme fakt, dokázaný v (a), že je f_p, a tudíž i f_p^d automorfismus. Nechť $a, b \in U_d$, potom

$$f_p^d(a + b) = f_p^d(a) + f_p^d(b) = a + b, \quad f_p^d(a \cdot b) = f_p^d(a) \cdot f_p^d(b) = a \cdot b, \quad f_p^d(0) = 0, \quad f_p^d(1) = 1,$$

tedy $a + b, a \cdot b, 0, 1 \in U_d$. Je-li navíc $a \neq 0$, pak

$$1 = f_p^d(1) = f_p^d(a \cdot a^{-1}) = f_p^d(a) \cdot f_p^d(a^{-1}) = a \cdot f_p^d(a^{-1}), \quad \text{proto} \quad f_p^d(a^{-1}) = a^{-1}$$

a $a^{-1} \in U_d$.