Grupa automorfismů rozšíření těles

Definice. Automorfismem tělesa K rozumíme libovolný izomorfismus okruhů $\sigma : K \to K$. Množinu všech automorfismů tělesa K značíme $\mathrm{Aut}(K)$.

Věta 1. *Pro libovolné těleso K je $(\mathrm{Aut}(K), \circ)$ grupa.*

Definice. Nechť $F \subseteq K$ je rozšíření těles. Automorfismem tohoto rozšíření rozumíme libovolný automorfismus σ tělesa K splňující $\sigma(a) = a$ pro každé $a \in F$. Množinu všech automorfismů rozšíření $F \subseteq K$ značíme $\mathrm{Aut}(K/F)$.

Věta 2. *Pro libovolné rozšíření těles $F \subseteq K$ je $\mathrm{Aut}(K/F)$ podgrupa grupy $\mathrm{Aut}(K)$.*

Věta 3. *Nechť $F \subseteq K$ je rozšíření těles, $\alpha \in K$ prvek algebraický nad F, $g(x) \in F[x]$ je libovolný polynom mající kořen α. Pak pro každý automorfismus $\sigma \in \mathrm{Aut}(K/F)$ je $\sigma(\alpha)$ kořen polynomu $g(x)$.*

Důkaz. Protože pro libovolné $a \in F$ platí $\sigma(a) = a$ a $g(x) \in F[x]$, pro každé $\beta \in K$ platí $\sigma(g(\beta)) = g(\sigma(\beta))$. Odtud $\sigma(g(\alpha)) = 0$.

Poznámka. Libovolný $\sigma \in \mathrm{Aut}(K/F)$ tedy permutuje množinu kořenů polynomu $g(x)$ ležících v K. Předchozí věta platí i pro minimální polynom $f(x) \in F[x]$ prvku $\alpha \in K$ nad F.

Fixní těleso podgrupy grupy automorfismů

Věta 4. *Pro libovolná podtělesa F_1, F_2 tělesa K platí*

$$F_1 \subseteq F_2 \implies \mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1).$$

Věta 5. *Nechť K je těleso, $H \leq \mathrm{Aut}(K)$ libovolná podgrupa grupy automorfismů. Pak $\mathrm{Fix}(H) = \{\alpha \in K; \forall \sigma \in H : \sigma(\alpha) = \alpha\}$ je podtěleso tělesa K.*

Definice. Podtěleso $\mathrm{Fix}(H)$ z předchozí věty se nazývá fixní těleso grupy automorfismů H.

Věta 6. *Pro libovolné podgrupy H_1, H_2 grupy $\mathrm{Aut}(K)$ automorfismů tělesa K platí*

$$H_1 \leq H_2 \implies \mathrm{Fix}(H_2) \subseteq \mathrm{Fix}(H_1).$$

Příklad

Víme, že pro libovolné konečné těleso K mající p^m prvků, kde p je prvočíslo, je $\mathrm{Aut}(K)$ cyklická grupa řádu m generovaná Frobeniovým automorfismem $\varphi : K \to K$, který je definován předpisem $\varphi(a) = a^p$ pro každé $a \in K$. Libovolné podtěleso F tělesa K má p^d prvků pro jisté $d \mid m$, a platí $\mathrm{Aut}(K/F) = \langle \varphi^d \rangle$.

Naopak libovolná podgrupa grupy $\mathrm{Aut}(K) = \langle \varphi \rangle$ je tvaru $\langle \varphi^d \rangle$ pro jisté $d \mid m$ a $\mathrm{Fix}(\langle \varphi^d \rangle)$ je jediné podtěleso tělesa F mající p^d prvků.

Nechť $\mathcal{H}$ je množina všech podgrup grupy $\mathrm{Aut}(K)$ a $\mathcal{P}$ je množina všech podtěles tělesa K.

Pro každé $F \in \mathcal{P}$ je $\mathrm{Fix}(\mathrm{Aut}(K/F)) = F$, pro každé $H \in \mathcal{H}$ $\mathrm{Aut}(K/\mathrm{Fix}(H)) = H$, tedy předpisy $F \mapsto \mathrm{Aut}(K/F)$, $H \mapsto \mathrm{Fix}(H)$ zadávají navzájem inverzní bijekce.

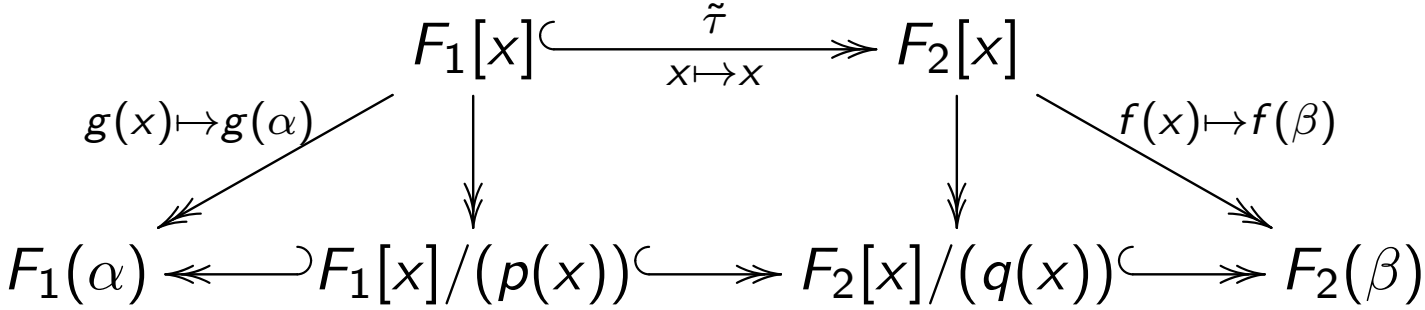
Z vět 4 a 6 plyne, že svaz $(\mathcal{P}, \subseteq)$ je izomorfní se svazem $(\mathcal{H}, \supseteq)$, tj. duálním svazem ke svazu $(\mathcal{H}, \subseteq)$.

V dalším textu budeme studovat, kdy máme takový vztah mezi podtělesy daného tělesa a podgrupami jeho grupy automorfismů.

Věta o rozšíření izomorfismu těles

Věta 7. *Nechť $\tau : F_1 \to F_2$ je izomorfismus těles, nechť je $\tilde{\tau} : F_1[x] \to F_2[x]$ indukovaný izomorfismus okruhů polynomů (pro libovolný polynom $g(x) \in F_1[x]$ je $\tilde{\tau}(g(x)) \in F_2[x]$ polynom získaný z polynomu $g(x)$ aplikací τ na jeho koeficienty). Nechť $p(x) \in F_1[x]$ je normovaný polynom, který je ireducibilní nad F_1. Pak $q(x) = \tilde{\tau}(p(x)) \in F_2[x]$ je normovaný polynom ireducibilní nad F_2. Nechť α je kořen polynomu $p(x)$ v nějakém rozšíření K_1 tělesa F_1 a β je kořen polynomu $q(x)$ v nějakém rozšíření K_2 tělesa F_2. Pak existuje, a to jediný, izomorfismus $\sigma : F_1(\alpha) \to F_2(\beta)$ splňující $\sigma(a) = \tau(a)$ pro každé $a \in F_1$ a současně $\sigma(\alpha) = \beta$. Navíc $[F_1(\alpha) : F_1] = [F_2(\beta) : F_2]$.*

Důkaz. Platí $F_1(\alpha) \cong F_1[x]/(p(x))$, $F_2(\beta) \cong F_2[x]/(q(x))$, a tedy



Definice. Polynom $f(x) \in F[x]$ nad tělesem F se nazývá separabilní, jestliže nemá žádný násobný kořen, tj. jestliže je nesoudělný se svou derivací $f'(x)$.

Věta 8. *Nechť $\tau : F_1 \to F_2$ je izomorfismus těles, nechť je $\tilde{\tau} : F_1[x] \to F_2[x]$ indukovaný izomorfismus okruhů polynomů (pro libovolný polynom $f(x) \in F_1[x]$ je $\tilde{\tau}(f(x)) \in F_2[x]$ polynom získaný z polynomu $f(x)$ aplikací τ na jeho koeficienty). Nechť $f(x) \in F_1[x]$ je normovaný polynom. Označme $g(x) = \tilde{\tau}(f(x))$. Nechť E_1 je rozkladové těleso polynomu $f(x)$ nad F_1 a E_2 je rozkladové těleso polynomu $g(x)$ nad F_2.*
Pak existuje alespoň jeden izomorfismus $\sigma : E_1 \to E_2$ splňující $\sigma(a) = \tau(a)$ pro každé $a \in F_1$. Počet takových izomorfismů σ je nejvýše roven stupni $[E_1 : F_1] = [E_2 : F_2]$. Jestliže polynom $f(x)$ je separabilní (tj. nemá žádný násobný kořen), je těchto automorfismů σ právě $[E_1 : F_1]$.

Důsledek. *Nechť E je rozkladové těleso polynomu $f(x) \in F[x]$ nad tělesem F. Pak $|\mathrm{Aut}(E/F)| \leq [E : F]$. Je-li navíc polynom $f(x)$ separabilní, platí $|\mathrm{Aut}(E/F)| = [E : F]$.*

Důkaz věty 8. Nechť $f(x) = f_1(x) \cdot f_2(x) \cdots f_t(x)$ je rozklad polynomu $f(x)$ na normované ireducibilní polynomy nad F_1, označme $g_i(x) = \tilde{\tau}(f_i(x))$ pro každé i. Pak $g(x) = g_1(x) \cdot g_2(x) \cdots g_t(x)$ je rozklad polynomu $g(x)$ na normované ireducibilní polynomy nad F_2, neboť $\tilde{\tau}$ je izomorfismus.

Důkaz provedeme indukcí vůči $[E_1 : F_1]$. V případě $[E_1 : F_1] = 1$ věta zřejmě platí; předpokládejme, že $[E_1 : F_1] > 1$ a že pro rozšíření menšího stupně byla už věta dokázána. Z předpokladu plyne, že nejsou všechny polynomy $f_i(x)$ lineární, předpokládejme, že $\mathrm{st}(f_1(x)) > 1$. Zvolme kořen $\alpha \in E_1$ polynomu $f_1(x)$. Podle věty 7 pro každý kořen $\beta \in E_2$ polynomu $g_1(x)$ existuje jediný izomorfismus $\mu : F_1(\alpha) \to F_2(\beta)$ takový, že zúžení $\mu|_{F_1} = \tau$ a platí $\mu(\alpha) = \beta$, přitom $[F_2(\beta) : F_2] = [F_1(\alpha) : F_1] = \mathrm{st}(f_1(x)) > 1$. Zřejmě $[E_1 : F_1(\alpha)] < [E_1 : F_1]$.

Užitím indukčního předpokladu pro izomorfismus μ a polynom $f(x)$ dostáváme izomorfismus $\sigma : E_1 \to E_2$ s vlastností $\sigma|_{F_1} = \tau$. Je-li polynom $f(x)$ separabilní, má polynom $g_1(x)$ v E_2 právě $\mathrm{st}(f_1(x))$ kořenů, odtud tvrzení o počtu takových izomorfismů σ.

Galoisovo rozšíření

Definice. Nechť $F \subseteq K$ je konečné rozšíření těles. Řekneme, že toto rozšíření je Galoisovo, jestliže $|\mathrm{Aut}(K/F)| = [K : F]$.
V takovém případě nazýváme grupu $\mathrm{Aut}(K/F)$ Galoisovou grupou tohoto rozšíření a užíváme pro ni označení $\mathrm{Gal}(K/F)$.

Věta 9. Nechť $f(x) \in F[x]$ je separabilní polynom nad tělesem F, nechť E je rozkladové těleso polynomu $f(x) \in F[x]$ nad tělesem F. Pak $F \subseteq E$ je Galoisovo rozšíření.

Příklad. Pro libovolné prvočíslo p a libovolné $m \in \mathbb{N}$ je těleso K mající p^m prvků rozkladové těleso separabilního polynomu $x^{p^m} - x$ nad tělesem $\mathbb{Z}_p$. Proto $\mathbb{Z}_p \subseteq K$ je Galoisovo rozšíření. (To jsme ovšem věděli už dříve, neboť pro každý prvek $\sigma \in \mathrm{Aut}(K)$ a každé $a \in \mathbb{Z}_p$ platí $\sigma(a) = a$, a tedy $\mathrm{Aut}(K/\mathbb{Z}_p) = \mathrm{Aut}(K) = \langle\varphi\rangle$, kde φ je Frobeniův automorfismus, odkud $|\mathrm{Aut}(K/\mathbb{Z}_p)| = m = [K : \mathbb{Z}_p]$.)

Definice. Nechť $f(x) \in F[x]$ je separabilní polynom nad tělesem F, nechť E je rozkladové těleso polynomu $f(x) \in F[x]$ nad tělesem F. Galoisovou grupou polynomu $f(x)$ nad tělesem F rozumíme $\mathrm{Gal}(E/F)$.

První informace o Galoisově grupě polynomu

Věta 10. *Nechť $K = F(\alpha_1, \ldots, \alpha_n)$ je konečné rozšíření tělesa F. Jsou-li $\sigma, \tau \in \mathrm{Aut}(K/F)$ takové, že $\sigma(\alpha_1) = \tau(\alpha_1)$, $\ldots$, $\sigma(\alpha_n) = \tau(\alpha_n)$, pak $\sigma = \tau$.*

Důkaz. $L = \mathrm{Fix}(\langle \sigma^{-1} \circ \tau \rangle)$ je podtěleso tělesa K obsahující všechny prvky tělesa F a také $\alpha_1, \ldots, \alpha_n$. Proto $L = K$ a $\sigma^{-1} \circ \tau$ je identita na K, tj. $\sigma = \tau$.

Příklad. Nechť $f(x) \in F[x]$ je normovaný separabilní polynom nad tělesem F stupně r, nechť E je rozkladové těleso polynomu $f(x) \in F[x]$ nad tělesem F. Pak $f(x)$ se nad E rozkládá na součin lineárních činitelů $f(x) = (x - \alpha_1) \ldots (x - \alpha_r)$. Pak platí $E = F(\alpha_1, \ldots, \alpha_r)$ a každý $\sigma \in \mathrm{Gal}(E/F)$ permutuje množinu kořenů $\{\alpha_1, \ldots, \alpha_r\}$, přičemž touto permutací je σ jednoznačně určen. Je tedy (při zvoleném očíslování kořenů polynomu f) možné $\mathrm{Gal}(E/F)$ ztotožnit s jistou podgrupou grupy permutací $\mathbb{S}_r$. Uvidíme, že to nemusí být celá grupa $\mathbb{S}_r$, protože některé permutace kořenů nemusí být dány žádným automorfismem $\sigma \in \mathrm{Gal}(E/F)$ (to nastane právě tehdy, když $[E : F] < r!$).

Příklady

Příklad. Rozšíření $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ není Galoisovo, neboť minimální polynom čísla $\sqrt[3]{2}$ nad $\mathbb{Q}$ je $x^3 - 2$, tedy $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Těleso $\mathbb{Q}(\sqrt[3]{2})$ obsahuje jen kořen $\sqrt[3]{2}$ polynomu $x^3 - 2$, neboť zbylé dva kořeny nejsou reálné, a tedy pro libovolný $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ podle věty 3 platí $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Proto podle věty 10 je $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ triviální grupa (obsahuje jen identitu).

Příklad. Označme E rozkladové těleso polynomu $x^3 - 2$ nad tělesem $\mathbb{Q}$. Platí $x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2})$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, a tedy $E = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Protože $\omega^2 + \omega + 1 = 0$, platí $[E : \mathbb{Q}(\sqrt[3]{2})] \leq 2$. Protože $\omega \notin \mathbb{Q}(\sqrt[3]{2})$, je $[E : \mathbb{Q}(\sqrt[3]{2})] > 1$, a tedy $[E : \mathbb{Q}(\sqrt[3]{2})] = 2$, odkud $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$. Proto podle věty 9 $|\mathrm{Gal}(E/\mathbb{Q})| = 6$. Už víme, že $\mathrm{Gal}(E/\mathbb{Q})$ je izomorfní s podgrupou grupy $\mathbb{S}_3$, a proto $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{S}_3$.

Lineární nezávislost různých vnoření tělesa

Poznámka. Pro libovolné těleso L a libovolnou množinu A tvoří množina všech zobrazení množiny A do tělesa L vektorový prostor L^A nad tělesem L: součtem dvou zobrazení $f, g : A \to L$ je zobrazení $(f + g) : A \to L$ určené předpisem $(f + g)(a) = f(a) + g(a)$ a pro libovolné $r \in L$ je zobrazení $(rf) : A \to L$ určené předpisem $(rf)(a) = r \cdot f(a)$.
Jsou-li K, L tělesa, je libovolné vnoření $K \to L$ (tj. homomorfismus okruhů) prvkem vektorového prostoru L^K, můžeme se tedy ptát, zda mohou být různá vnoření $K \to L$ lineárně závislá nad L.

Věta 11. *Nechť $\sigma_1, \ldots, \sigma_n$ jsou různá vnoření tělesa K do tělesa L. Pak jsou $\sigma_1, \ldots, \sigma_n$ lineárně nezávislé nad L.*

Důsledek. *Různé prvky grupy $\mathrm{Aut}(K)$ jsou lineárně nezávislé nad K (i nad každým tělesem L obsahujícím těleso K jako své podtěleso).*

Důkaz věty 11. Postupujme sporem, předpokládejme, že $\sigma_1, \ldots, \sigma_n$ jsou lineárně závislé nad L. Ze všech jejich lineárních závislostí vyberme takovou, která má co nejméně nenulových koeficientů. Nechť je to (po případném přeindexování) závislost $a_1\sigma_1 + \cdots + a_m\sigma_m = 0$, kde všechny koeficienty $a_1, \ldots, a_m \in L$ jsou nenulové. Pro každé $\alpha \in K$ tedy $a_1\sigma_1(\alpha) + \cdots + a_m\sigma_m(\alpha) = 0$.

Zřejmě $m > 1$, protože $a_1\sigma_1(1) = a_1 \neq 0$. Proto $\sigma_1 \neq \sigma_m$, a tedy existuje $\beta \in K$ splňující $\sigma_1(\beta) \neq \sigma_m(\beta)$. Pro každé $\alpha \in K$ je $\alpha\beta \in K$, a tedy $a_1\sigma_1(\alpha\beta) + \cdots + a_m\sigma_m(\alpha\beta) = 0$.

Odečtením $\sigma_m(\beta)$-násobku předchozí rovnosti od této rovnosti dostáváme

$$a_1 \cdot (\sigma_1(\beta) - \sigma_m(\beta)) \cdot \sigma_1(\alpha) + \cdots + a_m \cdot (\sigma_m(\beta) - \sigma_m(\beta)) \cdot \sigma_m(\alpha) = 0.$$

Protože $a_1 \cdot (\sigma_1(\beta) - \sigma_m(\beta)) \neq 0$, jde o lineární závislost s méně než m nenulovými koeficienty, spor.

Fixní těleso konečné podgrupy grupy automorfismů

Věta 12. Nechť K je těleso, $G \leq \mathrm{Aut}(K)$ konečná podgrupa grupy automorfismů tělesa K, nechť $F = \mathrm{Fix}(G)$ je odpovídající fixní těleso. Pak platí $[K : F] = |G|$.

Důkaz. Označme $n = |G|$.
Sporem dokažme, že neplatí ani $[K : F] < n$ ani $[K : F] > n$.
Nechť $G = \{\sigma_1, \ldots, \sigma_n\}$, kde σ_1 je identita.

Předpokládejme $[K : F] < n$ a zvolme bázi $\omega_1, \ldots, \omega_m$ tělesa K nad F, tedy $m = [K : F]$. Pak systém m rovnic o n neznámých

$$\sum_{i=1}^{n} \sigma_i(\omega_j) x_i = 0, \qquad j = 1, \ldots, m,$$

má nenulové řešení $\beta_1, \ldots, \beta_n \in K$. Libovolné $\alpha \in K$ je tvaru $\alpha = \sum_{j=1}^{m} a_j \omega_j$ pro vhodné $a_1, \ldots, a_m \in F$. Platí

$$\sum_{i=1}^{n} \beta_i \sigma_i(\alpha) = \sum_{i=1}^{n} \beta_i \sum_{j=1}^{m} \sigma_i(a_j \omega_j) =$$
$$= \sum_{i=1}^{n} \beta_i \sum_{j=1}^{m} a_j \sigma_i(\omega_j) = \sum_{j=1}^{m} a_j \sum_{i=1}^{n} \beta_i \sigma_i(\omega_j) = 0,$$

protože $\sigma_i(a_j) = a_j$. Odvodili jsme

$$\beta_1 \sigma_1 + \cdots + \beta_n \sigma_n = 0,$$

což je spor s větou 11.

Předpokládejme $[K : F] > n$ a zvolme prvky $\alpha_1, \ldots, \alpha_{n+1} \in K$, které jsou lineárně nezávislé nad F. Pak systém n rovnic o $n+1$ neznámých

$$\sum_{i=1}^{n+1} \sigma_j(\alpha_i) x_i = 0, \qquad j = 1, \ldots, n,$$

má nenulové řešení. Mezi všemi nenulovými řešeními vyberme řešení, které má co nejméně nenulových hodnot. Po případném přeindexování prvků α_i tedy lze předpokládat, že řešení $\beta_1, \ldots, \beta_{n+1} \in K$ této soustavy splňuje, že $\beta_i \neq 0$ pro $i = 1, \ldots, r$, přičemž $\beta_1 = 1$, $\beta_{r+1} = \cdots = \beta_{n+1} = 0$, a že neexistuje nenulové řešení této soustavy mající méně než r nenulových hodnot. Protože σ_1 je identita a $\alpha_1, \ldots, \alpha_{n+1}$ jsou lineárně nezávislé nad F, nemohou všechny $\beta_i \in F$, lze tedy předpokládat $\beta_r \notin F$, odkud $r > 1$. Z definice F plyne existence $\tau \in G$ takového, že $\tau(\beta_r) \neq \beta_r$ (toto $\tau = \sigma_{i_0}$ pro jisté i_0). Aplikací τ na rovnosti

$$\sigma_j(\alpha_1) + \sum_{i=2}^{r} \sigma_j(\alpha_i)\beta_i = 0, \qquad j = 1, \ldots, n,$$

dostáváme

$$(\tau \circ \sigma_j)(\alpha_1) + \sum_{i=2}^{r} (\tau \circ \sigma_j)(\alpha_i)\tau(\beta_i) = 0, \qquad j = 1, \ldots, n.$$

G je grupa, a tedy $\{\tau \circ \sigma_j; j = 1, \ldots, n\} = G = \{\sigma_1, \ldots, \sigma_n\}$.

Odečtením získaných rovností

$$\sigma_j(\alpha_1) + \sum_{i=2}^{r} \sigma_j(\alpha_i)\beta_i = 0, \qquad j = 1, \ldots, n,$$
$$\sigma_j(\alpha_1) + \sum_{i=2}^{r} \sigma_j(\alpha_i)\tau(\beta_i) = 0, \qquad j = 1, \ldots, n,$$

dostáváme spor, protože naše soustava má nenulové řešení $\beta_i - \tau(\beta_i)$ mající méně než r nenulových hodnot:

$$\sum_{i=2}^{r} \sigma_j(\alpha_i)(\beta_i - \tau(\beta_i)) = 0, \qquad j = 1, \ldots, n.$$

Důsledek. *Nechť $F \subseteq K$ je konečné rozšíření těles. Pak $|\operatorname{Aut}(K/F)| \leq [K : F]$.*

Důkaz. Z vět 3 a 10 plyne, že $\operatorname{Aut}(K/F)$ je konečná. Nechť $F_1 = \operatorname{Fix}(\operatorname{Aut}(K/F))$. Pak $F \subseteq F_1 \subseteq K$. Podle věty 12 je $[K : F_1] = |\operatorname{Aut}(K/F)|$. Proto $[K : F] = |\operatorname{Aut}(K/F)| \cdot [F_1 : F]$.

Důsledek. *Nechť K je těleso, $G \leq \operatorname{Aut}(K)$ konečná podgrupa grupy automorfismů tělesa K, nechť $F = \operatorname{Fix}(G)$ je odpovídající fixní těleso. Pak každý automorfismus tělesa K ponechávající na místě všechny prvky tělesa F patří do G, tj. $\operatorname{Aut}(K/F) = G$, a tedy $F \subseteq K$ je Galoisovo rozšíření s Galoisovou grupou $\operatorname{Gal}(K/F) = G$.*

Důkaz. Jistě $G \leq \operatorname{Aut}(K/F)$, proto podle věty 12 a předchozího důsledku je $[K : F] = |G| \leq |\operatorname{Aut}(K/F)| \leq [K : F]$. Proto $|G| = |\operatorname{Aut}(K/F)|$, a tedy $G = \operatorname{Aut}(K/F)$.

Různé charakterizace Galoisova rozšíření

Definice. Nechť $F \subseteq K$ je algebraické rozšíření. Řekneme, že toto rozšíření je

- separabilní, jestliže pro libovolný $\alpha \in K$ platí, že minimální polynom $p(x)$ prvku α nad F je separabilní;
- normální, jestliže pro libovolný $\alpha \in K$ platí, že minimální polynom $p(x)$ prvku α nad F se rozkládá nad K na součin lineárních činitelů.

Věta 13. Nechť $F \subseteq K$ je konečné rozšíření. Pak následující podmínky jsou ekvivalentní:

1. *rozšíření $F \subseteq K$ je Galoisovo;*
2. *rozšíření $F \subseteq K$ je separabilní a normální;*
3. *K je rozkladové těleso vhodného normovaného separabilního polynomu $f(x) \in F[x]$ nad tělesem F;*
4. $F = \mathrm{Fix}(\mathrm{Aut}(K/F))$.

Důkaz. Označme $G = \mathrm{Aut}(K/F)$, $F_1 = \mathrm{Fix}(G)$. Z důkazu prvního důsledku věty 12 víme, že $[K : F] = |G| \cdot [F_1 : F]$, tedy (1) $\Longrightarrow$ (4). Z věty 9 plyne (3) $\Longrightarrow$ (1).

(4) $\Longrightarrow$ (2): Zvolme libovolné $\alpha \in K$ a označme $p(x)$ minimální polynom prvku α nad F. Nechť $M = \{\sigma(\alpha); \sigma \in G\}$, $f(x) = \prod_{\beta \in M}(x - \beta) \in K[x]$.
Polynom $f(x)$ má jen jednoduché kořeny a podle věty 3 každý z nich je kořenem polynomu $p(x)$, proto $f(x) \mid p(x)$.
Protože G je grupa, pro každé $\tau \in G$ je $\{\tau(\beta); \beta \in M\} = M$.
Protože až na znaménko jsou koeficienty polynomu $f(x)$ hodnoty elementárních symetrických polynomů v jeho kořenech, jsou fixovány τ, a tedy platí $f(x) \in F[x]$. Z vlastnosti minimálního polynomu plyne $p(x) \mid f(x)$. Protože jsou oba polynomy normované, platí $p(x) = f(x)$. Dokázali jsme (2).

(2) $\Longrightarrow$ (3): Nechť $K = F(\alpha_1, \ldots, \alpha_n)$, označme $p_i(x)$ minimální polynom prvku α_i nad F. Protože $p_i(x) \in F[x]$ jsou separabilní a rozkládají se nad K na součin lineárních činitelů, platí totéž i pro jejich nejmenší společný násobek $f(x) \in F[x]$. Rozkladové těleso polynomu $f(x)$ nad F je K.

Poznámka. V důkazu části (4) $\Longrightarrow$ (2) je popsána konstrukce minimálního polynomu pro prvky Galoisova rozšíření.

Kompositum těles

Poznámka. Víme, že množina všech podtěles tělesa K uspořádaná inkluzí je úplný svaz, ve kterém infimum libovolné neprázdné množiny podtěles je průnik těchto podtěles.

Definice. Nechť E_1 a E_2 jsou podtělesa tělesa K. Kompositum E_1E_2 těles E_1 a E_2 je definováno jako supremum $E_1 \vee E_2$ ve svazu všech podtěles telesa K. Kompositum E_1E_2 těles E_1 a E_2 je tedy to nejmenší podtěleso tělesa K obsahující obě tělesa E_1 a E_2, neboli podtěleso tělesa K generované sjednocením $E_1 \cup E_2$.

Poznámka. Nechť $F \subseteq K$ je libovolné konečné rozšíření těles. Označme $\mathcal{P}$ množinu všech mezitěles tohoto rozšíření, tj. těles E splňujících $F \subseteq E \subseteq K$. Pak $(\mathcal{P}, \subseteq)$ je svaz, v němž infima jsou průniky a suprema jsou kompositа těles.

Připomenutí příkladu s konečným tělesem K

Pro libovolné konečné těleso K mající p^n prvků, kde p je charakteristika tělesa K, víme, že K je Galoisovo rozšíření tělesa $\mathbb{Z}_p$ a že $\mathrm{Gal}(K/\mathbb{Z}_p) = \langle\varphi\rangle$, kde φ je Frobeniův automorfismus.

Označme $\mathcal{P}$ množinu všech mezitěles rozšíření $\mathbb{Z}_p \subseteq K$ a $\mathcal{H}$ množinu všech podgrup grupy $\mathrm{Gal}(K/\mathbb{Z}_p)$. Víme, že zobrazení

$$\begin{array}{ccc} \mathcal{P} \to \mathcal{H} & & \mathcal{H} \to \mathcal{P} \\ E \mapsto \mathrm{Aut}(K/E) & & H \mapsto \mathrm{Fix}(H) \end{array}$$

jsou navzájem inverzní bijekce, které jsou antiizomorfismus svazů $(\mathcal{P}, \subseteq)$ a $(\mathcal{H}, \subseteq)$ (tj. izomorfismus jednoho svazu s duálním svazem k druhému svazu). To znamená, že jsou-li $H_1, H_2 \in \mathcal{H}$ a označíme-li $E_1 = \mathrm{Fix}(H_1)$, $E_2 = \mathrm{Fix}(H_2)$, pak kompositum $E_1E_2 = \mathrm{Fix}(H_1 \cap H_2)$ a průnik $E_1 \cap E_2 = \mathrm{Fix}(\langle H_1 \cup H_2\rangle)$.

Tento fakt platí pro každé Galoisovo rozšíření, jak se dozvíme z následující věty.

Hlavní věta Galoisovy teorie

Věta 14. *Nechť $F \subseteq K$ je libovolné Galoisovo rozšíření těles. Označme $\mathcal{P}$ množinu všech mezitěles rozšíření $F \subseteq K$ a $\mathcal{H}$ množinu všech podgrup grupy $G = \mathrm{Gal}(K/F)$. Pak zobrazení*

$$\begin{aligned} \mathcal{A} : \mathcal{P} &\to \mathcal{H} & \qquad \mathcal{F} : \mathcal{H} &\to \mathcal{P} \\ E &\mapsto \mathrm{Aut}(K/E) & \qquad H &\mapsto \mathrm{Fix}(H) \end{aligned}$$

jsou navzájem inverzní bijekce, které jsou antiizomorfismus svazů $(\mathcal{P}, \subseteq)$ a $(\mathcal{H}, \subseteq)$. Pro libovolné $H \in \mathcal{H}$ označme $E = \mathrm{Fix}(H)$. Pak platí

1. $[K : E] = |H|$, $[E : F] = |G/H|$ *(index podgrupy H v grupě G),*
2. $E \subseteq K$ *je vždy Galoisovo,* $\mathrm{Gal}(K/E) = H$,
3. $F \subseteq E$ *je Galoisovo, právě když H je normální podgrupa grupy G, v tom případě* $\mathrm{Gal}(E/F) \cong G/H$ *(faktorgrupa grupy G podle podgrupy H).*
4. *Pro $H_1, H_2 \in \mathcal{H}$ označme $E_1 = \mathrm{Fix}(H_1)$, $E_2 = \mathrm{Fix}(H_2)$, pak kompositum $E_1E_2 = \mathrm{Fix}(H_1 \cap H_2)$ a průnik $E_1 \cap E_2 = \mathrm{Fix}(\langle H_1 \cup H_2 \rangle)$.*

Důkaz. Podle věty 13, podmínka (4), platí $\mathcal{F} \circ \mathcal{A} = \mathrm{id}_{\mathcal{P}}$.
Z druhého důsledku věty 12 plyne, že $\mathcal{F}$ je injektivní, proto jsou $\mathcal{F}$ a $\mathcal{A}$ navzájem inverzní bijekce.
Z vět 4 a 6 plyne, že to jsou antiizomorfismy uspořádaných množin, a tedy i svazů. Odtud plyne (4).

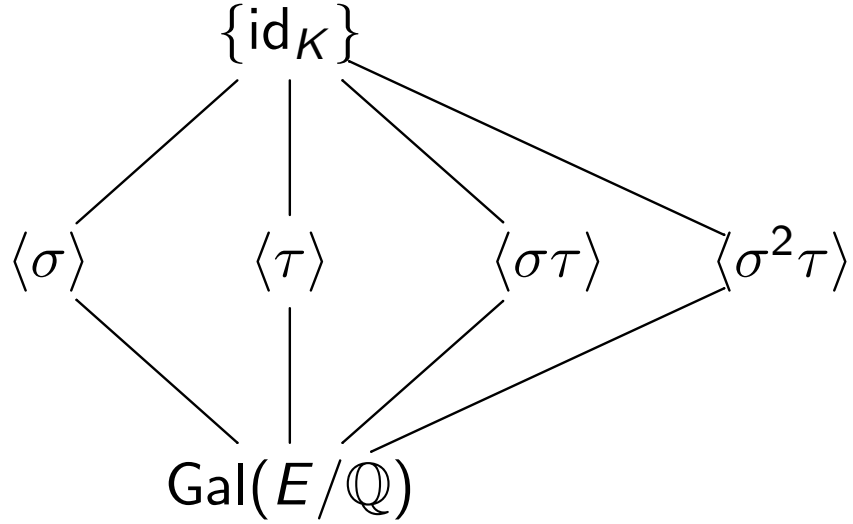
Pro libovolné $H \in \mathcal{H}$ podle druhého důsledku věty 12 pro těleso $E = \mathrm{Fix}(H)$ platí, že $E \subseteq K$ je Galoisovo rozšíření, přičemž Galoisovou grupou je H. Odtud plyne (1) a (2).

Podle věty 13, podmínka (2), je rozšíření $F \subseteq K$ separabilní a normální. Proto je rozšíření $F \subseteq E$ separabilní, avšak normální být nemusí. Pro libovolné $\alpha \in K$ je $\{\sigma(\alpha); \alpha \in G\}$ množina všech kořenů minimálního polynomu prvku α nad K. Proto je $F \subseteq E$ normální, právě když pro každé $\sigma \in G$ je $\sigma(E) \subseteq E$, tj. $\sigma(E) = E$. To nastane, právě když platí $\mathrm{Gal}(K/\sigma(E)) = \mathrm{Gal}(K/E) = H$. Ovšem $\tau \in G$ ponechá na místě všechny prvky tělesa $\sigma(E)$, právě když $\sigma^{-1} \circ \tau \circ \sigma$ ponechá na místě všechny prvky tělesa E, tj. $\sigma^{-1} \circ \tau \circ \sigma \in H$. Odtud plyne, že rozšíření $F \subseteq E$ je normální, právě když H je normální podgrupa grupy G.

Předpokládejme dále, že H je normální podgrupa grupy G. Pro libovolné $\sigma \in G$ je restrikce $\sigma|_E$ automorfismus tělesa E, a tedy prvek $\mathrm{Gal}(E/F)$. Proto $\sigma \mapsto \sigma|_E$ je homomorfismus grup $G \to \mathrm{Gal}(E/F)$, jehož jádro je H a který je podle věty 8 surjektivní. Proto $G/H \cong \mathrm{Gal}(E/F)$. Dokázali jsme (3).

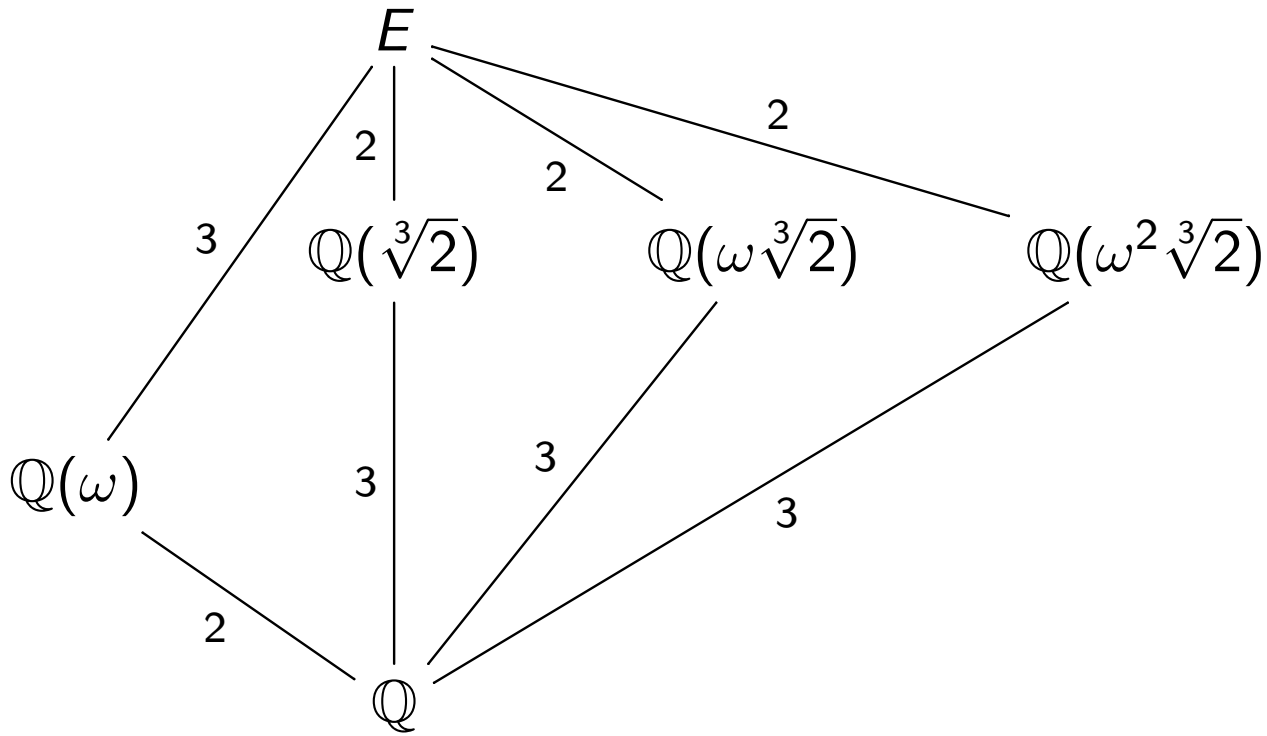
Pokračování dříve uvedeného příkladu

Příklad. Označme E rozkladové těleso polynomu $x^3 - 2$ nad tělesem $\mathbb{Q}$. Platí $x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2})$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, a tedy $E = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Pro každé $\rho \in \mathrm{Gal}(E/\mathbb{Q})$ platí $\rho(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$, $\rho(\omega) \in \{\omega, \omega^2\}$. Víme, že $[E : \mathbb{Q}] = 6$, proto každá z šesti možností je dána nějakým automorfismem. Nechť $\sigma, \tau \in \mathrm{Gal}(E/\mathbb{Q})$ jsou určeny podmínkami $\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$, $\sigma(\omega) = \omega$ a $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, $\tau(\omega) = \omega^2$. Pak $\sigma^3 = \tau^2 = \mathrm{id}_K$, $\mathrm{Gal}(E/\mathbb{Q}) = \langle\sigma, \tau\rangle \cong \mathbb{S}_3$. Duální svaz k svazu podgrup grupy $\mathrm{Gal}(E/\mathbb{Q})$ a odpovídající fixní tělesa:



$\mathrm{Fix}(\{\mathrm{id}_K\}) = E,$
$\mathrm{Fix}(\langle\sigma\rangle) = \mathbb{Q}(\omega),$
$\mathrm{Fix}(\langle\tau\rangle) = \mathbb{Q}(\sqrt[3]{2}),$
$\mathrm{Fix}(\langle\sigma\tau\rangle) = \mathbb{Q}(\omega^2\sqrt[3]{2}),$
$\mathrm{Fix}(\langle\sigma^2\tau\rangle) = \mathbb{Q}(\omega\sqrt[3]{2}),$
$\mathrm{Fix}(\langle\sigma, \tau\rangle) = \mathbb{Q}.$

Svaz všech podtěles tělesa E s vyznačenými stupni je tedy



Zatímco pro konečnou grupu $\mathrm{Gal}(E/\mathbb{Q})$ lze nalézt všechny podgrupy procházením všech možností, pro nalezení všech podtěles tělesa E jsme potřebovali hlavní větu Galoisovy teorie.