

Grupa automorfismů rozšíření těles

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

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

Definice. Necht' $F \subseteq K$ 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 $\text{Aut}(K/F)$.

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

Věta 3. Necht' $F \subseteq K$ 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 $\sigma \in \text{Aut}(K/F)$ je $\sigma(\alpha)$ kořen polynomu $g(x)$.

Poznámka. Libovolný $\sigma \in \text{Aut}(K/F)$ 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

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

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

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

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

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

Příklad

Víme, že pro libovolné konečné těleso K mající p^m prvků, kde p je prvočíslo, je $\text{Aut}(K)$ cyklická grupa řádu m generovaná Frobeniovým automorfismem $\varphi : K \rightarrow K$, 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 $\text{Aut}(K/F) = \langle \varphi^d \rangle$.

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

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

Pro každé $F \in \mathcal{P}$ je $\text{Fix}(\text{Aut}(K/F)) = F$, pro každé $H \in \mathcal{H}$ $\text{Aut}(K/\text{Fix}(H)) = H$, tedy předpisy $F \mapsto \text{Aut}(K/F)$, $H \mapsto \text{Fix}(H)$ 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 $\tau : F_1 \rightarrow F_2$ je izomorfismus těles, nechť je $\tilde{\tau} : F_1[x] \rightarrow F_2[x]$ 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 $\sigma : F_1(\alpha) \rightarrow F_2(\beta)$ 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

$$\begin{array}{ccccc} F_1[x] & \xrightarrow[\substack{\tilde{\tau} \\ x \mapsto x}]{} & F_2[x] & & \\ \swarrow \substack{g(x) \mapsto g(\alpha)} & \downarrow & \downarrow & \searrow \substack{f(x) \mapsto f(\beta)} & \\ F_1(\alpha) & \longleftarrow F_1[x]/(p(x)) & \longrightarrow F_2[x]/(q(x)) & \longrightarrow & F_2(\beta) \end{array}$$

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. Necht' $\tau : F_1 \rightarrow F_2$ je izomorfismus těles, necht' je $\tilde{\tau} : F_1[x] \rightarrow F_2[x]$ 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). Necht' $f(x) \in F_1[x]$ je normovaný polynom. Označme $g(x) = \tilde{\tau}(f(x))$. Necht' 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 $\sigma : E_1 \rightarrow E_2$ 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. Necht' E je rozkladové těleso polynomu $f(x) \in F[x]$ nad tělesem F . Pak $|\text{Aut}(E/F)| \leq [E : F]$. Je-li navíc polynom $f(x)$ separabilní, platí $|\text{Aut}(E/F)| = [E : F]$.

Galoisovo rozšíření

Definice. Necht' $F \subseteq K$ je konečné rozšíření těles. Řekneme, že toto rozšíření je Galoisovo, jestliže $|\text{Aut}(K/F)| = [K : F]$.

V takovém případě nazýváme grupu $\text{Aut}(K/F)$ Galoisovou grupou tohoto rozšíření a užíváme pro ni označení $\text{Gal}(K/F)$.

Věta 9. Necht' $f(x) \in F[x]$ je separabilní polynom nad tělesem F , necht' 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 $\sigma \in \text{Aut}(K)$ a každé $a \in \mathbb{Z}_p$ platí $\sigma(a) = a$, a tedy $\text{Aut}(K/\mathbb{Z}_p) = \text{Aut}(K) = \langle \varphi \rangle$, kde φ je Frobeniův automorfismus, odkud $|\text{Aut}(K/\mathbb{Z}_p)| = m = [K : \mathbb{Z}_p]$.)

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

První informace o Galoisově grupě polynomu

Věta 10. Necht' $K = F(\alpha_1, \dots, \alpha_n)$ je konečné rozšíření tělesa F . Jsou-li $\sigma, \tau \in \text{Aut}(K/F)$ takové, že $\sigma(\alpha_1) = \tau(\alpha_1), \dots, \sigma(\alpha_n) = \tau(\alpha_n)$, pak $\sigma = \tau$.

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

Příklad. Necht' $f(x) \in F[x]$ je normovaný separabilní polynom nad tělesem F stupně r , necht' E je rozkladové těleso polynomu $f(x) \in F[x]$ nad tělesem F . Pak $f(x)$ se nad E rozkládá na součin lineárních činitelů $f(x) = (x - \alpha_1) \dots (x - \alpha_r)$. Pak platí $E = F(\alpha_1, \dots, \alpha_r)$ a každý $\sigma \in \text{Gal}(E/F)$ permutuje množinu kořenů $\{\alpha_1, \dots, \alpha_r\}$, přičemž touto permutací je σ jednoznačně určen. Je tedy (při zvoleném očíslování kořenů polynomu f) možné $\text{Gal}(E/F)$ 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 $\sigma \in \text{Gal}(E/F)$ (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 $\sigma \in \text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ podle věty 3 platí $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Proto podle věty 10 je $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ 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 $|\text{Gal}(E/\mathbb{Q})| = 6$. Už víme, že $\text{Gal}(E/\mathbb{Q})$ je izomorfní s podgrupou grupy \mathbb{S}_3 , a proto $\text{Gal}(E/\mathbb{Q}) \cong \mathbb{S}_3$.

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 $f, g : A \rightarrow L$ je zobrazení $(f + g) : A \rightarrow L$ určené předpisem $(f + g)(a) = f(a) + g(a)$ a pro libovolné $r \in L$ je zobrazení $(rf) : A \rightarrow L$ určené předpisem $(rf)(a) = r \cdot f(a)$. Jsou-li K, L tělesa, je libovolné vnoření $K \rightarrow L$ (tj. homomorfismus okruhů) prvkem vektorového prostoru L^K , můžeme se tedy ptát, zda mohou být různá vnoření $K \rightarrow L$ lineárně závislá nad L .

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

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

Fixní těleso konečné podgrupy grupy automorfismů

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

Důsledek. Necht' $F \subseteq K$ je konečné rozšíření těles. Pak $|\text{Aut}(K/F)| \leq [K : F]$.

Důkaz. Necht' $F_1 = \text{Fix}(\text{Aut}(K/F))$. Pak $F \subseteq F_1 \subseteq K$. Podle věty 12 je $[K : F_1] = |\text{Aut}(K/F)|$. Proto $[K : F] = |\text{Aut}(K/F)| \cdot [F_1 : F]$.

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

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

Různé charakterizace Galoisova rozšíření

Definice. Necht' $F \subseteq K$ 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. Necht' $F \subseteq K$ 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. $F = \text{Fix}(\text{Aut}(K/F))$.

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. Necht' 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 tělesa 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. Necht' $F \subseteq K$ 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 komposita 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 $\text{Gal}(K/\mathbb{Z}_p) = \langle \varphi \rangle$, kde φ je Frobeniův automorfismus.

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

$$\begin{array}{ll} \mathcal{P} \rightarrow \mathcal{H} & \mathcal{H} \rightarrow \mathcal{P} \\ E \mapsto \text{Aut}(K/E) & H \mapsto \text{Fix}(H) \end{array}$$

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 $E_1 = \text{Fix}(H_1)$, $E_2 = \text{Fix}(H_2)$, pak kompositum $E_1 E_2 = \text{Fix}(H_1 \cap H_2)$ a průnik $E_1 \cap E_2 = \text{Fix}(\langle H_1 \cup H_2 \rangle)$.

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

Hlavní věta Galoisovy teorie

Věta 14. *Necht' $F \subseteq K$ je libovolné Galoisovo rozšíření těles.*

Označme \mathcal{P} množinu všech mezitěles rozšíření $F \subseteq K$ a

\mathcal{H} množinu všech podgrup grupy $\text{Gal}(K/F)$. Pak předpisy

$$\begin{array}{ll} \mathcal{P} \rightarrow \mathcal{H} & \mathcal{H} \rightarrow \mathcal{P} \\ E \mapsto \text{Aut}(K/E) & H \mapsto \text{Fix}(H) \end{array}$$

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

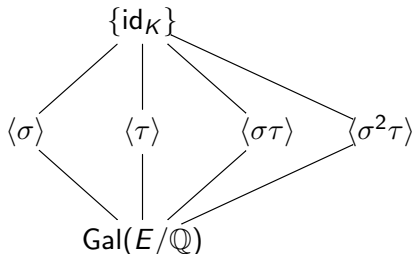
Pak platí

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

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 $\rho \in \text{Gal}(E/\mathbb{Q})$ 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 $\sigma, \tau \in \text{Gal}(E/\mathbb{Q})$ 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 $\sigma^3 = \tau^2 = \text{id}_K$, $\text{Gal}(E/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong S_3$. Duální svaz k svazu podgrup grupy $\text{Gal}(E/\mathbb{Q})$ a odpovídající fixní tělesa:



$$\text{Fix}(\{\text{id}_K\}) = E,$$

$$\text{Fix}(\langle \sigma \rangle) = \mathbb{Q}(\omega),$$

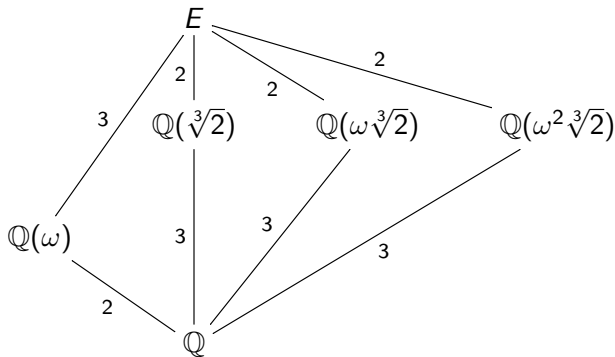
$$\text{Fix}(\langle \tau \rangle) = \mathbb{Q}(\sqrt[3]{2}),$$

$$\text{Fix}(\langle \sigma\tau \rangle) = \mathbb{Q}(\omega^2\sqrt[3]{2}),$$

$$\text{Fix}(\langle \sigma^2\tau \rangle) = \mathbb{Q}(\omega\sqrt[3]{2}),$$

$$\text{Fix}(\langle \sigma, \tau \rangle) = \mathbb{Q}.$$

Svaz všech podtělů tělesa E s vyznačenými stupni je tedy



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