# Úvod do komutativní algebry: cvičení 5

7. prosince 2023

**Ukážeme si:**

**1.** Urči, zda je Galoisovu grupu $T \supset \mathbb{Q}$ a všechna tělesa $U$, $T \supset U \supset \mathbb{Q}$, jestliže

a) $T = \mathbb{Q}(i, \sqrt{2})$,

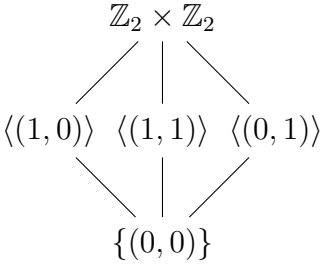
b) $T =$ rozkladové nadtěleso $x^3 - 2$ nad $\mathbb{Q}$.

*Řešení.*

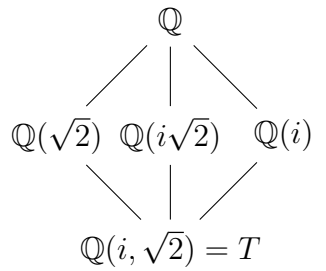
a) Zjevně máme $[T : \mathbb{Q}] = [T : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$, navíc jde o rozkladové nadtěleso polynomu $(x^2 - 2)(x^2 + 1)$, tedy je normální, separabilní (charakteristika 0) a konečného stupně, tedy Galoisovo. Hned tedy víme, že $\#\operatorname{Gal}(T/\mathbb{Q}) = 4$. Zároveň jakýkoliv $\mathbb{Q}$-automorfismus $\varphi \in \operatorname{Gal}(T/\mathbb{Q})$ má dvě možnosti kam poslat $\sqrt{2}$ a dvě kam poslat $i$. Mají-li skutečně vzniknout 4 automorfismy, musí každá kombinace těchto dvou možností dát validní automorfismus, tedy máme čtyři automorfismy tvaru

$$\begin{aligned} \sigma_{a,b} : T &\to T, \\ i &\mapsto (-1)^a i, \\ \sqrt{2} &\mapsto (-1)^b \sqrt{2} \end{aligned}$$

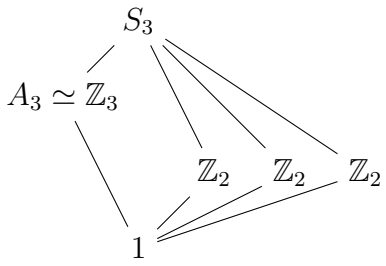
pro $a, b \in \mathbb{Z}_2$. Snadno nahlédneme, že skládání bude odpovídat sčítání dvojic $(a, b)$ v grupě $\mathbb{Z}_2 \times \mathbb{Z}_2$, tedy $\operatorname{Gal}(T/\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.
K určení podtěles prozkoumejme podgrupy $\mathbb{Z}_2 \times \mathbb{Z}_2$. Zjevně kromě triviálních $\mathbb{Z}_2 \times \mathbb{Z}_2$ a $\{(0,0)\}$ můžeme mít jen dvouprvkové podgrupy, přitom ale vše kromě $(0,0)$ má řád 2, takže každý ze tří nenulových prvků generuje dvouprvkovou podgrupu. Tedy:



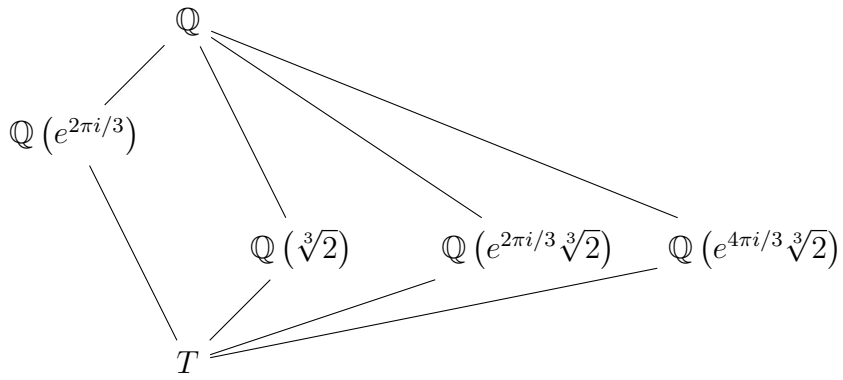

Aplikujeme nyní Galoisovu korespondenci, pokud zachováme orientaci diagramu, pak u vzniklých Fixů budeme kreslit větší tělesa níže. U triviálních podgrup víme okamžitě, že příslušný Fix musí být $\mathbb{Q}$ resp. $T$, zatímco u dvouprvkových podgrup snadno Fix určíme, neboť se fixování identitou je triviální, takže zbývá vždy jen jedna podmínka, např. $\operatorname{Fix}(T, \langle\sigma_{1,0}\rangle) = \operatorname{Fix}(T, i \mapsto -i) = \mathbb{Q}(\sqrt{2})$, protože $\sqrt{2}$ je fixovaná a už generuje rozšíření stupně 2, což víme, že má vyjít. Podobně dostaneme i zbylé Fixy:




b) Na předchozích cvičeních jsme už viděli, že $T = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ a že $[T : \mathbb{Q}] = 6$. Jedná se o Galoisovo rozšíření, přitom se ale šestiprvková $\operatorname{Gal}(T/\mathbb{Q})$ má vnořovat do $S_3$ (permutace tří kořenů $x^3 - 2$), takže už musí být $\operatorname{Gal}(T/\mathbb{Q}) \simeq S_3$.
$S_3$ má následující strukturu podgrup: jedinou podgrupou řádu 3 je grupa generovaná kterýmkoliv ze dvou trojcyklů, což je shodou okolností taky alternující grupa $A_3$. Řádu 2 jsou jen podgrupy generované každou ze tří transpozic, tyto jsou samozřejmě izomorfní $\mathbb{Z}_3$. Schématicky tedy můžeme kreslit:




Jak nyní určit Fixy? Dvouprvkové grupy jsou generované transpozicemi dvou kořenů a mají odpovídat kubickému rozšíření – do toho ale přesně sedí těleso generované třetím kořenem, který transpozice nechává na místě. Naproti tomu Fix od $A_3$ má být kvadratické rozšíření $\mathbb{Q}$, a vzhledem k tomu, že víme, že má být jen jedno, stačí si všimnout podtělesa $\mathbb{Q}\left(e^{2\pi i/3}\right)$. Tedy:




**2.** Pro rozšíření těles $U \supset T$ urči $[U : T]$ spolu s bází $U$ jako vektorového prostoru nad $T$, rozhodni, zda jde o Galoisovo rozšíření, a pokud ano, urči také všechna tělesa $V$, $U \supset V \supset T$, jestliže

a) $U = \mathbb{Q}(\sqrt{2}, e^{2\pi i/3})$, $T = \mathbb{Q}$,
b) $U = \mathbb{Q}(\sqrt[3]{3})$, $T = \mathbb{Q}$,
c) $U = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $T = \mathbb{Q}$,
d) $U = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$, $T = \mathbb{Q}$.

*Řešení.* Uvádím jen Galoisovy grupy a mezitělesa, pokud nejsou příliš komplikovaná.

a) Trikově si lze povšimnout $\mathbb{Q}(e^{2\pi i/3}) = \mathbb{Q}(\sqrt{-3})$, takže $U = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$. Podobně jako v **1.**a) vyjde $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, mezitělesa jsou $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-6})$, $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$.
b) Není Galoisovo, protože $x^3 - 3$ má ještě další dva komplexní kořeny, které budou v $U \subset \mathbb{R}$ chybět.
c) $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_2^3$. Mezitěles bude mnoho; pokud jsem se nepřepočítal, tak sedm stupně 2 a sedm stupně 1:

$$\mathbb{Q}(\sqrt{2}),\quad \mathbb{Q}(\sqrt{3}),\quad \mathbb{Q}(\sqrt{5}),\quad \mathbb{Q}(\sqrt{6}),\quad \mathbb{Q}(\sqrt{10}),\quad \mathbb{Q}(\sqrt{15}),\quad \mathbb{Q}(\sqrt{30}),$$
$$\mathbb{Q}(\sqrt{3}, \sqrt{5}),\quad \mathbb{Q}(\sqrt{2}, \sqrt{5}),\quad \mathbb{Q}(\sqrt{2}, \sqrt{3}),\quad \mathbb{Q}(\sqrt{5}, \sqrt{6}),\quad \mathbb{Q}(\sqrt{3}, \sqrt{10}),\quad \mathbb{Q}(\sqrt{2}, \sqrt{25}),$$
$$\mathbb{Q}(\sqrt{6}, \sqrt{10}).$$

d) Není Galoisovo. Zjevně je $\sqrt{1+\sqrt{2}}$ kořenem $(x^2-1)^2-2$, což můžeme při substituci $x = y+1$ přepsat jako $(y^2+2y)^2 - 2 = y^4 + 4y^3 + 4y^2 - 2$, což je ireducibilní dle Eisensteinova kritéria s $p = 2$, tedy už $(x^2-1)^2 - 2$ musí být minimálním polynomem $\sqrt{1+\sqrt{2}}$. Jeho dalším kořenem je ale také třeba $\sqrt{1-\sqrt{2}} \notin \mathbb{R}$, přitom však $U \subset \mathbb{R}$, což už dosvědčuje, že $U$ není normální.

**3.** Buď $U$ rozkladové nadtěleso polynomu $f$ nad tělesem $T$. Urči $U$, $[U : T]$, bázi $U$ nad $T$ a $\mathrm{Gal}(U/T)$ (můžeš se taky zamyslet nad tělesy $V$, $U \supset V \supset T$, ale mnohdy vypadají dost ošklivě), jestliže

a) $f = x^2 - 5$, $T = \mathbb{Q}$,
b) $f = x^3 - 2$, $T = \mathbb{Q}(e^{2\pi i/3})$,
c) $f = (x^2-3)(x^2-5)$, $T = \mathbb{Q}(\sqrt{2})$,
*d) $f = (x^2-1)^2 - 2$, $T = \mathbb{Q}$.

*Řešení.*

a) $U = T(\sqrt{5})$, $[U:T] = 2$, $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_2$, mezitělesa jsou jen triviální.
b) $U = T(\sqrt[3]{2})$, $[U:T] = 3$, $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_3$, mezitělesa jsou jen triviální.
c) $[U:T] = 4$, $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_2^2$, mezitělesa jsou triviální a $T(\sqrt{3})$, $T(\sqrt{15})$, $T(\sqrt{5})$.
d) $U = T(\sqrt{1+\sqrt{2}}, i)$, $[U:T] = 8$, $\mathrm{Gal}(U/T) \simeq D_8$, mezitělesa vypadají komplikovaně, proto si je dovolím vynechat.

**4.** Mějme tělesa $V \supset U \supset T$ taková, že jak $V \supset T$, tak $U \supset T$ jsou normální rozšíření. Pak $\mathrm{Gal}(V/U) \triangleleft \mathrm{Gal}(V/T)$ a $\mathrm{Gal}(V/T)/\mathrm{Gal}(V/U) \simeq \mathrm{Gal}(U/T)$.

*Řešení.* Uvážím zobrazení definované restrikcí

$$\begin{aligned} \mathrm{Gal}(V/T) &\to \mathrm{Gal}(U/T), \\ \varphi &\mapsto \varphi|_U . \end{aligned}$$

Nejprve zdůvodním, že $\varphi|_U$ je skutečně $T$-homomorfismus $U \to U$. $T$-homomorfismus je jasný. Pak určitě přinejmenším víme, že je to $T$-homomorfismus $U \to \overline{T}$. Definicí normality je tedy ve skutečnosti $U \to U$. Je to tělesový homomorfismus, takže i prosté $T$-lineární zobrazení. $U$ má nad $T$ konečnou dimenzi, takže lineární endomorfismus je prostý, právě když je na, tedy právě když je to automorfismus. Tím je dokázáno, že $\varphi|_U$.

Že restrikce zachová skládání automorfismů, je zřejmé. Máme tedy homomorfismus grup. Tvrdím, že je surjektivní, buď tedy dáno $\varphi \in \mathrm{Gal}(U/T)$ a najdu jeho vzor. Buď $V = T(\alpha)$ (Galoisovo rozšíření, tedy speciálně spearabilní konečného stupně). Pak je $V$ rozkladové nadtěleso polynomu $m_{\alpha,T}$ nad $T$. Podle tvrzení 2.5 ze skript ale umíme $T$-izomorfismus $U =: T_1 \to T_2 := U$ rozšířit na nějaké $\psi$ mezi rozkladovými nadtělesy polynomu $f$ resp. $\varphi(f)$. Jenže $f$ má koeficienty z $T$, takže $\varphi(f) = f$, a rozkladové nadtěleso $f$ nad $U$ je určitě $V$ (je rozkladové už nad $T$). Takže jsme $\varphi : U \to U$ rozšířili nad $\psi : V \to V$, což jsme chtěli.

Tedy máme surjektivní homomorfismus grup. Co je jeho jádro? $\varphi|_U = \mathrm{id}_U$ nastává právě tehdy, když $\varphi$ nechává $U$ na msítě, tedy $\varphi \in \mathrm{Gal}(V/U)$. Jádro je tedy $\mathrm{Gal}(V/U) \leq \mathrm{Gal}(V/T)$, což z této podgrupy okamžitě činí podgrupu normální a navíc máme první větou o izomorfismu

$$\mathrm{Gal}(V/T)/\mathrm{Gal}(V/U) \simeq \mathrm{Gal}(U/T),$$

jak jsme chtěli.

**5.** Uvažujme cyklotomická tělesa.

a) Připomeň si, že $\mathrm{Gal}\left(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}\right) \simeq \mathbb{Z}_n^\times$. Předpokládej, že už víš $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \varphi(n)$.
b) Buď $U$ rozkladové nadtěleso $x^{20} - 1$ nad $\mathbb{Q}(i)$. Urči $\mathrm{Gal}(U/\mathbb{Q}(i))$ a všechna mezitělesa $V$, $U \supset V \supset \mathbb{Q}(i)$.
c) * Buď $U$ kořenové nadtěleso $x^3 + x^2 - 2x - 1$ nad $\mathbb{Q}$. Urči $\mathrm{Gal}(U/\mathbb{Q})$.

*Řešení.*

a) Buď $\zeta := e^{2\pi i/n}$. Víme, že toto je kořenem $n$-tého cyklotomického polynomu, jehož kořeny jsou přesně $\zeta^k$ pro $k \in \mathbb{Z}_n^*$. Z toho jednak plyne, že $\mathbb{Q}(\zeta)$ je rovnou i rozkladové nadtěleso $n$-tého cyklotomického polynomu, takže je to Galoisovo rozšíření $\mathbb{Q}$. Také ale máme nanejvýš $\varphi(n)$ možných obrazů pro $\zeta$, jmenovitě jednotlivá $\zeta^k$, $k \in \mathbb{Z}_n^*$, takže všechna tato $k$ musí dát automorfismus. Při skládání uvidíme

$$\zeta \mapsto \zeta^{k_1} \mapsto (\zeta^{k_1})^{k_2} = \zeta^{(k_1 k_2)},$$

z čehož je hned už vidět $\mathrm{Gal}\left(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}\right) \simeq \mathbb{Z}_n^\times$.

b) Víme, že $\mathrm{Gal}(U/\mathbb{Q}) \simeq \mathbb{Z}_{20}^*$ a $\mathrm{Gal}(U/\mathbb{Q}(i))$ je její podgrupou. Potřebujeme tedy automorfismus zadaný pomocí $\zeta \mapsto \zeta^k$, $k \in \{1,3,7,9,11,13,17,19\}$ takový, že $i \mapsto i$. Díky $i = \zeta^5$ to znamená $i^k = i$, tedy $k \equiv 1 \pmod 4$, což nám ponechá pogrupu tvaru $\{1,9,13,17\} \simeq \mathbb{Z}_5^* \simeq \mathbb{Z}_4$ (jelikož $13^2 \equiv 9$, musí už 13 mít řád 4). To má tedy jen jednu netriviální podgrupu $\{1,9\}$.
Tvrdím, že příslušný Fix mohu popsat třeba jako $T(\zeta^4+\zeta^{-4}-\zeta^8-\zeta^{-8})$. K tomu si všimněme, že $\zeta \mapsto \zeta^9 = -\zeta^-4$, takže $\zeta^4 \mapsto (-1)^4\zeta^{-4}$, z čehož se

$$\zeta^4 + \zeta^{-4} - \zeta^8 - \zeta^{-8} \mapsto \zeta^{-4} + \zeta^4 - \zeta^{-8} - \zeta^8$$

fixuje. Tento výraz je ve skutečnosti roven $\sqrt{5}$ (jde to vykoukat z poznatků z druhácké Teorie čísel o Gaussových charakterech[1]), takže jediným netriviálním tělesem ležícím mezi $U$ a $\mathbb{Q}(i)$ je $\mathbb{Q}(i,\sqrt{5})$.

c) Označme $\zeta := e^{2\pi i/7}$ a podívejme se na úlohu uvnitř $V := \mathbb{Q}(\zeta)$. Tvrdím, že $U = \mathbb{Q}(\zeta+\zeta^{-1})$. Že $\zeta+\zeta^{-1}$ je kořenem $f$ se dověří dosazením, stejně tak se ověří, že dalšími dvěma kořeny jsou $\zeta^2+\zeta^{-2}$ a $\zeta^3+\zeta^{-3}$. Snadno taky vyjádříme, že tyto už leží v $\mathbb{Q}(\zeta+\zeta^{-1})$ skrze

$$\zeta^2+\zeta^{-2} = (\zeta+\zeta^{-1})^2 - 2, \qquad \zeta^3+\zeta^{-3} = (\zeta+\zeta^{-1})^3 - 3(\zeta+\zeta^{-1}).$$

Potom už vidíme, že máme Galoisovo rozšíření (rozkladové nadtěleso) stupně 3 (je to zároveň kořenové a $f$ je ireducibilní, např. vyzkoušením všech možností z věty o racionálním kořeni), takže už musí být $\mathrm{Gal}(U/\mathbb{Q}) \simeq \mathbb{Z}_3$ (jediná trojprvková grupa). Z toho také plyne, že $U$ nemá žádná netriviální podtělesa.

**6.** Mějme rozšíření $U \supset \mathbb{Q}$ konečného stupně, které ale není normální. Zamysli se, jestli přesto nedovedeme *nějak* pomocí Galoisovy korespondence najít všechna tělesa $V$, $U \supset V \supset \mathbb{Q}$. Obecněji uvažuj totéž pro rozšíření $U \supset T$, jež je separabilní a konečného stupně, ale není normální.

*Řešení.* Minule jsme viděli, že k separabilnímu rozšíření $U \supset T$ umíme najít $V \supset U$ tak, že $V \supset T$ je Galoisovo. Potom můžeme spočíst $\mathrm{Gal}(V/T)$ a hledat podtělesa většího $V$ pomocí Galoisovy korespondence. Přitom ta z nich, která budou dokonce podtělesy $U$, budou odpovídat nadgrupám podgrupy $\mathrm{Gal}(V/U) < \mathrm{Gal}(V/T)$.

**7.** * Buď $U$ rozkladové nadtěleso polynomu $f$ nad tělesem $T$. Urči $U$, $[U:T]$, bázi $U$ nad $T$ a $\mathrm{Gal}(U/T)$ a všechna tělesa $V$, $U \supset V \supset T$, jestliže

a) $f = x^3 - 5$, $T = \mathbb{Z}_7$,
b) $f = x^4 - 3$, $T = \mathbb{Z}_5$,
c) $f = x^{p^k} - x$, $T = \mathbb{Z}_p$.

*Řešení.*

a) $f$ nemá v $T$ kořen a je kubický, takže už je ireducibilní. Jelikož jsou 1, 2 a 4 třetí odmocniny z jedničky v $\mathbb{Z}_7$, je-li $\alpha$ kořenem $f$, pak jsou jimi i $2\alpha$ a $4\alpha$, takže kořenové nadtěleso $\mathbb{Z}_7(\alpha)$ bude i rozkladové $U$. Z toho $[U:T] = 3$, takže Galoisova grupa je $\mathbb{Z}_3$ a nemáme žádná netriviální mezitělesa.

b) $f$ nemá v $T$ kořen a rozepsání rovnic plynoucích z rozkladu $x^4-3 = (x^2-ax+b)(x^2-cx+d)$ ukáže, že takový rozklad neexistuje, takže $f$ je ireducibilní. Nyní jsou 1, 2, 3, 4 primitivní odmocniny z jedničky v $\mathbb{Z}_5$, takže pro kořen $\alpha$ polynomu $f$ už násobky $\alpha$ představují všechny kořeny, tedy opět je kořenové nadtěleso $\mathbb{Z}_5(\alpha)$ rovnou i rozkladové. Pak vidíme $[U:T] = 4$. Automorfismy musí odpovídat $\alpha \mapsto k\alpha$, $k = 1,2,3,4$, což bude při skládání vypadat jako

$$\alpha \mapsto k_1\alpha \mapsto k_1(k_2\alpha) = (k_1k_2)\alpha,$$

z čehož je vidět $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_5^* \simeq \mathbb{Z}_4$. Dvouprvkovou podgrupou je zde $\{1,4\}$. Čtyřka odpovídá $\alpha \mapsto 4\alpha = -\alpha$, takže se v tomto automorfismu musí fixovat $\alpha^2$. To je kořenem kvadratického polynomu $x^2-3$, takže skutečně obdržíme kvadratické rozšíření

$$\mathrm{Fix}(U,\{1,4\}) = \mathbb{Z}_5(\alpha^2).$$

[1] Taky bych očekával, že to člověk uvidí, pokud bude dost dlouho zírat na pravidelný pětiúhelník.

c) V charakteristice $p$ je $a \mapsto a^p$ okruhový homomorfismus (respektuje násobení i sčítání), takže i jeho $k$-násobné složení $a \mapsto a^{p^k}$ bude homomorfismus. Sama množina kořenů $f = x^{p^k} - x$ je tedy uzavřená na sčítání, násobení i multiplikativní inverzy, tvoří tedy těleso. To pak tedy má $p^k$ prvků, tedy je to rozšíření $\mathbb{Z}_p$ stupně $k$. Homorfismus $a \mapsto a^p$ je automorfismem a jeho skládáním vyrobíme $k$-různých automorfismů (protože teprve $k$-násobné složení $a \mapsto a^{p^k} = a$ je identita). To znamená, že Galoisova grupa je cyklická. Podtělesy jsou rozkladová nadtělesa polynomů $f_\ell = x^{p^\ell} - x$ pro $\ell \mid k$.

**8.** ** Nahlédni, že pokud $\mathrm{Gal}(T/\mathbb{Q}) \simeq A_4$, pak neexistuje žádné těleso $U$, $T \supset U \supset \mathbb{Q}$ se stupněm $[U : \mathbb{Q}] = 2$. Pokud si věříš, zkus dokázat, že rozkladové nadtěleso $f = x^4 + 8x + 12$ nad $\mathbb{Q}$ je příkladem takového $T$. (Mně se to zatím nepovedlo dokázat, ale podle důvěryhodného zdroje by to měla být pravda.)

*Řešení.* Galoisovou korespondencí odpovídají mezitělesa v $T \supset \mathbb{Q}$ podgrupám v $\mathrm{Gal}(T/\mathbb{Q})$. Stupeň $[U : \mathbb{Q}] = 2$ by musel odpovídat podgrupě $\mathrm{Gal}(T/\mathbb{Q})$ indexu 2, jenže $A_4$ žádné takové nemá.

Důkaz, že Galoisova grupa $A_4$ skutečně nastane pro rozkladové nadtěleso $f = x^4 + 8x + 12$, může horlivý zájemce najít zde:
`https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf` (Example 3.3)