Cvičení 5, 23.11.2020

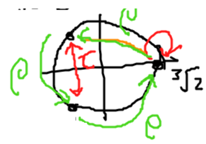
Příklady označené (!) jsou zásadní a nutně musíte pochopit řešení. Příklady označené (*) jsou těžší.

Označ $\zeta_n = e^{2\pi i/n}$.

Buď U rozkladové nadtěleso polynomu f nad tělesem T. Urči $[U : T]$, $\mathrm{Gal}(U/T)$ (její prvky i izomorfismus na některou známou grupu) a popiš všechna tělesa $U \supset V \supset T$.

1. (! *ukážu, jak se dělá*) $f(x) = x^3 - 2, T = \mathbb{Q}$.

Př.: $f = x^3 - 2$ $\quad U = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ $\quad \zeta_3 = e^{2\pi i/3}$



1) $[U:\mathbb{Q}] = \underline{6}$ $\quad \ldots \quad \mathbb{Q} \underset{3}{\leq} \mathbb{Q}(\sqrt[3]{2}) \underset{2}{\leq} \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

$\;\;\; \overset{\text{|| věta}}{|\mathrm{Gal}(U/\mathbb{Q})|}$

2) $\zeta_3 \mapsto \begin{cases} \zeta_3 \\ \bar{\zeta}_3 \end{cases} \leq 2$

$\sqrt[3]{2} \mapsto \begin{cases} \sqrt[3]{2} \\ \sqrt[3]{2}\zeta_3 \\ \sqrt[3]{2}\zeta_3^2 \end{cases} \leq 3$

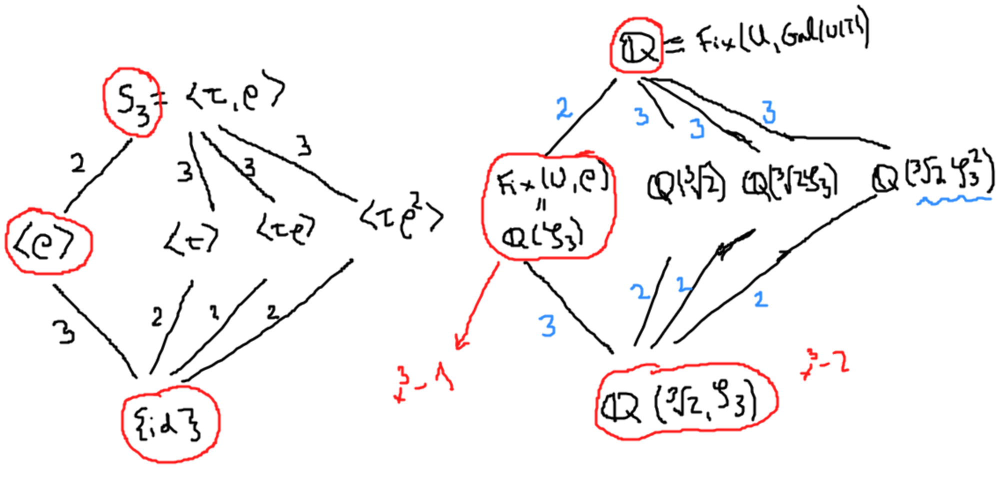
každá kombinace dá automorfismus

$\tau: \zeta_3 \mapsto \bar{\zeta}_3 = \zeta_3^2, \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}$

$\rho: \zeta_3 \mapsto \zeta_3, \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta_3$

$\mathrm{Gal}(U/T) = \langle \tau, \rho \rangle \leq S_3$ (permutace na kořenech)

$= S_3$



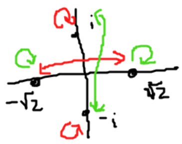
2. (! *ukážu, jak se dělá*) $f(x) = (x^2 - 2)(x^2 + 1), T = \mathbb{Q}$.

Př.: $f = (x^2-2)(x^2+1)$ $U = \mathbb{Q}(\sqrt{2}, i)$

1) $\mathbb{Q} \underset{2}{\leq} \mathbb{Q}(\sqrt{2}) \underset{2}{\leq} \mathbb{Q}(\sqrt{2}, i) \longrightarrow [U : T] = 4$, báze $1, \sqrt{2}, i, \sqrt{2}i$

$[U:T] = |Gal|$

2) x^2-2: $\sqrt{2} \mapsto \pm\sqrt{2}$; x^2+1: $i \mapsto \pm i$ $\Big\}$ ≤ 4 možnosti — všechny fungují



označ:

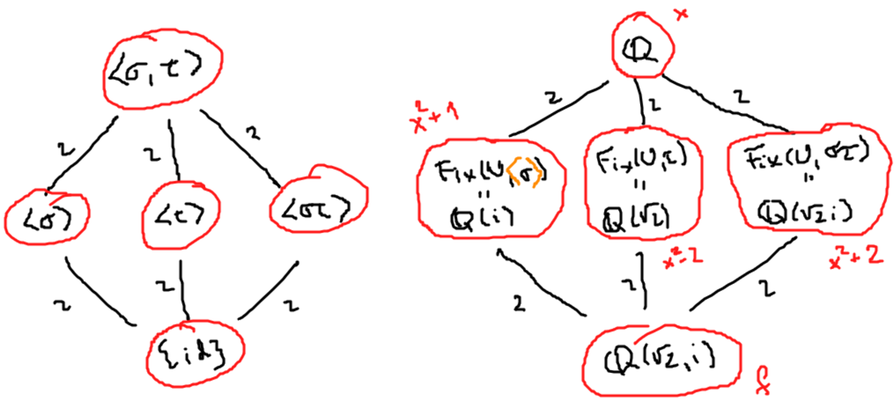
$(\cdot)(\cdot)(\cdot\cdot)$ σ: $\sqrt{2} \mapsto -\sqrt{2}$, $i \mapsto i$

$(\cdot\cdot)(\cdot)(\cdot)$ τ: $\sqrt{2} \mapsto \sqrt{2}$, $i \mapsto -i$

$(\cdot\cdot)(\cdot\cdot)$ $\sigma\tau = \tau\sigma$

$Gal(U/\mathbb{Q}) = \langle \sigma, \tau \rangle_{S_4} = \{id, \sigma, \tau, \sigma\tau\}$ $\leq S_4$

$\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.



3. (!) $f(x) = (x^2 - 2)(x^2 + 1)(x^2 - 3), T = \mathbb{Q}$. Vycházejte z faktu, že $[U : \mathbb{Q}] = 8$. *Řešení:* 1) $U = \mathbb{Q}(\sqrt{2}, i, \sqrt{3})$ je stupně 8. 2) $Gal = \langle \rho, \sigma, \tau \rangle \leq S_6$, kde ρ, σ, τ jsou právě ty tři transpozice na kořenech, tj.

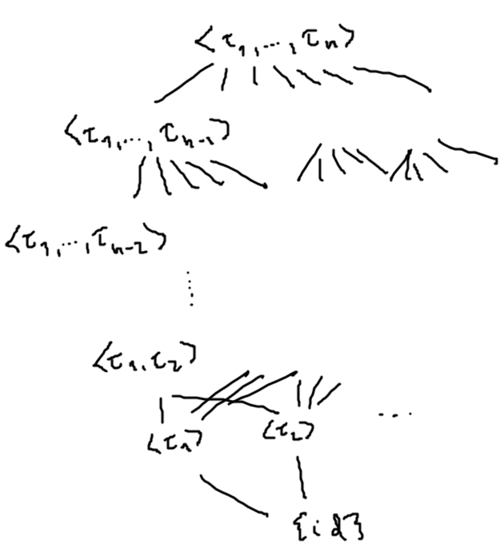
- $\rho(\sqrt{2}) = -\sqrt{2}$, $\rho(i) = i$, $\rho(\sqrt{3}) = \sqrt{3}$
- $\sigma(\sqrt{2}) = \sqrt{2}$, $\sigma(i) = -i$, $\sigma(\sqrt{3}) = \sqrt{3}$
- $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(i) = i$, $\tau(\sqrt{3}) = -\sqrt{3}$

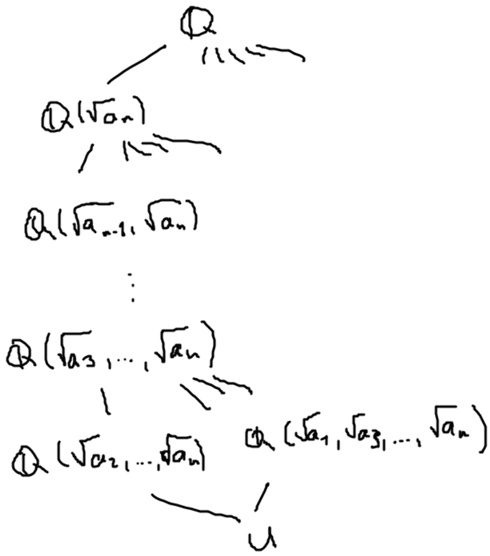
$Gal \simeq \mathbb{Z}_2^3$, vektor (a_1, a_2, a_3) indikuje, zda se kořen daného kvadratického činitele fixuje (hodnota 0) nebo prohazuje (1). 3) Mezitělesa:

- $\langle \rho \rangle$ odpovídá $Fix(U, \rho) = \mathbb{Q}(i, \sqrt{3})$
- $\langle \rho\sigma \rangle$ odpovídá $Fix(U, \rho\sigma) = \mathbb{Q}(\sqrt{2}i, \sqrt{3})$
- atd. pro ostatní cyklické podgrupy řádu 2 (je jich 7)
- $\langle \rho, \sigma \rangle$ odpovídá $Fix(U, \{\rho, \sigma\}) = \mathbb{Q}(\sqrt{3})$
- atd. pro ostatní dvougenerované podgrupy řádu 4 (je jich 7)

4. (!) $f(x) = (x^2 - a_1)\dots(x^2 - a_n), T = \mathbb{Q}$, kde $a_1, ..., a_n$ splňují předpoklady věty 2.28. Vycházejte z faktu, že $[U : \mathbb{Q}] = 2^n$. Řešení je popsáno ve skriptech (věta 2.28), pořádně si ho rozmyslete. Speciálně bych rád, abyste si pečlivě dokázali izomorfismus $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_2^n$.

   Návod: Je to pořád to samé. $\mathbb{Z}_2^n \to Gal(U/T)$, $(k_1, ..., k_n) \mapsto$ automorfismus, který posílá $\sqrt{a_i} \mapsto (-1)^{k_i}\sqrt{a_i}$. Stejně jako výše je zřejmé, že takový automorfismus je právě jeden, tedy jde o bijekci. Dokažte pečlivě, že to je grupový homomorfismus. Mezitěles je tolik, kolik je podporstorů vektorového prostoru $\mathbb{Z}_2^n$, princip je asi jasný z výše uvedených příkladů.



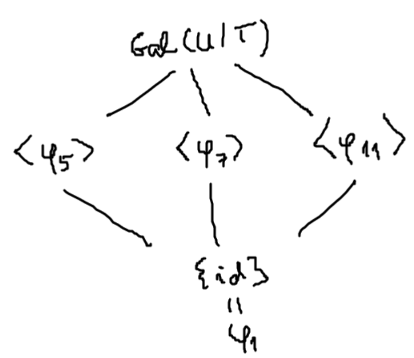


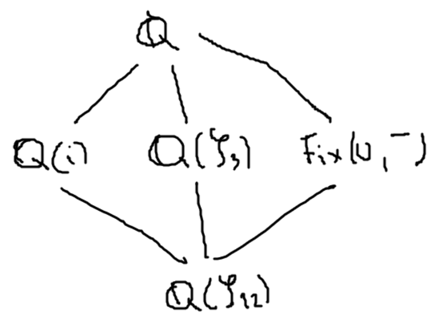
5. (!*) $f(x) = x^{12} - 1, T = \mathbb{Q}$.

Řešení: 1) Zřejmě $U = \mathbb{Q}(\zeta_{12})$, ale není jasný stupeň. Spočteme minimální polynom pro ζ_{12}. Rozlož $x^{12} - 1 = (x^6 - 1)(x^6 + 1) = (x^6 - 1)(x^2 + 1)(x^4 - x^2 + 1)$, ten poslední činitel m je ireducibilní, ζ_{12} není kořen ani jednoho z těch první dvou činitelů, čili musí být kořenem m. Čili $[U : T] = \#Gal(U/T) = 4$. Další kořeny $m = m_{\zeta_{12}}$ jsou $\zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$, ze stejného důvodu.

2) Automorfismy zobrazí ζ_{12} na kořen m, takže jsou nejvýše čtyři možnosti $\varphi_k : \zeta_{12} \mapsto \zeta_{12}^k$, kde $k = 1, 5, 7, 11$. Protože $\#Gal = 4$, všechny tyto možnosti dají automorfismus. Čili $Gal(U/T) = \{\varphi_1, \varphi_5, \varphi_7, \varphi_{11}\}$. Všechny tyto automorfismy kromě φ_1 jsou řádu 2, takže $Gal(U/T) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. [Pro účely dalšího výkladu si rozmyslete obecnější argument: všimněte si, že zobrazení $\mathbb{Z}_{12}^\times \to Gal(U/T)$, $k \mapsto \varphi_k$ je grupový izomorfismus (proč?!), a dále nahlédněte, že $\mathbb{Z}_{12}^\times \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.]

3) Podgrupě $\langle \varphi_k \rangle$ odpovídá mezitěleso $Fix(U, \varphi_k)$. Dvě vlastní mezitělesa vidíme hned: $\mathbb{Q}(i) = \mathbb{Q}(\zeta_{12}^3)$ a $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_{12}^4)$. Rychle zjistíme, že φ_5 fixuje i a že φ_7 fixuje ζ_3. Zbývá rozmyslet, co fixuje φ_{11}. To je zobrazení komplexního sdružení, $z \mapsto \bar{z}$, takže fixpointy jsou jasné (v prvku $\sum a_i \zeta_{12}^i$ musí být $a_1 = a_{11}$, $a_2 = a_{10}$, ...). Protože je Gal abelovská, všechna mezitělesa jsou normální.





Jiné zábavné cvičení: Dokažte, že $Fix(\mathbb{Q}(\zeta_n), z \mapsto \bar{z}) = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

6. (!) $f(x) = x^n - 1$, $T = \mathbb{Q}$. Vycházejte z faktu, že $[U : \mathbb{Q}] = \varphi(n)$, kde φ je Eulerova funkce (to je ta těžší část). Řešení je popsáno ve skriptech (pod větou 2.28), pořádně si ho rozmyslete. Speciálně bych rád, abyste si pečlivě dokázali izomorfismus $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_n^\times$.

Návod: $\mathbb{Z}_n^\times \to Gal(U/T)$, $k \mapsto \varphi_k$, což je automorfismus, který posílá $\zeta_n \mapsto \zeta_n^k$. Rozmyslete si, že automorfismy musí posílat ζ_n na ζ_n^k, kde $NSD(k, n) = 1$. Z vlatnosti "stupeň $= \#Gal$"pak plyne, že to je bijekce. Dokažte pečlivě, že to je grupový homomorfismus: pokud chcete dokázat, že $\varphi_k \circ \varphi_m = \varphi_l$, stačí dokázat, že levá i pravá strana se shodují na generátoru ζ_n. Mezitěles je tedy stejně jako podgrup grupy $\mathbb{Z}_n^\times$, ale obecně není snadné je popsat ve formě $\mathbb{Q}(a)$.

7. (!) $f(x) = x^5 - 2, T = \mathbb{Q}(e^{2\pi i/5})$

   Návod: 1) $U = \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$, čili $[U : T] = 5$. 2) $\zeta_5 \mapsto \zeta_5$ a $\sqrt[5]{2} \mapsto$ nějaký kořen polynomu $x^5 - 2$. Označme φ_k ten automorfismus, který pošle $\sqrt[5]{2} \mapsto \sqrt[5]{2}\zeta_5^k$, $k = 0, ..., 4$. Podobně jako v předchozí úloze nahlédněte, že $\mathbb{Z}_5 \to Gal(U/T)$, $k \mapsto \varphi_k$ je grupový izomorfismus. 3) Grupa $\mathbb{Z}_5$ nemá vlastní podgrupy, čili nebudou ani vlastní mezitělesa.

8. (!*) $f(x) = x^{20} - 1, T = \mathbb{Q}(i)$.

   Řešení: V předminulé úloze jsme spočítali, že $Gal(U/\mathbb{Q}) = \{\varphi_k : NSD(k, 20) = 1\}$. Prvek $i = \zeta_{20}^5$ zachovávají ty φ_k, pro která $\zeta_{20}^{5k} = \varphi_k(\zeta_{20}^5) = \zeta_{20}^5$, tedy ta, pro která $5k \equiv 5 \pmod{20}$. Tato k tvoří podgrupu $\{1, 9, 13, 17\} \leq \mathbb{Z}_{20}^\times$, která je cyklická, generátorem je 13 nebo 17. Vlastní podgrupa Gal bude jedna, $\langle\zeta_9\rangle$, mezitěleso tedy bude jedno, $Fix(U, \zeta_9)$.