Proposição 9.4. *Seja Ω um corpo contendo $\mathbb{E}_1, \mathbb{E}_2, \mathbb{F}$. Assuma que $\mathbb{E}_1/\mathbb{F}$ e $\mathbb{E}_2/\mathbb{F}$ são galoisianas finitas. Então, $\mathbb{E}_1 \cdot \mathbb{E}_2/\mathbb{F}$ é galoisiana finita. Além disso, o mapa*

$$\sigma \in \mathrm{Aut}(\mathbb{E}_1\mathbb{E}_2/\mathbb{F}) \mapsto (\sigma|_{\mathbb{E}_1}, \sigma|_{\mathbb{E}_2}) \in \mathrm{Aut}(\mathbb{E}_1/\mathbb{F}) \times \mathrm{Aut}(\mathbb{E}_2/\mathbb{F})$$

é injetor, e sua imagem é $\{(\sigma_1, \sigma_2) \mid \sigma_1|_{\mathbb{E}_1\cap\mathbb{E}_2} = \sigma_2|_{\mathbb{E}_1\cap\mathbb{E}_2}\}$. Em particular, se $\mathbb{E}_1 \cap \mathbb{E}_2 = \mathbb{F}$, então o mapa acima é um isomorfismo.

Proposição 3.6. *Sejam $\mathbb{F}$ um corpo, Ω um corpo algebricamente fechado e $\varphi_0 : \mathbb{F} \to \Omega$ um monomorfismo de corpos. Seja $\mathbb{E} = \mathbb{F}(a)$ uma extensão de corpos algébrica e simples, e seja p_a o polinômio minimal de a sobre $\mathbb{F}$. Então, para cada raiz $\omega \in \Omega$ de $\varphi_0(p_a)$, existe um único homomorfismo de anéis $\varphi : \mathbb{E} \to \Omega$ que estende φ_0 e que satisfaz $\varphi(a) = \omega$. Todo homomorfismo $\mathbb{E} \to \Omega$ que estende φ_0 é construído dessa forma.*

(1) Calcule $\mathrm{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$, em que $d \in \mathbb{Z}$ é livre de quadrados (isto é, se p é primo, então p^2 não divide d).
(2) Calcule $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$.

(3) Seja $\mathbb{L}$ o corpo de raízes de $f \in \mathbb{Q}[X]$ sobre $\mathbb{Q}$. Descreva $\mathrm{Aut}(\mathbb{L}/\mathbb{Q})$, e os subcorpos de $\mathbb{L}$, em que:
   (a) $f = X^5 - 1$
   (b) $f = X^3 - 2$
   (c) $f = ~~X^4 - 2~~$ $X^4 - 3$

Prop. Sejam $f \in \mathbb{F}[X]$, $n = \#$ raízes dist. de f e $\mathbb{L}$ o corpo de raízes de f sobre $\mathbb{F}$. Então

$$\mathrm{Aut}(\mathbb{L}/\mathbb{F}) \hookrightarrow S_n.$$

Dem.: Denote $\mathcal{R}(f) = \{a_1, \dots, a_n\}$. Então

$$\mathbb{L} = \mathbb{F}(a_1, \dots, a_n).$$

Dado $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$, temos que

$$f(\sigma(a_i)) = \sigma(f(a_i)) = 0.$$

Assim, existe $\tau \in S_n$ tal que $\sigma(a_i) = a_{\tau(i)}$.

Portanto, obtemos um hom. de grupos

$$\Psi : \mathrm{Aut}(\mathbb{L}/\mathbb{F}) \longrightarrow S_n.$$

Assuma que $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$ é tal que $\sigma(a_i) = a_i$, para todo $i = 1, \dots, n$. Então, $\sigma = \mathrm{id}_{\mathbb{F}(a_1, \dots, a_n)}$. Ou seja, o mapa Ψ é injetora. □

(1) Calcule $\mathrm{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$, em que $d \in \mathbb{Z}$ é livre de quadrados (isto é, se p é primo, então p^2 não divide d).
(2) Calcule $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$.

(1) Temos que $\mathrm{Irr}(\sqrt{d}, \mathbb{Q}) = X^2 - d$. Assim, um $\mathbb{Q}$-monomorfismo $\sigma : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ é totalmente definido por $\sigma(\sqrt{d}) \in \{\sqrt{d}, -\sqrt{d}\}$.

Assim, $\mathrm{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{id, \sigma\} \cong C_2$, em que $\sigma(\sqrt{d}) = -\sqrt{d}$ (então, $\sigma^2 = id$).

(2) Note que $\mathbb{Q}(\sqrt{2}) \cdot \mathbb{Q}(i) = \mathbb{Q}(\sqrt{2}, i)$, e

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong C_2 \cong \mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q}).$$

Ainda, $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(i) = \mathbb{Q}$. Daí

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \cong C_2 \times C_2.$$

Temos as seguintes elementos de $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$:

$\mathbb{Q}(\sqrt{2})(i)$
$|\ \mathrm{Irr}(i, \mathbb{Q}(\sqrt{2})) = X^2+1$
$\mathbb{Q}(\sqrt{2})$
$|\ \mathrm{Irr}(\sqrt{2}, \mathbb{Q}) = X^2-2$
$\mathbb{Q}$

$$\sigma_1(\sqrt{2}) = -\sqrt{2}, \quad \sigma_1(i) = i.$$
$$\sigma_2(\sqrt{2}) = \sqrt{2}, \quad \sigma_2(i) = -i.$$

Temos que $\sigma_1^2 = id$. De fato

$$\sigma_1^2(\sqrt{2}) = \sigma_1(-\sqrt{2}) = \sqrt{2}, \quad \sigma_1^2(i) = i.$$

Da mesma forma, $\sigma_2^2 = id$. Além disso $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

Assim, $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) = \langle \sigma_1, \sigma_2 \rangle \cong C_2 \times C_2$.

$$\mathbb{Q}(\sqrt{2}, i)^{\langle \sigma_1 \rangle} = \mathbb{Q}(i), \quad \mathbb{Q}(\sqrt{2}, i)^{\langle \sigma_2 \rangle} = \mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(\sqrt{2}, i)^{\langle \sigma_1\sigma_2 \rangle} = \mathbb{Q}(\sqrt{2}i).$$

(3) Seja $\mathbb{L}$ o corpo de raízes de $f \in \mathbb{Q}[X]$ sobre $\mathbb{Q}$. Descreva $\mathrm{Aut}(\mathbb{L}/\mathbb{Q})$, e os subcorpos de $\mathbb{L}$, em que:

(a) $f = X^5 - 1$

(b) $f = X^3 - 2$

(c) $f = X^4 - 2$ ~~$X^4 - 2$~~ $X^4 - 3$

(b) $X^3 - 2$, sejam $\alpha \in \mathbb{R}$ tal que $\alpha^3 = 2$, e $\xi \in \mathbb{C}$ tal que $\xi \neq \xi^3 = 1$.

$$\mathcal{R}(X^3-2) = \{\alpha, \xi\alpha, \xi^2\alpha\}.$$

Daí $\mathbb{L} = \mathbb{Q}(\mathcal{R}(X^3-2)) = \mathbb{Q}(\alpha, \xi)$.

Vimos também que $[\mathbb{L}:\mathbb{Q}] = 6$. Assim, $|\mathrm{Aut}(\mathbb{L}/\mathbb{Q})| = 6$, e $\mathrm{Aut}(\mathbb{L}/\mathbb{Q}) \hookrightarrow S_3$, e $|S_3| = 6$. Assim, $\mathrm{Aut}(\mathbb{L}/\mathbb{Q}) \cong S_3$. Assim, cada $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{Q})$ fica completamente determinado por uma permutação de $\{\alpha, \xi\alpha, \xi^2\alpha\}$.

$\mathbb{Q}(\alpha)(\xi)$

$\mid \mathrm{Irr}(\xi, \mathbb{Q}(\alpha)) = X^2 + X + 1$

$\mathbb{Q}(\alpha)$

$\mid \mathrm{Irr}(\alpha, \mathbb{Q}) = X^3 - 2$

$\mathbb{Q}$

Sejam $\sigma, \tau \in \mathrm{Aut}(\mathbb{L}/\mathbb{Q})$ tais que

$\sigma(\alpha) = \xi\alpha$, $\sigma(\xi) = \xi$

$\tau(\alpha) = \alpha$, $\tau(\xi) = \xi^2$.

Temos que $\sigma^3 = \mathrm{id}$. Pois

$\sigma^3(\alpha) = \sigma^2(\xi\alpha) = \alpha$, $\sigma^3(\xi) = \xi$.

Da mesma forma, $\tau^2 = id$. Além disso,

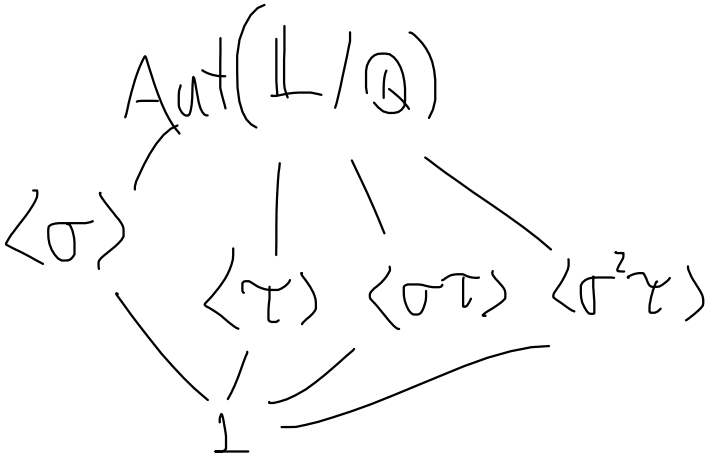
$$\sigma\tau(\alpha) = \sigma(\alpha) = \xi\alpha, \quad \sigma\tau(\xi) = \xi^2,$$

$$\tau\sigma^2(\alpha) = \tau(\xi^2\alpha) = \xi^4\alpha = \xi\alpha, \quad \tau\sigma^2(\xi) = \tau(\xi) = \xi^2.$$

Portanto, $\sigma\tau = \tau\sigma^2$. Assim

$$Aut(\mathbb{L}/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^3 = id, \tau^2 = id, \sigma\tau = \sigma^{-1}\tau \rangle.$$

(igualdade é válida, pois ambos possuem o mesmo número de elementos).

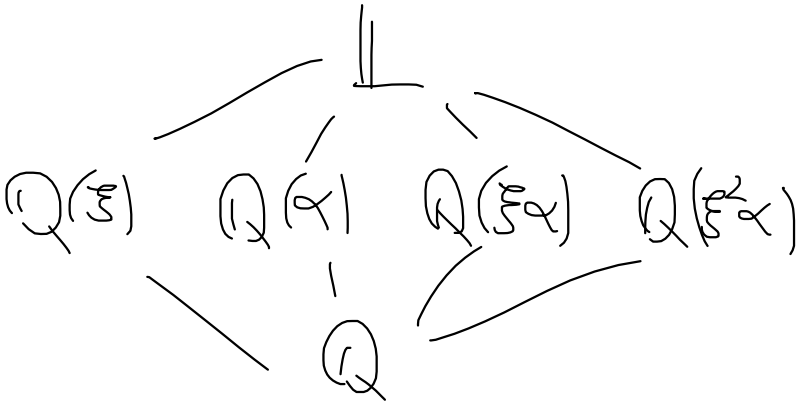


$$\mathbb{L}^{\langle\sigma\rangle} = \mathbb{Q}(\xi)$$

$$\mathbb{L}^{\langle\tau\rangle} = \mathbb{Q}(\alpha)$$

$$\mathbb{L}^{\langle\sigma\tau\rangle} = \mathbb{Q}(\xi^2\alpha)$$

$$\mathbb{L}^{\langle\sigma^2\tau\rangle} = \mathbb{Q}(\xi\alpha)$$



$$\sigma\tau(\xi\alpha) = \sigma(\xi^2\alpha) = \alpha$$

$$\sigma\tau(\xi^2\alpha) = \sigma(\xi\alpha) = \xi\alpha$$

$$\sigma^2\tau(\xi\alpha) = \sigma^2(\xi^2\alpha) = \xi^2\xi^2\alpha = \xi\alpha.$$

(a) $f = x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$

$\mathcal{R}(x^5-1) = \{1, \mu, \mu^2, \mu^3, \mu^4\}$, $\mu \neq \mu^5 = 1$.

$\mathbb{L} = \mathbb{Q}(\mathcal{R}(x^5-1)) = \mathbb{Q}(\mu)$.

$\mathbb{Q}(\mu)$

$|$

$\mathbb{Q}$

Assim, $Aut(\mathbb{Q}(\mu)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$.

$Irr(\mu, \mathbb{Q}) = x^4 + \cdots + x + 1$ tal que

$\sigma_i(\mu) = \mu^i$.

Seja $\tau = \sigma_2$. Note que $\sigma_1 = id$.

$\tau^2(\mu) = \tau(\mu^2) = \mu^4 = \sigma_4(\mu)$.

Assim, $\mu_4 = \tau^2$.

$\tau^3(\mu) = \mu^8 = \mu^3 = \sigma_3(\mu)$. $\Rightarrow \sigma_3 = \tau^3$.

$\tau^4(\mu) = \mu^{16} = \mu = id$.

Assim, $Aut(\mathbb{L}/\mathbb{Q}) = \langle\tau\rangle \cong C_4$. Temos que

$\langle\tau\rangle$

$|$

$\langle\tau^2\rangle$

$|$

$\{id\}$

$\tau^2(\mu^2 + \mu^3) = \tau^2(\mu^2) + \tau^2(\mu^3) = \mu^8 + \mu^{12}$

$= \mu^3 + \mu^2$.

Assim, $\mathbb{L}^{\langle\tau^2\rangle} = \mathbb{Q}(\mu^2 + \mu^{-2})$.

$\mu = e^{2\pi/5 i} = \cos(2\pi/5) + i \operatorname{Sen}(2\pi/5)$.

Assim, $\mu^2 + \mu^{-2} = 2\cos(4\pi/5)$.

Daí, $\mathbb{L}^{\langle\tau^2\rangle} = \mathbb{Q}(2\cos(4\pi/5))$.

(c) $x^4 - 3$. Seja $\alpha \in \mathbb{R}$ tal que $\alpha^4 = 3$. Então

$$\mathcal{R}(x^4-3) = \{\alpha, i\alpha, -\alpha, -i\alpha\}.$$

$$\mathbb{L} = \mathbb{Q}(\mathcal{R}(x^4-3)) = \mathbb{Q}(\alpha, i). \qquad [\mathbb{L}:\mathbb{Q}] = 8$$

Sejam $\sigma, \tau \in \operatorname{Aut}(\mathbb{L}/\mathbb{Q})$ tais que

$\mathbb{Q}(\alpha)(i)$
| $\operatorname{Irr}(i, \mathbb{Q}(\alpha)) = x^2+1$
$\mathbb{Q}(\alpha)$
| $\operatorname{Irr}(\alpha, \mathbb{Q}) = x^4-3$
$\mathbb{Q}$

$\sigma(\alpha) = i\alpha$, $\sigma(i) = i$,

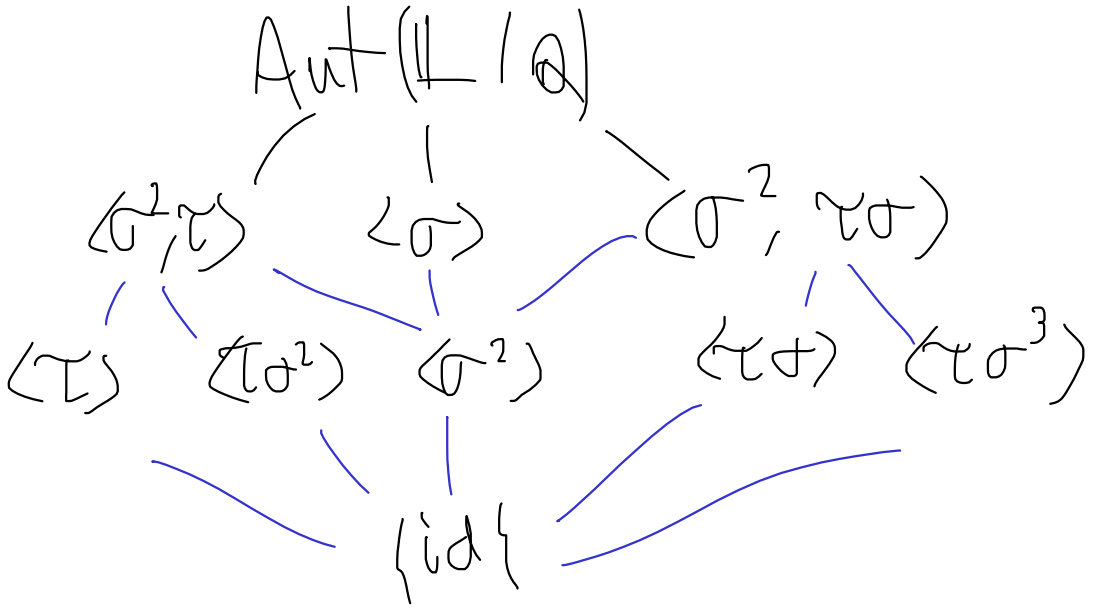
$\tau(\alpha) = \alpha$, $\tau(i) = -i$.

Além disso, $\sigma^4 = id = \tau^2$.

Ainda mais, $\sigma\tau = \sigma^{-1}\tau$. Daí, temos que

$$\operatorname{Aut}(\mathbb{L}/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = id, \sigma\tau = \sigma^{-1}\tau \rangle \cong D_4.$$

O grupo $\operatorname{Aut}(\mathbb{L}/\mathbb{Q})$ admite os seguintes subgrupos:



$L^{\langle\tau\rangle} = \mathbb{Q}(\alpha)$ $\quad L^{\langle\sigma^2\rangle} = \mathbb{Q}(\alpha^2, i)$ $\quad L^{\langle\tau\sigma\rangle} = \mathbb{Q}(\alpha - \alpha i)$

$L^{\langle\tau\sigma^3\rangle} = \mathbb{Q}(\alpha + \alpha i)$

$L^{\langle\tau\sigma^2\rangle} = \mathbb{Q}(\alpha i)$

$L^{\langle\sigma^2,\tau\rangle} = \mathbb{Q}(\alpha^2)$ $\quad L^{\langle\sigma^2,\tau\sigma\rangle} = \mathbb{Q}(\alpha^2 i)$

$L^{\langle\sigma\rangle} = \mathbb{Q}(i)$

Detalhes ficam de exercício.

Problemas:

Seja G um grupo finito.

(1) Existe $\mathbb{E}/\mathbb{F}$ gal. fin. tal que $G \cong \mathrm{Aut}(\mathbb{E}/\mathbb{F})$?

(2) Fixado corpo $\mathbb{F}$, existe ext. gal. fin. $\mathbb{E}/\mathbb{F}$ tal que $G \cong \mathrm{Aut}(\mathbb{E}/\mathbb{F})$?

(2') fixe $\mathbb{F} = \mathbb{Q}$ no anterior.