Grupos e Corpos

Prof. Lucas Calixto

Aula 12 - Teoria de Galois

Extensões normais

Uma extensão $\mathbb{F} \subset \mathbb{E}$ é chamada de extensão normal se todo $f(x) \in \mathbb{F}[x]$ irredutível que tem pelo menos uma raiz em E tem todas as raízes em $\mathbb{E}$, ou seja, $f(x)$ se decompõe como produto de fatores lineáres em $\mathbb{E}[x]$

Teorema: Seja $\mathbb{F} \subset \mathbb{E}$. As seguintes afirmações são equivalentes:

1. $\mathbb{E}$ é extensão finita, separável e normal de $\mathbb{F}$
2. $\mathbb{E}$ é o corpo de decomposição de um poli separável em $\mathbb{F}[x]$
3. $\mathbb{F} = \mathbb{E}_G$ para algum subgrupo finito $G \leq \mathrm{Aut}(\mathbb{E})$

Prova: (1) $\Rightarrow$ (2): Sabemos que $\mathbb{E} = \mathbb{F}(\alpha)$ para algum $\alpha \in \mathbb{E}$

$\mathbb{F} \subset \mathbb{E}$ separável $\Rightarrow m_\alpha(x) \in \mathbb{F}[x]$ é separável

$\mathbb{F} \subset \mathbb{E}$ normal $\Rightarrow \mathbb{E}$ é corpo de decomposição de $m_\alpha(x)$

(2) $\Rightarrow$ (3): Segue da aula passada que nesse caso $\mathbb{F} = \mathbb{E}_{G(\mathbb{E}/\mathbb{F})}$ (Teorema 23.17)

(3) $\Rightarrow$ (1): Da aula passada, temos $[\mathbb{E} : \mathbb{F}] \leq |G| < \infty \Rightarrow \mathbb{F} \subset \mathbb{E}$ é extensão finita

Seja $f(x) \in \mathbb{F}[x]$ irredutível (monico) que tem uma raiz $\alpha \in \mathbb{E} \Rightarrow f(x) = m_\alpha(x)$

$\Rightarrow \{\sigma(\alpha) \mid \sigma \in G\} = \{\alpha_1, \ldots, \alpha_n\}$ também são raízes (todas distintas, pois G é grupo) de $f(x)$. Seja $g(x) = (x - \alpha_1) \cdots (x - \alpha_n)$

Para todo $\sigma \in G$, temos $g^\sigma(x) = (x - \sigma(\alpha_1)) \cdots (x - \sigma(\alpha_n)) = g(x) \Rightarrow G$ fixa os coeficientes de $g(x) \Rightarrow g(x) \in \mathbb{F}[x]$ e $g(\alpha) = 0 \Rightarrow f(x) \mid g(x)$

$\Rightarrow g(x) = f(x)$, já que $\mathrm{gr}(g(x)) \leq \mathrm{gr}(f(x))$ e ambos não monicos. Assim, todas as raízes de $f(x)$ vivem em $\mathbb{E} \Rightarrow \mathbb{F} \subset \mathbb{E}$ é normal

O fato de $[\mathbb{E} : \mathbb{F}] < \infty$ junto com a conta acima mostra que $\mathbb{F} \subset \mathbb{E}$ é separável (o poli $m_\beta(x) \in \mathbb{F}[x]$ será separável para todo $\beta \in \mathbb{E}$) ∎

Corolário: Se $\mathbb{F} \subset \mathbb{E}$ é tal que $\mathbb{F} = \mathbb{E}_G$ para algum $G \leq \mathrm{Aut}(\mathbb{E})$, então $G = G(\mathbb{E}/\mathbb{F})$.

Prova: $\mathbb{F} = \mathbb{E}_G \Rightarrow G \leq G(\mathbb{E}/\mathbb{F})$ e $[\mathbb{E} : \mathbb{F}] = |G(\mathbb{E}/\mathbb{F})|$ pelo item (2) do teorema anterior e aula passada

Logo, $[\mathbb{E} : \mathbb{F}] \leq |G| \leq |G(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}] \Rightarrow G = G(\mathbb{E}/\mathbb{F})$ ∎

Uma extensão que satisfaz uma (e portanto todas) das condições do teorema é chamada uma extensão de Galois

Se $\mathbb{F} \subset \mathbb{E}$ é Galois e $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$, então $\mathbb{K} \subset \mathbb{E}$ é Galois (pelo item 2)

Exemplo: Considere $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}, \sqrt{5})$ como na aula passada. Temos a seguinte correspondência

$$\text{subcorpos de } \mathbb{Q}(\sqrt{3}, \sqrt{5}) \leftrightarrow \text{subgrupos de } G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$$

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{3}, \sqrt{5}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{5}) \arrow[d, dash] & \mathbb{Q}(\sqrt{15}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \{\mathrm{id}, \sigma, \tau, \mu\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{\mathrm{id}, \sigma\} \arrow[dr, dash] & \{\mathrm{id}, \tau\} \arrow[d, dash] & \{\mathrm{id}, \mu\} \arrow[dl, dash] \\
 & \{\mathrm{id}\} &
\end{tikzcd}$$

Teorema fundamental da teoria de Galois (TFTG)

Teorema (TFTG): Seja $\mathbb{F}$ um corpo finito ou de característica zero. Se $\mathbb{F} \subset \mathbb{E}$ é extensão de Galois, então as seguintes afirmações são verdadeiras:

1. Existe bijeção
$$\{\mathbb{K} \mid \mathbb{F} \subset \mathbb{K} \subset \mathbb{E}\} \leftrightarrow \{G \leq G(\mathbb{E}/\mathbb{F})\}$$
$$\mathbb{K} \mapsto G(\mathbb{E}/\mathbb{K})$$

2. Se $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$, então
$$[\mathbb{E} : \mathbb{K}] = |G(\mathbb{E}/\mathbb{K})| \quad \text{e} \quad [\mathbb{K} : \mathbb{F}] = [G(\mathbb{E}/\mathbb{F}) : G(\mathbb{E}/\mathbb{K})]$$

3.
$$\mathbb{F} \subset \mathbb{K} \subset \mathbb{L} \subset \mathbb{E} \Leftrightarrow \{\mathrm{id}\} = G(\mathbb{E}/\mathbb{E}) \subset G(\mathbb{E}/\mathbb{L}) \subset G(\mathbb{E}/\mathbb{K}) \subset G(\mathbb{E}/\mathbb{K}) \subset G(\mathbb{E}/\mathbb{F})$$

4. $\mathbb{K}$ (subcorpo de $\mathbb{E}$) é extensão de Galois de $\mathbb{F}$ se e só se $G(\mathbb{E}/\mathbb{K}) \lhd G(\mathbb{E}/\mathbb{F})$. Nesse caso, temos
$$G(\mathbb{K}/\mathbb{F}) \cong G(\mathbb{E}/\mathbb{F})/G(\mathbb{E}/\mathbb{K})$$

Prova: (1): Suponha $H = G(\mathbb{E}/\mathbb{K}) = G(\mathbb{E}/\mathbb{L}) \leq G = G(\mathbb{E}/\mathbb{F})$. Então $\mathbb{K} = \mathbb{E}_H = \mathbb{L}$ (por ambos serem extenão de Galois) $\Rightarrow$ injetividade

Seja $G \leq G(\mathbb{E}/\mathbb{F})$ e considere $\mathbb{K} = \mathbb{E}_G \Rightarrow \mathbb{K} \subset \mathbb{E}$ é Galois (pelo item 3 do teorema anterior) e obviamente $\mathbb{F} \subset \mathbb{K}$

(2): Suponha $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$

$\mathbb{K} \subset \mathbb{E}$ Galois $\Rightarrow [\mathbb{E} : \mathbb{K}] = |G(\mathbb{E}/\mathbb{K})|$. Como, $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{K}][\mathbb{K} : \mathbb{F}]$, temos

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{E} : \mathbb{F}]/[\mathbb{E} : \mathbb{K}] = |G(\mathbb{E}/\mathbb{F})|/|G(\mathbb{E}/\mathbb{K})| = [G(\mathbb{E}/\mathbb{F}) : G(\mathbb{E}/\mathbb{K})]$$

(3): Segue do item (1). Isso é descrito pelo diagrama

$$
\begin{tikzcd}[arrows=dash]
\mathbb{E} \arrow[r] \arrow[d] & \{\mathrm{id}\} \arrow[d] \\
\mathbb{L} \arrow[r] \arrow[d] & G(\mathbb{E}/\mathbb{L}) \arrow[d] \\
\mathbb{K} \arrow[r] \arrow[d] & G(\mathbb{E}/\mathbb{K}) \arrow[d] \\
\mathbb{F} \arrow[r] & G(\mathbb{E}/\mathbb{F})
\end{tikzcd}
$$

(4): ($\Rightarrow$) Seja $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$ tal que $\mathbb{F} \subset \mathbb{K}$ é Galois. Afirmamos que $G(\mathbb{E}/\mathbb{K}) \triangleleft G(\mathbb{E}/\mathbb{F})$

Tome $\sigma \in G(\mathbb{E}/\mathbb{F})$ e $\tau \in G(\mathbb{E}/\mathbb{K})$

Para $\alpha \in \mathbb{K}$, tome $f(x) \in \mathbb{F}[x]$ seu poli minimal

$f(\alpha) = 0$ e $\sigma \in G(\mathbb{E}/\mathbb{F}) \Rightarrow f(\sigma(\alpha)) = 0 \Rightarrow \sigma(\alpha) \in \mathbb{K}$ pois $\mathbb{F} \subset \mathbb{K}$ é normal

Logo, $\sigma^{-1}\tau\sigma(\alpha) = \sigma^{-1}\sigma(\alpha) = \alpha \Rightarrow \sigma^{-1}\tau\sigma \in G(\mathbb{E}/\mathbb{K}) \Rightarrow G(\mathbb{E}/\mathbb{K}) \lhd G(\mathbb{E}/\mathbb{F})$

$(\Leftarrow)$: Suponha $G(\mathbb{E}/\mathbb{K}) \lhd G(\mathbb{E}/\mathbb{F})$. Vamos ver que $\mathbb{F} = \mathbb{E}_{G(\mathbb{K}/\mathbb{F})}$ e portanto que $\mathbb{F} \subset \mathbb{K}$ é Galois

Se $\sigma \in G(\mathbb{E}/\mathbb{F})$, então $\sigma_{\mathbb{K}} : \sigma|_{\mathbb{K}} \in G(\mathbb{K}/\mathbb{F})$. De fato, basta provar que $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{K}$ faz sentido, ou seja, que $\sigma_{\mathbb{K}}(\mathbb{K}) \subset \mathbb{K}$ (pq?)

Seja $\tau \in G(\mathbb{E}/\mathbb{K})$

$G(\mathbb{E}/\mathbb{K}) \lhd G(\mathbb{E}/\mathbb{F}) \Rightarrow \exists \tau' \in G(\mathbb{E}/\mathbb{K})$ tal que $\tau\sigma = \sigma\tau'$. Logo, se $\alpha \in \mathbb{K}$, temos

$$\tau(\sigma(\alpha)) = \sigma(\tau'(\alpha)) = \sigma(\alpha) \Rightarrow \sigma(\alpha) \subset \mathbb{E}_{G(\mathbb{E}/\mathbb{K})} = \mathbb{K}, \quad \text{pois } \mathbb{K} \subset \mathbb{E} \text{ é Galois}$$

$\Rightarrow \sigma_{\mathbb{K}} \in G(\mathbb{K}/\mathbb{F})$

Afirmamos que $\mathbb{F} = \mathbb{K}_{G(\mathbb{K}/\mathbb{F})}$. Óbvio que $\mathbb{F} \subset \mathbb{K}_{G(\mathbb{K}/\mathbb{F})}$. Por outro lado, se $\beta \in \mathbb{K}_{G(\mathbb{K}/\mathbb{F})}$

$\Rightarrow \beta = \sigma_{\mathbb{K}}(\beta) = \sigma(\beta) \Rightarrow \beta \in \mathbb{E}_{G(\mathbb{E}/\mathbb{F})} = \mathbb{F} \Rightarrow \mathbb{F} = \mathbb{K}_{G(\mathbb{K}/\mathbb{F})} \Rightarrow \mathbb{F} \subset \mathbb{K}$ é Galois (pelo item 3 do teorema anterior)

Por fim, a função $\varphi : G(\mathbb{E}/\mathbb{F}) \to G(\mathbb{K}/\mathbb{F})$, $\varphi(\sigma) = \sigma_{\mathbb{K}}$ define um homomorfismo de grupos (verifique)

Note:

$$\ker \varphi = \{\sigma \in G(\mathbb{E}/\mathbb{F}) \mid \sigma_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}\} = G(\mathbb{E}/\mathbb{K})$$

Além disso, por 1ºTI e por (2), temos

$$|\operatorname{im} \varphi| = |G(\mathbb{E}/\mathbb{F})/G(\mathbb{E}/\mathbb{K})| = [\mathbb{K} : \mathbb{F}] = |G(\mathbb{K}/\mathbb{F})| \quad (\text{pois } \mathbb{F} \subset \mathbb{E} \text{ é Galois})$$

Logo, φ é sobrejetiva, e segue

$$G(\mathbb{E}/\mathbb{F})/G(\mathbb{E}/\mathbb{K}) \cong G(\mathbb{K}/\mathbb{F})$$

■

Exemplo: Tome $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. O corpo de fatoração de $f(x)$ é $\mathbb{Q}(\sqrt[4]{2}, i)$ (as raízes são $\pm\sqrt[4]{2}$ e $\pm i\sqrt[4]{2}$)

Como $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ (raiz de $x^4 - 2$) e $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$ (raiz de $x^2 + 1$), temos $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$. Sabemos que uma base de $\mathbb{Q}(\sqrt[4]{2}, i)$ sobre $\mathbb{Q}$ é

$$\{1, \sqrt[4]{2}, (\sqrt[4]{2})^2, (\sqrt[4]{2})^3, i, i\sqrt[4]{2}, i(\sqrt[4]{2})^2, i(\sqrt[4]{2})^3\}$$

Como a extensão $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}, i)$ é Galois, temos que $|G = G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})| = 8$

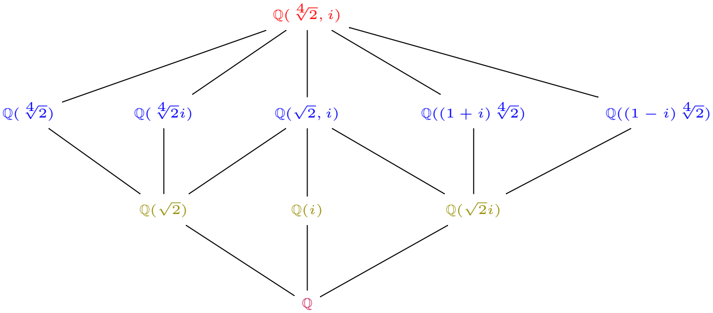
Vamos determinar G. Tome $\sigma \in G$ tal que $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ e $\sigma(i) = i$

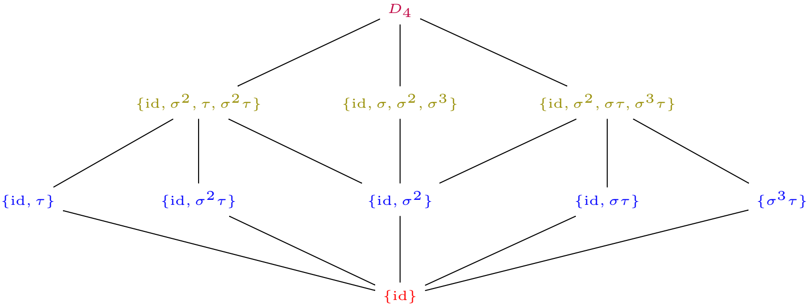
Tome também $\tau \in G$ tal que $\tau(i) = -i$

Veja que $G = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$ (por quantidade de elementos)

Pelas relações ($\sigma^4 = \mathrm{id}$, $\tau^2 = \mathrm{id}$, $\tau\sigma\tau = \sigma^{-1}$), vemos que $G \cong D_4$

Os reticulados são:


$\mathbb{Q}(\sqrt[4]{2}, i)$
$\mathbb{Q}(\sqrt[4]{2})$
$\mathbb{Q}(\sqrt[4]{2}i)$
$\mathbb{Q}(\sqrt{2}, i)$
$\mathbb{Q}((1+i)\sqrt[4]{2})$
$\mathbb{Q}((1-i)\sqrt[4]{2})$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Q}(i)$
$\mathbb{Q}(\sqrt{2}i)$
$\mathbb{Q}$


D_4
$\{\mathrm{id}, \sigma^2, \tau, \sigma^2\tau\}$
$\{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$
$\{\mathrm{id}, \sigma^2, \sigma\tau, \sigma^3\tau\}$
$\{\mathrm{id}, \tau\}$
$\{\mathrm{id}, \sigma^2\tau\}$
$\{\mathrm{id}, \sigma^2\}$
$\{\mathrm{id}, \sigma\tau\}$
$\{\sigma^3\tau\}$
$\{\mathrm{id}\}$

Solubilidade por radicais

Assumiremos que os corpos são de caracteristica zero $\Rightarrow$ polis irredutíveis são separáveis

Votemos ao problema de dizer quando um poli é solúvel por radicais

Diremos que uma extensão $\mathbb{F} \subset \mathbb{E}$ é uma extensão por radicais se existe uma cadeia

$$\mathbb{F} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_{n-1} \subset \mathbb{F}_n = \mathbb{E}$$

tal que $\mathbb{F}_i = \mathbb{F}_{i-1}(\alpha_i)$ e $\alpha_i^{n_i} \in \mathbb{F}_{i-1}$ para algum $n_i \in \mathbb{N}$

Um poli $f(x) \in \mathbb{F}[x]$ é solúvel por radicais se seu corpo de fatoração for uma extensão por radicais sobre $\mathbb{F}$. Pense por que essa definição é equivalente à do início

Exemplo: O poli $x^n - 1 \in \mathbb{Q}[x]$ é solúvel por radicais. De fato, as raízes desse poli são $1, w, w^2, \dots, w^{n-1}$, onde $w = e^{\frac{2i\pi}{n}}$. Logo, o corpo de fatoração é $\mathbb{Q}(w)$ e $\mathbb{Q} \subset \mathbb{Q}(w)$ é extensão por radicais, já que $w^n \in \mathbb{Q}$

Lembre: um grupo G é solúvel se existe série subnormal

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \subset H_0 = \{e\}$$

tal que H_i/H_{i-1} é abeliano

Veremos que $f(x) \in \mathbb{F}[x]$ é solúvel por radicais se e só se seu grupo de Galois é solúvel

Lema 1: Se $\operatorname{car} \mathbb{F} = 0$ e $\mathbb{E}$ é o corpo de fatoração de $x^n - a \in \mathbb{F}[x]$, então o grupo de Galois $G(\mathbb{E}/\mathbb{F})$ é solúvel

Lema 2: Suponha que $\operatorname{car} \mathbb{F} = 0$ e que

$$\mathbb{F} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_{n-1} \subset \mathbb{F}_n = \mathbb{E}$$

é extensão por radicais. Então existe uma extensão de Galois por radicais

$$\mathbb{F} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_{n-1} \subset \mathbb{K}_n = \mathbb{K}$$

tal que $\mathbb{E} \subset \mathbb{K}$ e cada $\mathbb{K}_i$ é Galois sobre $\mathbb{K}_{i-1}$

Teorema: Seja $f(x) \in \mathbb{F}[x]$, onde $\operatorname{car} \mathbb{F} = 0$. Se $f(x)$ é solúvel por radicais, então seu grupo de Galois é solúvel

Prova: Tome $\mathbb{E}$ o corpo de decomposição de $f(x)$ e

$$\mathbb{F} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \cdots \subset \mathbb{F}_{n-1} \subset \mathbb{F}_n = \mathbb{E}$$

uma extensão por radicais, onde $\mathbb{F}_i = \mathbb{F}_{i-1}(\alpha_i)$ com $\alpha_i^{n_i} \in \mathbb{F}_{i-1}$. Lema 2 $\Rightarrow$ podemos assumir que $\mathbb{F}_i$ é Galois sobre $\mathbb{F}_{i-1}$

Pelo TFTG, temos uma série subnormal

$$G(\mathbb{E}/\mathbb{F}) \supset G(\mathbb{E}/\mathbb{F}_1) \supset \cdots \supset G(\mathbb{E}/\mathbb{F}_{n-1}) \supset G(\mathbb{E}/\mathbb{E}) = \{\mathrm{id}\},$$

onde $G(\mathbb{E}/\mathbb{F}_{i-1})/G(\mathbb{E}/\mathbb{F}_i) \cong G(\mathbb{F}_i/\mathbb{F}_{i-1})$

$\mathbb{F}_i$ é corpo de fatoração de $x - \alpha_i^{n_i} \in \mathbb{F}_{i-1}[x] \Rightarrow G(\mathbb{F}_{i-1}/\mathbb{F}_i)$ é solúvel, pelo Lema 2

Insolubilidade dos quinticos

Vamos ver que existem polis de grau 5 que não são solúveis por radicais

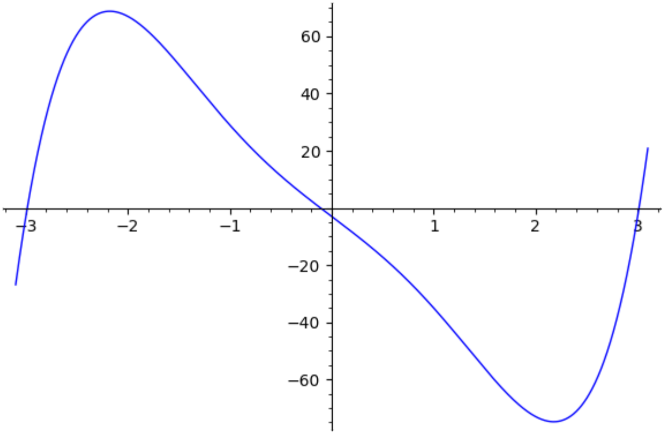
Lema: Se p é primo, então todo subgrupo de S_p que contem uma transposição e um ciclo de comprimento p deve ser igual a S_p

Exemplo: Vamos ver que $f(x) = x^5 - 6x^3 - 27x - 3 \in \mathbb{Q}[x]$ não é solúvel por radicais

Eisenstein $\Rightarrow f(x)$ é irredutível $\Rightarrow f(x)$ é separável, pois $\operatorname{car} \mathbb{Q} = 0$

$f'(x) = 5x^4 - 18x^2 - 27$. Logo, $f'(x) = 0 \Leftrightarrow x = \pm\sqrt{\frac{6\sqrt{6}+9}{5}} \Rightarrow f(x)$ possui no máximo um ponto de máximo e um ponto de mínimo

$f(x)$ troca de sinal em $[-3,-2]$, $[-2,0]$, e em $[0,4] \Rightarrow$ os pontos críticos de $f(x)$ estão nesses intervalos e portanto $f(x)$ tem 3 raízes reais e 2 complexas (que são conjugadas uma da outra). Sejam elas $R = \{r_1, r_2, r_3, c_1, c_2\}$



Seja $\mathbb{E} = \mathbb{Q}(r_1, r_2, r_3, c_1, c_2) \subset \mathbb{C}$ o corpo de decomposição de $f(x)$

Lembrem: todo $\sigma \in G(\mathbb{E}/\mathbb{Q})$ é completamente determinado por sua restrição a $R \Rightarrow G(\mathbb{E}/\mathbb{Q}) \leq X_R = S_5$

Note que a função conjugação complexa $z = a + bi \mapsto \bar{z} = a - bi$ (na verdade sua restrição a $\mathbb{E}$) pertence a $G(\mathbb{E}/\mathbb{Q}) \Rightarrow$ $G(\mathbb{E}/\mathbb{Q})$ contem uma transposição

Por outro lado, $[\mathbb{Q}(r_1) : \mathbb{Q}] = 5 \Rightarrow [\mathbb{E} : \mathbb{Q}]$ é divisível por 5, pois $\mathbb{Q} \subset \mathbb{Q}(r_1) \subset \mathbb{E}$

Como $|G(\mathbb{E}/\mathbb{Q})| = [\mathbb{E} : \mathbb{Q}]$ é divisível por 5, e $G(\mathbb{E}/\mathbb{Q}) \leq S_5$ ($|S_5| = 5!$) $\Rightarrow G(\mathbb{E}/\mathbb{Q})$ tem 5-subgrupo de Sylow de ordem $5 \Rightarrow G(\mathbb{E}/\mathbb{Q})$ tem subgrupo cíclico de ordem $5 \Rightarrow$ $G(\mathbb{E}/\mathbb{Q})$ tem ciclo de comprimento 5 (lembrem: se $\tau = \tau_1 \cdots \tau_k$ é produto de cíclos disjuntos, então $|\tau| = mmc(|\tau_1|, \ldots, |\tau_k|)$. Em S_5 as únicas ordens possíveis de elementos são $1, 2, 3, 4, 5, 6$, o último sendo produto de um 2-ciclo com um 3-ciclo)

Lema anterior $\Rightarrow G(\mathbb{E}/\mathbb{Q}) = S_5$, que não é solúvel (já vimos isso antes)

Logo, $f(x)$ não é solúvel por radicais