(6) Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana tal que $[\mathbb{E} : \mathbb{F}] = p^2q$, em que p e q são primos, $q < p$ e q não divide $p^2 - 1$. Mostre que:
   (a) Existem subcorpos intermediários $\mathbb{K}_1, \mathbb{K}_2$, tais que $\mathbb{K}_1/\mathbb{F}$ e $\mathbb{K}_2/\mathbb{F}$ são galoisianas, $[\mathbb{K}_1 : \mathbb{F}] = p^2$ e $[\mathbb{K}_2 : \mathbb{F}] = q$.
   (b) Prove que $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é abeliano.

(17) Fixe $n \in \mathbb{N}$, e seja $\mathbb{E} = \mathbb{Q}(X_1, \ldots, X_n)$. Para cada $\pi \in \mathcal{S}_n$, defina $\pi : \mathbb{E} \to \mathbb{E}$ via $\pi(X_i) = X_{\pi(i)}$.
   (a) Prove que π está bem definida, e que $\pi \in \mathrm{Aut}(\mathbb{E})$. Portanto, temos um mapa $\mathcal{S}_n \to \mathrm{Aut}(\mathbb{E})$.
   (b) Prove que o mapa $\mathcal{S}_n \to \mathrm{Aut}(\mathbb{E})$ é injetiva. Portanto, podemos identificar $\mathcal{S}_n \subseteq \mathrm{Aut}(\mathbb{E})$.
   (c) Conclua que, se $\mathbb{F} = \mathbb{E}^{\mathcal{S}_n}$, então $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) \cong \mathcal{S}_n$. Conclua que, para todo grupo finito G, existe uma extensão de corpos galoisiana finita $\mathbb{L}/\mathbb{K}$ tal que $G \cong \mathrm{Aut}(\mathbb{L}/\mathbb{K})$.

(18) Seja $p \geq 5$ um número primo e $f(X) \in \mathbb{Q}[X]$ irredutível de grau p. Assuma que f tenha exatamente duas raízes não reais em $\mathbb{C}$. Seja $\mathbb{L}$ o corpo de raízes de f sobre $\mathbb{Q}$. Prove que $\mathrm{Aut}(\mathbb{L}/\mathbb{Q}) \cong \mathcal{S}_p$. Conclua que f não é solúvel por radicais.

(18) Seja $p \geq 5$ um número primo e $f(X) \in \mathbb{Q}[X]$ irredutível de grau p. Assuma que f tenha exatamente duas raízes não reais em $\mathbb{C}$. Seja $\mathbb{L}$ o corpo de raízes de f sobre $\mathbb{Q}$. Prove que $\mathrm{Aut}(\mathbb{L}/\mathbb{Q}) \cong S_p$. Conclua que f não é solúvel por radicais.

Lema. Seja p um número primo. Sejam $\tau, \sigma \in S_p$ uma transposição e um p-ciclo. Então τ e σ geram S_p.

Dem.: Renomeando os índices, se necessário, podemos assumir que $\tau = (1\ 2)$. Escreva $\sigma = (1\ j_2 \cdots j_p)$. As potências de σ continuam sendo p-ciclos, e então existe i tal que $\sigma^i = (1\ 2\ j_3 \cdots j_p)$. Daí, a menos de renomear índices, podemos assumir que

$$\tau = (1\ 2), \text{ e } \sigma_0 := \sigma^i = (1\ 2\ 3 \cdots p).$$

Daí

$$\sigma_0^j \tau \sigma_0^{-j} = \left(\sigma_0^j(1)\ \ \sigma_0^j(2)\right) = (j\ \ j+1).$$

Daí $\langle \tau, \sigma \rangle \ni (1\,2), (2\,3), \ldots, (p-1\ p) \Rightarrow \langle \tau, \sigma \rangle = S_p$. □

Seja f um polinômio de grau p, irredutível em $\mathbb{Q}[X]$, com duas raízes não reais. Denote $R(f) = \{\alpha_1, \ldots, \alpha_{p-2}, \beta_1, \beta_2\}$, em que $\alpha_1, \ldots, \alpha_{p-2} \in \mathbb{R}$, e $\beta_1, \beta_2 \notin \mathbb{R}$. Seja

$$G = \mathrm{Aut}(\mathbb{Q}(R(f))/\mathbb{Q}).$$

Vimos que podemos identificar $G \subseteq S_p$. Temos também que

$$p = \mathrm{gr}\, f = [\mathbb{Q}(\alpha_1) : \mathbb{Q}] \mid [\mathbb{L} : \mathbb{Q}] = |G|.$$

Da teoria de grupos, como $p \mid |G|$, existe $\sigma \in G$ de ordem p. Assim, na identificação $\sigma \in G \subseteq S_p$, σ é um p-ciclo.

Seja $\tau : \mathbb{L} \to \mathbb{L}$ a conjugação complexa. Sendo τ um $\mathbb{Q}$-automorfismo, e $\mathbb{L}/\mathbb{Q}$ normal, segue que $\tau \in Aut(\mathbb{L}/\mathbb{Q})$.

Note que $\tau(\alpha_i) = \alpha_i$, e $\tau(\beta_1) \neq \beta_1$. Então $\tau(\beta_1) = \beta_2$.

Portanto, na nossa identificação $\tau \in G \subseteq S_p$, τ é uma transposição (que permuta β_1 e β_2). Daí G contém uma transposição τ e um p-ciclo σ. Do lema anterior, segue que $G = S_p$.

Por fim, como $p \geq 5$, S_p não é solúvel. Portanto, f não é solúvel por radicais.

Exemplo. Seja

$$f(X) = (X^2+2)(X-2)X(X+2) - 2 = X^5 - 2X^3 - 8X - 2.$$

Por critério de Eisenstein, f é irredutível em $\mathbb{Q}[X]$.

Além disso, f possui exatamente 3 raízes reais (verifique).

Portanto, $G_f \cong S_5$ não é solúvel.

(17) Fixe $n \in \mathbb{N}$, e seja $\mathbb{E} = \mathbb{Q}(X_1, \ldots, X_n)$. Para cada $\pi \in \mathcal{S}_n$, defina $\pi : \mathbb{E} \to \mathbb{E}$ via $\pi(X_i) = X_{\pi(i)}$.
(a) Prove que π está bem definida, e que $\pi \in \mathrm{Aut}(\mathbb{E})$. Portanto, temos um mapa $\mathcal{S}_n \to \mathrm{Aut}(\mathbb{E})$.
(b) Prove que o mapa $\mathcal{S}_n \to \mathrm{Aut}(\mathbb{E})$ é injetiva. Portanto, podemos identificar $\mathcal{S}_n \subseteq \mathrm{Aut}(\mathbb{E})$.
(c) Conclua que, se $\mathbb{F} = \mathbb{E}^{\mathcal{S}_n}$, então $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) \cong \mathcal{S}_n$. Conclua que, para todo grupo finito G, existe uma extensão de corpos galoisiana finita $\mathbb{L}/\mathbb{K}$ tal que $G \cong \mathrm{Aut}(\mathbb{L}/\mathbb{K})$.

(a) Seja $\mathcal{R} = \mathbb{Q}[X_1, \ldots, X_n]$. Então $\mathbb{E}$ é o corpo de frações de $\mathcal{R}$. Assim, dado $\pi \in S_n$, defina o homomorfismo de anéis

$$\pi : \mathcal{R} \longrightarrow \mathbb{E}$$

tal que $\pi(X_i) = X_{\pi(i)}$. Note que se $f(X_1, \ldots, X_n) \in \mathcal{R}$, então

$$\pi\left(f(X_1, \ldots, X_n)\right) = f\left(X_{\pi 1}, \ldots, X_{\pi(n)}\right) \in \mathcal{R} \subseteq \mathbb{E}.$$

Ainda, se $\sigma \in S_n$, então

$$\sigma\left(\pi\left(f(X_1, \ldots, X_n)\right)\right) = f\left(X_{\sigma\pi 1}, \ldots, X_{\sigma\pi(n)}\right) = (\sigma \circ \pi)\left(f(X_1, \ldots, X_n)\right)$$

Por fim, se $\ker \pi = 0$, então π admite uma única extensão $\pi : \mathbb{E} \longrightarrow \mathbb{E}$. Assuma que $f \in \ker \pi$. Então $\pi^{-1} \in S_n \Rightarrow \pi^{-1} : \mathcal{R} \to \mathbb{E}$

$$0 = \pi^{-1}\left(\pi\left(f(X_1, \ldots, X_n)\right)\right) = f(X_1, \ldots, X_n).$$

Assim $\ker \pi = 0$, e daí, existe extensão única $\pi : \mathbb{E} \to \mathbb{E}$.

Temos que $\pi : \mathbb{E} \longrightarrow \mathbb{E}$ é automorfismo, pois sua inversa é o homomorfismo $\mathbb{E} \longrightarrow \mathbb{E}$ definido por $\pi^{-1} \in S_n$. Segue que $\pi \in \mathrm{Aut}(\mathbb{E})$. Ou seja, temos um homomorfismo de grupos $S_n \longrightarrow \mathrm{Aut}(\mathbb{E})$.

(b) Assuma que $\sigma \in S_n$ é tal que $\sigma \mapsto id_E \in Aut(\mathbb{E})$.
Então, $\forall i \in \{1,\dots,n\}$, temos que

$$X_i = \sigma(X_i) = X_{\sigma(i)} \Rightarrow \sigma(i) = i, \ \forall i.$$

Daí, $\sigma = 1 \in S_n$. Portanto, podemos identificar $S_n \subseteq Aut(\mathbb{E})$.

(c) Do Teorema de Artin, $Aut(\mathbb{E}/\mathbb{E}^{S_n}) = S_n$.

Por fim, seja G um grupo finito de ordem n. Sabe-se que podemos identificar $G \subseteq S_n$. Seja $\mathbb{K} = \mathbb{E}^G$. Então, do Teorema de Artin, $\mathbb{E}/\mathbb{E}^G$ é galoisiana finita, e

$$Aut(\mathbb{E}/\mathbb{E}^G) \cong G.$$

(6) Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana tal que $[\mathbb{E} : \mathbb{F}] = p^2q$, em que p e q são primos, $q < p$ e q não divide $p^2 - 1$. Mostre que:

(a) Existem subcorpos intermediários $\mathbb{K}_1, \mathbb{K}_2$, tais que $\mathbb{K}_1/\mathbb{F}$ e $\mathbb{K}_2/\mathbb{F}$ são galoisianas, $[\mathbb{K}_1 : \mathbb{F}] = p^2$ e $[\mathbb{K}_2 : \mathbb{F}] = q$.

(b) Prove que $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é abeliano.

Relembre os Teoremas de Sylow:

Teorema. Sejam p um primo e G um grupo de ordem $p^n \cdot m$, em que p não divide m. Então:

(i) Existe um subgrupo $H \leq G$ com $|H| = p^n$ (denominado de p-subgrupo de Sylow).

(ii) Seja n_p o número de p-subgrupos de Sylow de G. Então $n_p \mid m$ e $n_p \equiv 1 \pmod p$.

(iii) Seja H um p-subgrupo de Sylow. Então $n_p = 1$ se, e só se, $H \lhd G$.

(a) Seja $G = \mathrm{Aut}(\mathbb{E}/\mathbb{F})$. Então G tem ordem p^2q. Sejam H_p um p-subgrupo de Sylow, e H_q um q-subgrupo de Sylow. Sejam n_p e n_q o número de p-subgrupos de Sylow, e de q-subgrupos de Sylow, respectivamente.

Sabe-se que $n_p \equiv 1 \pmod p$ e $n_p \mid q$. Então, $n_p = 1 + kp$, e $n_p \leq q$. Sendo $q < p$, segue que $n_p = 1$. Portanto, H_p é um subgrupo normal. Seja $\mathbb{K}_2 = \mathbb{E}^{H_p}$. Então, $\mathbb{K}_2/\mathbb{F}$ é galoisiana, e $[\mathbb{K}_2 : \mathbb{F}] = [G : H_p] = q$.

Sabe-se que $n_q \equiv 1 \pmod q$ e $n_q \mid p^2$. Daí $n_q \in \{1, p, p^2\}$.

Se $n_q = p$, então

$$1 \equiv n_q \equiv p \pmod q \Rightarrow q \mid (p-1) \Rightarrow$$
$$\Rightarrow q \mid (p-1)\cdot(p+1) = q \mid p^2 - 1,$$ contradizendo a hipótese.

Se $n_q = p^2$, então

$$1 \equiv n_q \equiv p^2 \pmod q \Rightarrow q \mid p^2 - 1,$$ absurdo.

Portanto, $n_q = 1$. Daí $H_q \trianglelefteq G$. Assim se $\mathbb{K}_1 = \mathbb{E}^{H_q}$, então $\mathbb{K}_1/\mathbb{F}$ é galoisiana, e $[\mathbb{K}_1 : \mathbb{F}] = [G : H_q] = p^2$.

(b) Provemos que $\mathbb{K}_1 \cdot \mathbb{K}_2 = \mathbb{E}$. Temos que

$$q = [\mathbb{K}_1 : \mathbb{F}] \,/\, [\mathbb{K}_1 \cdot \mathbb{K}_2 : \mathbb{F}] \Rightarrow qp^2 / [\mathbb{K}_1 \mathbb{K}_2 : \mathbb{F}].$$
$$p^2 = [\mathbb{K}_2 : \mathbb{F}] \,/\, [\mathbb{K}_1 \cdot \mathbb{K}_2 : \mathbb{F}]$$

Como $[\mathbb{K}_1 \cdot \mathbb{K}_2 : \mathbb{F}] \leq [\mathbb{E} : \mathbb{F}] = p^2 q$, segue que $[\mathbb{K}_1 \cdot \mathbb{K}_2 : \mathbb{F}] = p^2 q$. Daí $\mathbb{E} = \mathbb{K}_1 \cdot \mathbb{K}_2$. Vimos então, que existe um homomorfismo de grupos injetor

$$\mathrm{Aut}(\mathbb{K}_1 \cdot \mathbb{K}_2 / \mathbb{F}) \longrightarrow \mathrm{Aut}(\mathbb{K}_1/\mathbb{F}) \times \mathrm{Aut}(\mathbb{K}_2/\mathbb{F}).$$

Como $|\mathrm{Aut}(\mathbb{K}_2/\mathbb{F})| = q$, temos que $\mathrm{Aut}(\mathbb{K}_2/\mathbb{F})$ é cíclico (e portanto é abeliano). Temos que $|\mathrm{Aut}(\mathbb{K}_1/\mathbb{F})| = p^2$, e da teoria de grupos, sabe-se então que $\mathrm{Aut}(\mathbb{K}_1/\mathbb{F})$ é abeliano.

Portanto, $Aut(K_1/F) \times Aut(K_2/F)$ é abeliano. Conclui-se que $Aut(E/F) = Aut(K_1 \cdot K_2/F)$ é abeliano (pois é isomorfo a um subgrupo de um grupo abeliano).