8. Teorema Fundamental da Teoria de Galois

Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos, e identifique $\mathbb{F}$ como um subcorpo de $\mathbb{E}$. Relembre que denotamos por $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ como sendo o conjunto dos $\mathbb{F}$-automorfismos de $\mathbb{E}$. Defina $\mathcal{K}$ como o conjunto dos corpos intermediários entre $\mathbb{F}$ e $\mathbb{E}$. Seja $\mathcal{G}$ o conjunto dos subgrupos de $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$. Mais precisamente:

$$\mathcal{K} = \{\mathbb{K} \text{ corpo} \mid \mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}\},$$
$$\mathcal{G} = \{H \subseteq \mathrm{Aut}(\mathbb{E}/\mathbb{F}) \text{ subgrupo}\}.$$

Temos duas funções entre esses conjuntos:

(1) $\mathcal{K} \to \mathcal{G}$, em que $\mathbb{K} \mapsto \mathrm{Aut}(\mathbb{E}/\mathbb{K}) = \{\sigma \in \mathrm{Aut}(\mathbb{E}) \mid \sigma(\ell) = \ell, \forall \ell \in \mathbb{K}\}$, o conjunto dos $\mathbb{K}$-automorfismos de $\mathbb{E}$,
(2) $\mathcal{G} \to \mathcal{K}$, em que $H \mapsto \mathbb{E}^H := \{a \in \mathbb{E} \mid \sigma(a) = a, \forall \sigma \in H\}$, o *corpo fixo* do subgrupo H.

O objetivo desta seção é estudar as funções definidas acima. Um tal par de mapas é denominado de *conexão de Galois*. O resultado principal é o seguinte: se a extensão $\mathbb{E}/\mathbb{F}$ é galoisiana e finita, então obtemos uma *correspondência de Galois*, isto é, as funções acima são bijeções, e uma é a inversa da outra. Relembre que uma extensão de corpos é dita ser galoisiana se a mesma é separável e normal.

Lema 8.1. *Os mapas definidos acima invertem inclusão. Além disso, sejam $\mathbb{K} \in \mathcal{K}$ e $H \in \mathcal{G}$. Então $\mathbb{K} \subseteq \mathbb{E}^{\mathrm{Aut}(\mathbb{E}/\mathbb{K})}$, e $H \subseteq \mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)$.*

Demonstração. Exercício. □

Teorema 8.2 (Artin)**.** *Seja $H \in \mathcal{G}$ um grupo finito. Então $\mathbb{E}/\mathbb{E}^H$ é uma extensão galoisiana finita. Além disso, $H = \mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)$.*

Demonstração. Seja $a \in \mathbb{E}$, e defina $C_a = \{\sigma(a) \mid \sigma \in H\}$. Temos que $|C_a| \leq |H|$ (pode ocorrer de $\sigma a = \sigma' a$, com $\sigma \neq \sigma'$). Note que cada $\sigma \in H$ induz uma bijeção $\sigma : C_a \to C_a$. Defina o polinômio

$$f_a(X) := \prod_{b \in C_a} (X - b).$$

Para cada $\sigma \in H$, vale que

$$f_a^\sigma = \prod_{b \in C_a} (X - \sigma b) = f_a.$$

Daí, $f_a \in \mathbb{E}^H[X]$. Além disso, por construção, as raízes de f_a são distintas. Portanto, como $f_a(a) = 0$, segue que a é separável sobre $\mathbb{E}^H$. Assim, $\mathbb{E}/\mathbb{E}^H$ é separável. Mais ainda, vale que

$$[\mathbb{E}^H(a) : \mathbb{E}] = \mathrm{gr}(\mathrm{Irr}(a, \mathbb{E}^H)) \leq \mathrm{gr}(f_a) = |C_a| \leq |H|. \tag{8.1}$$

Agora,

$$\mathscr{R}(\mathrm{Irr}(a, \mathbb{E}^H)) \subseteq \mathscr{R}(f_a) = C_a \subseteq \mathbb{E}.$$

Portanto, $\mathbb{E}/\mathbb{E}^H$ é uma extensão normal.

Provemos agora que $[\mathbb{E} : \mathbb{E}^H] \leq |H|$. Assuma que existam $a_1, \ldots, a_s \in \mathbb{E}$, que são $\mathbb{E}^H$-linearmente independentes, com $s > |H|$. Então $\mathbb{L} := \mathbb{E}^H(a_1, \ldots, a_s)$ é uma extensão finita de $\mathbb{E}^H$ tal que $[\mathbb{L} : \mathbb{E}^H] > |H|$. Como $a_1, \ldots, a_s$ são separáveis

sobre $\mathbb{E}^H$, segue que $\mathbb{L}/\mathbb{F}$ é separável. Portanto, do Teorema do Elemento Primitivo (Corolário 7.15.(i)), existe $b \in \mathbb{L}$ de modo que $\mathbb{L} = \mathbb{E}^H(b)$. De (8.1), segue que

$$|H| < [\mathbb{L} : \mathbb{E}^H] = [\mathbb{E}^H(b) : \mathbb{E}^H] \leq |H|,$$

uma contradição. Portanto, $\mathbb{E}/\mathbb{E}^H$ é finita, e $[\mathbb{E} : \mathbb{E}^H] \leq |H|$.

Para concluir, note primeiro que, por construção, $H \subseteq \mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)$. Ainda, como $\mathbb{E}/\mathbb{E}^H$ é normal e separável, do Corolário 7.9, vale que $|\mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)| = [\mathbb{E} : \mathbb{E}^H]$. Assim, $|H| \leq |\mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)| = [\mathbb{E} : \mathbb{E}^H] \leq |H|$. Concluímos que $H = \mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)$. □

Corolário 8.3. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana e finita. Então $\mathbb{E}^{\mathrm{Aut}(\mathbb{E}/\mathbb{F})} = \mathbb{F}$.*

Demonstração. Seja $\mathbb{F}' = \mathbb{E}^{\mathrm{Aut}(\mathbb{E}/\mathbb{F})}$. Então, por construção, $\mathbb{F} \subseteq \mathbb{F}'$. Do teorema anterior, temos que

$$[\mathbb{E} : \mathbb{F}'] = |\mathrm{Aut}(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{F}'][\mathbb{F}' : \mathbb{F}].$$

Portanto, $[\mathbb{F}' : \mathbb{F}] = 1$, ou seja, $\mathbb{F}' = \mathbb{F}$. □

Exemplo 8.1. O corolário anterior não é válido se a extensão $\mathbb{E}/\mathbb{F}$ não é galoisiana. Lembre-se que $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$. Portanto,

$$\mathbb{Q}(\sqrt[3]{2})^{\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})} = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}.$$

Precisaremos, num futuro, da seguinte caracterização de extensões galoisianas finitas:

Proposição 8.4. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos. As seguintes afirmações são equivalentes:*

(i) *$\mathbb{E}/\mathbb{F}$ é uma extensão galoisiana finita,*
(ii) *$\mathbb{F} = \mathbb{E}^H$, para algum subgrupo finito $H \subseteq \mathrm{Aut}(\mathbb{E})$,*
(iii) *$\mathbb{E}$ é o corpo de raízes, sobre $\mathbb{F}$, de um polinômio separável $f \in \mathbb{F}[X]$.*

Demonstração. (i)⇒(ii): Pelo corolário anterior, basta tomar $H = \mathrm{Aut}(\mathbb{E}/\mathbb{F})$.
(ii)⇒(iii): do Teorema de Artin (Teorema 8.2), segue que $\mathbb{E}/\mathbb{F}$ é galoisiana e finita. Pelo Teorema do Elemento Primitivo (Corolário 7.15.(i)), existe $a \in \mathbb{E}$ tal que $\mathbb{E} = \mathbb{F}(a)$. Como $\mathbb{E}/\mathbb{F}$ é separável, segue que $\mathrm{Irr}(a, \mathbb{F})$ é um polinômio separável. Como $\mathbb{E}/\mathbb{F}$ é normal, $\mathbb{E}$ contém todas as raízes de $\mathrm{Irr}(a, \mathbb{F})$. Portanto, $\mathbb{E} = \mathbb{F}(a) \subseteq \mathbb{F}(\mathscr{R}(\mathrm{Irr}(a, \mathbb{F}))) \subseteq \mathbb{E}$. Segue que $\mathbb{E}$ é o corpo de raízes do polinômio separável $\mathrm{Irr}(a, \mathbb{F})$ sobre $\mathbb{F}$.
(iii)⇒(i): Sejam $a_1, \ldots, a_s$ as raízes de f. Então $\mathbb{E} = \mathbb{F}(a_1, \ldots, a_s)$ é uma extensão finita de $\mathbb{F}$. Como $\mathbb{E}$ é o corpo de raízes de f sobre $\mathbb{F}$, segue que $\mathbb{E}/\mathbb{F}$ é normal. Como cada a_i é raiz de um polinômio separável (o próprio f), segue que a_i é separável sobre $\mathbb{F}$. Portanto, $\mathbb{E}/\mathbb{F}$ é uma extensão separável. Assim, $\mathbb{E}/\mathbb{F}$ é galoisiana e finita. □

Lema 8.5. *Sejam $H \subseteq \mathrm{Aut}(\mathbb{E}/\mathbb{F})$ um subgrupo e $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$. Então*

$$\mathbb{E}^{\sigma H \sigma^{-1}} = \sigma \mathbb{E}^H.$$

Demonstração. Dado $\sigma(a) \in \sigma\mathbb{E}^H$, e $\sigma\tau\sigma^{-1} \in \sigma H \sigma^{-1}$, temos que $\tau(a) = a$. Daí,

$$\sigma\tau\sigma^{-1}(\sigma(a)) = \sigma\tau(a) = \sigma(a).$$

Portanto, $\sigma\mathbb{E}^H \subseteq \mathbb{E}^{\sigma H\sigma^{-1}}$. Reciprocamente, dado $a \in \mathbb{E}^{\sigma H\sigma^{-1}}$, escreva $a = \sigma(\sigma^{-1}(a))$. Provemos que $\sigma^{-1}(a) \in \mathbb{E}^H$. Dado $\tau \in H$, temos que

$$\tau(\sigma^{-1}(a)) = \sigma^{-1}(\sigma\tau\sigma^{-1}(a)) = \sigma^{-1}(a).$$

Assim, $a \in \sigma\mathbb{E}^H$. Portanto, vale que $\mathbb{E}^{\sigma H\sigma^{-1}} = \sigma\mathbb{E}^H$. □

Assim, já provamos todas as etapas do nosso resultado principal. Enunciamos da seguinte forma:

Teorema 8.6 (Teorema Fundamental da Teoria de Galois)**.** *Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana finita. Denote por $\mathcal{G}$ o conjunto dos subgrpos de* $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$*, e $\mathcal{K}$ o conjunto dos corpos $\mathbb{K}$, com $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$. Então, os mapas $\mathbb{K} \in \mathcal{K} \mapsto \mathrm{Aut}(\mathbb{E}/\mathbb{K}) \in \mathcal{G}$ e $H \in \mathcal{G} \mapsto \mathbb{E}^H \in \mathcal{K}$ são inversas uma da outra. Além disso:*

(1) *$H_1 \subseteq H_2$ se, e somente se, $\mathbb{E}^{H_2} \subseteq \mathbb{E}^{H_1}$, para $H_1, H_2 \in \mathcal{G}$.*
(2) *Se $H_1 \subseteq H_2$, então $[\mathbb{E}^{H_1} : \mathbb{E}^{H_2}] = [H_2 : H_1]$.*
(3) *Se $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$, então $\mathbb{K}/\mathbb{F}$ é normal se, e somente se,* $\mathrm{Aut}(\mathbb{E}/\mathbb{K})$ *é um subgrupo normal de* $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$*. Neste caso,* $\mathrm{Aut}(\mathbb{K}/\mathbb{F}) \cong \mathrm{Aut}(\mathbb{E}/\mathbb{F})/\mathrm{Aut}(\mathbb{E}/\mathbb{K})$.

Demonstração. Dado $H \in \mathcal{H}$, o Teorema 8.2 diz que $H = \mathrm{Aut}(\mathbb{E}/\mathbb{E}^H)$. Seja $\mathbb{K} \in \mathcal{K}$. Então, Corolário 7.8 e Proposição 4.9 dizem que $\mathbb{E}/\mathbb{K}$ é uma extensão galoisiana. Daí, o Corolário 8.3 conclui que $\mathbb{K}^{\mathrm{Aut}(\mathbb{E}/\mathbb{K})} = \mathbb{K}$. Portanto, as aplicações são inversas uma da outra.
(1) Segue do enunciado do Lema 8.1, combinado com o fato dos mapas serem uma a inversa da outra.
(2) Do Teorema de Artin, $[\mathbb{E} : \mathbb{E}^{H_i}] = |H_i|$. Além disso,

$$|H_2| = [\mathbb{E} : \mathbb{E}^{H_2}] = [\mathbb{E} : \mathbb{E}^{H_1}][\mathbb{E}^{H_1} : \mathbb{E}^{H_2}] = |H_1|[\mathbb{E}^{H_1} : \mathbb{E}^{H_2}].$$

Portanto, $[\mathbb{E}^{H_1} : \mathbb{E}^{H_2}] = |H_2|/|H_1| = [H_2 : H_1]$.
(3) Seja $H = \mathrm{Aut}(\mathbb{E}/\mathbb{K})$. Do Corolário 8.3, $\mathbb{K} = \mathbb{E}^H$.

Assuma que H é um subgrupo normal, e seja $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$. Do Lema 8.5, obtemos que $\sigma\mathbb{E}^H = \mathbb{E}^{\sigma H\sigma^{-1}} = \mathbb{E}^H$. Portanto, do Teorema 5.6, $\mathbb{K}/\mathbb{F}$ é uma extensão normal. Reciprocamente, dado $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$, do Lema 8.5, temos

$$\mathbb{E}^{\sigma H\sigma^{-1}} = \sigma\mathbb{E}^H = \mathbb{E}^H.$$

Portanto, $\sigma H\sigma^{-1} = H$. Assim, H é um subgrupo normal de $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$. A conclusão foi provada no Teorema 5.6. □