## 9. Exemplos de Grupo de Galois

Nesta seção, vamos enunciar e demonstrar algumas ferramentas úteis para calcular o grupo de automorfismos de uma extensão de corpos.

**Definição 9.1.** Sejam $\mathbb{F}_1$ e $\mathbb{F}_2$ subcorpos de um corpo $\mathbb{E}$. O *compósito* de $\mathbb{F}_1$ e $\mathbb{F}_2$, denotado por $\mathbb{F}_1 \cdot \mathbb{F}_2$, é o menor subcorpo de $\mathbb{E}$ contendo $\mathbb{F}_1$ e $\mathbb{F}_2$. Analogamente define-se o compósito de um número finito de subcorpos de $\mathbb{E}$, denotado por $\mathbb{F}_1 \cdots \mathbb{F}_s$.

*Exemplo* 9.1. (1) Note que $\mathbb{F}_1 \cdot \mathbb{F}_2 = \mathbb{F}_1(\mathbb{F}_2) = \mathbb{F}_2(\mathbb{F}_1)$.
(2) Como subcorpos de $\mathbb{C}$, vale que $\mathbb{Q}(\sqrt{2}) \cdot \mathbb{Q}(i) = \mathbb{Q}(\sqrt{2}, i)$.
(3) Considere o corpo $\mathbb{C}(X)$, e seus subcorpos $\mathbb{Q}(X)$, e algum $\mathbb{K} \subseteq \mathbb{C} \subset \mathbb{C}(X)$. Então $\mathbb{K} \cdot \mathbb{Q}(X) = \mathbb{K}(X)$.

**Proposição 9.2.** *Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana finita, e sejam $\mathbb{K}_1, \ldots, \mathbb{K}_s$ corpos intermediários, isto é, $\mathbb{F} \subseteq \mathbb{K}_i \subseteq \mathbb{E}$. Seja $\mathbb{K} = \mathbb{K}_1 \cdots \mathbb{K}_s$. Então*

$$\mathrm{Aut}(\mathbb{E}/\mathbb{K}) = \bigcap_{i=1}^{s} \mathrm{Aut}(\mathbb{E}/\mathbb{K}_i).$$

*Demonstração.* Pela correspondência de Galois, como $\mathbb{K}$ é o menor corpo contendo $\mathbb{K}_1, \ldots, \mathbb{K}_s$, então $\mathrm{Aut}(\mathbb{E}/\mathbb{K})$ é o maior grupo contido em $\mathrm{Aut}(\mathbb{E}/\mathbb{K}_i)$, para cada $i$. Portanto, vale o resultado. □

**Proposição 9.3.** *Seja $\Omega$ um corpo contendo os corpos $\mathbb{L}, \mathbb{E}, \mathbb{F}$, e assuma que $\mathbb{L} \supseteq \mathbb{F}$, e que $\mathbb{E}/\mathbb{F}$ é galoisiana finita. Então $\mathbb{E}\cdot\mathbb{L}/\mathbb{L}$ e $\mathbb{E}/\mathbb{E}\cap\mathbb{L}$ são galoisianas finitas. Mais ainda:*

(i) *Via restrição de monomorfismo, vale que* $\mathrm{Aut}(\mathbb{E} \cdot \mathbb{L}/\mathbb{L}) \cong \mathrm{Aut}(\mathbb{E}/\mathbb{E} \cap \mathbb{L})$.
(ii) $[\mathbb{E} \cdot \mathbb{L} : \mathbb{L}]$ *divide* $[\mathbb{E} : \mathbb{F}]$. *Ainda mais, se* $[\mathbb{L} : \mathbb{F}] < \infty$, *então*

$$[\mathbb{E} \cdot \mathbb{L} : \mathbb{F}] = \frac{[\mathbb{E} : \mathbb{F}][\mathbb{L} : \mathbb{F}]}{[\mathbb{E} \cap \mathbb{L} : \mathbb{F}]}.$$

(iii) $[\mathbb{E} \cdot \mathbb{L} : \mathbb{L}] = [\mathbb{E} : \mathbb{F}]$ *se, e somente se,* $\mathbb{E} \cap \mathbb{L} = \mathbb{F}$. *Neste caso, vale que* $\mathrm{Aut}(\mathbb{E} \cdot \mathbb{L}/\mathbb{L}) \cong \mathrm{Aut}(\mathbb{E}/\mathbb{F})$.

*Demonstração.* (i) Como $\mathbb{E}/\mathbb{F}$ é galoisiana finita, segue que $\mathbb{E}/\mathbb{E} \cap \mathbb{L}$ é galoisiana finita. Ainda, existe $f \in \mathbb{F}[X]$ separável tal que $\mathbb{E} = \mathbb{F}(\mathscr{R}(f))$. Portanto, $\mathbb{E} \cdot \mathbb{L} = \mathbb{F}(\mathscr{R}(f))(\mathbb{L}) = \mathbb{F}(\mathbb{L})(\mathscr{R}(f)) = \mathbb{L}(\mathscr{R}(f))$. Daí, $\mathbb{E} \cdot \mathbb{L}/\mathbb{L}$ é galoisiana finita.

Dado $\sigma \in \mathrm{Aut}(\mathbb{E} \cdot \mathbb{L}/\mathbb{L})$, denote por $\psi(\sigma) = \sigma|_{\mathbb{E}}$ a sua restrição em $\mathbb{E}$. Dado $a \in \mathbb{E} \cap \mathbb{L} \subseteq \mathbb{L}$, temos que $\sigma(a) = a$. Portanto, $\sigma|_{\mathbb{E}}$ é um $\mathbb{E} \cap \mathbb{L}$-monomorfismo. Agora, a extensão $\mathbb{E}/\mathbb{E} \cap \mathbb{L}$ é normal, e portanto, $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{E} \cap \mathbb{L})$. Isso mostra que o mapa $\psi : \mathrm{Aut}(\mathbb{E}\cdot\mathbb{L}/\mathbb{L}) \to \mathrm{Aut}(\mathbb{E}/\mathbb{E}\cap\mathbb{F})$ dada por restrição está bem definido. Além disso, o mesmo é um homomorfismo de grupos. Se $\sigma$ é um $\mathbb{L}$-automorfismo de $\mathbb{E} \cdot \mathbb{L} = \mathbb{L}(\mathbb{E})$ tal que $\sigma|_{\mathbb{E}} = 1_{\mathbb{E}}$, então $\sigma = 1$. Portanto, $\psi$ é injetora.

Por fim, seja $H = \mathrm{Im}\,\psi$. Então, $\mathbb{E} \cap \mathbb{L} \subseteq \mathbb{E}^H \subseteq (\mathbb{E} \cdot \mathbb{L})^{\mathrm{Aut}(\mathbb{E}\cdot\mathbb{L}/\mathbb{L})} \cap \mathbb{E} = \mathbb{E} \cap \mathbb{L}$. Portanto, $H = \mathrm{Aut}(\mathbb{E}/\mathbb{E} \cap \mathbb{L})$. Daí $\psi$ é sobrejetor, e então, um isomorfismo de grupos.

(ii) Do item (i), temos que $[\mathbb{E}\cdot\mathbb{L}:\mathbb{L}] = [\mathbb{E}:\mathbb{E}\cap\mathbb{L}]$. O último divide $[\mathbb{E}:\mathbb{F}]$. Se $[\mathbb{L}:\mathbb{F}]<\infty$, temos então

$$[\mathbb{E}\cdot\mathbb{L}:\mathbb{F}] = [\mathbb{E}\cdot\mathbb{L}:\mathbb{L}][\mathbb{L}:\mathbb{F}] = [\mathbb{E}:\mathbb{E}\cap\mathbb{L}][\mathbb{L}:\mathbb{F}] = [\mathbb{E}:\mathbb{E}\cap\mathbb{L}][\mathbb{L}:\mathbb{F}]\frac{[\mathbb{E}\cap\mathbb{L}:\mathbb{F}]}{[\mathbb{E}\cap\mathbb{L}:\mathbb{F}]}$$
$$= \frac{[\mathbb{E}:\mathbb{F}][\mathbb{L}:\mathbb{F}]}{[\mathbb{E}\cap\mathbb{L}:\mathbb{F}]}.$$

(iii) Segue dos items (i) e (ii). □

*Exemplo* 9.2. Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana finita. Então, a extensão de corpos $\mathbb{E}(X_1,\ldots,X_m)/\mathbb{F}(X_1,\ldots,X_m)$ é galoisina finita. Além disso,

$$\mathrm{Aut}(\mathbb{E}(X_1,\ldots,X_m)/\mathbb{F}(X_1,\ldots,X_m)) \cong \mathrm{Aut}(\mathbb{E}/\mathbb{F}).$$

De fato, basta tomar $\mathbb{L} = \mathbb{F}(X_1,\ldots,X_m)$, e $\Omega = \mathbb{E}(X_1,\ldots,X_m)$ na proposição anterior. Neste caso, temos que $\mathbb{E}\cap\mathbb{L} = \mathbb{F}$.

*Exemplo* 9.3. Seja $\Omega$ um corpo algebricamente fechado e $\mathbb{F}$ o seu corpo primo. Sejam $f\in\mathbb{F}[X]$ um polinômio separável, e $\mathbb{E}\subseteq\Omega$ um corpo. Então

$$\mathrm{Aut}(\mathbb{E}(\mathscr{R}(f))/\mathbb{E}) \cong \mathrm{Aut}(\mathbb{F}(\mathscr{R}(f))/\mathbb{F}(\mathscr{R}(f))\cap\mathbb{E}).$$

**Proposição 9.4.** *Seja $\Omega$ 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.*

*Demonstração.* Temos que, para $i=1,2$, existem $f_i\in\mathbb{F}[X]$ separável de modo que $\mathbb{E}_i = \mathbb{F}(\mathscr{R}(f_i))$. Então $\mathbb{E}_1\cdot\mathbb{E}_2 = \mathbb{F}(\mathscr{R}(\{f_1,f_2\}))$. Portanto, $\mathbb{E}_1\cdot\mathbb{E}_2/\mathbb{F}$ é galoisiana finita. Seja

$$H = \{(\sigma_1,\sigma_2)\in\mathrm{Aut}(\mathbb{E}_1/\mathbb{F})\times\mathrm{Aut}(\mathbb{E}_2/\mathbb{F}) \mid \sigma_1|_{\mathbb{E}_1\cap\mathbb{E}_2} = \sigma_2|_{\mathbb{E}_1\cap\mathbb{E}_2}\}.$$

Por construção, o mapa $\sigma\mapsto(\sigma|_{\mathbb{E}_1},\sigma|_{\mathbb{E}_2})$ é um homomorfismo de grupos injetor, e sua imagem está contida em $H$. Provaremos que a cardinalidade de $H$ coincide com a de $\mathrm{Aut}(\mathbb{E}_1\cdot\mathbb{E}_2/\mathbb{F})$. Temos que existem $[\mathbb{E}_1:\mathbb{F}]$ $\mathbb{F}$-automorfismos de $\mathbb{E}_1$. Para cada automorfismo $\sigma$, existem exatamente $[\mathbb{E}_2:\mathbb{E}_1\cap\mathbb{E}_2]$ extensões de $\sigma|_{\mathbb{E}_1\cap\mathbb{E}_2}$ para $\mathbb{E}_2$. Daí

$$|H| = [\mathbb{E}_1:\mathbb{F}][\mathbb{E}_2:\mathbb{E}_1\cap\mathbb{E}_2] = [\mathbb{E}_1:\mathbb{F}][\mathbb{E}_2:\mathbb{E}_1\cap\mathbb{E}_2]\frac{[\mathbb{E}_1\cap\mathbb{E}_2:\mathbb{F}]}{[\mathbb{E}_1\cap\mathbb{E}_2:\mathbb{F}]}$$
$$= \frac{[\mathbb{E}_1:\mathbb{F}][\mathbb{E}_2:\mathbb{F}]}{[\mathbb{E}_1\cap\mathbb{E}_2:\mathbb{F}]} = [\mathbb{E}_1\cdot\mathbb{E}_2:\mathbb{F}],$$

em que a última passagem foi utilizada a Proposição 9.3.(ii). Isso conclui o resultado. □

**Corolário 9.5.** *Sejam $\mathbb{F}\subseteq\mathbb{K}_1,\ldots,\mathbb{K}_m\subseteq\mathbb{E}$ corpos. Assuma que, para cada $i=1,\ldots,m$, $\mathbb{K}_i/\mathbb{F}$ é galoisiana e finita. Assuma ainda que $\mathbb{K}_i\cap(\mathbb{K}_1\cdots\mathbb{K}_{i-1}\cdot\mathbb{K}_{i+1}\cdots\mathbb{K}_m)=\mathbb{F}$, para cada $i$. Então $\mathbb{K}_1\cdots\mathbb{K}_m/\mathbb{F}$ é galoisiana finita, e*

$$\mathrm{Aut}(\mathbb{K}_1\cdots\mathbb{K}_m/\mathbb{F}) \cong \mathrm{Aut}(\mathbb{K}_1/\mathbb{F})\times\cdots\times\mathrm{Aut}(\mathbb{K}_m/\mathbb{F}).$$

□

9.1. **Exercícios e Exemplos.**

(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) $f = X^4 - 2$