AULA

# 13

# O teorema fundamental da teoria de Galois

**META:**

Demonstrar o teorema fundamental da teoria de Galois.

**OBJETIVOS:**

Ao final da aula o aluno deverá ser capaz de:

Enunciar o teorema fundamental da teoria de Galois.

Determinar e exibir a correspondência de Galois de certas extensões.

**PRÉ-REQUISITOS**

Aula 12.

**O teorema fundamental**
**da teoria de Galois**

## 13.1 Introdução

Todo o esforço de nossos estudos serão compensados após apreciarmos os resultados desta aula. Na aula anterior, estabelecemos a correspondência de Galois $E \overset{\Gamma}{\longmapsto} \Gamma(E)$ e $H \overset{\Phi}{\longmapsto} \Phi(H)$ entre o conjunto de corpos intermediários de uma extensão $F \subset K$ e os subgrupos do grupo de Galois $Gal_F K = \Gamma(F)$. O teorema fundamental da teoria de Galois mostra que esta correspondência é biunívoca quando a extensão é finita, normal e separável. Uma extensão reunindo estas três propriedades é chamada extensão de Galois.

## 13.2 O Lema Principal

**Lema 13.3.** *Se $F \subset K$ é finita então $K$ é simples, normal e separável sobre o corpo fixado de qualquer subgrupo $H$ de $Gal_F K$.*

**Prova:** Esboço:
Seja $H$ um subgrupo de $Gal_F K$ e $\Phi(H)$ seu corpo fixado.

1. $K$ é algébrico sobre $\Phi(H)$.
2. Para cada $\alpha \in K$ e $\sigma \in H$, $\sigma(\alpha)$ é raiz do polinômio mínimo de $\alpha$ sobre $\Phi(H)$, $m_{\alpha,\Phi(H)}(x)$.
3. O conjunto das imagens de $\alpha$ por automorfismo em $H$ é finito.
4. Sejam
$$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_t \in K$$
todas as imagens distintas de $\alpha$ por elementos em $H$. Então,
$$\sigma(\alpha_i) \in \{\alpha_1, \alpha_2, \ldots, \alpha_t\}$$
para todo $i = 1, 2, \ldots, t$ e a aplicação restrição
$$\sigma : \{\alpha_1, \alpha_2, \ldots, \alpha_t\} \to \{\alpha_1, \alpha_2, \ldots, \alpha_t\}$$

define uma permutação no conjunto $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ qualquer que seja $\sigma \in H$.

5. O polinômio

$$f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_t)$$

é separável, tem $\alpha$ como raiz e $\sigma(f(x)) = f(x)$ para todo $\sigma \in H$. Logo, $f(x) \in \Phi(H)[x]$.

6. $K$ é uma extensão separável de $\Phi(H)$ e finitamente gerada sobre $\Phi(H)$.

7. Pelo teorema do elemento primitivo, $K = \Phi(H)(\theta)$ para algum $\theta \in K$.

8. $K = \Phi(H)(\theta)$ é o corpo de raízes de $f(x)$ sobre $\Phi(H)$, logo, normal sobre $\Phi(H)$. $\square$

## 13.3 Sobrejetividade

**Teorema 13.1.** *Se $F \subset K$ é finita então $H = \Gamma(\Phi(H))$ e $|H| = [K : \Phi(H)]$ para todo subgrupo $H$ de $Gal_F K$.*

**Prova:** $K = \Phi(H)(\theta)$ é normal e separável, pelo lema fundamental. Então,

$$[K : \Phi(H)] = \text{ deg } m_{\theta,\Phi(H)}(x) = n$$

com $m_{\theta,\Phi(H)}(x)$ separável e fatorando-se completamente sobre $K$. Se $\sigma \in \Gamma(\Phi(H))$ então $\sigma$ fixa todos os elementos do corpo $\Phi(H)$. Em particular, fixa todos os coeficientes do polinômio $m_{\theta,\Phi(H)}(x)$. Então, para todo $\sigma \in \Gamma(\Phi(H))$, $\sigma$ leva $\theta$ numa das $n$ raízes distintas de $m_{\theta,\Phi(H)}(x)$. Desde que um automorfismo $\sigma \in \Gamma(\Phi(H))$ fica

completamente determinado pela imagem em $\theta$, existem no máximo $n$ elementos em $\Gamma(\Phi(H))$. Da inclusão $H \subset \Gamma(\Phi(H))$, segue as desigualdades

$$|H| \leq |\Gamma(\Phi(H))| \leq n = [K : \Phi(H)].$$

Seja

$$f(x) = (x - \theta)(x - \theta_2) \cdots (x - \theta_t)$$

como no esboço da prova do lema fundamental com $\alpha = \theta$. Então, existem ao menos $t$ elementos em $H$, pela definição de $f(x)$. Além disso, $f(x) \in \Phi(H)[x]$ e tem $\theta$ como raiz. Então, $m_{\theta,\Phi(H)}(x)$ divide $f(x)$. Daí,

$$|H| \geq t = \text{ deg } f(x) \geq \text{ deg } m_{\theta,\Phi(H)}(x) = n = [K : \Phi(H)]$$

Combinando todas as desigualdades obtidas, temos

$$|H| \leq |\Gamma(\Phi(H))| \leq [K : \Phi(H)] \leq |H|.$$

Assim, $|H| = |\Gamma(\Phi(H))| = [K : \Phi(H)]$ e $H = \Gamma(\Phi(H))$. □

**Corolário 13.1.** *A correspondência de Galois é sobrejetiva para extensões finitas.* □

## 13.4 Injetividade

**Lema 13.4.** *Seja $F \subset E \subset K$ extensões de corpos. Se $K$ é Galois sobre $F$ então $K$ é Galois sobre $E$.* □

**Teorema 13.2.** *Se $F \subset K$ é uma extensão de Galois então $E = \Phi(\Gamma(E))$ para todo corpo intermediário $E$.*

**Prova:** Temos $E \subset \Phi(\Gamma(E))$. Resta mostrar que $\Phi(\Gamma(E)) \subset E$, ou seja, $\forall x \in \Phi(\Gamma(E)) \Rightarrow x \in E$. Por contrapositiva, esta implicação

é equivalente à mostrar que se $x \notin E$ então $x \notin \Phi(\Gamma(E))$. Mas, por definição de corpo fixado, $x \notin \Phi(\Gamma(E))$ significa dizer que existe $\sigma \in \Gamma(E)$ tal que $\sigma(x) \neq x$. Assim, o resultado fica provado se conseguirmos mostrar a seguinte implicação:

$$x \notin E \Rightarrow \sigma(x) \neq x \text{ para algum } \sigma \in \Gamma(E).$$

Pelo lema acima, $K$ é Galois sobre $E$. Assim, $K$ é extensão algébrica de $E$. Seja $\alpha \in K$. Se $\alpha \notin E$, então $m_{\alpha,E}(x)$ tem grau $\geq 2$ (se deg $m_{\alpha,E}(x) = 1$, $\alpha$ estaria em $E$). As raízes de $m_{\alpha,E}(x)$ são todas distintas por separabilidade, e todas estão em $K$ por normalidade. Seja $\beta \in K$ uma outra raiz de $m_{\alpha,E}(x)$ distinta de $\alpha$. Pelo fato 2 da seção 12.3, existe $\sigma \in \Gamma(E) = Gal_E K$ tal que $\sigma(\alpha) = \beta \neq \alpha$. Assim, $\alpha \notin \Phi(\Gamma(E))$, como queríamos demonstrar. □.

**Corolário 13.2.** *A correspondência de Galois é injetiva para extensões de Galois.* □

**Corolário 13.3.** *Seja $K$ uma extensão finita sobre $F$. Então*

$$K \text{ é Galois sobre } F \iff F = \Phi(Gal_F K). \quad \square$$

## 13.5 O Teorema Fundamental

**Teorema 13.3.** *Se $K$ é uma extensão de Galois sobre $F$, então:*

1. *Existe uma bijeção entre o conjunto de todos os corpos intermediários da extensão e os subgrupos do grupo de Galois $Gal_F K$, dada por associar à cada corpo intermediário $E$ o subgrupo $\Gamma(E) = Gal_E K$.*

2. *Esta correspondência é reversa com respeito à inclusão, isto é, $E_1 \subset E_2$ se e somente se $\Gamma(E_2) \subset \Gamma(E_2)$.*

*3.* $[K : E] = |\Gamma(E)|$ *e* $[E : F] = |\Gamma(F) : \Gamma(E)|$, *para todo* $E$, $F \subset E \subset K$.

*4. Um corpo intermediário* $E$ *é normal sobre* $F$ *se e somente se* $\Gamma(E)$ *é um subgrupo normal de* $\Gamma(F)$, *e neste caso* $\Gamma(F)/\Gamma(E) \cong Gal_F E$.

**Prova:**

1. A bijetividade de tal correspondência já foi provada nas seções 13.3, 13.4.

2. i) $E_1 \subset E_2 \Rightarrow$ todo $E_2$-automorfismo de $K$ é $E_1$-automorfismo de $K$, por definição de $F$-automorfismos $\Rightarrow \Gamma(E_2) \subset \Gamma(E_1)$.

   ii) Suponha $H_1 \subset H_2$. Se $x \in K$ é fixado por todo automorfismo em $H_2$, é, em particular, fixado por todo automorfismo em $H_1$. Assim, $\Phi(H_2) \subset \Phi(H_1)$.

3. Pelo teorema 13.2, $E = \Phi(\Gamma(E))$. Por outro lado, o teorema 13.1 diz que $|H| = [K : \Phi(H)]$. Fazendo $H = \Gamma(E)$, temos

$$[K : E] = [K : \Phi(\Gamma(E))] = |\Gamma(E)|.$$

   Em particular, se $F = E$, $[K : F] = |\Gamma(F)| = |Gal_F K|$. Pelo teorema de Lagrange,

$$\begin{aligned} [K : E][E : F] &= [K : F] \\ &= |Gal_F K| = |Gal_E K||Gal_F K : Gal_E K| \end{aligned}$$

   onde $|Gal_F K : Gal_E K|$ denota o índice do subgrupo $Gal_E K$ em $Gal_F K$. Dividindo a equação acima por $[K : E] = |Gal_E K|$ segue que $[E : F] = |Gal_F K : Gal_E K|$.

4. Suponha $Gal_E K \trianglelefteq Gal_F K$ (subgrupo normal). Se $p(x)$ é um polinômio irredutível em $F[x]$ com uma raiz $\alpha$ em $E$, devemos mostrar que $p(x)$ fatora-se em $E[x]$, ou seja, cada raiz $\beta$ de $p(x)$ está em $E$. Como $K$ é normal sobre $F$, sabemos que $p(x)$ fatora-se em $K[x]$. Existe um automorfismo $\sigma \in Gal_F K$ tal que $\sigma(\alpha) = \sigma(\beta)$, pois $\alpha$ e $\beta$ têm mesmo polinômio mínimo (fato 2). Por definição de subgrupo normal, $\sigma Gal_E K = Gal_E K \sigma$. Deste modo, qualquer que seja $\tau \in Gal_E K$, existe $\tau_1 \in Gal_E K$ para o qual vale a igualdade $\tau \circ \sigma = \sigma \circ \tau_1$. Como $\alpha \in E$, temos

$$\tau(\beta) = \tau(\sigma(\alpha)) = \sigma(\tau_1(\alpha)) = \sigma(\alpha) = \beta$$

Assim, $\beta$ é fixado por cada elemento de $\tau \in Gal_E K$. Logo, por definição de corpo fixado, $\beta \in \Phi(Gal_E K) = \Phi(\Gamma(E)) = E$.

Reciprocamente, suponha $E$ normal sobre $F$. $E$ é finito sobre $F$, pois $F \subset E \subset K$ e $K$ é finito sobre $F$. Defina a aplicação

$$\varphi : Gal_F K \to Gal_F E$$

onde $\varphi(\sigma) = \sigma_{|_E}$ é a restrição de um $F$-automorfismo de $K$ ao corpo $E$. Temos

i) $\varphi$ está bem definida. De fato, seja $\sigma \in Gal_F K$. Devemos mostrar que $\sigma_{|_E} \in Gal_F E$. Observe que

   a) Dado $\alpha \in E$, seja $p(x) = m_{\alpha,F}(x)$. $E$ é normal sobre $F$, logo, $p(x)$ fatora-se em $E[x]$. Assim, todas as raízes de $p(x)$ estão em $E$. Como $\sigma(\alpha)$ é raiz de $p(x)$ então $\sigma(\alpha) \in E$. Portanto, $\sigma(E) \subset E$ e $\sigma_{|_E}$ define um endomorfismo em $E$.

   b) Para todo $\alpha \in E$, $\sigma$ define uma permutação no conjunto $\{\alpha = \alpha_1, \alpha_2, \ldots, \alpha_t\}$ das raízes do polinômio

mínimo $m_{\alpha,F}(x)$. Então, $\alpha = \sigma(\alpha_i)$ para algum $i = 1, 2 \ldots, t$. Pela normalidade de $E$ sobre $F$, $\alpha_i \in E$. Isto mostra a sobrejetividade de $\sigma_{|_E}$.

Então, $\sigma_{|_E} : E \to E$ é um automorfismo. Como $\sigma \in Gal_F K$, $\sigma$ fixa cada elemento de $F$. Logo, $\sigma_{|_E} \in Gal_F E$.

ii) $\varphi : Gal_F K \to Gal_F E$ é um homomorfismo sobrejetivo de grupos. Fica como exercício provar que $\varphi$ é homomorfismo. Provaremos a sobrejetividade. Como $K$ é uma extensão normal e finita sobre $F$, $K = SF_F(f(x))$ para algum $f(x) \in F[x]$. Desde que $F \subset E$, $K = SF_E(f(x))$. Consequentemente, cada $\tau \in Gal_F E$ pode ser estendido à um $F$-automorfismo $\sigma \in Gal_F K$ tal que $\sigma_{|_E} = \tau$ (ver teorema 10.2).

iii)

$$\begin{aligned} Ker\ \varphi &= \{\sigma \in\ Gal_F K\ :\ \sigma_{|_E} = I_E \text{ identidade em } E\} \\ &= \{\sigma \in Gal_F K\ :\ \sigma(x) = x\ \forall\ x \in E\} \\ &= \{\sigma \in Gal_F K\ : \sigma \in Gal_E K\} \\ &= Gal_E K \end{aligned}$$

Assim, $Gal_E K \trianglelefteq Gal_F K$.

v) Pelo teorema fundamental do isomorfismo,

$$Gal_F K / Gal_E K \cong Gal_F E. \quad \square$$

## 13.6 Conclusão

Em geral, finitude é suficiente para caracterizar a sobrejetividade na correspondência de Galois. As condições que faltam à finitude para determinar a injetividade são normalidade e separabilidade.

# AULA 13

Além da bijetividade na correspondência de Galois para extensões de Galois, o teorema fundamental caracteriza a normalidade de um dado corpo intermediário $E$ via normalidade do subgrupo associado $\Gamma(E)$. Tal relação completamente fechada entre duas estruturas distintas confere à teoria de Galois uma beleza estética e profundidade teórica raramente vista na história do pensamento humano.

## RESUMO

Finitude $\Rightarrow$ sobrejetividade da correspondência de Galois.

Finitude + Normalidade + Separabilidade $\Rightarrow$ injetividade da correspondência de Galois.

### TEOREMA FUNDAMETAL DA TEORIA DE GALOIS

Se $K$ é uma extensão de Galois sobre $F$, então:

1. Existe uma bijeção entre o conjunto de todos os corpos intermediários da extensão e os subgrupos do grupo de Galois $Gal_F K$, dada por associar à cada corpo intermediário $E$ o subgrupo $\Gamma(E) = Gal_E K$.
2. Esta correspondência é reversa com respeito à inclusão, isto é, $E_1 \subset E_2$ se e somente se $\Gamma(E_2) \subset \Gamma(E_2)$.
3. $[K : E] = |\Gamma(E)|$ e $[E : F] = |\Gamma(F) : \Gamma(E)|$, para todo $E$, $F \subset E \subset K$.
4. Um corpo intermediário $E$ é normal sobre $F$ se e somente se $\Gamma(E)$ é um subgrupo normal de $\Gamma(F)$, e neste caso $\Gamma(F)/\Gamma(E) \cong Gal_F E$.

## PRÓXIMA AULA

Estudaremos a solubilidade por radicais de uma equação algébrica definida sobre um corpo de característica zero. Veremos que uma equação algébrica é solúvel por radicais se e somente se o grupo de Galois do polinômio $f(x)$ é um grupo solúvel.

## ATIVIDADES

**ATIV. 13.1.** Prove todos os itens do esboço da prova do lema principal.

**ATIV. 13.2.** Mostre a sobrejetividade da correspondência de Galois para extensõs finitas.

**ATIV. 13.3.** Mostre o lema 13.4: Seja $F \subset E \subset K$ extensões de corpos. Se $K$ é Galois sobre $F$ então $K$ é Galois sobre $E$.

**ATIV. 13.4.** Prove o corolário 13.3: Seja $K$ uma extensão finita sobre $F$. Então

$$K \text{ é Galois sobre } F \iff F = \Phi(Gal_F K).$$

**ATIV. 13.5.** Se $K$ é Galois sobre $F$ mostre que existe uma quantidade finita de subcorpos intermediários.

**ATIV. 13.6.** Se $K$ é uma extensão normal de grau primo sobre $\mathbb{Q}$ então $Gal_{\mathbb{Q}} k \cong \mathbb{Z}_n$.

**ATIV. 13.7.** Mostre que a aplicação $\varphi : Gal_F K \to Gal_F E$, $\sigma \mapsto \sigma_{|_E}$ define um homomorfismo de grupos.

**ATIV. 13.8.** Seja $K$ uma extensão de Galois de $F$ e $E$ um corpo intermediário. Mostre que todo $F$-automorfismo $\tau : E \to E$ estende-se à um $F$-automorfismo $\sigma : K \to K$.

**ATIV. 13.9.** Determine a correspondência de Galois das seguintes extensões:

a) $\mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$.

b) $SF_{\mathbb{Q}}(x^2 + x + 1)$ sobre $\mathbb{Q}$.

c) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$.

d) $\mathbb{Q}(i, \sqrt{2})$ sobre $\mathbb{Q}$.

## LEITURA COMPLEMENTAR

DUMMIT, David S., FOOTE, Richard M. Abstract Algebra. John Wiley and Sons, 3.ed., USA, 2004.

GONÇALVES, Adilson, Introdução à álgebra, IMPA, Projeto Euclides, 5.ed., Rio de Janeiro, 2008.

HUNGERFORD, Thomas W., Abstract algebra: an introduction, Saunders College Publishing, 1990.

STEWART, Ian. Galois Theory, Chapman & Hall, 3.ed, 2004.