

# El teorema de Galois

Facultad de Ciencias UNAM

# Introducción

En esta sección (por fin) demostramos el teorema de Galois. De nuevo, hacemos la siguiente convención:

*Todos los campos tienen característica 0.*

# Condiciones suficientes para que $\text{Gal}(L/F)$ sea resoluble

## Lema 1

Supongamos que  $L/F$  es de Galois y radical con subcampos

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = L$$

tales que  $F_i = F_{i-1}(\gamma_i)$  donde  $\gamma_i \in F_i$  es tal que  $\gamma_i^{m_i} \in F_{i-1}$  p.a.  $m_i \in \mathbb{Z}_{\geq 1}$ .  
Mas aun, supongamos que para cada  $i \in \{1, \dots, n\}$  existe  $\zeta_i \in F$  tal que  $\zeta_i$  es una  $m_i$ -esima raíz primitiva de la unidad. Entonces

1.  $F_i/F_{i-1}$  es Galois.
2.  $\text{Gal}(F_i/F_{i-1})$  es cíclico.
3.  $\text{Gal}(L/F)$  es resoluble.

## Demostración.

1.  $F_i/F_{i-1}$  es Galois:

Considera el polinomio  $x^{m_i} - \gamma_i^{m_i} \in F_{i-1}[x]$ . Como  $\zeta_i$  es una  $m_i$ -esima raíz primitiva, entonces

$$\gamma_i, \ \zeta_i\gamma_i, \ \zeta_i^2\gamma_i, \ \dots, \ \zeta_i^{m_i-1}\gamma_i$$

son las raíces de  $x^{m_i} - \gamma_i^{m_i} \in F_{i-1}[x]$ . En particular, su campo de descomposición sobre  $F_{i-1}$  es

$$F_{i-1} \left( \gamma_i, \ \zeta_i\gamma_i, \ \zeta_i^2\gamma_i, \ \dots, \ \zeta_i^{m_i-1}\gamma_i \right) = F_{i-1}(\gamma_i) = F_i$$

donde la primera igualdad se cumple porque  $\zeta_i \in F \subset F_{i-1}$ .

En resumen,  $F_i$  es un campo de descomposición sobre  $F_{i-1}$  y por lo tanto,  $F_i/F_{i-1}$  es Galois.

## 2. $\text{Gal}(F_i/F_{i-1})$ es cíclico:

Antes que nada, recordemos que si  $\sigma \in \text{Gal}(F_i/F_{i-1})$ , entonces  $\sigma(\gamma_i)$  debe ser una raíz de  $x^{m_i} - \gamma_i^{m_i}$ . Como las raíces de  $x^{m_i} - \gamma_i^{m_i}$  son precisamente

$$\gamma_i, \ \zeta_i \gamma_i, \ \zeta_i^2 \gamma_i, \ \dots, \ \zeta_i^{m_i-1} \gamma_i,$$

entonces para cada  $\sigma \in \text{Gal}(F_i/F_{i-1})$  existe un único entero  $l \in \{1, \dots, m_i - 1\}$  tal que  $\sigma(\gamma_i) = \zeta_i^l \gamma_i$ .

Con esta notación, definimos

$$\begin{aligned}\text{Gal}(F_i/F_{i-1}) &\rightarrow \mathbb{Z}/m_i\mathbb{Z} \\ \sigma &\mapsto [l]\end{aligned}$$

El lector podrá fácilmente verificar que esta función es un homomorfismo inyectivo. Esto implica que  $\text{Gal}(F_i/F_{i-1})$  es isomorfo a un subgrupo de  $\mathbb{Z}/m_i\mathbb{Z}$  y como todo subgrupo de  $\mathbb{Z}/m_i\mathbb{Z}$  es cíclico, obtenemos lo deseado.

3.  $\text{Gal}(L/F)$  es resoluble:

Antes que nada, recordemos que tenemos subcampos

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = L \quad (1)$$

con  $F_i = F_{i-1}(\gamma_i)$  donde  $\gamma_i \in F_i$  es tal que  $\gamma_i^{m_i} \in F_{i-1}$  p.a.  $m_i \in \mathbb{Z}_{\geq 1}$ .

Considera  $G_i := \text{Gal}(L/F_i) \subset \text{Gal}(L/F)$ . Como la correspondencia de Galois revierte inclusiones, entonces (1) implica que tenemos subgrupos

$$\begin{aligned} \{1_L\} &= \text{Gal}(L/L) = \text{Gal}(L/F_n) = G_n \subset G_{n-1} \subset \cdots \\ &\subset G_1 \subset G_0 = \text{Gal}(L/F_0) = \text{Gal}(L/F). \end{aligned}$$

Por otro lado, como (i)  $L/F_{i-1}$  es Galois (pues  $L/F$  lo es) y (ii)  $F_i/F_{i-1}$  también (esto es el inciso (1)), entonces el teorema 2.23.6 implica que  $G_i = \text{Gal}(L/F_i)$  es normal en  $G_{i-1} = \text{Gal}(L/F_{i-1})$  y que

$$G_{i-1}/G_i = \text{Gal}(L/F_{i-1})/\text{Gal}(L/F_i) \cong \text{Gal}(F_i/F_{i-1}).$$

Por el inciso (2) ( $\text{Gal}(F_i/F_{i-1})$  es cíclico), lo anterior implica que  $G_{i-1}/G_i$  es cíclico y en particular abeliano. Pero todo grupo finito abeliano es resoluble (c.f. proposición 2.26.9) y por lo tanto obtenemos lo deseado.

# Una mitad del teorema de Galois

## Lema 2

Supongamos que  $L/F$  es Galois. Si  $L/F$  es resoluble, entonces  $\text{Gal}(L/F)$  es resoluble.

*Demostración.* Como  $L/F$  es resoluble, existe una extensión  $L'$  de  $L$  tal que  $L'/F$  es radical. Entonces  $L'/F$  es finita<sup>1</sup> separable<sup>2</sup> y por lo tanto tiene cerradura de Galois (c.f. corolario 2.22.2), digamos  $M$ .

---

<sup>1</sup>Toda extensión radical es finita.

<sup>2</sup>Estamos asumiendo que todos los campos tienen característica 0 y recuerda que en campos de característica 0, “polinomio irreducible  $\implies$  polinomio separable.”

Ahora bien, como  $L/F$  y  $M/F$  son Galois, el teorema 2.23.6 implica que

$$\text{Gal}(L/F) \cong \text{Gal}(M/F)/\text{Gal}(M/L). \quad (2)$$

Por otro lado, recordemos que en la proposición 2.26.4 vimos que

$$\forall G \text{ grupo } \forall H \triangleleft G \ (G \text{ resoluble} \implies G/H \text{ resoluble}) \quad (3)$$

Juntando (2) y (3) es fácil ver que si  $\text{Gal}(M/F)$  es resoluble, entonces  $\text{Gal}(L/F)$  también. Por eso, en lo que sigue veremos que  $\text{Gal}(M/F)$  es resoluble.

Antes que nada, recordemos que como (i)  $M$  es la cerradura de Galois de  $L'/F$  y (ii)  $L'/F$  es una extensión radical<sup>3</sup> y separable<sup>4</sup>, entonces por la proposición 2.25.4,  $M/F$  es radical. Supongamos que tenemos subcampos

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = M$$

tales que  $F_i = F_{i-1}(\gamma_i)$  donde  $\gamma_i \in F_i$  es tal que  $\gamma_i^{m_i} \in F_{i-1}$  p.a.  $m_i \in \mathbb{Z}_{\geq 1}$ .

---

<sup>3</sup>Por definición de  $L'$ .

<sup>4</sup>Todos los campos tienen característica 0.

Mas aun, supongamos que para cada  $i \in \{1, \dots, n\}$ ,  $\zeta_i$  es una  $m_i$ -esima raíz primitiva de la unidad en  $F$ .

Por otro lado, recordemos que en la proposición 2.27.2 demostramos que si  $\zeta$  es cualquier  $m$ -esima raíz primitiva de la unidad en  $F$ , entonces

$$\text{Gal}(M/F) \text{ es resoluble} \iff \text{Gal}(M(\zeta)/F(\zeta)) \text{ es resoluble}$$

Por lo tanto,

$$\begin{aligned} \text{Gal}(M/F) \text{ es resoluble} &\iff \text{Gal}(M(\zeta_1)/F(\zeta_1)) \text{ es resoluble} \\ &\iff \text{Gal}\left((M(\zeta_1))(\zeta_2)/(F(\zeta_1))(\zeta_2)\right) \text{ es resoluble} \\ &\iff \text{Gal}\left(M(\zeta_1, \zeta_2)/F(\zeta_1, \zeta_2)\right) \text{ es resoluble} \\ &\vdots \\ &\iff \text{Gal}\left(M(\zeta_1, \dots, \zeta_n)/F(\zeta_1, \dots, \zeta_n)\right) \text{ es resoluble.} \end{aligned}$$

Es fácil ver que la extensión  $M(\zeta_1, \dots, \zeta_n)/F(\zeta_1, \dots, \zeta_n)$  satisface las hipótesis del lema anterior y por lo tanto,  $\text{Gal}(M(\zeta_1, \dots, \zeta_n)/F(\zeta_1, \dots, \zeta_n))$  es resoluble. Usando todo lo anterior, obtenemos lo deseado.  $\square$

# Condiciones suficientes para que $L/F$ sea radical

## Lema 3

Supongamos que  $L/F$  es Galois. Si  $\text{Gal}(L/F)$  es resoluble y  $F$  tiene una  $p$ -esima raíz primitiva de la unidad para cada primo  $p$  que divide a  $|\text{Gal}(L/F)|$ , entonces  $L/F$  es radical.

*Demostración.* Como  $\text{Gal}(L/F)$  es resoluble, existen  $G_0, G_1, \dots, G_n$  subgrupos de  $G$  tales que

1.  $G_n \subset G_{n-1} \subset G_{n-2} \subset \cdots \subset G_2 \subset G_1 \subset G_0$  donde  $G_0 = G$  y  $G_n = \{e_G\}$ .
2.  $G_i$  es normal en  $G_{i-1}$  para toda  $i = 1, \dots, n$ .
3.  $[G_{i-1} : G_i]$  es un numero primo para toda  $i = 1, \dots, n$ .

Para ver que  $L/F$  es radical, considera los campos fijos

$$F_i := L_{G_i} \subset L$$

Como la correspondencia de Galois revierte inclusiones, tenemos

$$\begin{aligned} F &= L_{\text{Gal}(L/F)} = L_{G_0} = F_0 \subset F_1 \subset \cdots \\ F_{n-1} &\subset F_n = L_{G_n} = L_{\{1_L\}} = L \end{aligned}$$

Por otro lado, notemos que

$$\begin{aligned}\text{Gal}(F_i/F_{i-1}) &= \text{Gal}(L_{G_i}/L_{G_{i-1}}) && (\text{por def. de } F_j) \\ &\cong \text{Gal}(L/L_{G_{i-1}})/\text{Gal}(L/L_{G_i}) && (\text{por el teorema 2.23.6}) \\ &= G_{i-1}/G_i && (\text{por el teorema 2.24.2})\end{aligned}$$

Y como  $L/F$  y  $F_i/F_{i-1}$  son Galois, también tenemos que

$$|\text{Gal}(L/F)| = [L : F] = [L : F_i] \underbrace{[F_i : F_{i-1}]}_{|\text{Gal}(F_i/F_{i-1})|} [F_{i-1} : F] \quad (4)$$

Como  $[G_{i-1} : G_i]$  es primo, entonces (por el teorema 2.24.2) y (4) implican que  $|\text{Gal}(F_i/F_{i-1})|$  es un primo que divide a  $|\text{Gal}(L/F)|$ . Pero entonces, (por hipótesis)  $F$  tiene una  $|\text{Gal}(F_i/F_{i-1})|$ -esima raíz primitiva de la unidad.

# La otra mitad del teorema de Galois

## Lema 4

Supongamos que  $L/F$  es Galois. Si  $\text{Gal}(L/F)$  es resoluble, entonces  $L/F$  es resoluble.

*Demostración.* Denotemos  $m = |\text{Gal}(L/F)|$  y supongamos que  $\zeta$  es una  $m$ -esima raíz primitiva de la unidad en  $F$ . Como  $\text{Gal}(L/F)$  es resoluble, la proposición 2.27.2 implica que  $\text{Gal}(L(\zeta)/F(\zeta))$  también es resoluble.

En lo que sigue, veremos que  $L(\zeta)/F(\zeta)$  satisface las hipótesis del lema anterior (esto implicara que  $L(\zeta)/F(\zeta)$  es radical y después veremos que esto implica que  $L/F$  es resoluble). Como  $\text{Gal}(L(\zeta)/F(\zeta))$  es resoluble, solo resta probar que  $F(\zeta)$  tiene una  $p$ -esima raíz primitiva de la unidad para cada primo  $p$  que divide a  $|\text{Gal}(L(\zeta)/F(\zeta))|$ .

Para esto, considera el homomorfismo

$$\begin{aligned}\Phi : \text{Gal}(L(\zeta)/F(\zeta)) &\rightarrow \text{Gal}(L/F) \\ \sigma &\mapsto \sigma \upharpoonright_L\end{aligned}$$

Como los elementos de  $\ker \Phi$  son la identidad en  $F(\zeta)$  (pues pertenecen a  $\text{Gal}(L(\zeta)/F(\zeta))$ ) y también son la identidad en  $L$  (pues  $\sigma \upharpoonright_L = \text{id}_L$ ), entonces  $\ker \Phi = \{\text{id}_{L(\zeta)}\}$  y por lo tanto  $\Phi$  es inyectivo.

Usando esto y el teorema de Lagrange obtenemos que

$$|\text{Gal}(L(\zeta)/F(\zeta))| \text{ divide a } m = |\text{Gal}(L/F)|$$

Ahora bien, supongamos que  $p$  es un primo que divide a  $|\text{Gal}(L(\zeta)/F(\zeta))|$ . Por lo anterior,  $p$  divide a  $m$ . Mas aun, como  $\zeta$  es una  $m$ -esima raíz primitiva de la unidad, entonces (el lector podrá fácilmente verificar que)  $\zeta^{m/p}$  es una  $p$ -esima raíz primitiva de la unidad.

Como  $\zeta^{m/p} \in F(\zeta)$ , acabamos de demostrar que  $F(\zeta)$  tiene una  $p$ -esima raíz primitiva de la unidad para cada primo  $p$  que divide a  $|\text{Gal}(L(\zeta)/F(\zeta))|$ .

Es decir,  $L(\zeta)/F(\zeta)$  satisface las hipótesis del lema anterior y por lo tanto,  $L(\zeta)/F(\zeta)$  es radical. En lo que sigue, usaremos esto para demostrar que  $L/F$  es resoluble.

Antes que nada, notemos que  $F(\zeta)/F$  es radical (pues  $\zeta^m = 1 \in F$ ). Juntando esto con el hecho de que  $L(\zeta)/F(\zeta)$  es radical, obtenemos que  $L(\zeta)/F$  también es radical. Como  $L \subset L(\zeta)$ , lo anterior implica que  $L/F$  es resoluble.  $\square$

Antes de enunciar el teorema de Galois, notemos que como  $[L : F] = |\text{Gal}(L/F)|$  cuando  $L/F$  es Galois, entonces también acabamos de demostrar el siguiente resultado (c.f. lo que esta en azul):

### Corolario 5

Supongamos que  $L/F$  es Galois y resoluble. Si  $m = [L : F]$  y  $\zeta$  es una  $m$ -esima raíz primitiva de la unidad, entonces  $L(\zeta)/F$  es radical.

Ahora si, acabamos esta sección enunciando el teorema de Galois.

# El teorema de Galois

## Teorema 6

Si  $L/F$  es Galois, entonces

$$L/F \text{ es resoluble} \iff \text{Gal}(L/F) \text{ es resoluble.}$$

*Demostración.* Es consecuencia inmediata de los lemas 2 y 4. □