

UNIVERSIDAD DE MURCIA

GRADO EN MATEMÁTICAS

## Ecuaciones Algebraicas

*Notas de Clase*

---

**Laura Fernández Sánchez**

Curso 2025 – 2026



# Índice general

<b>1. Extensiones de Galois</b>	<b>5</b>
1.1. La correspondencia de Galois . . . . .	5
1.2. Extensiones de Galois . . . . .	12



# Capítulo 1

## Extensiones de Galois

### 1.1. La correspondencia de Galois

#### Definición 1.1.1: Homomorfismos de extensiones

Dadas  $K \subseteq L_1, L_2$  extensiones.

Si  $L_1$  y  $L_2$  son dos extensiones de  $K$ , entonces un **homomorfismo** de  $L_1/K$  en  $L_2/K$  (también llamado  $K$ -homomorfismo) es un homomorfismo de cuerpos  $f : L_1 \rightarrow L_2$  tal que  $f(a) = a$  para todo  $a \in K$ .

Un **endomorfismo** de una extensión  $L/K$  es un homomorfismo de  $L/K$  en sí misma. Un **isomorfismo** de extensiones (o  $K$ -isomorfismo) es un homomorfismo de extensiones que es isomorfismo de cuerpos y un **automorfismo** de extensiones (o  $K$ -automorfismo) es un isomorfismo de una extensión de  $K$  en sí misma.

#### Definición 1.1.2: Grupo de Galois

El **grupo de Galois** de  $L/K$  es el conjunto de  $K$ -automorfismos de  $L/K$  con la composición de aplicaciones.

Lo denotamos por  $\text{Gal}(L/K)$ .

#### Definición 1.1.3: Subextensión

Una **subextensión** de  $L/K$  es un cuerpo  $M$  tal que  $K \subseteq M \subseteq L$ .

#### Definición 1.1.4: Extensiones admisibles

Dos extensiones  $L_1/K$  y  $L_2/K$  son **admisibles** si existe un cuerpo  $L$  tal que  $L_1 \subseteq L$  y  $L_2 \subseteq L$ .

#### Observación 1.1.1: Convenios y propiedades básicas

En todo momento supondremos  $1 \neq 0 \implies$  Todos los homomorfismos entre cuerpos son inyectivos. Además, los  $K$ -homomorfismos son homomorfismos de  $K$ -espacios vectoriales. De esta forma siempre que exista un homomorfismo de cuerpos  $f : K \rightarrow L$ , el cuerpo  $L$  contiene un subcuerpo isomorfo a  $K$ , la imagen  $f(K)$  de  $f$ . Por otro lado  $K$  admite una extensión isomorfa a  $L$ , a saber el conjunto  $K \cup (L \setminus f(K))$ , en el que se define el producto

de la forma obvia.

Abusaremos a menudo de la notación y cada vez que tengamos un homomorfismo de cuerpos  $f : K \rightarrow L$ , simplemente consideraremos  $K$  como subcuerpo de  $L$ , identificando los elementos de  $K$  y  $f(K)$ , a través de  $f$ .

De aquí tenemos que, si  $f : K \rightarrow L$  es un homomorfismo de cuerpos:

#### Observación 1.1.2:

1.  $f(K) \simeq K$  (como cuerpos). A veces simplemente escribiremos  $K$  para referirnos a  $f(K)$ .
2. Por convenio,  $K$  es subcuerpo de  $L$  identificando  $K$  con  $f(K)$ .

#### Ejemplo 1.1.1:

Claramente  $\text{Gal}(K/K) = 1$ , pero no son éstas las únicas extensiones con grupo de Galois trivial. Por ejemplo, si  $a$  es un número racional positivo que no es el cubo de un número racional, entonces  $p = X^3 - a$  es irreducible en  $\mathbb{Q}[X]$ . Las raíces de  $p$  son  $\alpha = \sqrt[3]{a}$ ,  $\omega\alpha$  y  $\omega^2\alpha$ , donde  $\omega$  es una raíz tercera primitiva de la unidad. Como  $\omega$  no es un número real, la única raíz de  $p$  que pertenece a  $K(\alpha)$  es  $\alpha$  y por tanto  $\text{Gal}(K(\alpha)/K) = 1$  (¿por qué?).

#### Observación 1.1.3: Justificación del Ejemplo 1

Cualquier  $K$ -automorfismo  $\sigma \in \text{Gal}(K(\alpha)/K)$  está completamente determinado por la imagen del generador de la extensión, es decir, por  $\sigma(\alpha)$ . Además, los homomorfismos de cuerpos preservan las raíces de los polinomios con coeficientes en el cuerpo base. Como  $\alpha$  es raíz de  $p \in K[X]$ , su imagen  $\sigma(\alpha)$  debe ser obligatoriamente otra raíz de  $p$ .

Por tanto, las únicas opciones teóricas son  $\sigma(\alpha) \in \{\alpha, \omega\alpha, \omega^2\alpha\}$ . Sin embargo,  $\sigma$  es un endomorfismo de  $K(\alpha)$ , lo que exige que  $\sigma(\alpha) \in K(\alpha)$ . Dado que  $a > 0$  es racional, podemos considerar  $K(\alpha) \subset \mathbb{R}$ . Como  $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \notin \mathbb{R}$ , se sigue que  $\omega\alpha \notin \mathbb{R}$  y  $\omega^2\alpha \notin \mathbb{R}$ , por lo que ninguna de estas dos raíces pertenece a  $K(\alpha)$ . La única asignación bien definida y posible es  $\sigma(\alpha) = \alpha$ , lo que implica que  $\sigma$  es la aplicación identidad.

#### Ejemplo 1.1.2:

Si  $L/K$  es una extensión de grado 2 y  $\text{car}(K) \neq 2$ , entonces  $\text{Gal}(L/K)$  tiene dos elementos. En efecto, si  $\alpha \in L \setminus K$ , entonces  $L = K(\alpha)$  y por tanto  $p = \text{Min}_K(\alpha)$  tiene grado 2. Pongamos  $p = X^2 + aX + b = (X + \frac{a}{2})^2 + b - \frac{a^2}{4}$  y sean  $\beta = \alpha + \frac{a}{2}$  y  $c = \frac{a^2}{4} - b$ . Entonces  $q = \text{Min}_K(\beta) = X^2 - c$  y  $L = K(\beta) = K(\sqrt{c})$ . Como las raíces de  $q$  son  $\pm\beta$ , si  $\sigma \in \text{Gal}(L/K)$  entonces  $\sigma(\beta) = \pm\beta$ , con lo que efectivamente  $\text{Gal}(L/K)$  tiene dos elementos. (¿Seguro que tiene dos?). En particular,  $\text{Gal}(\mathbb{C}/\mathbb{R})$  tiene orden 2 y de hecho está formado por la identidad y la conjugación.

#### Observación 1.1.4: Justificación del Ejemplo 2

Para asegurar que efectivamente tiene *exactamente* dos elementos, debemos garantizar que las dos opciones teóricas ( $\sigma(\beta) = \beta$  y  $\sigma(\beta) = -\beta$ ) generan automorfismos distintos y bien definidos.

Primero, comprobamos que son distintos: como  $\text{car}(K) \neq 2$ , se cumple que  $2\beta \neq 0$  (ya que

$\beta \notin K \implies \beta \neq 0$ ), por lo que  $\beta \neq -\beta$ . Segundo, comprobamos que ambas opciones dan lugar a automorfismos válidos:  $L$  es el cuerpo de escisión del polinomio  $X^2 - c$  sobre  $K$ . Al ser irreducible y tener raíces simples (es separable por ser de característica distinta de 2), la teoría elemental de extensiones asegura que por cada raíz en el cuerpo de escisión existe un  $K$ -automorfismo que envía el generador a dicha raíz. Por consiguiente, existe el automorfismo identidad ( $\beta \mapsto \beta$ ) y un automorfismo no trivial ( $\beta \mapsto -\beta$ ), formando un grupo de Galois de orden 2.

### Ejemplo 1.1.3:

Como un automorfismo de  $\mathbb{R}$  ha de ser una aplicación creciente (¿por qué?), necesariamente  $\text{Gal}(\mathbb{R}/\mathbb{Q}) = 1$  y por tanto  $\text{Gal}(\mathbb{R}/K) = 1$  para todo subcuerpo  $K$  de  $\mathbb{R}$  (¿por qué?). De hecho, el único automorfismo de  $\mathbb{R}$  es la identidad (¿por qué?).

### Observación 1.1.5: Justificación del Ejemplo 3

Vamos a responder a las tres preguntas secuencialmente:

1. **¿Por qué ha de ser creciente?** Sea  $\sigma \in \text{Aut}(\mathbb{R})$ . Todo número real positivo  $x > 0$  admite una raíz cuadrada real, es decir,  $x = (\sqrt{x})^2$ . Al aplicar  $\sigma$ , obtenemos  $\sigma(x) = \sigma((\sqrt{x})^2) = (\sigma(\sqrt{x}))^2$ . Un cuadrado en  $\mathbb{R}$  es siempre positivo o cero. Como  $\sigma$  es un automorfismo (y por tanto inyectivo, enviando  $0 \mapsto 0$ ), para  $x > 0$  se tiene estrictamente que  $\sigma(x) > 0$ . Si tomamos  $a < b$ , entonces  $b - a > 0$ . Por la propiedad anterior,  $\sigma(b - a) > 0$ , y por linealidad  $\sigma(b) - \sigma(a) > 0$ , lo que implica  $\sigma(a) < \sigma(b)$ . Por lo tanto,  $\sigma$  preserva el orden estrictamente.
2. **¿Por qué el único automorfismo es la identidad?** Sabemos que todo automorfismo fija el cuerpo primo; por tanto,  $\sigma(q) = q$  para todo  $q \in \mathbb{Q}$ . Sea  $x \in \mathbb{R}$  un número irracional. Por la densidad de  $\mathbb{Q}$  en  $\mathbb{R}$ , podemos acotarlo entre dos sucesiones de racionales tales que  $q_1 < x < q_2$ . Dado que  $\sigma$  es creciente (como demostramos arriba), preserva estas desigualdades:  $\sigma(q_1) < \sigma(x) < \sigma(q_2)$ . Como  $\sigma$  fija los racionales, esto se traduce en  $q_1 < \sigma(x) < q_2$ . Al tomar el límite cuando  $q_1$  y  $q_2$  tienden a  $x$ , por el Teorema del Sandwich (o encaje de intervalos), obtenemos forzosamente que  $\sigma(x) = x$ . Por tanto,  $\sigma$  es la identidad en todo  $\mathbb{R}$ .
3. **¿Por qué  $\text{Gal}(\mathbb{R}/K) = 1$ ?** El grupo  $\text{Gal}(\mathbb{R}/K)$  está formado por los automorfismos de  $\mathbb{R}$  que fijan  $K$ . Pero acabamos de demostrar que el único automorfismo general de  $\mathbb{R}$  (es decir, el único elemento de  $\text{Aut}(\mathbb{R})$ ) es la identidad. Por tanto, exijamos que fije  $K$  o que fije  $\mathbb{Q}$ , el único candidato posible sigue siendo la aplicación identidad.

### Ejemplo 1.1.4:

Sean  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  y  $\sigma \in \text{Gal}(K/\mathbb{Q})$ . Entonces  $\sigma(\sqrt{2}) = \pm\sqrt{2}$  y  $\sigma(\sqrt{3}) = \pm\sqrt{3}$  y por tanto  $\text{Gal}(K/\mathbb{Q})$  tiene al menos 4 elementos. De hecho  $\text{Gal}(K/\mathbb{Q})$  tiene exactamente cuatro elementos. En efecto, en el Ejemplo (2) hemos visto que  $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$  tiene 2 elementos. Por otro lado  $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$  (ver Ejercicio 1.11 del Capítulo 1). Por tanto,  $K/\mathbb{Q}(\sqrt{2})$  es una extensión separable (¿por qué?) de grado 2, con lo que cada uno de los dos elementos de  $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$  tiene dos extensiones a un homomorfismo de  $K$  en una clausura algebraica de  $K$  que, como además  $K/\mathbb{Q}$  es normal (¿por qué?), estas dos extensiones son elementos

de  $\text{Gal}(K/\mathbb{Q})$ . Por tanto  $\text{Gal}(K/\mathbb{Q})$  tiene cuatro elementos:  $\sigma_{++}, \sigma_{+-}, \sigma_{-+}, \sigma_{--}$  dados por  $\sigma_{ab}(\sqrt{2}) = a\sqrt{2}$  y  $\sigma_{ab}(\sqrt{3}) = b\sqrt{3}$ .

#### Observación 1.1.6: Justificación del Ejemplo 4

- ¿Por qué  $K/\mathbb{Q}(\sqrt{2})$  es separable?** Esta extensión se obtiene adjuntando  $\sqrt{3}$ , cuyo polinomio mínimo sobre  $\mathbb{Q}(\sqrt{2})$  es divisor de  $X^2 - 3$ . Estamos trabajando sobre una extensión de  $\mathbb{Q}$ , lo que significa que el cuerpo base tiene característica cero. Todo polinomio irreducible sobre un cuerpo de característica cero es separable (sus derivadas formales nunca son nulas), por lo que toda extensión algebraica en característica cero es automáticamente separable.
- ¿Por qué  $K/\mathbb{Q}$  es normal?** Una extensión finita es normal si y solo si es el cuerpo de escisión de algún polinomio sobre el cuerpo base. En este caso,  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  contiene todas las raíces del polinomio  $f(X) = (X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$ , y de hecho es generado por ellas. Al ser cuerpo de escisión, la extensión es normal.

#### Ejemplo 1.1.5:

Sea  $\xi$  una raíz  $n$ -ésima primitiva de la unidad y sea  $L = K(\xi)/K$  una extensión ciclotómica. Si  $\sigma \in \text{Gal}(L/K)$ , entonces  $\sigma(\xi) = \xi^i$  para algún entero  $i$  coprimo con  $n$ , y  $\sigma$  está completamente determinada por el resto de  $i$  módulo  $n$ . Por tanto, tenemos una aplicación  $\psi : \text{Gal}(L/K) \rightarrow \mathbb{Z}_n^*$  que asocia  $\sigma \in \text{Gal}(L/K)$  con la única clase en  $\mathbb{Z}_n^*$  que contiene a  $i$  (con  $\sigma(\xi) = \xi^i$ ). Entonces  $\psi$  es un homomorfismo inyectivo de grupos (comprobarlo) y por tanto  $\text{Gal}(L/K)$  es isomorfo a un subgrupo de  $\mathbb{Z}_n^*$ . En particular, el grupo de Galois de toda extensión ciclotómica es abeliano. Si además  $K = \mathbb{Q}$ , entonces  $\text{Min}_{\mathbb{Q}}(\xi) = \Phi_n$ , el  $n$ -ésimo polinomio ciclotómico (Teorema 3.9). Por tanto, para cada  $i$  coprimo con  $n$  existe un elemento  $\sigma \in \text{Gal}(L = \mathbb{Q}(\xi)/\mathbb{Q})$  con  $\sigma(\xi) = \xi^i$ . En otras palabras,  $\text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$  es isomorfo a  $\mathbb{Z}_n^*$  y un isomorfismo  $\tau : \mathbb{Z}_n^* \rightarrow \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$  viene dado asociando  $i \in \mathbb{Z}_n^*$  con el único automorfismo  $\tau_i$  de  $\mathbb{Q}(\xi)$  tal que  $\tau_i(\xi) = \xi^i$ .

#### Observación 1.1.7: Justificación del Ejemplo 5

##### Comprobación de que $\psi$ es un homomorfismo inyectivo:

Primero, veamos que respeta la operación del grupo (la composición). Sean  $\sigma, \tau \in \text{Gal}(L/K)$ . Supongamos que  $\psi(\sigma) = [i]$  y  $\psi(\tau) = [j]$ , lo que significa por definición que  $\sigma(\xi) = \xi^i$  y  $\tau(\xi) = \xi^j$ . Calculemos la imagen de  $\xi$  bajo la composición  $\sigma \circ \tau$ :

$$(\sigma \circ \tau)(\xi) = \sigma(\tau(\xi)) = \sigma(\xi^j)$$

Como  $\sigma$  es un homomorfismo de cuerpos, preserva los exponentes:

$$\sigma(\xi^j) = (\sigma(\xi))^j = (\xi^i)^j = \xi^{ij}$$

Esto nos dice que el automorfismo composición  $\sigma \circ \tau$  eleva  $\xi$  a la potencia  $ij$ . Por tanto,  $\psi(\sigma \circ \tau) = [ij] = [i][j] = \psi(\sigma)\psi(\tau)$  en el grupo multiplicativo  $\mathbb{Z}_n^*$ . Esto demuestra que  $\psi$  es un homomorfismo.

Segundo, evaluemos la inyectividad estudiando el núcleo. Supongamos que  $\sigma \in \ker(\psi)$ . Esto significa que  $\psi(\sigma)$  es el elemento neutro de  $\mathbb{Z}_n^*$ , es decir, la clase  $[1]$ . Entonces,  $\sigma(\xi) = \xi^1 = \xi$ . Dado que el cuerpo  $L = K(\xi)$  está generado en su totalidad por  $\xi$  y los elementos

de  $K$  (los cuales todo automorfismo de Galois deja fijos por definición), si un automorfismo deja fijo al generador  $\xi$ , obligatoriamente deja fijo a todo elemento de  $L$ . Luego  $\sigma = \text{id}_L$ . Al ser su núcleo trivial,  $\psi$  es inyectiva.

#### Observación 1.1.8: Isomorfismos de grupos de Galois

Obsérvese que si  $\phi : L \rightarrow L^*$  es un  $K$ -isomorfismo, entonces la aplicación  $\text{Gal}(L/K) \rightarrow \text{Gal}(L^*/K)$  dada por  $\sigma \mapsto \phi\sigma\phi^{-1}$  es un isomorfismo.

Si  $L/K$  es una extensión algebraica y  $\bar{L}$  una clausura algebraica de  $L$ , entonces podemos ver cada elemento de  $\text{Gal}(L/K)$  como un elemento de  $S_1^L = \{\sigma : L \rightarrow \bar{L} \mid \sigma|_K = 1_K\}$ . Por tanto de la Proposición 4.9 deducimos:

#### Proposición 1.1.1:

Si  $L/K$  es una extensión finita entonces  $|\text{Gal}(L/K)| \leq [L : K]_s \leq [L : K]$ .

Recordemos que  $\text{Sub}(L/K)$  denota el conjunto de las subextensiones de  $L/K$ . Si  $G$  es un grupo, entonces vamos a denotar por  $\text{Sub}(G)$  al conjunto de todos los subgrupos de  $G$  y si  $H$  es un subgrupo de  $G$ , entonces  $\text{Sub}(G/H)$  es el conjunto de los subgrupos de  $G$  que contienen a  $H$ . En realidad esta última notación es ambigua pues si  $N$  es un subgrupo normal de  $G$ , entonces  $\text{Sub}(G/N)$  tiene dos significados: el conjunto de los subgrupos de  $G$  que contienen a  $N$  y el conjunto de los subgrupos del cociente  $G/N$ . El Teorema de la Correspondencia (Teorema 5.4 de GyA) nos muestra que esta ambigüedad no es muy grave.

Consideramos  $\text{Sub}(L/K)$  y  $\text{Sub}(G/H)$  como conjuntos ordenados por la inclusión. Una aplicación  $f : (A, \leq) \rightarrow (B, \leq)$  entre conjuntos ordenados se dice que es un homomorfismo de conjuntos ordenados si conserva el orden, es decir, si para cada  $x, y \in A$  tales que  $x \leq y$  se verifica que  $f(x) \leq f(y)$  y se dice que es un anti-homomorfismo de conjuntos ordenados si  $f(x) \geq f(y)$  para todo  $x, y \in A$  con  $x \leq y$ .

Si  $L/K$  es una extensión de cuerpos entonces tenemos dos aplicaciones:

$$\begin{aligned} (-)^\circ &= \text{Gal}(L/-) : \text{Sub}(L/K) \longrightarrow \text{Sub}(\text{Gal}(L/K)) \\ (-)^\circ &= L^{(-)} : \text{Sub}(\text{Gal}(L/K)) \longrightarrow \text{Sub}(L/K) \end{aligned}$$

La aplicación que va para la derecha asocia  $F \in \text{Sub}(L/K)$  con

$$F^\circ = \text{Gal}(L/F) = \{\sigma \in \text{Gal}(L/K) \mid \sigma(x) = x \text{ para todo } x \in F\}$$

y la que va para la izquierda asocia  $H \in \text{Sub}(\text{Gal}(L/K))$  con

$$H^\circ = L^H = \{a \in L \mid \sigma(a) = a \text{ para todo } \sigma \in H\}.$$

El par formado por estas aplicaciones se llama correspondencia de Galois de la extensión  $L/K$ . Veamos algunas propiedades de la correspondencia de Galois.

Recordemos que tanto la unidad de un anillo, como el neutro de un grupo o el subgrupo trivial del grupo lo denotamos siempre como 1. Por el contexto no debería haber confusión. En la siguiente proposición 1 siempre denota el subgrupo trivial de  $\text{Gal}(L/K)$ .

**Proposición 1.1.2:**

Sea  $L/K$  una extensión de cuerpos y sea  $G = \text{Gal}(L/K)$ . [La correspondencia de Galois  $(-)^{\circ} : \text{Sub}(L/K) \rightleftharpoons \text{Sub}(G)$  satisface las siguientes propiedades, donde  $X$  e  $Y$  son ambos subextensiones de  $L/K$  o ambos subgrupos de  $G$ :

- (1)  $L^{\circ} = 1$ ,  $K^{\circ} = G$  y  $1^{\circ} = L$ . ]
- (1)  $(-)^{\circ} = \text{Gal}(L/-)$  y  $(-)^{\circ} = L^{(-)}$  son antihomomorfismos de conjuntos ordenados, es decir, si  $X \subseteq Y$  entonces  $Y^{\circ} \subseteq X^{\circ}$ . ]
- (1)  $X \subseteq X^{\circ\circ}$  y  $X^{\circ} = X^{\circ\circ\circ}$ .
- (1) Las dos aplicaciones que forman la correspondencia de Galois se restringen a un anti-isomorfismo de conjuntos ordenados entre sus dos imágenes.

*Demostración.* (1) y (2) y la inclusión  $X \subseteq X^{\circ\circ}$  son sencillos ejercicios. Por tanto  $X^{\circ} \subseteq X^{\circ\circ\circ} \subseteq X^{\circ}$ , lo que prueba la igualdad de (3). Finalmente (4) es consecuencia inmediata de (2) y la igualdad de (3).  $\square$

Los elementos de las imágenes de las dos aplicaciones de la correspondencia de Galois se dice que son respectivamente subextensiones cerradas en  $L/K$  y subgrupos cerrados en  $\text{Gal}(L/K)$ . Obsérvese que de la propiedad (3) de la Proposición 5.3 se tiene que  $X$  es cerrado si y solo si  $X = X^{\circ\circ\circ}$ .

**Corolario 1.1.1:**

Las aplicaciones de la correspondencia de Galois de una extensión de cuerpos  $L/K$  se restringen a un anti-isomorfismo de conjuntos ordenados entre las subextensiones cerradas en  $L/K$  y los subgrupos cerrados en  $\text{Gal}(L/K)$ .

Por la Proposición 5.3,  $L$ ,  $1$  y  $\text{Gal}(L/K)$  son cerrados en  $L/K$ , pero  $K$  no tiene por qué serlo. Por ejemplo, si  $L \neq K$  y  $\text{Gal}(L/K) = 1$  (ver Ejemplos 5.1) entonces  $K^{\circ\circ\circ} = 1^{\circ} = L \neq K$ .

**Proposición 1.1.3:**

Sea  $L/K$  una extensión de cuerpos.

- (1) Si  $E_1 \subseteq E_2$  son subextensiones de  $L/K$  con  $E_2/E_1$  finita entonces  $[E_1^{\circ} : E_2^{\circ}] \leq [E_2 : E_1]$ .
- (1) Si  $H_1 \leq H_2$  son subgrupos de  $\text{Gal}(L/K)$  con  $[H_2 : H_1] < \infty$ , entonces  $[H_1^{\circ} : H_2^{\circ}] \leq [H_2 : H_1]$ .

*Demostración.* (1) Razonamos por inducción sobre  $n = [E_2 : E_1]$  con el caso  $n = 1$  obvio. Supongamos pues que  $n > 1$  y la hipótesis de inducción. Sean  $\alpha \in E_2 \setminus E_1$ ,  $p = \text{Min}_{E_1}(\alpha)$  y  $s = \text{gr}(p)$ . Entonces  $s = [E_1(\alpha) : E_1]$  y  $[E_2 : E_1(\alpha)] < n$ . Si  $s < n$ , entonces por la hipótesis de inducción tenemos:

$$[E_1^{\circ} : E_2^{\circ}] = [E_1^{\circ} : E_1(\alpha)^{\circ}][E_1(\alpha)^{\circ} : E_2^{\circ}] \leq [E_1(\alpha) : E_1][E_2 : E_1(\alpha)] = [E_2 : E_1].$$

En caso contrario,  $E_2 = E_1(\alpha)$ . Sean  $R$  el conjunto de raíces de  $p$  y  $\phi : E_1^\circ/E_2^\circ \rightarrow R$  la aplicación dada por  $\phi(\sigma E_2^\circ) = \sigma(\alpha)$ . Es fácil ver que esta aplicación está bien definida y es inyectiva. Por tanto  $[E_1^\circ : E_2^\circ] \leq |R| \leq \text{gr}(p) = [E_2 : E_1]$ .

(2) Pongamos  $[H_2 : H_1] = n$ ,  $H_2/H_1 = \{\tau_1 H_1, \dots, \tau_n H_1\}$  con  $\tau_1 = 1$  y razonemos por reducción al absurdo, es decir, supondremos que  $[H_1^\circ : H_2^\circ] > n$ . Entonces existen  $\alpha_1, \dots, \alpha_n, \alpha_{n+1} \in H_1^\circ$  linealmente independientes sobre  $H_2^\circ$ . Consideremos la matriz:

$$A = \begin{pmatrix} \tau_1(\alpha_1) & \tau_1(\alpha_2) & \dots & \tau_1(\alpha_{n+1}) \\ \tau_2(\alpha_1) & \tau_2(\alpha_2) & \dots & \tau_2(\alpha_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_n(\alpha_1) & \tau_n(\alpha_2) & \dots & \tau_n(\alpha_{n+1}) \end{pmatrix}$$

y sea  $r$  el rango de  $A$ . Reordenamos los  $\alpha_i$  para que las primeras  $r$  columnas sean linealmente independientes. Entonces la columna  $r+1$  es combinación lineal de las  $r$  primeras (obsérvese que  $r \leq n < n+1 = \text{número de columnas de } A$ ) y por tanto existe  $a = (a_1, \dots, a_r, 1, 0, \dots, 0)^T \in (L)^{n+1}$  tal que  $Aa = 0$ . Como  $\tau_1 = 1$  tenemos:

$$\alpha_1 a_1 + \dots + \alpha_r a_r + \alpha_{r+1} = 0$$

y, como los  $\alpha_i$  son linealmente independientes sobre  $H_2^\circ$ , existe  $1 \leq i \leq r$  tal que  $a_i \notin H_2^\circ$ . Reordenando  $a_1, \dots, a_r$  podemos suponer que  $a_1 \notin H_2^\circ$ , es decir  $\sigma(a_1) \neq a_1$  para algún  $\sigma \in H_2$ . La aplicación  $H_2/H_1 \rightarrow H_2/H_1$  dada por  $\tau H_1 \mapsto \sigma\tau H_1$  es inyectiva pues si  $\sigma\sigma_1 H_1 = \sigma\sigma_2 H_1$  entonces  $\sigma_2^{-1}\sigma_1 = (\sigma\sigma_2)^{-1}(\sigma\sigma_1) \in H_1$ , luego  $\sigma_1 H_1 = \sigma_2 H_1$ . Por tanto existe una permutación  $\rho \in S_n$  tal que  $\sigma^{-1}\tau_i = \tau_{\rho(i)}$  para todo  $i = 1, \dots, n$ , con lo que la matriz:

$$B = \begin{pmatrix} \sigma^{-1}\tau_1(\alpha_1) & \sigma^{-1}\tau_1(\alpha_2) & \dots & \sigma^{-1}\tau_1(\alpha_{n+1}) \\ \sigma^{-1}\tau_2(\alpha_1) & \sigma^{-1}\tau_2(\alpha_2) & \dots & \sigma^{-1}\tau_2(\alpha_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^{-1}\tau_n(\alpha_1) & \sigma^{-1}\tau_n(\alpha_2) & \dots & \sigma^{-1}\tau_n(\alpha_{n+1}) \end{pmatrix}$$

se obtiene permutando las filas de la matriz  $A$ . Eso implica que  $Ba = 0$  y por tanto  $A\sigma(a) = 0$ . Luego  $A(a - \sigma(a)) = 0$  y:

$$a - \sigma(a) = \begin{pmatrix} a_1 - \sigma(a_1) \\ \vdots \\ a_r - \sigma(a_r) \\ 1 - 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_1 - \sigma(a_1) \\ \vdots \\ a_r - \sigma(a_r) \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

con  $a_1 - \sigma(a_1) \neq 0$ . Eso implica que las primeras  $r$  columnas de  $A$  son linealmente dependientes en contra de la elección, lo que proporciona la contradicción deseada.  $\square$

**Corolario 1.1.2:**

Sea  $L/K$  una extensión de cuerpos.

1. Si  $K \subseteq E_1 \subseteq E_2 \subseteq L$  es una torre de cuerpos, con  $[E_2 : E_1] < \infty$  y  $E_1$  cerrado en  $L/K$  entonces  $E_2$  es cerrado en  $L/K$  y  $[E_1^\circ : E_2^\circ] = [E_2 : E_1]$ .
2. Si  $H_1 \leq H_2 \leq \text{Gal}(L/K)$  son subgrupos de  $\text{Gal}(L/K)$  con  $[H_2 : H_1] < \infty$  y  $H_1$  cerrado en  $L/K$  entonces  $H_2$  es cerrado en  $L/K$  y  $[H_1^\circ : H_2^\circ] = [H_2 : H_1]$ .

*Demostración.* (1) Aplicando el primer apartado de la Proposición 5.5 a  $E_1 \leq E_2$  obtenemos que  $[E_1^\circ : E_2^\circ] \leq [E_2 : E_1]$  y aplicando el segundo apartado a  $E_2^\circ \subseteq E_1^\circ$  obtenemos  $[E_2^{\circ\circ} : E_1^{\circ\circ}] \leq [E_1^\circ : E_2^\circ]$ . Como  $E_1$  es cerrado tenemos que  $[E_2^{\circ\circ} : E_1] = [E_2^{\circ\circ} : E_1^\circ] \leq [E_2 : E_1]$  y como  $E_2 \subseteq E_2^{\circ\circ}$  concluimos que  $E_2 = E_2^{\circ\circ}$ , es decir  $E_2^{\circ\circ}$  es cerrado.

(2) Es completamente análoga. □

Como consecuencia del segundo apartado del Corolario 5.6 y el primero de la Proposición 5.3 se tiene el siguiente corolario:

**Corolario 1.1.3:**

Todo subgrupo finito de  $\text{Gal}(L/K)$  es cerrado en  $L/K$ .

## 1.2. Extensiones de Galois

**Definición 1.2.1: Extensión de Galois**

Una extensión de Galois es una extensión de cuerpos que es normal y separable.

**Observación 1.2.1:**

Obsérvese que toda extensión de Galois es algebraica (por ser separable).

La siguiente proposición es consecuencia inmediata de las Proposiciones 2.15 y 4.16.

**Proposición 1.2.1:**

La clase de extensiones de Galois es cerrada para levantamientos.

El siguiente teorema caracteriza las extensiones de Galois.

**Teorema 1.2.1:**

Las siguientes condiciones son equivalentes para una extensión de cuerpos  $L/K$  con  $G = \text{Gal}(L/K)$ :

- (1)  $L/K$  es una extensión de Galois.
- (1)  $L/E$  es una extensión de Galois para todo  $E \in \text{Sub}(L/K)$ .
- (1)  $L/K$  es algebraica y toda subextensión de  $L/K$  es cerrada.
- (1)  $L/K$  es algebraica y  $K$  es una subextensión cerrada de  $L/K$ .
- (1)  $L/K$  es algebraica y  $G^\circ = K$ , o sea, si  $\alpha \in L$  satisface  $\sigma(\alpha) = \alpha$  para todo  $\sigma \in G$  entonces  $\alpha \in K$ .
- (1)  $L/K$  es algebraica y para todo  $\alpha \in L \setminus K$  existe  $\sigma \in \text{Gal}(L/K)$  tal que  $\sigma(\alpha) \neq \alpha$ .

*Demostración.* (1)  $\implies$  (2) es consecuencia de la Proposición 5.9.

(2)  $\implies$  (3). Supongamos que  $L/K$  satisface (2) y sea  $E \in \text{Sub}(L/K)$ . De la Proposición 5.3 se tiene que  $E \subseteq E^{\circ\circ}$  y tenemos que demostrar que se verifica la igualdad, o lo que es lo mismo, tenemos que demostrar que si  $\alpha \in L \setminus E$  entonces existe  $\sigma \in \text{Gal}(L/E)$  tal que  $\sigma(\alpha) \neq \alpha$ . Sea  $\alpha \in L \setminus E$  y sea  $p = \text{Min}_E(\alpha)$ . Este polinomio tiene una raíz en  $L$  y, como  $L/E$  es normal,  $p$  es completamente factorizable en  $L$ . Como además  $L/E$  es separable y  $\alpha \notin E$ , existe  $\beta \in L$ , con  $\alpha \neq \beta$ , tal que  $\beta$  también es raíz de  $p$ . De la Proposición 1.10 se deduce que existe un  $E$ -isomorfismo  $\sigma : E(\alpha) \rightarrow E(\beta)$ . Sea  $\bar{L}$  una clausura algebraica de  $L$ . Como  $L/E$  es algebraica (y por tanto también lo es  $L/E(\alpha)$ ),  $\sigma$  se extiende a un homomorfismo de  $L$  en  $\bar{L}$  que también denotaremos por  $\sigma$ , y como  $L/E$  es normal,  $\sigma(L) \subseteq L$ , con lo que  $\sigma \in \text{Gal}(L/E)$ . Deducimos que  $\alpha \neq \beta = \sigma(\alpha)$ .

(3)  $\implies$  (4), (4)  $\implies$  (5), y que (5) y (6) son equivalentes, está claro.

(5)  $\implies$  (1). Supongamos que  $L/K$  verifica (5). Sea  $\alpha \in L$ ; sean  $p = \text{Min}_K(\alpha)$  y  $n = \text{gr}(p)$ . Tenemos que demostrar que  $p$  factoriza completamente en  $L$  (para demostrar que  $L/K$  es normal) y que  $p$  no tiene raíces múltiples (para mostrar que  $L/K$  es separable). Esto equivale a demostrar que  $p$  tiene  $n$  raíces (distintas) en  $L$ . Sea  $R = \{\alpha = \alpha_1, \dots, \alpha_r\}$  el conjunto de las (distintas) raíces de  $p$  en  $L$  y sea  $q = (X - \alpha_1) \cdots (X - \alpha_r)$ . Si  $\sigma \in \text{Gal}(L/K)$ , entonces  $\sigma(\alpha_i)$  es una raíz de  $p$  en  $L$ , lo que implica que  $\sigma$  induce una permutación de  $R$  y por tanto  $\sigma(q) = q$ , es decir  $\sigma(a) = a$  para cada uno de los coeficientes  $a$  de  $q$ . Como estamos suponiendo que  $L/K$  satisface la propiedad (5), concluimos que cada uno de estos coeficientes pertenece a  $K$ , es decir  $q \in K[X]$ . Como  $r = \text{gr}(q) \leq n = \text{gr}(p)$  y  $p$  tiene grado mínimo entre los polinomios de  $K[X]$  que tienen a  $\alpha$  como raíz deducimos que  $p = q$  y por tanto  $r = n$ .  $\square$

La siguiente proposición muestra criterios para decidir si una extensión es de Galois para el caso de extensiones finitas.

**Proposición 1.2.2:**

Las siguientes condiciones son equivalentes para una extensión finita  $L/K$ :

- (1)  $L/K$  es una extensión de Galois.
- (1)  $[L : K] = |\text{Gal}(L/K)|$ .
- (1)  $[L : E] = |\text{Gal}(L/E)|$  para todo  $E \in \text{Sub}(L/K)$ .

*Demostración.* Sea  $\bar{L}$  una clausura algebraica. Podemos ver cada elemento de  $\text{Gal}(L/K)$  como un  $K$ -homomorfismo de  $L$  en  $\bar{L}$ . De esta manera, si  $\sigma$  denota la inclusión de  $K$  en  $L$  tenemos que  $\text{Gal}(L/K) \subseteq S_\sigma^L$ . Combinando esto con la Proposición 5.2 tenemos que:

$$|\text{Gal}(L/K)| \leq [L : K]_s \leq [L : K]$$

Por el Teorema 4.12, la segunda desigualdad es una igualdad si y solo si  $L/K$  es separable. La primera desigualdad es una igualdad si y solo si todo  $K$ -homomorfismo de  $L$  a  $\bar{L}$  cumple  $\tau(L) \subseteq L$  si y solo si  $L/K$  es normal. Esto demuestra que (1) y (2) son equivalentes.  $\square$

Combinando la equivalencia entre (1) y (2) y el Teorema 5.10 se deduce de forma inmediata que (1) y (3) son equivalentes.  $\square$

**Teorema 1.2.2: Teorema Fundamental de la Teoría de Galois**

Sea  $L/K$  una extensión de Galois finita y sea  $G = \text{Gal}(L/K)$ . Entonces se verifican las siguientes propiedades:

- (1) La correspondencia de Galois es un anti-isomorfismo de conjuntos ordenados entre  $\text{Sub}(L/K)$  y  $\text{Sub}(G)$ .
- (1) Si  $X$  e  $Y$  están ambos en  $\text{Sub}(L/K)$  o en  $\text{Sub}(G)$  y  $X \subseteq Y$  entonces  $[X^\circ : Y^\circ] = [Y : X]$ . En particular:
  - (a) Si  $E \in \text{Sub}(L/K)$  entonces  $[L : E] = |E^\circ|$  y  $[E : K] = [G : E^\circ]$ .
  - (a) Si  $H \in \text{Sub}(G)$  entonces  $|H| = [L : H^\circ]$  y  $[G : H] = [H^\circ : K]$ .

*Demostración.* (1) A la vista de la Proposición 5.3 y el Teorema 5.10, para demostrar (1) sólo falta demostrar que todo subgrupo  $H$  de  $G$  es cerrado, pero eso es consecuencia inmediata del Corolario 5.7.

(2) Es consecuencia de la Proposición 5.6.  $\square$

Si  $K \subseteq E \subseteq L$  es una torre de cuerpos y  $\sigma \in \text{Gal}(L/K)$ , entonces  $\text{Res}_E^L(\sigma)$  denota la restricción de  $\sigma$  a  $E$ . En principio  $\text{Res}_E^L(\sigma)$  es un  $K$ -homomorfismo de  $E$  en  $L$ , pero si  $E/K$  es normal entonces  $\sigma \in \text{Gal}(E/K)$ . Eso es lo que pasa en las condiciones de la siguiente proposición y está claro que en tal caso  $\text{Res}_E^L : \text{Gal}(L/K) \rightarrow \text{Gal}(E/K)$  es un homomorfismo de grupos.

**Proposición 1.2.3:**

Sea  $L/K$  una extensión finita de Galois. Si  $E \in \text{Sub}(L/K)$  entonces las siguientes condiciones son equivalentes:

- (1)  $E/K$  es de Galois.
- (1)  $E/K$  es normal.
- (1)  $\sigma(E) \subseteq E$  para todo  $\sigma \in \text{Gal}(L/K)$ .
- (1)  $\text{Gal}(L/E)$  es normal en  $\text{Gal}(L/K)$ .

Además, si estas condiciones se satisfacen, entonces la aplicación de restricción

$$\text{Res}_E^L : \text{Gal}(L/K) \rightarrow \text{Gal}(E/K), \quad \sigma \mapsto \sigma|_E$$

es suprayectiva y como su núcleo es  $\text{Gal}(L/E)$ , se tiene que

$$\text{Gal}(E/K) \simeq \frac{\text{Gal}(L/K)}{\text{Gal}(L/E)}$$

*Demostración.* La equivalencia entre (1) y (2) es consecuencia inmediata de que la clase de extensiones separables es multiplicativa (Proposición 4.13).

(2)  $\implies$  (3). Supongamos que  $E/K$  es normal y sean  $\alpha \in E$  y  $\sigma \in \text{Gal}(L/K)$ . Entonces  $p = \text{Min}_K(\alpha)$  es completamente factorizable en  $E$ , o sea  $p = (X - \alpha_1) \cdots (X - \alpha_n)$  con  $\alpha_1, \dots, \alpha_n \in E$ . Entonces  $\sigma(\alpha)$  es raíz de  $p$  y por tanto  $\sigma(\alpha) = \alpha_i \in E$ , para algún  $i$ . Esto prueba que  $\sigma(E) \subseteq E$ .

(3)  $\implies$  (4). Supongamos que se verifica (3) y sean  $\sigma \in \text{Gal}(L/K)$  y  $\tau \in \text{Gal}(L/E)$ . Entonces  $\sigma(E) \subseteq E$  y por tanto  $\tau(\sigma(\alpha)) = \sigma(\alpha)$ , es decir  $\sigma^{-1}\tau\sigma(\alpha) = \alpha$ , para todo  $\alpha \in E$ . Esto prueba que  $\sigma^{-1}\tau\sigma \in \text{Gal}(L/E)$  para todo  $\sigma \in \text{Gal}(L/K)$  y todo  $\tau \in \text{Gal}(L/E)$ , es decir  $\text{Gal}(L/E)$  es normal en  $\text{Gal}(L/K)$ .

(4)  $\implies$  (2). Supongamos que  $\text{Gal}(L/E)$  es normal en  $\text{Gal}(L/K)$ . Sea  $\rho : E \rightarrow \bar{L}$  un  $K$ -homomorfismo. Como  $L/E$  es algebraica,  $\rho$  se extiende a un  $K$ -homomorfismo  $\sigma : L \rightarrow \bar{L}$ . Como  $L/K$  es normal,  $\sigma(L) = L$  (Teorema 2.11), y por tanto podemos considerar  $\sigma$  como un elemento de  $\text{Gal}(L/K)$ . Por hipótesis,  $\sigma^{-1}\tau\sigma \in \text{Gal}(L/E)$  para todo  $\tau \in \text{Gal}(L/E)$ , con lo que  $\tau\sigma(\alpha) = \sigma(\alpha)$ , para todo  $\tau \in \text{Gal}(L/E)$  y todo  $\alpha \in E$ . Esto muestra que  $\rho(\alpha) = \sigma(\alpha) \in \text{Gal}(L/E)^\circ = E^{\circ\circ} = E^{65}]$ . Como  $L/E$  es algebraica,  $\bar{L}$  es una clausura algebraica de  $E$  con lo que hemos comprobado que  $E/K$  satisface las condiciones del Teorema 2.11, es decir  $E/K$  es normal<sup>65]</sup>.

Supongamos ahora que las condiciones (1)-(4) se verifican. Entonces la aplicación de restricción

$$f = \text{Res}_E^L : \text{Gal}(L/K) \rightarrow \text{Gal}(E/K), \quad \sigma \mapsto \sigma|_E$$

es un homomorfismo de grupos cuyo núcleo es  $\text{Gal}(L/E)$ . Aplicando el Primer Teorema de Isomorfía y que todas las extensiones  $L/K$ ,  $E/K$  y  $L/E$  son de Galois deducimos que

$$|\text{Im } f| = \frac{|\text{Gal}(L/K)|}{|\text{Gal}(L/E)|} = \frac{[L : K]}{[L : E]} = [E : K] = |\text{Gal}(E/K)|,$$

lo que implica que  $f$  es suprayectiva y  $\text{Gal}(E/K) \simeq \frac{\text{Gal}(L/K)}{\text{Gal}(L/E)}$ . □

En el siguiente Teorema volvemos a encontrar una versión diferente de homomorfismo de restricción.

### Teorema 1.2.3: Teorema de las Irracionalidades Accesorias de Lagrange

Sean  $L/K$  y  $E/K$  dos extensiones admisibles y supongamos que la primera es finita y de Galois. Entonces  $LE/E$  y  $L/L \cap E$  son extensiones de Galois finitas y el homomorfismo de restricción

$$\text{Res}_L^{LE} : \text{Gal}(LE/E) \rightarrow \text{Gal}(L/L \cap E)$$

es un isomorfismo de grupos.

*Demostración.* Como  $L/K$  es de Galois, del Teorema 5.10 se deduce que  $L/L \cap E$  también es de Galois y de la Proposición 5.9 que lo es  $LE/E$ [76]. Que la primera es finita es obvio y que lo sea la segunda es consecuencia de la Proposición 1.18[76].

Sea  $f = \text{Res}_L^{LE}$ [77]. Que  $f$  es inyectiva es obvio ya que un elemento del núcleo es un automorfismo  $\sigma$  de  $LE$  que verifica  $\sigma(x) = x$  para todo  $x \in L$  y todo  $x \in E$ [77].

Para ver que  $f$  es suprayectiva ponemos  $H = \text{Im } f \subseteq \text{Gal}(L/L \cap E)$ [78]. Entonces  $L \cap E = (L \cap E)^{\circ\circ} = \text{Gal}(L/L \cap E)^{\circ} \subseteq H^{\circ}$ [78]. Sea  $\alpha \in H^{\circ}$ [78]. Entonces para todo  $\sigma \in \text{Gal}(LE/E)$  se verifica  $\sigma(\alpha) = f(\sigma)(\alpha) = \alpha$ , pues  $f(\sigma) \in H$ [79]. Esto demuestra que  $\alpha \in \text{Gal}(LE/E)^{\circ} = E^{\circ\circ} = E$ , pues  $LE/E$  es de Galois[79]. Como esto se verifica para cada  $\alpha \in H^{\circ}$  y  $H^{\circ} \subseteq L$  deducimos que  $H^{\circ} \subseteq L \cap E = (L \cap E)^{\circ\circ}$ [80]. Por tanto,  $H^{\circ} = (L \cap E)^{\circ\circ}$ [80]. Como  $L/L \cap E$  es de Galois, concluimos que  $\text{Im } f = H = (L \cap E)^{\circ\circ} = \text{Gal}(L/L \cap E)$ , o sea  $f$  es suprayectiva[80].  $\square$

### Ejemplo 1.2.1:

Vamos a calcular los subcuerpos del cuerpo de escisión  $F$  del polinomio  $X^5 - p$ , donde  $p$  es un número primo, y cuáles son normales sobre  $\mathbb{Q}$ [83].

Los subcuerpos de  $F$  son precisamente las subextensiones de  $F/\mathbb{Q}$ [84]. Por el Teorema Fundamental de la Teoría de Galois (Teorema 5.12) dichos cuerpos están en correspondencia biunívoca con los subgrupos de  $G = \text{Gal}(F/\mathbb{Q})$  y los normales son los que corresponden con subgrupos normales de  $G$ [84]. Sea  $\alpha = \sqrt[5]{p}$ [84].

Entonces  $F = \mathbb{Q}(\alpha, \zeta_5)$ . Además,  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$  y  $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \varphi(5) = 4$ [85]. Por tanto  $[F : \mathbb{Q}]$  es al menos 20[85]. Por otro lado  $[F : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$  y por tanto  $[F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 20$ [85]. Luego  $|G| = [F : \mathbb{Q}] = 20$ [86]. Además  $G$  contiene a  $\text{Gal}(F/\mathbb{Q}(\alpha))$  y a  $\text{Gal}(F/\mathbb{Q}(\zeta_5))$  que serán dos subgrupos de órdenes 4 y 5 respectivamente[86].

Por el Teorema de las Irracionalidades Accesorias (Teorema 5.14),  $\text{Res}_{\mathbb{Q}(\zeta_5)}^F : \text{Gal}(F/\mathbb{Q}(\alpha)) \rightarrow \text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$  es un isomorfismo[87]. Usando el isomorfismo entre  $\text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$  y  $\mathbb{Z}_5^*$  (Problema (3.15)) deducimos que  $\text{Gal}(F/\mathbb{Q}(\alpha)) = \langle \tau \rangle$  con  $\tau(\zeta_5) = \zeta_5^2$ [88]. Por otro lado tenemos otro elemento  $\sigma \in \text{Gal}(F/\mathbb{Q}(\zeta_5))$  con  $\sigma(\alpha) = \zeta_5\alpha$  y claramente  $\text{Gal}(F/\mathbb{Q}(\zeta_5)) = \langle \sigma \rangle$ [88].

Por otro lado, como  $\mathbb{Q}(\zeta_5)/\mathbb{Q}$  es de Galois pero  $\mathbb{Q}(\alpha)/\mathbb{Q}$  no lo es, deducimos que  $\langle \sigma \rangle$  es normal en  $G$  pero  $\langle \tau \rangle$  no es normal en  $G$ [89]. Por tanto  $\tau\sigma\tau^{-1} = \sigma^i$  para algún  $i \in \{2, 3, 4\}$ [89]. De hecho  $i = 2$  pues  $\tau\sigma\tau^{-1}(\alpha) = \tau\sigma(\alpha) = \tau(\zeta_5\alpha) = \zeta_5^2\alpha = \sigma^2(\alpha)$ [90]. Por tanto, todos los elementos de  $G$  tienen una única forma  $\sigma^i\tau^j$  con  $0 \leq i \leq 4$  y  $0 \leq j \leq 390$ . Vamos a calcular los subgrupos cíclicos. Ya tenemos tres: 1,  $\langle \sigma \rangle$  y  $\langle \tau \rangle$ , que tienen orden 1, 5 y 4, respectivamente[91]. Todos los elementos de la forma  $\sigma^i$  generan  $\langle \sigma \rangle$  y  $\tau$  y  $\tau^{-1}$

generan  $\langle \tau \rangle 92]$ . Otro subgrupo cíclico más será  $\langle \tau^2 \rangle 92]$ . Este último tiene orden 293]. Solo nos falta calcular los subgrupos cíclicos generados por los elementos de la forma  $\sigma^i \tau^j$  con  $1 \leq i \leq 4$  y  $1 \leq j \leq 393]$ .

Comenzamos con los de la forma  $\sigma^i \tau^2$ . De la igualdad  $\tau\sigma = \sigma^2\tau$  observamos que  $\tau^2\sigma = \sigma^4\tau^2 = \sigma^{-1}\tau^2 94]$ . Por tanto, para cada  $i$  tenemos que  $(\sigma^i\tau^2)^2 = 195]$ . O sea, cada  $\sigma^i\tau^2$  tiene orden 295]. Esto nos proporciona cinco subgrupos de orden 2, uno de los cuales es  $\langle \tau^2 \rangle 95]$ .

Por otro lado  $(\sigma^i\tau)^2 = \sigma^{3i}\tau^2$ , que tiene orden 296]. Por tanto,  $\langle \sigma^i\tau \rangle$  tiene orden 4 y su único subgrupo de orden 2 es  $\langle \sigma^{3i}\tau^2 \rangle 96]$ . Como estos últimos son distintos para los cinco valores distintos de  $i$ , obtenemos de esta forma cinco subgrupos cíclicos de orden 4, uno de los cuales es  $\langle \tau \rangle 96]$ . Cada uno de estos subgrupos tiene dos elementos de orden 497]. Más concretamente  $\langle \sigma^i\tau \rangle$  también está generado por  $(\sigma^i\tau)^3 = \sigma^i\tau\sigma^{3i}\tau^2 = \sigma^{2i}\tau^3 97]$ . Por tanto, ya tenemos todos los subgrupos cíclicos<sup>97]</sup>:

- De orden 1: 1.
- De orden 2:  $\langle \sigma^i\tau^2 \rangle$  con  $0 \leq i \leq 4$ .
- De orden 4:  $\langle \sigma^i\tau \rangle$  con  $0 \leq i \leq 4$ .
- De orden 5:  $\langle \sigma \rangle 101]$ .

Calculamos ahora los grupos generados por dos elementos  $g$  y  $h$ <sup>103]</sup>. Por supuesto, si uno de ellos está en el subgrupo generado por el otro lo que obtendremos es uno de los grupos cíclicos, con lo que suponemos que  $g \notin \langle h \rangle$  y  $h \notin \langle g \rangle$ <sup>104]</sup>.

Supongamos primero que uno de los dos tiene orden 5<sup>105]</sup>. Por ejemplo, supongamos que  $|g| = 5$  y por tanto  $h$  tiene orden 2 ó 4<sup>105]</sup>. Si  $h$  tiene orden 4 entonces  $\langle g, h \rangle = G$ <sup>105]</sup>. Sin embargo si  $h$  tiene orden 2 entonces  $\langle g, h \rangle = \langle \sigma, \tau^2 \rangle$  y como  $\tau^2\sigma = \sigma^{-1}\tau^2$  tenemos que  $\langle \sigma, \tau^2 \rangle$  tiene orden 10105].

En los demás casos  $g$  y  $h$  tienen orden 2 ó 4 y vamos a ver que siempre  $\langle g, h \rangle = G$ <sup>105]</sup>. Si  $|g| = |h| = 4$  entonces podemos suponer que  $g = \sigma^i\tau$  y  $h = \sigma^j\tau$  con  $i \neq j$ <sup>105]</sup>. Por tanto,  $\langle g, h \rangle$  contiene a  $gh^{-1} = \sigma^{i-j} 105]$ . Como este elemento genera a  $\langle \sigma \rangle$ , tenemos que  $\langle g, h \rangle = \langle \sigma, \tau \rangle = G$ <sup>105]</sup>. El mismo argumento muestra que si  $g$  y  $h$  tienen orden 2 y son distintos, entonces generan  $G$ <sup>106]</sup>. Finalmente si uno tiene orden 2 y el otro 4, por ejemplo  $h$ , entonces  $\langle g, h \rangle$  contiene a  $\langle g, h^2 \rangle$  con  $g$  y  $h^2$  distintos de orden 2 y de nuevo obtenemos que  $\langle g, h \rangle = G$ .

El retículo de subgrupos que obtenemos es el siguiente: Dando la vuelta al diagrama obtenemos las inclusiones entre los subcuerpos de  $F$ . Pero antes de hacerlo vamos a calcular los cuerpos.

Claramente  $G^\circ = \mathbb{Q}$ ,  $1^\circ = F$ ,  $\langle \sigma \rangle^\circ = \mathbb{Q}(\zeta_5)$ ,  $\langle \tau \rangle^\circ = \mathbb{Q}(\alpha)$ . Cada uno de los  $\langle \sigma^i\tau \rangle^\circ$  tiene que tener grado 5 sobre  $\mathbb{Q}$  y serán los únicos subcuerpos de grado 5 sobre  $\mathbb{Q}$ , que necesariamente son  $\mathbb{Q}(\alpha)$ ,  $\mathbb{Q}(\zeta_5\alpha)$ ,  $\mathbb{Q}(\zeta_5^2\alpha)$ ,  $\mathbb{Q}(\zeta_5^3\alpha)$  y  $\mathbb{Q}(\zeta_5^4\alpha)$ . Observamos que  $\sigma^i\tau(\zeta_5^{-i}\alpha) = \sigma^i(\zeta_5^{-2i}\alpha) = \zeta_5^{-i}\alpha$ . Por tanto  $\langle \sigma^i\tau \rangle^\circ = \mathbb{Q}(\zeta_5^{-i}\alpha)$ .

Por otro lado  $\langle \sigma, \tau^2 \rangle$  es el único subgrupo que tiene grado 2 sobre  $\mathbb{Q}$ , cuyo cuerpo fijo además está contenido en  $\langle \sigma \rangle^\circ = \mathbb{Q}(\zeta_5)$ . Observando que  $\beta = \zeta_5 + \zeta_5^{-1} = 2\cos(2\pi/5) \in \mathbb{R}$ , tenemos que  $\mathbb{Q}(\beta)$  está contenido en  $\mathbb{Q}(\zeta_5)$ . Además, como  $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$  tenemos que  $\beta^2 = \zeta_5^2 + \zeta_5^{-2} + 2 = -\beta + 1$ , con lo que  $\beta$  es raíz de  $X^2 + X - 1$ , de donde  $\beta = \frac{-1+\sqrt{5}}{2}$  y por tanto  $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{5})$ .

Por tanto  $\langle \sigma, \tau^2 \rangle^\circ = \mathbb{Q}(\sqrt{5})$ . Ahora observamos que  $\langle \sigma^{3i}\tau^2 \rangle = \langle \sigma, \tau^2 \rangle \cap \langle \sigma^i\tau \rangle$ . Como la correspondencia de Galois es un anti-isomorfismo de retículos deducimos que  $\langle \sigma^{3i}\tau^2 \rangle^\circ =$

$$\langle \sigma, \tau^2 \rangle^\circ \langle \sigma^i \tau \rangle^\circ = \mathbb{Q}(\sqrt{5}, \zeta_5^{-i} \alpha).$$

Por tanto el retículo de subcuerpos es el siguiente:

Obsérvese que los únicos subgrupos normales de  $G$  son 1,  $\langle \sigma \rangle$ ,  $\langle \sigma, \tau^2 \rangle$  y  $G$ . Por tanto, los únicos subcuerpos de  $F$  que son normales sobre  $\mathbb{Q}$  son  $\mathbb{Q}$ ,  $\mathbb{Q}(\sqrt{5})$ ,  $\mathbb{Q}(\zeta_5)$  y  $F$ .