

# Álgebra III

Foto: José Juan Castro

FACULTAD  
DE  
CIENCIAS  
UNIVERSIDAD DE GRANADA



**Los Del DGIIM**, [losdeldgiim.github.io](https://losdeldgiim.github.io)

Doble Grado en Ingeniería Informática y Matemáticas  
Universidad de Granada



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0).

Eres libre de compartir y redistribuir el contenido de esta obra en cualquier medio o formato, siempre y cuando des el crédito adecuado a los autores originales y no persigas fines comerciales.

# Álgebra III

Los Del DGIIM, [losdeldgiim.github.io](https://losdeldgiim.github.io)

José Juan Urrutia Milán

Granada, 2025



# Índice general

<b>1. Extensiones de cuerpos y raíces de polinomios</b>	<b>5</b>
1.1. Extensiones de cuerpos y elementos algebraicos . . . . .	10
1.1.1. Elementos algebraicos . . . . .	15
1.1.2. Ejercicios . . . . .	18
1.2. Extensiones finitas y extensiones algebraicas . . . . .	19
1.2.1. Ejercicios . . . . .	24
1.3. Construcciones con regla y compás . . . . .	28
1.4. Homomorfismos de cuerpos . . . . .	39
1.5. Clasificación de los cuerpos finitos . . . . .	53
1.6. El grupo de automorfismos de una extensión . . . . .	55
1.7. Ejercicios . . . . .	57
<b>2. Extensiones de Galois</b>	<b>69</b>
2.1. Extensiones de Galois . . . . .	69
2.2. Teorema fundamental de la Teoría de Galois . . . . .	78
2.3. El Teorema Fundamental del Álgebra . . . . .	86
2.4. Ejercicios . . . . .	87
<b>3. Teoría de Galois de Ecuaciones</b>	<b>95</b>
3.1. Grupo de Galois de un polinomio . . . . .	95
3.2. Extensiones ciclotómicas . . . . .	102
3.3. Construcciones con regla y compás II . . . . .	106
3.4. Extensiones cíclicas . . . . .	109
3.5. Ecuaciones resolubles por radicales . . . . .	113
3.6. Ecuación general de grado $n$ . . . . .	118
3.7. Resolución de las ecuaciones de grado hasta 4 . . . . .	121
3.7.1. Cuadrática . . . . .	121
3.7.2. Cúbica . . . . .	122
3.7.3. Cuártica . . . . .	123
3.8. Cuerpos finitos . . . . .	126
<b>4. Ejercicios</b>	<b>131</b>

Antes de proceder con la asignatura de Álgebra III, cuyo principal objetivo es dar solución a las ecuaciones polinómicas mediante el uso y estudio de los cuerpos finitos, recomendamos repasar en anteriores apuntes los siguientes conceptos:

- En los apuntes de Álgebra I los conceptos de: anillo, subanillo, homomorfismo de anillos, cuerpo de fracciones e ideal; así como la forma en la que se estudiaba que un polinomio era irreducible, mediante la teoría de DFUs y Teoremas como el de reducción o de Eisenstein.
- En los apuntes de Álgebra II los conceptos de: grupo, subgrupo, homomorfismo de grupos, monoide; y conceptos más avanzados como el de grupo resoluble o acción transitiva.

Una vez repasados dichos conceptos, estamos en condiciones de comenzar la asignatura.

# 1. Extensiones de cuerpos y raíces de polinomios

Comenzamos definiendo el objeto de estudio protagonista a lo largo de esta asignatura: los cuerpos, llamados a veces campos, del inglés *fields*.

**Notación.** Aunque las dos operaciones de los anillos (y también de los cuerpos) no tengan por qué ser una suma y una multiplicación, optaremos por dichas notaciones, junto con las notaciones de “cero” para el elemento neutro de la operación “suma” y de “uno” para el elemento neutro de la operación “producto”; por ser familiares a los anillos a los que estamos acostumbrados. De esta forma, para nosotros un anillo será una tupla  $(A, +, 0, \cdot, 1)$ , a la que podremos referirnos simplemente por  $A$  cuando las dos operaciones y elementos neutros estén claros por el contexto.

Recordamos que en un anillo la operación  $\cdot$  no tiene por qué ser conmutativa, por lo que se dice que un anillo es comutativo cuando esta sí lo es.

**Definición 1.1** (Cuerpo). Un cuerpo es un anillo comutativo  $A$  en el que  $A \setminus \{0\}$  es un grupo con la operación  $\cdot$ .

Observamos que estamos suponiendo implícitamente que el anillo  $\{0\}$  jamás puede ser un cuerpo, puesto que el conjunto vacío jamás puede ser un grupo.

*Observación.* Una definición equivalente de cuerpo es:

Un cuerpo es un anillo comutativo  $A$  en el que  $A \setminus \{0\}$  es el conjunto de unidades de  $A$ .

**Ejemplo.** Algunos ejemplos de los cuerpos más famosos son:

- $\mathbb{Q}$ .
- $\mathbb{R}$ .
- $\mathbb{C}$ .
- $\mathbb{Z}_p$  con  $p$  primo.

Con el objetivo de definir de forma totalmente rigurosa lo que es la característica de un anillo (concepto que puede que se haya mencionado ya en cursos anteriores), nos es necesaria la siguiente proposición:

**Proposición 1.1.** *Sea  $A$  un anillo, existe un único homomorfismo de anillos*

$$\chi : \mathbb{Z} \rightarrow A$$

Además,  $\text{Im}\chi$  es el menor subanillo de  $A$ .

*Demostración.* Tenemos que probar:

**Unicidad.** Sean  $\chi, \varphi : \mathbb{Z} \rightarrow A$  dos homomorfismos de anillos, demostremos por inducción que  $\chi(k) = \varphi(k)$  para todo  $k \in \mathbb{Z}$ :

**Para  $k = 0$ .** Como  $\chi$  y  $\varphi$  son homomorfismos de anillos, estos han de cumplir:

$$\chi(0) = 0 = \varphi(0)$$

**Para  $k = 1$ .** De manera análoga se tiene que  $\chi(1) = 1 = \varphi(1)$ .

**Supuesto para todo**  $0 \leq s \leq k$ , vemos que:

$$\begin{aligned} \chi(k+1) &= \chi(k) + \chi(1) = \varphi(k) + \varphi(1) = \varphi(k+1) \\ \chi(-(k+1)) &= -\chi(k+1) = -\varphi(k+1) = \varphi(-(k+1)) \end{aligned}$$

Acabamos de probar que  $\chi = \varphi$ , por lo que en caso de existir solo existe un único homomorfismo  $\chi : \mathbb{Z} \rightarrow A$ .

**Existencia.** Definimos  $\chi : \mathbb{Z} \rightarrow A$  dada por:

$$\begin{aligned} \chi(0) &= 0 \\ \chi(1) &= 1 \\ \chi(k) &= \sum_{i=1}^k 1, \quad k \geq 1 \\ \chi(-k) &= -\chi(k), \quad k \geq 1 \end{aligned}$$

A partir de su definición es claro que  $\chi$  es un homomorfismo de anillos.

**Minimalidad.** Para ver que  $\text{Im}\chi$  es el menor subanillo contenido en  $A$ , vimos ya en Álgebra I que  $\text{Im}\chi$  es un subanillo de  $A$ , como imagen de un homomorfismo de anillos. Para ver que es el menor, sea  $S \subseteq A$  otro subanillo de  $A$ , como subanillo de  $A$  que es ha de contener al 1, al 0 y ser cerrado para sumas y opuestos, luego ha de contener también a  $n \cdot 1$  y  $-(n \cdot 1)$ , para todo  $n \in \mathbb{N}$ . Sin embargo, tenemos que:

$$\text{Im}\chi = \{\chi(n) : n \in \mathbb{Z}\} = \{0\} \cup \left\{ \sum_{k=1}^n \chi(1) : n \in \mathbb{N} \right\} \cup \left\{ \sum_{k=1}^n \chi(-1) : n \in \mathbb{N} \right\}$$

Por lo que  $\text{Im}\chi \subseteq S$ , de donde todo subanillo de  $A$  contiene a  $\text{Im}\chi$  como subanillo.

□

**Definición 1.2** (Característica de un anillo). Sea  $A$  un anillo, sabemos por la Proposición anterior que existe un único homomorfismo de anillos

$$\chi : \mathbb{Z} \rightarrow A$$

En dicho caso, sabemos de Álgebra I que  $\ker \chi$  es un ideal en  $\mathbb{Z}$ , y como todos los ideales de  $\mathbb{Z}$  son principales (por ser  $\mathbb{Z}$  un Dominio Euclídeo), sabemos que  $\exists n \in \mathbb{N}$  de forma que  $\ker \chi = n\mathbb{Z}$ . Dicho número  $n$  recibe el nombre de “característica de  $A$ ” (aunque varios números cumplen esta definición, suele tomarse el más pequeño de ellos que sea positivo, en caso de no ser el ideal trivial), notado por  $\text{car}(A)$ .

**Proposición 1.2.** *La característica de un cuerpo ha de ser un número primo o cero.*

*Demostración.* Supongamos que  $A$  es un cuerpo de característica  $n \neq 0$ , por lo que:

$$\sum_{k=1}^n 1 = n \cdot 1 = 0$$

Por reducción al absurdo, supongamos que  $n$  no es primo, con lo que puedo encontrar un primo  $p$  y  $m \neq 0$  de forma que:

$$0 = n \cdot 1 = p \cdot m$$

Como  $0 \neq m \in A$ , existe  $m^{-1} \in A$ , que puede multiplicarse a ambos lados de la igualdad, obteniendo que  $p = 0$ , contradicción, por lo que  $n$  ha de ser primo.  $\square$

**Definición 1.3** (Subcuerpos y extensiones de cuerpos). Si  $K$  es un cuerpo, un subcuerpo de  $K$  es un subanillo  $F$  de  $K$  tal que  $F$  es un cuerpo. En dicho caso, diremos que  $K$  es una extensión del cuerpo  $F$ , y notaremos ambas afirmaciones por:

$$F \leqslant K$$

Una forma rápida de ver si un subconjunto de un anillo es un subanillo<sup>1</sup>, condición que tendremos que comprobar para ver si un subconjunto de un cuerpo es un subcuerpo, la obtenemos de la siguiente proposición:

**Proposición 1.3.** *Sea  $A$  un anillo y  $B \subseteq A$ ,  $B$  es un subanillo de  $A$  si y solo si se cumplen las tres condiciones siguientes:*

1.  $1 \in B$ .
2.  $a, b \in B \implies a - b \in B$ .
3.  $a, b \in B \implies a \cdot b \in B$ .

*Demostración.* Por doble implicación:

$\implies$ ) Si  $B$  es un subanillo de  $A$ , está claro que se cumplen dichas propiedades.

---

<sup>1</sup>Recordemos que un subanillo de un anillo es un subconjunto del anillo que contiene al 0, al 1, y que es cerrado para opuestos, para la suma y para el producto del anillo, como operaciones inducidas en el subconjunto.

$\iff$ ) Supuesto que  $B$  cumple dichas propiedades, veamos que  $B$  cumple todas las condiciones necesarias para ser un subanillo de  $A$ :

- $1 \in B$ .
- Como  $1 \in B$ , tenemos que  $0 = 1 - 1 \in B$ .
- Como  $0 \in B$ , tenemos que si  $b \in B$ , entonces  $-b = 0 - b \in B$ .
- Sean  $a, b \in B$ , como  $-b \in B$  tenemos que  $a + b = a - (-b) \in B$ .
- Finalmente, si  $a, b \in B$  es claro que  $a \cdot b \in B$ .

□

Es fácil ver (hágase) que la intersección arbitraria de subcuerpos de un cuerpo fijo sigue siendo un subcuerpo del mismo, propiedad que justifica el concepto que vamos a introducir.

**Definición 1.4** (Subcuerpo generado por un conjunto). Sea  $K$  un cuerpo y  $S \subseteq K$ , si consideramos:

$$\Gamma = \{F \subseteq K : F \leqslant K \text{ y } S \subseteq F\}$$

el conjunto de todos los subcuerpos de  $K$  que contienen a  $S$ , definimos el subcuerpo de  $K$  generado por  $S$  como el subcuerpo:

$$\bigcap_{F \in \Gamma} F$$

Que se caracteriza por ser el menor subcuerpo de  $K$  que contiene a  $S$ .

**Definición 1.5** (Subcuerpo primo de un cuerpo). Si dado un cuerpo  $K$  consideramos el subcuerpo generado por el conjunto vacío ( $\emptyset \subseteq K$ ) obtenemos el “subcuerpo primo de  $K$ ”, que viene dado por:

$$\bigcap_{F \in \Gamma} F$$

donde  $\Gamma = \{F \subseteq K : F \leqslant K\}$ . Obtenemos así el menor subcuerpo de  $K$ .

**Proposición 1.4.** *Sea  $K$  un cuerpo de característica  $p$ , entonces el subcuerpo primo de  $K$  es isomorfo a:*

- $\mathbb{Z}_p$  si  $p > 0$ .
- $\mathbb{Q}$  si  $p = 0$ .

*Demostración.* Denotaremos por  $\Pi$  al subcuerpo primo de  $K$ . Si consideramos el único homomorfismo de anillos  $\chi : \mathbb{Z} \rightarrow K$ , tenemos que  $Im\chi$  es el menor subanillo de  $K$ , por lo que estará contenido en  $\Pi$ , por ser este un subanillo de  $K$ . Aplicando el Primer Teorema de Isomorfía sobre  $\chi$  obtenemos que:

$$\frac{\mathbb{Z}}{p\mathbb{Z}} = \frac{\mathbb{Z}}{\ker \chi} \cong Im\chi$$

**Si**  $p > 0$  tendremos que:

$$\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}} \cong Im\chi$$

Y como  $p$  es primo por la Proposición 1.2 tenemos que  $Im\chi$  es isomorfo a un cuerpo, por lo que  $Im\chi$  es un subcuerpo de  $K$ , y como teníamos que  $Im\chi \subseteq \Pi$  con  $\Pi$  el menor subcuerpo de  $K$  tiene que ser  $\Pi \subseteq Im\chi$ , de donde:

$$\Pi = Im\chi \cong \mathbb{Z}_p$$

**Si**  $p = 0$  tendremos entonces que:

$$\mathbb{Z} = \frac{\mathbb{Z}}{0\mathbb{Z}} \cong Im\chi$$

por lo que, si denotamos al cuerpo de fracciones de  $Im\chi$  por  $Q$ , tendremos entonces que:

$$\mathbb{Q} \cong Q$$

Como teníamos que  $Im\chi \subseteq \Pi$ , podemos calcular  $Q$  dentro<sup>2</sup> de  $\Pi$ , obteniendo que  $Q \subseteq \Pi$ , pero como  $\Pi$  es el menor subcuerpo de  $K$ , tendremos  $\Pi \subseteq Q$ , de donde:

$$\Pi = Q \cong \mathbb{Q}$$

□

*Observación.* Si tenemos  $F \leq K$  una extensión de cuerpos, la propia definición de cuerpo nos demuestra que  $K$  es un espacio vectorial sobre el cuerpo  $F$ . Con esta visión podemos ver los elementos de  $F$  como escalares dentro de  $K$ , por lo que podremos considerar  $F$ -bases de  $K$  y copiar toda la teoría de álgebra lineal vista anteriormente al contexto de los cuerpos.

**Definición 1.6.** Sea  $F \leq K$  una extensión de cuerpos, decimos que una aplicación  $\sigma : K \rightarrow K$  es  $F$ -lineal si verifica que:

$$\begin{aligned}\sigma(x + y) &= \sigma(x) + \sigma(y) && \forall x, y \in K \\ \sigma(a \cdot x) &= a \cdot \sigma(x) && \forall a \in F, \forall x \in K\end{aligned}$$

**Definición 1.7.** Si  $F \leq K$  es una extensión, la dimensión de  $K$  sobre  $F$  como espacio vectorial recibe el nombre de “grado de la extensión  $F \leq K$ ”, denotado por:

$$[K : F]$$

Si  $[K : F]$  es un número finito, decimos que  $F \leq K$  es (una extensión) finita. En caso contrario, diremos que es una extensión infinita, denotado por  $\overline{[K : F]} = \infty$ .

**Ejemplo.** Como ejemplos a destacar:

- $\mathbb{R} \leq \mathbb{C}$  tiene grado de extensión 2, ya que  $\{1, i\}$  es una  $\mathbb{R}$ -base de  $\mathbb{C}$ :

$$[\mathbb{C} : \mathbb{R}] = 2$$

---

<sup>2</sup>Si  $A \subseteq B$  como subanillo, entonces el cuerpo de fracciones de  $A$  está dentro del cuerpo de fracciones de  $B$ . Si además  $B$  es un cuerpo entonces este coincide con su cuerpo de fracciones.

- Si  $[\mathbb{R} : \mathbb{Q}] = n$ , entonces tendríamos de la existencia de un isomorfismo lineal  $\mathbb{R} \xrightarrow{f} \mathbb{Q}^n$ , por lo que  $\mathbb{R}$  sería numerable. Por tanto, podemos decir que  $[\mathbb{R} : \mathbb{Q}] = \infty$ .

**Ejercicio 1.** Demostrar que el cardinal de un cuerpo finito es de la forma  $p^n$ , con  $p$  primo y  $n \geq 1$ .

Sea  $K$  un cuerpo finito, este no podrá tener característica cero, porque entonces seríamos capaces de obtener una cantidad infinita de elementos de  $K$ . Tenemos por tanto que  $p = \text{car}(K) > 0$ , y por la Proposición 1.2 sabemos que  $p$  tiene que ser un número primo. De esta forma, el cuerpo primo de  $K$  es isomorfo a  $\mathbb{Z}_p$ . Así, podemos ver  $K$  como un espacio vectorial sobre un cuerpo isomorfo a  $\mathbb{Z}_p$ , con cierto grado de extensión  $n \in \mathbb{N} \setminus \{0\}$ , por lo que como espacio vectorial será isomorfo a:

$$\underbrace{\mathbb{Z}_p \times \dots \times \mathbb{Z}_p}_{n \text{ veces}}$$

Luego  $K$  ha de tener cardinal  $p^n$ .

Haremos próximamente una clasificación de cuerpos finitos, en la que cada primo y natural no nulo nos definan un único cuerpo de cardinal  $p^n$ .

## 1.1. Extensiones de cuerpos y elementos algebraicos

**Definición 1.8** (Extensión generada por un subconjunto). Sea  $F \leq K$  una extensión de cuerpos y  $S \subseteq K$ , definimos la “extensión de  $F$  generada por  $S$ ” como el menor subcuerpo de  $K$  que contiene a  $F \cup S$ , denotado por  $F(S)$ .

- Si  $S = \{s_1, \dots, s_t\}$ , simplificaremos la notación y escribiremos  $F(s_1, \dots, s_t)$ .
- Si  $K = F(\alpha_1, \dots, \alpha_t)$  para ciertos elementos  $\alpha_1, \dots, \alpha_t \in K$ , diremos entonces que  $F \leq K$  es una extensión finitamente generada.

*Observación.* No debemos confundir una extensión de cuerpos finitamente generada con el concepto de que un espacio vectorial sea finitamente generado. Más aún, si  $F \leq K$  es una extensión de cuerpos, no es lo mismo que  $F \leq K$  sea finita o que sea finitamente generada:

- Toda extensión finita es finitamente generada, pues si  $F \leq K$  es finita entonces existirá  $\{u_1, \dots, u_n\}$  una  $F$ -base de  $K$ , por lo que tendremos entonces que:

$$K = F(u_1, \dots, u_n)$$

- ⊇) Es claro que  $K$  contiene a  $F$  y a  $u_1, \dots, u_n$ , por lo que debemos tener  $F(u_1, \dots, u_n) \leq K$ , por definición de  $F(u_1, \dots, u_n)$ .
- ⊆) Como  $\{u_1, \dots, u_n\}$  es una  $F$ -base de  $K$ , todo elemento  $g \in K$  puede escribirse como:

$$g = a_1 u_1 + \dots + a_n u_n$$

para ciertos elementos  $a_1, \dots, a_n \in F$ . Vemos por la descomposición de  $g$  que  $g \in F(u_1, \dots, u_n)$ , lo que nos da la inclusión  $K \leq F(u_1, \dots, u_n)$ .

- No toda extensión finitamente generada es finita. Veremos que a veces no se cumple esta propiedad y otras veces sí:

- La extensión  $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2})$  es una extensión finita y claramente es finitamente generada.
- La extensión  $\mathbb{R} \leq \mathbb{R}(i)$  es una extensión finitamente generada pero no es finita (veremos que  $\mathbb{R}(i) = \mathbb{C}$ ).

**Ejemplo.**  $\mathbb{Q}(\sqrt{2})$  es el menor subcuerpo de  $\mathbb{R}$  que contiene a  $\sqrt{2}$ , y viene dado por:

$$\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} : a, b \in \mathbb{Q} \right\}$$

*Demostración.* Veámoslo:

$\supseteq$ ) Sean  $a, b \in \mathbb{Q}$ , tenemos que  $a, b, \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ , y este último es un cuerpo, por lo que  $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ .

$\subseteq$ ) Si demostramos que  $Q = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$  es un cuerpo, entonces tenemos esta inclusión, ya que  $\mathbb{Q}(\sqrt{2})$  es el menor subcuerpo de  $\mathbb{R}$  que contiene a  $\sqrt{2}$ . Es evidente que  $Q$  es un anillo commutativo. Para ver que es un cuerpo, dado  $\alpha = a + b\sqrt{2} \in Q \setminus \{0\}$ , buscamos calcular un elemento inverso al mismo que también esté en  $Q$ . Observamos que:

$$(a + \sqrt{2}b)(a - \sqrt{2}b) = a^2 - 2b^2 = 0 \iff \begin{cases} a/b = \sqrt{2} \\ \vee \\ -a/b = \sqrt{2} \end{cases}$$

situación imposible, puesto que  $\sqrt{2} \notin \mathbb{Q}$ . Esto nos permite considerar:

$$\beta = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in Q$$

Observamos que:

$$\alpha\beta = (a + b\sqrt{2}) \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{(a + b\sqrt{2})(a - b\sqrt{2})}{(a + b\sqrt{2})(a - b\sqrt{2})} = 1$$

Por lo que dicho conjunto es un cuerpo, al tener todo elemento un inverso.

□

A partir de la igualdad anterior tenemos que  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ , puesto que  $\{1, \sqrt{2}\}$  es una  $\mathbb{Q}$ -base de  $\mathbb{Q}(\sqrt{2})$ . Debemos tener en cuenta que aunque este resultado pueda generalizarse a otro más general como que:

$$\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} : a, b \in \mathbb{Q}\} \quad \text{si } \sqrt{n} \notin \mathbb{Q}$$

En general, esta no es la definición del menor subcuerpo generado por cierto conjunto. Por ejemplo, se tiene que (lo veremos próximamente):

$$\mathbb{Q}(\sqrt[3]{2}) \neq \left\{ a + b\sqrt[3]{2} : a, b \in \mathbb{Q} \right\}$$

Por lo que debemos tener cuidado con el uso de esta propiedad.

**Definición 1.9** (Cuerpo de descomposición). Sea  $K \leq E$  una extensión de cuerpos y  $f \in K[x]$  un polinomio de forma que:

- $f$  se descompone en  $E[x]$  como producto de polinomios de grado 1, siendo  $\alpha_1, \dots, \alpha_t \in E$  todas las raíces de  $f$ .
- $E = K(\alpha_1, \dots, \alpha_t)$ .

Diremos entonces que  $E$  es un cuerpo de descomposición<sup>3</sup> de  $f$  sobre  $K$ .

**Ejemplo.** Veamos varios ejemplos de cuerpos de descomposición de polinomios:

- Si consideramos  $x^2 + 1 \in \mathbb{R}[x]$ , vemos que:

$$x^2 + 1 = (x + i)(x - i)$$

con  $(x + i), (x - i) \in \mathbb{C}[x]$ , y como además tenemos que  $\mathbb{C} = \mathbb{R}(i, -i)$  (de hecho  $\mathbb{C} = \mathbb{R}(i)$ ), tenemos entonces que  $\mathbb{C}$  es un cuerpo de descomposición de  $x^2 + 1 \in \mathbb{R}[x]$ .

- Por ejemplo, si  $x^2 + 1 \in \mathbb{Q}[x]$ , un cuerpo de descomposición en este caso es  $\mathbb{Q}(i)$ , ya que:

$$x^2 + 1 = (x + i)(x - i)$$

con  $(x + i), (x - i) \in \mathbb{Q}(i)$  y además se tiene que  $\mathbb{Q}(i) = \mathbb{Q}(i, -i)$ .

⊆) Trivial.

⊇) Tenemos que  $-i = -1 \cdot i$ , con  $-1, i \in \mathbb{Q}(i)$ .

*Observación.* Si  $f \in \mathbb{Q}[x]$  y tomo todas<sup>4</sup> sus raíces en  $\mathbb{C}$ , digamos  $\alpha_1, \dots, \alpha_t$ , entonces un cuerpo de descomposición de  $f$  es  $\mathbb{Q}(\alpha_1, \dots, \alpha_t)$ .

Por ejemplo, para  $f = x^2 - 2 \in \mathbb{Q}[x]$ , tenemos que un cuerpo de descomposición suyo es  $\mathbb{Q}(\sqrt{2})$ .

**Ejercicio 1.1.1.** Si tenemos  $F \leq K$  una extensión de cuerpos y  $S, T \subseteq K$ , demostrar que:

$$F(S \cup T) = F(S)(T)$$

*Demostración.* Veámoslo por doble inclusión:

- ⊆)  $F(S \cup T)$  es por definición el menor subcuerpo de  $K$  que contiene a  $F \cup S \cup T$ , por lo que para ver esta inclusión hemos de ver que  $F(S)(T)$  es un subcuerpo que contiene a  $F \cup S \cup T$ . Para ello,  $F(S)(T)$  es por definición el menor subcuerpo de  $K$  que contiene a  $F(S) \cup T$ , y  $F(S)$  es a su vez el menor subcuerpo de  $K$  que contiene a  $F \cup S$ . Por tanto,  $F(S)(T)$  es un subcuerpo de  $K$  que contiene a  $F \cup S \cup T$ , de donde  $F(S \cup T) \subseteq F(S)(T)$ .
- ⊇) El menor subcuerpo de  $K$  que contiene a  $F \cup S \cup T$  ha de contener al menor subcuerpo de  $K$  que contiene a  $F \cup S$ , por lo que  $F(S \cup T) \supseteq F(S)$ . Como ahora tenemos que  $F(S), T \subseteq F(S \cup T)$ , tenemos por tanto que el menor subcuerpo de  $K$  que contiene a  $F(S) \cup T$  está contenido en  $F(S \cup T)$ , es decir,  $F(S)(T) \subseteq F(S \cup T)$ .

□

---

<sup>3</sup>o de escisión.

<sup>4</sup>Fundamentado por el Teorema Fundamental del Álgebra.

### Raíces $n$ -ésimas

Para esta asignatura debemos repasar cómo calcular todas las raíces  $n$ -ésimas complejas de un número entero.

**Proposición 1.5.** *Sea  $r \in \mathbb{Z}$  con  $r \geq 0$ , el conjunto de todos los números complejos que satisfacen (para  $n \in \mathbb{N}$ ):*

$$z^n = r$$

*o equivalentemente, el conjunto de las raíces  $n$ -ésimas de  $r$ , es el conjunto:*

$$\left\{ \sqrt[n]{r} e^{i \frac{2\pi k}{n}} : k \in \{0, 1, \dots, n-1\} \right\}$$

*Demostración.* Por doble inclusión, queremos ver que  $R$ , el conjunto de todas las raíces  $n$ -ésimas de  $r$ , es igual a  $\mathcal{R} = \left\{ \sqrt[n]{r} e^{i \frac{2\pi k}{n}} : k \in \{0, 1, \dots, n-1\} \right\}$ :

$\supseteq$ ) Si tomamos  $k \in \{0, 1, \dots, n-1\}$  tenemos entonces que:

$$\left( \sqrt[n]{r} e^{i \frac{2\pi k}{n}} \right)^n = \left( \sqrt[n]{r} \right)^n \cdot \left( e^{i \frac{2\pi k}{n}} \right)^n = r \cdot e^{i 2\pi k} = r(\cos(2\pi k) + i \sin(2\pi k)) = r$$

$\subseteq$ ) Sea  $z \in \mathbb{C}$  con  $z^n = r$ , si expresamos  $z$  en forma polar:

$$z = |z|(\cos(\theta) + i \sin(\theta))$$

para cierto  $\theta \in [0, 2\pi[$ , elevando  $z$  a  $n$  vemos que:

$$r = z^n = |z|^n (\cos(\theta) + i \sin(\theta))^n \stackrel{(*)}{=} |z|^n (\cos(n\theta) + i \sin(n\theta))$$

donde en (\*) hemos usado la fórmula de Moivre. Si igualamos ahora partes reales e imaginarias vemos que:

$$\begin{aligned} r &= |z|^n \cos(n\theta) \\ 0 &= |z|^n \sin(n\theta) \end{aligned} \quad \iff \quad n\theta = 2\pi k \quad \iff \quad \theta = \frac{2\pi k}{n}$$

para cierto  $k \in \mathbb{Z}$ , pero como debe ser  $0 \leq \theta < 2\pi$  debemos tener  $0 \leq \frac{k}{n} < 1$ , lo que ocurre si y solo si  $k \in \{0, 1, \dots, n-1\}$ .

□

**Corolario 1.5.1.** *Sea  $r \in \mathbb{Z}$  con  $r \geq 0$  y  $n \in \mathbb{N}$ , tenemos que:*

$$w \text{ es raíz } n\text{-ésima de } 1 \iff \sqrt[n]{rw} \text{ es raíz } n\text{-ésima de } r$$

**Proposición 1.6.** *Sea  $n \in \mathbb{N}$ , tenemos que el conjunto de las raíces  $n$ -ésimas de 1 es un grupo cíclico de orden  $n$ .*

*Demostración.* Sabemos por la Proposición anterior que el conjunto de las raíces  $n$ -ésimas de la unidad es:

$$R = \left\{ e^{i \frac{2\pi k}{n}} : k \in \{0, 1, \dots, n-1\} \right\}$$

Si tomamos  $w = e^{i\frac{2\pi}{n}}$ , tenemos para  $k \in \mathbb{Z}$  que:

$$w^k = \left(e^{i\frac{2\pi}{n}}\right)^k = e^{i\frac{2\pi k}{n}}$$

de donde:

$$R = \{1, w, w^2, \dots, w^{n-1}\}$$

□

**Definición 1.10.** Sea  $r \in \mathbb{Z}$  con  $r \geq 0$  y  $n \in \mathbb{N}$ , decimos que  $w \in \mathbb{C}$  es una raíz  $n$ -ésima compleja primitiva de  $r$  si  $w$  es una raíz  $n$ -ésimas complejas de  $r$  que genera todas las raíces complejas  $n$ -ésimas de  $r$ .

Equivalentemente, si  $w$  tiene orden multiplicativo  $n$ .

**Ejemplo.** Si tomamos  $f = x^3 - 2 \in \mathbb{Q}[x]$ , vemos que  $f$  tiene 3 raíces distintas, ya que:

$$f' = 3x^2$$

con 0 la única raíz de  $f'$ , y sabemos que  $f$  tiene una raíz múltiple si y solo si  $f'$  tiene la misma raíz, pero  $f$  no tiene a 0 como raíz.

Observamos ahora que  $x^3 - 2 = 0$  si y solo si  $x$  es una raíz cúbica de 2, por lo que las raíces de  $f$  son exactamente:

$$R = \left\{ \sqrt[3]{2} e^{i\frac{2\pi k}{3}} : k \in \{0, 1, 2\} \right\} = \left\{ \sqrt[3]{2}, \sqrt[3]{2} e^{i\frac{2\pi}{3}}, \sqrt[3]{2} e^{i\frac{4\pi}{3}} \right\}$$

Si tomamos:

$$w = e^{i\frac{2\pi}{3}} = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

tenemos entonces que:

$$R = \left\{ \sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2} \right\}$$

Por lo que un cuerpo de descomposición de  $f$  será  $\mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, w)$ .

*Demostración.* Por doble inclusión:

$\subseteq$ ) Como  $\mathbb{Q}(\sqrt[3]{2}, \omega)$  es un cuerpo que contiene a  $\omega$  y a  $\sqrt[3]{2}$ , este ha de contener también a:

$$\sqrt[3]{2}, \quad \omega\sqrt[3]{2}, \quad \omega^2\sqrt[3]{2}$$

Por lo que el menor cuerpo que contiene a todos estos ha de estar contenido en  $\mathbb{Q}(\sqrt[3]{2}, \omega)$ .

$\supseteq$ ) De forma análoga, como  $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$  es un cuerpo que contiene a  $\sqrt[3]{2}$  y a  $\omega$ , ya que:

$$\omega = \frac{\omega\sqrt[3]{2}}{\sqrt[3]{2}} \in \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$$

debemos tener que  $\mathbb{Q}(\sqrt[3]{2}, w) \leq \mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2})$ .

□

**Ejemplo.** Tomamos  $f = x^n - 1 \in \mathbb{Q}[x]$  con  $n \geq 1$  y nos preguntamos sobre un cuerpo de descomposición de dicho polinomio, que tiene  $n$  raíces, y:

$$f' = nx^{n-1}$$

Por lo que no comparte raíces con  $f'$ , luego tiene  $n$  raíces distintas, todas ellas de multiplicidad 1, que serán:

$$\left\{ \left( e^{\frac{2\pi i}{n}} \right)^k : k \in \{0, \dots, n-1\} \right\}$$

Que es un subgrupo cíclico de orden  $n$  de  $\mathbb{C} \setminus \{0\}$ , generado por  $e^{\frac{2\pi i}{n}}$ .

Un cuerpo de descomposición de  $x^n - 1 \in \mathbb{Q}[x]$  es  $\mathbb{Q}(\eta)$ , donde  $\eta$  es una raíz  $n$ -ésima compleja primitiva de la unidad.

### 1.1.1. Elementos algebraicos

Algo que tienen en común todos los números complejos que aparecían en los ejemplos anteriores es que todos ellos son algebraicos sobre  $\mathbb{Q}$ :

**Definición 1.11** (Elemento algebraico). Sea  $F \leq K$  una extensión de cuerpos y  $\alpha \in K$ , diremos que  $\alpha$  es algebraico sobre  $F$  si  $f(\alpha) = 0$  para algún polinomio no constantemente igual a cero  $f \in F[x]$ . En caso contrario, diremos que  $\alpha$  es trascendente sobre  $F$ .

**Proposición 1.7.** Sean  $F \leq K$  una extensión de cuerpos y  $\alpha \in K$  un elemento algebraico sobre  $F$ . Tenemos entonces que existe un único polinomio mónico<sup>5</sup> irreducible  $f \in F[x]$  tal que  $f(\alpha) = 0$ .

En dicho caso, tenemos además un isomorfismo de anillos entre cuerpos:

$$F(\alpha) \cong \frac{F[x]}{\langle f \rangle}$$

donde  $\langle f \rangle$  es el ideal principal de  $F[x]$  generado por  $f$ :

$$\langle f \rangle = \{gf : g \in F[x]\}$$

Y la extensión  $F \leq F(\alpha)$  tiene grado  $\deg f$ , siendo  $\{1, \alpha, \dots, \alpha^{\deg f - 1}\}$  una  $F$ -base de  $F(\alpha)$ .

*Demostración.* Definimos la aplicación “evaluación en  $\alpha$ ”

$$\begin{aligned} e_\alpha : F[x] &\longrightarrow K \\ g &\longmapsto g(\alpha) \end{aligned}$$

que es un homomorfismo de anillos por la Propiedad Universal del Anillo de Polinomios, aplicado a la inclusión  $\iota : F \rightarrow K$  y al elemento  $\alpha \in K$ . Por tanto, su núcleo  $\ker e_\alpha$  es un ideal de  $F[x]$ . Como  $F$  es un cuerpo,  $F[x]$  es un Dominio Euclídeo, luego todo ideal es principal. Sea  $f \in F[x]$  el generador mónico de  $\ker e_\alpha$ , sabemos que es el polinomio de menor grado contenido en  $\ker e_\alpha$ . Veamos que  $f$  cumple con las condiciones descritas en el enunciado:

---

<sup>5</sup>El coeficiente líder es 1.

- Por la definición de  $f$  tenemos que  $f \in \ker e_\alpha$ , luego:

$$0 = e_\alpha(f) = f(\alpha)$$

- Por el Primer Teorema de Isomorfía,  $e_\alpha$  induce un isomorfismo de anillos:

$$\frac{F[x]}{\langle f \rangle} = \frac{F[x]}{\ker e_\alpha} \cong \text{Im } e_\alpha$$

dado por:

$$g + \langle f \rangle \mapsto g(\alpha)$$

Donde  $\text{Im } e_\alpha$  será un subanillo de  $K$ , que es un dominio de integridad por ser  $K$  un cuerpo, de donde  $\frac{F[x]}{\langle f \rangle}$  es un dominio de integridad también, luego por un teorema visto en Álgebra I deducimos que  $f$  tiene que ser irreducible.

- Para ver la unicidad, si tomamos  $h \in F[x]$  un polinomio mónico irreducible con  $h(\alpha) = 0$ , entonces  $h \in \ker e_\alpha = \langle f \rangle$ , por lo que existe  $g \in F[x]$  de forma que  $h = fg$ . Como  $h$  es irreducible, tiene que ser  $g \in \mathcal{U}(F[x])$ , por lo que  $h$  y  $f$  son asociados, pero en Álgebra I vimos que si dos polinomios mónicos son asociados entonces deben ser iguales, es decir,  $h = f$ .
- Para ver el isomorfismo, como  $\frac{F[x]}{\langle f \rangle}$  es un dominio de integridad, un Teorema de Álgebra I nos decía que entonces  $\frac{F[x]}{\langle f \rangle}$  es un cuerpo, de donde el isomorfismo

$$\begin{aligned} \frac{F[x]}{\langle f \rangle} &\cong \text{Im } e_\alpha \\ g + \langle f \rangle &\mapsto g(\alpha) \end{aligned}$$

nos dice que  $\text{Im } e_\alpha$  es un cuerpo, contenido en  $K$ . Si observamos que:

- Sea  $a \in F$ , podemos ver  $a$  dentro de  $F[x]$  como el polinomio constantemente igual a  $a$ , por lo que  $e_\alpha(a) = a$ , de donde  $a \in \text{Im } e_\alpha$ , luego  $F \leqslant \text{Im } e_\alpha$ .
- Si consideramos ahora el polinomio identidad  $h = x \in F[x]$ , tenemos que:  $e_\alpha(h) = h(\alpha) = \alpha$ , por lo que  $\alpha \in \text{Im } e_\alpha$ .

Vemos que  $\text{Im } e_\alpha$  es un cuerpo que contiene a  $F \cup \{\alpha\}$ , por lo que por definición de  $F(\alpha)$  tiene que ser  $F(\alpha) \subseteq \text{Im } e_\alpha$ . Para la otra inclusión, si cogemos un elemento de  $\text{Im } e_\alpha$ , este será de la forma  $g(\alpha)$  para cierto  $g \in F[x]$ , que tendrá la forma:

$$g(x) = \sum_{i=1}^n g_i x^i \quad g_i \in F$$

de donde:

$$g(\alpha) = \sum_{i=1}^n g_i \alpha^i$$

Con  $g_i \in F$  y  $\alpha \in F(\alpha)$ , luego  $g(\alpha) \in F(\alpha)$ , lo que nos da la inclusión  $\text{Im } e_\alpha \subseteq F(\alpha)$  que nos faltaba. En definitiva:

$$F(\alpha) = \text{Im } e_\alpha \cong \frac{F[x]}{\langle f \rangle}$$

- Para ver que  $\mathcal{B} = \{1, \alpha, \dots, \alpha^{\deg f - 1}\}$  es una  $F$ -base de  $F(\alpha)$ , usaremos que  $F(\alpha) \cong \frac{F[x]}{\langle f \rangle}$ , donde identificaremos  $F$  con su imagen por dicho isomorfismo, con lo que podemos comprobar que el isomorfismo es  $F$ -lineal:

$$(a + \langle f \rangle)(g + \langle f \rangle) = ag + \langle f \rangle \longmapsto (ag)(\alpha) = ag(\alpha) \quad \forall a \in F, \forall g \in F[x]$$

De esta forma, vamos a tratar de buscar una  $F$ -base de  $\frac{F[x]}{\langle f \rangle}$  cuya imagen por el isomorfismo con  $F(\alpha)$  sea la base buscada. Para ello, sea  $g + \langle f \rangle \in \frac{F[x]}{\langle f \rangle}$ , si  $\deg g \geq \deg f$ , entonces usando que  $F[x]$  es DE, podemos encontrar  $q, r \in F[x]$  de forma que:

$$g = fq + r \quad \text{con} \quad \deg r < \deg f$$

En dicho caso, tenemos que  $g + \langle f \rangle = r + \langle f \rangle$ . Por tanto, cualquier elemento  $g + \langle f \rangle$  de  $\frac{F[x]}{\langle f \rangle}$  puede escribirse como:

$$g(x) = \sum_{i=1}^{\deg f - 1} f_i x^i \quad f_i \in F$$

Luego  $B = \{1 + \langle f \rangle, x + \langle f \rangle, \dots, x^{\deg f - 1} + \langle f \rangle\}$  es un  $F$ -sistema de generadores de  $\frac{F[x]}{\langle f \rangle}$ , que además es una  $F$ -base por ser sus elementos  $F$ -linealmente independientes. Si consideramos su imagen por el isomorfismo  $F$ -lineal, obtenemos el conjunto  $\mathcal{B}$ . Como los isomorfismos  $F$ -lineales transforman  $F$ -bases en  $F$ -bases (visto en Geometría I), tenemos que  $\mathcal{B}$  es una  $F$ -base de  $F(\alpha)$ .

□

**Definición 1.12** (Polinomio irreducible). Sea  $F \leq K$  una extensión de cuerpos y  $\alpha \in K$  algebraico sobre  $F$ , la Proposición anterior nos da la existencia de un único polinomio mónico irreducible del que  $\alpha$  es raíz. Llamaremos a dicho polinomio “polinomio irreducible (o mínimo) de  $\alpha$  sobre  $F$ ”, y lo notaremos por  $\text{Irr}(\alpha, F)$ .

Observemos que este cumple  $[F(\alpha) : F] = \deg \text{Irr}(\alpha, F)$ . A dicho grado lo llamaremos a veces grado de  $\alpha$  sobre  $F$ .

Si  $F \leq K$  es una extensión de cuerpos y  $\alpha \in K$ , para buscar  $\text{Irr}(\alpha, F)$  tenemos que buscar un polinomio en  $F[x]$  que sea mónico, irreducible y que tenga a  $\alpha$  como raíz.

La notación de “mínimo” se debe por cómo se ha obtenido  $f$  en la demostración anterior: se ha obtenido como un generador de  $\ker e_\alpha$ , y en un cuerpo los generadores de los ideales se escogen tomando el polinomio de menor grado. Al ser mónico, tenemos garantizada su unicidad, por lo que es el polinomio de grado más pequeño del que  $\alpha$  es raíz.

*Observación.* Todo otro polinomio  $g \in F[x]$  con  $g(\alpha) = 0$  satisface que  $g = h \text{Irr}(\alpha, F)$  para cierto  $h \in F[x]$ , puesto que en dicho caso tendríamos que (según la demostración anterior):

$$g \in \ker e_\alpha = \langle f \rangle$$

Aquí vemos la minimalidad de  $\text{Irr}(\alpha, F)$ , puesto que la condición  $g(\alpha) = 0$  implica que  $\text{Irr}(\alpha, F)$  divide a  $g$ .

**Ejemplo.** Veamos ejemplos de esta última definición:

- $\text{Irr}(i, \mathbb{Q}) = x^2 + 1 \in \mathbb{Q}[x]$ , que es irreducible en  $\mathbb{Q}[x]$  por ser de grado 2 y no tener raíces en  $\mathbb{Q}$ . De aquí deducimos que  $\{1, i\}$  es una  $\mathbb{Q}$ -base de  $\mathbb{Q}(i)$ .
- $\text{Irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2 \in \mathbb{Q}[x]$ , que es irreducible en  $\mathbb{Q}[x]$  por Eisenstein para  $p = 2$ , luego  $\{1, \sqrt{2}\}$  es una  $\mathbb{Q}$ -base de  $\mathbb{Q}(\sqrt{2})$ .
- $\text{Irr}\left(e^{\frac{2\pi i}{3}}, \mathbb{Q}\right)$ . Podríamos pensar primero en el polinomio  $x^3 - 1$ , pero este no es irreducible, ya que 1 es una raíz suya:

$$x^3 - 1 = (x - 1)(x^2 + x + 1)$$

Ahora, tenemos que  $x^2 + x + 1$  es un polinomio del que  $e^{\frac{2\pi i}{3}}$  es raíz, y además es un polinomio irreducible, ya que es de grado 2 y no tiene raíces en  $\mathbb{Q}$ , por lo que  $\text{Irr}\left(e^{\frac{2\pi i}{3}}, \mathbb{Q}\right) = x^2 + x + 1$ .

Una  $\mathbb{Q}$ -base de  $\mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right)$  es  $\{1, e^{\frac{2\pi i}{3}}\}$ , luego:

$$\left[\mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right) : \mathbb{Q}\right] = 2$$

A lo largo de estos ejemplos sabíamos que los polinomios mencionados no tenían raíces en  $\mathbb{Q}$  porque en Álgebra I se vio que una condición necesaria para que un racional sea raíz de un polinomio mónico con coeficientes en  $\mathbb{Z}$  es que sea divisor del término independiente del polinomio.

### 1.1.2. Ejercicios

**Ejercicio 1.1.2.** Sea  $F \leq K$  extensión y  $\alpha \in K$  de grado 2 sobre  $F$ . Demostrar que  $F(\alpha)$  es un cuerpo de descomposición de  $\text{Irr}(\alpha, F)$ .

Si  $\alpha$  es de grado 2 sobre  $F$ , entonces tenemos que  $[F(\alpha) : F] = 2 = \deg \text{Irr}(\alpha, F)$ , por lo que tenemos que  $\exists a, b \in F$  de forma que:

$$\text{Irr}(\alpha, F) = x^2 + ax + b$$

puesto que sabemos que  $\text{Irr}(\alpha, F)$  es un polinomio mónico. Por la propia definición de  $\text{Irr}(\alpha, F)$ , sabemos que  $\alpha$  es raíz de este polinomio, por lo que el Teorema de Ruffini nos dice que  $\text{Irr}(\alpha, F)$  es divisible entre  $(x - \alpha)$  en  $K[x]$ , luego se cumple que:

$$\text{Irr}(\alpha, F) = (x - \alpha)(x - \beta)$$

para cierto  $\beta \in K$ . En este punto, de la igualdad:

$$x^2 + ax + b = (x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta$$

Dedujimos que  $a = -\alpha - \beta$ , por lo que  $\beta = -(\alpha + a) \in F(\alpha)$ . En definitiva, acabamos de ver que  $\text{Irr}(\alpha, F)$  se descompone como producto de polinomios de grado 1 en  $F(\alpha)[x]$ , con  $F(\alpha) = F(\alpha, \beta)$ , por ser  $\beta \in F(\alpha)$ ; es decir,  $F(\alpha)$  es un cuerpo de descomposición de  $\text{Irr}(\alpha, F)$ .

**Ejercicio 1.1.3.** Calcular  $\text{Irr}(w, \mathbb{Q}(\sqrt[3]{2}))$ , para  $w = e^{\frac{2\pi i}{3}}$ .

Sabemos que  $w$  es una raíz cúbica de la unidad, por lo que es raíz del polinomio mónico:

$$x^3 - 1$$

Sin embargo, este polinomio no es irreducible, ya que 1 es raíz suya. Lo dividimos entre  $x - 1$ , para obtener:

$$x^3 - 1 = (x - 1)(x^2 + x + 1)$$

Y tenemos que  $x^2 + x + 1$  es un polinomio del que  $w$  es raíz. Además, este polinomio es irreducible en  $\mathbb{Q}(\sqrt[3]{2})[x]$ , por ser de grado 2 y ser sus dos raíces complejas (son  $w$  y  $w^2$ ). En definitiva, hemos probado que:

$$\text{Irr}\left(w, \mathbb{Q}(\sqrt[3]{2})\right) = x^2 + x + 1$$

**Ejercicio 1.1.4.** Sea  $p$  un número primo y  $w \neq 1$  una raíz  $p$ -ésima compleja de la unidad, calcular  $\text{Irr}(w, \mathbb{Q})$ .

Como  $w$  es una raíz cúbica de la unidad, tenemos que  $w$  es raíz del polinomio:

$$x^p - 1$$

Que no es irreducible, ya que 1 es raíz suya. Si lo dividimos entre  $x - 1$ , obtenemos:

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \dots + x + 1)$$

Y la demostración se concluye (hágase) probando que  $x^{p-1} + x^{p-2} + \dots + x + 1$  es un polinomio irreducible, o bien que  $[\mathbb{Q}(w) : \mathbb{Q}] = p - 1$ , con lo que al final tendremos que:

$$\text{Irr}(w, \mathbb{Q}) = x^{p-1} + x^{p-2} + \dots + x + 1$$

## 1.2. Extensiones finitas y extensiones algebraicas

El siguiente Lema nos será de gran utilidad siempre que queramos calcular el grado de una extensión:

**Lema 1.8** (de la Torre). *Si  $F \leq K \leq L$  es una extensión de cuerpos, entonces:*

$$F \leq L \text{ es finita} \iff \begin{cases} F \leq K \\ K \leq L \end{cases} \text{ son finitas}$$

Además,  $[L : F] = [L : K][K : F]$ .

*Demostración.* Por doble implicación:

$\implies$ ) Notemos que  $K$  es un  $F$ -subespacio vectorial de  $L$ , del que suponíamos ser un  $F$ -espacio vectorial de dimensión finita, por lo que  $F \leq K$  será también una extensión finita. Como  $F \subseteq K$ , si tomamos  $\{\alpha_1, \dots, \alpha_t\}$  un  $F$ -sistema de generadores del  $F$ -espacio vectorial  $L$ , tendremos entonces que este mismo conjunto es un  $K$ -sistema de generadores del  $K$ -espacio vectorial  $L$ , por lo que  $K \leq L$  también es finita, ya que basta mirar los escalares de  $F$  como si fueran escalares de  $K$ .

$\iff$ ) Sean  $\{u_1, \dots, u_n\}$  una  $K$ -base de  $L$  y  $\{v_1, \dots, v_m\}$   $F$ -base de  $K$ , veamos entonces que:

$$\{u_i v_j : i \in \{1, \dots, n\}, j \in \{1, \dots, m\}\}$$

es una  $F$ -base de  $L$ :

- Si  $\alpha \in L$ , tenemos que existen  $k_1, \dots, k_n \in K$  de forma que:

$$\alpha = k_1 u_1 + \dots + k_n u_n$$

Para cada  $k_i$  existen  $a_{i,1}, \dots, a_{i,m} \in F$  de forma que:

$$k_i = a_{i,1} v_1 + \dots + a_{i,m} v_m$$

de donde:

$$\begin{aligned} \alpha &= u_1(a_{1,1} v_1 + \dots + a_{1,m} v_m) + \dots + u_n(a_{n,1} v_1 + \dots + a_{n,m} v_m) \\ &= a_{1,1} u_1 v_1 + a_{1,2} u_1 v_2 + \dots + a_{1,m} u_1 v_m + \dots + a_{n,m} u_n v_m \end{aligned}$$

Por lo que es un  $F$ -sistema de generadores.

- Si ahora tenemos que  $a_{i,j} \in F$  de forma que:

$$\sum_{j=1}^m \sum_{i=1}^n a_{i,j} v_j u_i = 0$$

Como  $\{u_1, \dots, u_n\}$  es un conjunto  $K$ -linealmente independiente y tenemos  $a_{i,j} v_j \in K$ , tendremos entonces que:

$$\sum_{j=1}^m a_{i,j} v_j = 0 \quad \forall i \in \{1, \dots, n\}$$

Pero como  $\{v_1, \dots, v_m\}$  es un conjunto  $F$ -linealmente independiente, tendremos entonces que  $a_{i,j} = 0 \quad \forall j \in \{1, \dots, m\}, \quad \forall i \in \{1, \dots, n\}$ , por lo que el conjunto es  $F$ -linealmente independiente.

Para la fórmula entre las dimensiones, si  $F \leq K$  o  $K \leq L$  no fuera finita, tendríamos entonces que  $F \leq L$  no sería finita y viceversa. Supuesto ahora que estamos en el caso en el que todas las extensiones son finitas, hemos visto en la implicación " $\iff$ ") que si tenemos una base de  $L$  sobre  $K$  de  $n$  vectores y una base de  $K$  sobre  $F$  de  $m$  vectores, entonces podemos construir una base de  $L$  sobre  $F$  de  $n \cdot m$  vectores. Observando que:

$$n \cdot m = [L : F], \quad n = [L : K], \quad m = [K : F]$$

tenemos la fórmula demostrada. □

**Notación.** Cuando tenemos extensiones de cuerpos de la forma:

$$F_1 \leq F_2 \leq \dots \leq F_s$$

se suele decir que tenemos una torre de cuerpos. A los cuerpos intermedios (aquellos entre  $F_2$  y  $F_s$ , ambos incluidos) se les llama a veces subextensiones.

**Ejemplo.** Sea  $w \in \mathbb{C}$ , una raíz cúbica primitiva de 1, vimos que  $\mathbb{Q}(w, \sqrt[3]{2})$  era un cuerpo de descomposición de  $x^3 - 2 \in \mathbb{Q}[x]$ . Queremos calcular:

$$[\mathbb{Q}(w, \sqrt[3]{2}) : \mathbb{Q}]$$

Calculemos mediante una torre:

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{Q}(\sqrt[3]{2})(w) = \mathbb{Q}(\sqrt[3]{2}, w)$$

Sabemos ya que:

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

ya que  $x^3 - 2 \in \mathbb{Q}[x]$  es irreducible por Eisenstein para  $p = 2$ . Ahora, por el Lema de la Torre:

$$[\mathbb{Q}(\sqrt[3]{2}, w) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2})(w) : \mathbb{Q}(\sqrt[3]{2})] [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$$

Sabemos que  $w$  es raíz de  $x^2 + x + 1 \in \mathbb{Q}(\sqrt[3]{2})[x]$ . Es irreducible porque tiene grado 2 y sus raíces no están en  $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ , de donde:

$$[\mathbb{Q}(\sqrt[3]{2})(w) : \mathbb{Q}(\sqrt[3]{2})] = 2$$

En definitiva:

$$[\mathbb{Q}(\sqrt[3]{2}, w) : \mathbb{Q}] = 2 \cdot 3 = 6$$

Una base de  $K = \mathbb{Q}(\sqrt[3]{2}, w)$  es (por el Lema de la Torre):

$$\left\{ 1, \sqrt[3]{2}, (\sqrt[3]{2})^2, w, w\sqrt[3]{2}, w(\sqrt[3]{2})^2 \right\}$$

**Ejemplo.** Queremos calcular  $\text{Irr}(\sqrt{5} + \sqrt{-2}, \mathbb{Q})$ , vamos a buscar primero información sobre el grado del polinomio que buscamos.

Su grado es  $[\mathbb{Q}(\sqrt{5} + \sqrt{-2}) : \mathbb{Q}]$ . Sea  $\alpha = \sqrt{5} + \sqrt{-2} \in \mathbb{C}$ :

$$\alpha - \sqrt{-2} = \sqrt{5} \implies \alpha^2 - 2 - 2\alpha\sqrt{-2} = 5$$

de donde:

$$\sqrt{-2} = \frac{\alpha^2 - 7}{2\alpha} \in \mathbb{Q}(\alpha)$$

de donde  $\mathbb{Q}(\sqrt{-2}) \leq \mathbb{Q}(\alpha)$ . Haciendo el mismo procedimiento con  $\sqrt{5}$ , llegamos a que  $\sqrt{5} \in \mathbb{Q}(\alpha)$ , luego  $\mathbb{Q}(\sqrt{5}) \leq \mathbb{Q}(\alpha)$ , de donde:

$$\mathbb{Q}(\sqrt{5}, \sqrt{-2}) \leq \mathbb{Q}(\alpha) \leq \mathbb{Q}(\sqrt{5}, \sqrt{-2})$$

Luego  $\mathbb{Q}(\sqrt{5}, \sqrt{-2}) = \mathbb{Q}(\alpha)$ . Ahora podemos considerar:

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{5}) \leq \mathbb{Q}(\sqrt{5})(\sqrt{-2}) = \mathbb{Q}(\sqrt{5} + \sqrt{-2})$$

por el Lema de la Torre:

$$[\mathbb{Q}(\sqrt{5} + \sqrt{-2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] [\mathbb{Q}(\sqrt{5})(\sqrt{-2}) : \mathbb{Q}(\sqrt{5})]$$

Sabemos que el primero vale 2 porque  $x^2 - 5$  es irreducible por Eisenstein. El segundo sabemos que es menor o igual que 2 por ser  $x^2 + 2$  un posible polinomio, pero por ser su raíz un número imaginario no puede estar en  $\mathbb{Q}(\sqrt{5})$ , tiene grado 2 y ninguna de sus raíces están en  $\mathbb{Q}(\sqrt{5})$ . En definitiva:

$$[\mathbb{Q}(\sqrt{5} + \sqrt{-2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] [\mathbb{Q}(\sqrt{5})(\sqrt{-2}) : \mathbb{Q}(\sqrt{5})] = 2 \cdot 2 = 4$$

Ahora, sabemos que el polinomio tiene grado 4, por lo que si encontramos uno de grado 4 del que  $\alpha$  sea raíz, no tenemos que probar que sea irreducible. De:

$$\sqrt{-2} = \frac{\alpha^2 - 7}{2\alpha} \in \mathbb{Q}(\alpha)$$

Elevamos al cuadrado, operamos y:

$$\alpha^4 - 6\alpha^2 + 49 = 0$$

De donde  $\alpha$  es raíz de  $x^4 - 6x^2 + 49 \in \mathbb{Q}[x]$ .

Esta técnica de saber el grado del polinomio irreducible es una técnica muy útil a la hora de calcular el polinomio irreducible.

**Proposición 1.9.** *Sea  $F \leq K$  y  $\alpha \in K$ , tenemos que  $\alpha$  es algebraico sobre  $F$  si y solo si existe una torre de cuerpos  $F \leq L \leq K$  tal que  $F \leq L$  es finita y  $\alpha \in L$ .*

*Demostración.* Por doble implicación:

$\Rightarrow$ ) Si  $\alpha$  es algebraico sobre  $F$ , si tomamos  $L = F(\alpha)$  es claro que  $F \leq L \leq K$  así como que  $\alpha \in L$ . La Proposición 1.7 nos dice que  $F \leq L$  es finita.

$\Leftarrow$ ) Sea  $L$  un cuerpo en las condiciones del enunciado, tenemos entonces que como  $F \leq L$  es finita y  $F \leq F(\alpha) \leq L$  entonces (usando el Lema de la Torre)  $F \leq F(\alpha)$  es finita, luego el conjunto  $\{\alpha^n : n \geq 0\}$  no puede ser  $F$ -linealmente independiente, si no que tiene que existir  $m \in \mathbb{N}$  con  $m \geq 1$  de forma que  $\alpha^m$  dependa linealmente de  $1, \alpha, \dots, \alpha^{m-1}$ , es decir, existen  $a_0, \dots, a_{m-1} \in F$  de forma que:

$$\alpha^m = \sum_{i=0}^{m-1} a_i \alpha^i$$

Por lo que tomando el polinomio:

$$f = x^m - \sum_{i=0}^{m-1} a_i x^i \in F[x]$$

Tenemos que  $f(\alpha) = 0$ , luego  $\alpha$  es algebraico sobre  $F$ .

□

**Definición 1.13** (Extensión algebraica). Una extensión  $F \leq K$  se dice algebraica si todo elemento  $\alpha \in K$  es algebraico sobre  $F$ .

**Teorema 1.10.** *Una extensión de cuerpos es finita si y solo si es algebraica y finitamente generada.*

*Demostración.* Sea  $F \leq K$  una extensión de cuerpos, por doble implicación:

- $\Rightarrow)$  Tomamos  $\{u_1, \dots, u_t\}$  una  $F$ -base de  $K$ , tenemos entonces que  $K = F(u_1, \dots, u_t)$ . Además, si  $\alpha \in K$ , tenemos entonces que  $F \leq F(\alpha) \leq K$  con  $F \leq K$  finita, por lo que por el Lema de la Torre tenemos que  $F \leq F(\alpha)$  es finita. Tomando  $L = F(\alpha)$  y aplicando la Proposición anterior tenemos que  $\alpha$  es algebraico sobre  $F$ .
- $\Leftarrow)$  Suponemos que  $K = F(\alpha_1, \dots, \alpha_n)$  y que  $\alpha_i$  es algebraico sobre  $F$  para todo  $i \in \{1, \dots, n\}$ . Por el lema de la torre y la Proposición 1.7, tenemos:

$$F \leq F(\alpha_1) \leq \dots \leq F(\alpha_1, \dots, \alpha_n)$$

cada uno es una extensión finita del anterior, por lo que  $F(\alpha_1, \dots, \alpha_n) \geq F$  es finita.

□

*Observación.* Hemos visto que si  $\alpha_1, \dots, \alpha_n \in K$  y  $\alpha_1$  es algebraico sobre  $F$ ,  $\alpha_2$  es algebraico sobre  $F(\alpha_1)$ , ...,  $\alpha_n$  es algebraico sobre  $F(\alpha_1, \dots, \alpha_{n-1})$ , entonces  $[F(\alpha_1, \dots, \alpha_n) : F] < \infty$ .

**Corolario 1.10.1.** *Si  $F \leq K$  extensión y llamamos:*

$$\Lambda = \{\alpha \in K : \alpha \text{ algebraico sobre } F\}$$

*Entonces,  $\Lambda$  es un subcuerpo de  $K$  y la extensión  $F \leq \Lambda$  es algebraica.*

*Demostración.* Tenemos que ver que  $\Lambda$  contiene al 0, al 1 y que es cerrada para sumas, productos e inversos:

- $0, 1 \in \Lambda$  es claro.
- Si  $\alpha, \beta \in \Lambda$ , tenemos entonces que:

$$\alpha - \beta, \alpha\beta \in F(\alpha, \beta)$$

Y como la extensión  $F \leq F(\alpha, \beta)$  es finita por ser  $\alpha$  y  $\beta$  algebraicos sobre  $F$ , deducimos que la extensión es algebraica, luego  $\alpha - \beta, \alpha\beta$  son algebraicos sobre  $F$ , es decir,  $\alpha - \beta, \alpha\beta \in \Lambda$ .

- Si  $\alpha \in \Lambda$ , tenemos entonces que:

$$\alpha^{-1} \in F(\alpha)$$

Y de forma análoga al punto anterior, como  $F \leq F(\alpha)$  es finita por ser  $\alpha$  algebraico sobre  $F$ , deducimos que la extensión es algebraica, luego  $\alpha^{-1} \in \Lambda$ .

En definitiva,  $\Lambda$  es un cuerpo contenido en  $K$ , luego es un subcuerpo de  $K$  y es claro que  $F \leq K$  es algebraico.  $\square$

**Definición 1.14** (Clausura algebraica). El conjunto  $\Lambda$  del Corolario anterior recibe el nombre de clausura algebraica de  $F$  en  $K$ .

**Ejemplo.** Si tomamos  $F = \mathbb{Q}$  y  $K = \mathbb{C}$ , notaremos a la clausura algebraica (en  $\mathbb{C}$ ) de  $\mathbb{Q}$  por  $\overline{\mathbb{Q}}$ , y nos referiremos a sus elementos como los números algebraicos.

Según el corolario, la extensión  $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$ , puesto que para todo  $n \in \mathbb{N}$  podemos considerar  $\mathbb{Q}(\sqrt[n]{2}) \leq \overline{\mathbb{Q}}$  y  $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ , que lo sabemos porque:

$$\text{Irr}(\sqrt[n]{2}, \mathbb{Q}) = x^n - 2$$

Ya que  $x^n - 2$  es irreducible, por el criterio de Eisenstein.

### 1.2.1. Ejercicios

**Ejercicio 1.2.1.** Calcular  $\text{Irr}(\sqrt{2} + i, \mathbb{Q})$ .

Sea  $\alpha = \sqrt{2} + i$ , observemos que tenemos ya  $\mathbb{Q}(\alpha) \leq \mathbb{Q}(\sqrt{2}, i)$ . Pero si nos damos cuenta de que:

$$\begin{aligned} \alpha - \sqrt{2} &= i \implies \alpha^2 + 2 - 2\alpha\sqrt{2} = -1 \implies \sqrt{2} = \frac{\alpha^2 + 3}{2\alpha} \in \mathbb{Q}(\alpha) \\ \alpha - i &= \sqrt{2} \implies \alpha^2 - 1 - 2\alpha i = 2 \implies i = \frac{\alpha^2 - 3}{2\alpha} \in \mathbb{Q}(\alpha) \end{aligned}$$

Tenemos entonces que  $\mathbb{Q}(\sqrt{2}, i) \leq \mathbb{Q}(\alpha)$ , de donde:

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i)$$

Si ahora tratamos de calcular  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ , podemos usar esta última igualdad y el lema de la torre para concluir que:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

- Como  $x^2 - 2$  es irreducible por Eisenstein para  $p = 2$ , tenemos que  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ .
- Como  $x^2 + 1$  es un polinomio de grado 2 cuyas dos raíces son complejas, tenemos que es irreducible en  $\mathbb{Q}(\sqrt{2})$ , por lo que  $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$ .

En definitiva:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$$

Con lo que si encontramos un polinomio mónico de grado 4 del que  $\alpha$  sea raíz, habremos encontrado  $\text{Irr}(\alpha, \mathbb{Q})$ . Para ello:

$$2i\alpha = \alpha^2 - 3 \implies -4\alpha^2 = \alpha^4 + 9 - 6\alpha^2 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Por lo que tomando:

$$g = x^4 - 2x^2 + 9 \in \mathbb{Q}[x]$$

Tenemos que  $\text{Irr}(\alpha, \mathbb{Q}) = g$ .

**Ejercicio 1.2.2.** Calcular  $\text{Irr}(\sqrt{2} + i\sqrt{3}, \mathbb{Q})$ .

Tomando  $\alpha = \sqrt{2} + i\sqrt{3}$ , procedemos de forma análoga al ejercicio anterior:

$$\begin{aligned}\alpha - \sqrt{2} = i\sqrt{3} &\implies \alpha^2 + 2 - 2\alpha\sqrt{2} = -3 \implies \sqrt{2} = \frac{\alpha^2 + 5}{2\alpha} \in \mathbb{Q}(\alpha) \\ \alpha - i\sqrt{3} = \sqrt{2} &\implies \alpha^2 - 3 - 2\alpha i\sqrt{3} = 2 \implies i\sqrt{3} = \frac{\alpha^2 - 5}{2\alpha} \in \mathbb{Q}(\alpha)\end{aligned}$$

De donde podemos escribir:

$$\mathbb{Q}(\sqrt{2}, i\sqrt{3}) \leqslant \mathbb{Q}(\alpha) \leqslant \mathbb{Q}(\sqrt{2}, i\sqrt{3})$$

Tratamos ahora de calcular  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$  usando el lema de la torre:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

- Como hemos visto en el ejercicio anterior,  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ .
- Como  $x^2 + 3$  es un polinomio de grado 2 cuyas raíces son complejas, tenemos que es irreducible en  $\mathbb{Q}(\sqrt{2})$ , por lo que  $[\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ .

En definitiva, al igual que antes tenemos que  $[\mathbb{Q}(\alpha), \mathbb{Q}] = 4$ , buscamos un polinomio mónico de grado 4 del que  $\alpha$  sea raíz. Para ello:

$$2\alpha\sqrt{2} = \alpha^2 + 5 \implies 8\alpha^2 = \alpha^4 + 25 + 10\alpha^2 \implies \alpha^4 + 2\alpha^2 + 25 = 0$$

Por lo que:

$$\text{Irr}(\alpha, \mathbb{Q}) = x^4 + 2x^2 + 25$$

**Ejercicio 1.2.3.** Calcular un cuerpo de descomposición de  $x^4 + 16 \in \mathbb{Q}[x]$  y su grado sobre  $\mathbb{Q}$ .

Sabemos que  $f$  tiene 4 raíces, y como  $f' = 4x^3$ , sabemos que todas estas son distintas entre sí. Las raíces de  $f$  resultan ser el conjunto:

$$\sqrt[4]{-16} = \sqrt[4]{16}\sqrt[4]{-1} = 2\sqrt[4]{-1}$$

Usando la fórmula de De Moivre:

$$\sqrt[n]{e^{i\theta}} = \left\{ e^{i\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)} : k \in \{0, \dots, n-1\} \right\} = \left\{ e^{i\left(\frac{\theta+2k\pi}{n}\right)} : k \in \{0, \dots, n-1\} \right\}$$

para nuestro caso tenemos  $n = 4$  y  $\theta = \pi$ :

$$\sqrt[4]{-1} = \left\{ e^{i\frac{\pi}{4}}, e^{i\frac{3\pi}{4}}, e^{i\frac{5\pi}{4}}, e^{i\frac{7\pi}{4}} \right\}$$

donde:

$$e^{i\frac{\pi}{4}} = \cos \frac{\pi}{4} + i \sin \frac{\pi}{4} = \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}$$

si usamos ahora que tanto los opuestos como conjugados también son raíces:

$$\sqrt[4]{-1} = \left\{ \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2} \right\}$$

de donde:

$$\sqrt[4]{-16} = 2\sqrt[4]{-1} = \left\{ \sqrt{2} + i\sqrt{2}, \sqrt{2} - i\sqrt{2}, -\sqrt{2} + i\sqrt{2}, -\sqrt{2} - i\sqrt{2} \right\}$$

En definitiva, el cuerpo de descomposición será:

$$K = \mathbb{Q}(\sqrt{2} + i\sqrt{2}, \sqrt{2} - i\sqrt{2}) \stackrel{(*)}{=} \mathbb{Q}(i, \sqrt{2})$$

la inclusión  $\subseteq$ ) está clara, para la otra:

$$\begin{aligned} \sqrt{2} \in K &\implies \mathbb{Q}(\sqrt{2}) \leqslant K \\ i\sqrt{2} \in K &\implies i \in K \implies \mathbb{Q}(\sqrt{2}, i) \leqslant K \end{aligned}$$

Finalmente, usando el Lema de la Torre llegamos a que:

$$[K : \mathbb{Q}] = 4$$

**Ejercicio 1.2.4.** Sea  $\alpha = \sqrt{2} + \sqrt[3]{2} \in \mathbb{R}$ , se pide:

a) Probar que  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ .

b) Calcular  $\text{Irr}(\alpha, \mathbb{Q})$ .

a) Para el primero:

$$\begin{aligned} \sqrt[3]{2} = \alpha - \sqrt{2} &\implies 2 = \alpha^3 - 3\alpha^2\sqrt{2} + 3\alpha(\sqrt{2})^2 - (\sqrt{2})^3 \\ &= \alpha^3 - 3\alpha^2\sqrt{2} + 6\alpha - 2\sqrt{2} \\ &= \alpha^3 + 6\alpha - (3\alpha^2 + 2)\sqrt{2} \end{aligned}$$

con lo que:

$$\sqrt{2} = \frac{\alpha^3 + 6\alpha - 2}{3\alpha^2 + 2} \in \mathbb{Q}(\alpha)$$

Como  $\sqrt[3]{2} = \alpha - \sqrt{2}$ , tenemos entonces que  $\sqrt[3]{2} \in \mathbb{Q}(\alpha)$ . Así, tenemos que:

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2})(\sqrt{2})$$

b) Probamos a calcular primero  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ . El Lema de la Torre nos dice que:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$$

Y sabemos que  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ , ya que  $x^3 - 2 = \text{Irr}(\sqrt[3]{2}, \mathbb{Q})$ , ya que por Eisenstein,  $x^3 - 2$  es irreducible para  $p = 2$ . Además, sabemos que:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt[3]{2})] \leqslant 2$$

Ya que  $\sqrt{2}$  es raíz de  $x^2 - 2$ . En consecuencia:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \leqslant 6$$

y múltiplo de 3. Si aplicamos el Lema en sentido contrario:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}][\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt[3]{2})]$$

Sabemos que  $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt[3]{2})] = 2$ , ya que  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ , al ser  $x^2 - 2 \in \mathbb{Q}[x]$  irreducible (también por Eisenstein).

En definitiva, tenemos que  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$  es múltiplo de 2, de 3 y que es menor o igual que 6, con lo que  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$ . Para terminar, elevar la expresión de antes de  $\sqrt{2}$  al cuadrado, con lo que obtenemos un polinomio de grado 6 mónico del que  $\alpha$  es raíz, con lo que ya sabemos que este es el irreducible.

**Ejercicio 1.2.5.** Calcular  $f = \text{Irr}(1 + \sqrt[3]{2}, \mathbb{Q})$ . Calcular las raíces complejas de  $f$  y un cuerpo de descomposición suyo.

Sea  $\alpha = 1 + \sqrt[3]{2}$ , tenemos que  $\alpha \in \mathbb{Q}(\sqrt[3]{2})$ , por lo que  $\mathbb{Q}(\alpha) \leq \mathbb{Q}(\sqrt[3]{2})$ . Además, como:

$$\sqrt[3]{2} = 1 + \sqrt[3]{2} - 1 \in \mathbb{Q}(\alpha)$$

tenemos que  $\mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{Q}(\alpha)$ , con lo que  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2})$ . Tenemos por tanto que:

$$[\mathbb{Q} : \mathbb{Q}(\alpha)] = \left[ \mathbb{Q} : \mathbb{Q}(\sqrt[3]{2}) \right] = 3$$

ya que  $x^3 - 2 \in \mathbb{Q}[x]$  es irreducible. Buscamos pues un polinomio de grado 3 del que  $\alpha$  sea raíz. Para ello:

$$\alpha - 1 = \sqrt[3]{2} \implies \alpha^3 - 3\alpha^2 + 3\alpha - 1 = 2 \implies \alpha^3 - 3\alpha^2 + 3\alpha - 3 = 0$$

Con lo que tomando  $f = x^3 - 3x^2 + 3x - 3 \in \mathbb{Q}[x]$  tenemos que  $f = \text{Irr}(\alpha, \mathbb{Q})$ . Tenemos que las raíces de  $f$  cumplen la relación:

$$(x - 1)^3 = 2$$

con lo que  $x - 1$  es cada una de las tres raíces cúbicas de 2, que son:

$$\left\{ \sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{\frac{4\pi i}{3}} \right\}$$

Y tenemos que:

$$\begin{aligned} e^{\frac{2\pi i}{3}} &= \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \\ e^{\frac{4\pi i}{3}} &= \cos\left(\frac{4\pi}{3}\right) + i \sin\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - i\frac{\sqrt{3}}{2} \end{aligned}$$

Por lo que notando  $\gamma = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$ , tenemos que las raíces de  $f$  son:

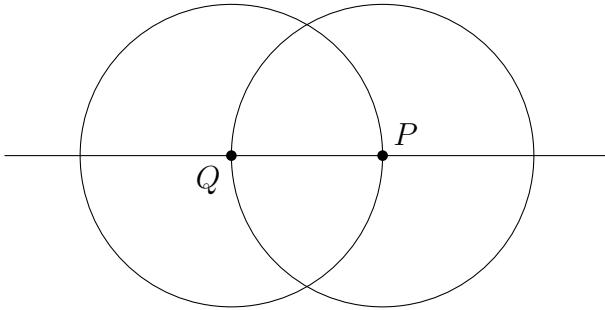
$$\left\{ 1 + \sqrt[3]{2}, 1 + \sqrt[3]{2}\gamma, 1 + \sqrt[3]{2}\bar{\gamma} \right\}$$

En definitiva, un cuerpo de descomposición de  $f$  es:

$$\mathbb{Q}\left(1 + \sqrt[3]{2}, 1 + \sqrt[3]{2}\gamma, 1 + \sqrt[3]{2}\bar{\gamma}\right)$$

y se verifica que es igual a:

$$\mathbb{Q}\left(\sqrt[3]{2}, \gamma\sqrt[3]{2}, \gamma^2\sqrt[3]{2}\right)$$

Figura 1.1: Prueba gráfica de que  $S \subseteq S^c$ .

### 1.3. Construcciones con regla y compás

Esta sección está dedicada a considerar ciertas construcciones geométricas en el plano afín euclídeo y su relación con ciertas extensiones de cuerpos. El origen de estas construcciones geométricas se remonta a los postulados de Euclides, un conjunto de reglas que trataba de axiomatizar el trabajo de los matemáticos de la época sobre un plano, un conjunto de normas que nos dicen qué podemos considerar como un punto del plano y qué no. Los puntos del plano se obtendrán como intersecciones de dos elementos geométricos como rectas y circunferencias, estando estos determinados a su vez por dos puntos del plano:

- Dos puntos a unir en el caso de una recta, que puede alargarse tanto como queramos.
- Dos puntos a considerar en el caso de una circunferencia: uno que juega el papel de “centro” de la circunferencia y otro cuya distancia a dicho punto centro determina el radio de la circunferencia.

No debemos pensar en estos elementos como en conjuntos de puntos (es lo que haría la matemática moderna), sino como meros elementos auxiliares que nos permiten construir más puntos del plano. Trataremos el plano euclídeo como una idea básica inherente al ser humano, y sobre esta idea plantearemos varias definiciones con el lenguaje matemático moderno, con el fin de alcanzar las relaciones con los cuerpos previamente comentada.

En lo que sigue, sea  $S$  un conjunto de puntos del plano con al menos dos puntos distintos (ya que bajo los postulados en los que nos basamos con cero o un punto no somos capaces de construir nada más), definimos ahora  $\Gamma$ , el conjunto cuyos elementos son las rectas y circunferencias que pueden trazarse al considerar dos puntos distintos de  $S$ . Definimos además  $S^c$ , el conjunto de puntos obtenidos al intersecar cualesquiera dos elementos de  $\Gamma$ . Llamaremos a los elementos de  $S^c$  puntos constructibles (con regla y compás) a partir de  $S$  en un paso. Es claro que  $S \subseteq S^c$ , ya que si consideramos cualesquiera dos puntos de  $S$  y trazamos la recta que los une y las dos circunferencias que estos definen obtenemos dichos dos puntos como intersecciones de la recta y las dos circunferencias, como podemos observar en la Figura 1.1.

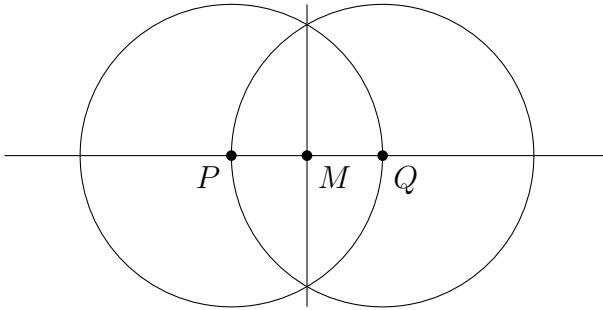


Figura 1.2: Construcción de la mediatrix.

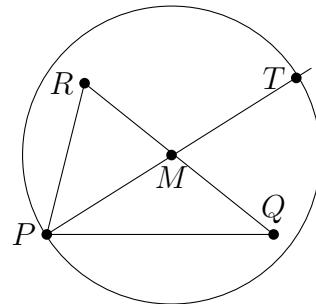


Figura 1.3: Completar el cuarto punto de un paralelogramo.

**Definición 1.15.** Dado un conjunto de puntos del plano  $S$ , definimos recursivamente:

$$S_0 = S, \quad S_{n+1} = S_n^c \quad \forall n \in \mathbb{N}$$

Llamamos al conjunto:

$$C(S) = \bigcup_{n \in \mathbb{N}} S_n$$

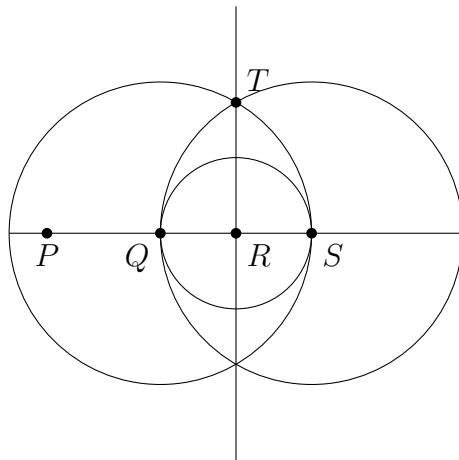
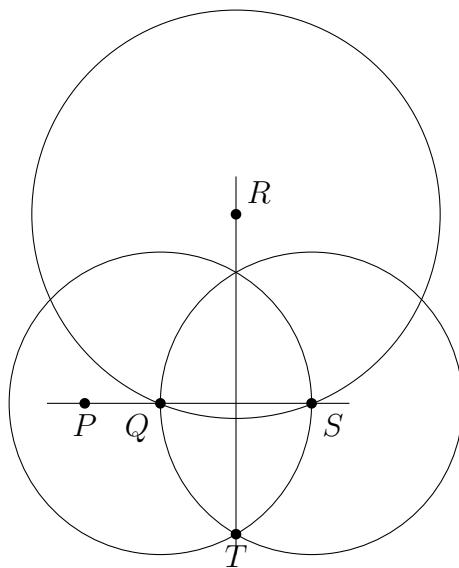
el conjunto de los puntos constructibles (con regla y compás) a partir de  $S$ .

**Ejercicio 1.3.1.** Construir a partir de tres puntos que no estén en la misma recta un cuarto punto que complete el paralelogramo.

Para ello, primero necesitamos considerar la construcción de la mediatrix, con la que obtenemos el punto medio entre dos puntos  $P$  y  $Q$ . Esta viene dada por la Figura 1.2. Una vez sabemos como realizar el punto medio de dos puntos dados, supongamos que tenemos 3 puntos:  $P$ ,  $Q$  y  $R$  no alineados y que queremos trazar el cuarto punto que completa el paralelogramo. En dicha situación, trazamos las rectas  $PQ$  y  $PR$ , así como la recta  $RQ$ . Trazamos el punto medio  $M$  entre los puntos  $R$  y  $Q$ , que hemos visto anteriormente cómo hacerlo. Ahora, trazamos la recta  $PM$  y la circunferencia con centro  $M$  y radio hasta  $P$ . El punto de intersección de estos dos últimos elementos geométricos nos dan el punto  $T$  que completa el paralelogramo. El procedimiento descrito se encuentra en la Figura 1.3

**Lema 1.11.** Sean  $P, Q, R$  puntos del plano con  $P$  y  $Q$  distintos, se puede construir con regla y compás a partir de ellos un punto  $T$  tal que las rectas  $PQ$  y  $RT$  son perpendiculares.

*Demostración.* Distinguimos casos en función de la posición relativa de  $P$ ,  $Q$  y  $R$ :

Figura 1.4: Trazar recta perpendicular por  $R$ .Figura 1.5: Trazar recta parpendicular por  $R$ .

**Suponiendo que  $R$  está en la recta  $PQ$ :** Trazamos la recta  $PQ$  y la circunferencia con centro  $R$  y que pasa por  $Q$  (si  $R = Q$ , la que pasa por  $P$ ), que nos da un punto intersección en  $PQ$ :  $S$ . Trazamos las circunferencias con centro  $Q$  y radio hasta  $S$ , y centro  $S$  y radio hasta  $Q$ . Estas dos circunferencias se cortan en dos puntos:  $T$  y  $T'$ . Uniéndolos, obtenemos lo buscado. El procedimiento descrito se encuentra en la Figura 1.4.

**Suponiendo que  $R$  no está en la recta  $PQ$ :** Trazamos la recta  $PQ$  así como la circunferencia de centro  $R$  y radio hasta  $Q$ , que nos da un punto de intersección con  $PQ$ :  $S$ . Trazamos la circunferencia de centro  $S$  y radio hasta  $Q$ , obteniendo un segundo punto de corte entre las dos circunferencias,  $T$ , que unimos con  $R$  y obtenemos la situación pedida. El procedimiento se ilustra en la Figura 1.5.

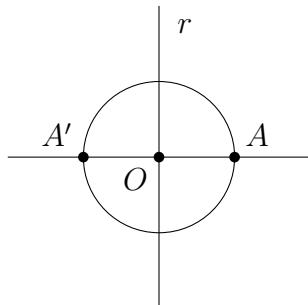
□

A partir del lema anterior, ya no será necesario recurrir a dichas construcciones

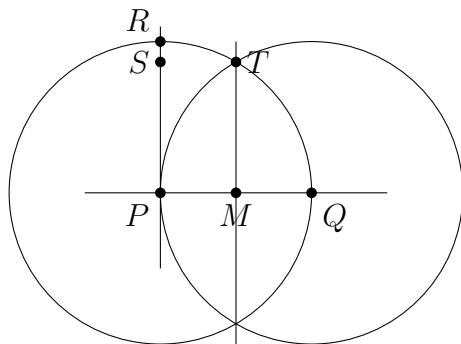
cada vez que tengamos dos puntos  $P$  y  $Q$  que determinan una recta y queramos construir una recta perpendicular a ella que pase por un tercer punto  $R$ .

**Ejercicio 1.3.2.** Dados dos puntos que determinan una recta  $r$  y un punto  $A$  no contenido en ella, construir el simétrico de  $A$  con respecto de  $r$ .

Sabemos ya por el lema anterior trazar una recta perpendicular a otra dada pasando por un punto, por lo que trazamos la recta perpendicular a  $r$  que pasa por  $A$ . Al punto de intersección entre ambas rectas lo nombramos  $O$ , y trazando la circunferencia de centro  $O$  y radio hasta  $A$  obtenemos como intersección con la recta perpendicular a  $r$  el punto  $A'$ , simétrico de  $A$  respecto de  $r$ .

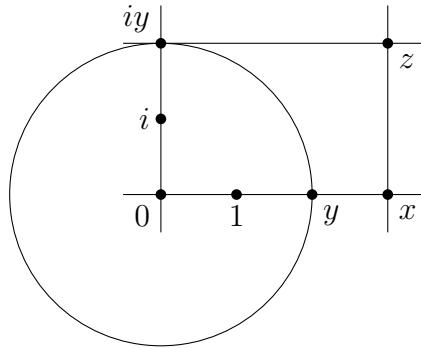


Si ahora elegimos dos puntos cualesquiera de  $S$ :  $P$  y  $Q$ , podemos realizar la siguiente construcción:



Trazar las dos circunferencias que definen los puntos  $P$  y  $Q$ , con lo que trazamos la mediatrix, la recta que se obtiene uniendo los puntos de intersección de las dos circunferencias. Nombramos a un punto de dicha intersección  $T$ . Trazamos la recta  $PQ$  y obtenemos su intersección con la recta previamente trazada en el punto  $M$ . A continuación, completamos el cuadrilátero que definen los puntos  $P$ ,  $M$  y  $T$  con el punto  $S$ , que nos permite considerar la recta  $PS$ . Si finalmente obtenemos la intersección de la recta  $PS$  con la circunferencia de centro  $P$  y radio hasta  $Q$  obtenemos el punto  $R$ , que pertenece a la recta  $PS$ , perpendicular a la recta  $PQ$  y el punto  $R$  se encuentra a la misma distancia que  $Q$  del punto  $P$ , corte de las dos rectas perpendiculares.

Hemos obtenido lo que consideraríamos un sistema de referencia ortonormal, y podemos renombrar los puntos  $P$ ,  $Q$  y  $R$  como  $(0,0)$ ,  $(1,0)$  y  $(0,1)$ , respectivamente.

Figura 1.6: Obtención de  $x, y$  a partir de  $z$ .

De esta forma, podemos ver el conjunto  $C(S)$  de puntos constructibles a partir de  $S$  como un subconjunto de  $\mathbb{C}$ . A partir de ahora, supondremos siempre que  $S$  es un conjunto que contiene a los números 0 y 1.

La pregunta natural que surge al hacer esta observación es la de fijado un conjunto inicial  $S \subseteq \mathbb{C}$ , qué puntos de  $\mathbb{C}$  son constructibles a partir de  $S$ . Es decir, obtener una descripción de  $C(S)$ .

*Observación.* Puesto que ahora suponemos que  $0, 1 \in S$ , siempre tendremos que  $i \in C(S)$ , ya que podemos realizar la construcción anterior para  $P = 0$ ,  $Q = 1$  y tomar  $R = i$ , por lo que podemos usar siempre que  $i \in C(S)$  bajo las hipótesis de  $0, 1 \in S$ .

**Lema 1.12.** *Dado  $z = x + iy \in \mathbb{C}$ , tenemos que:*

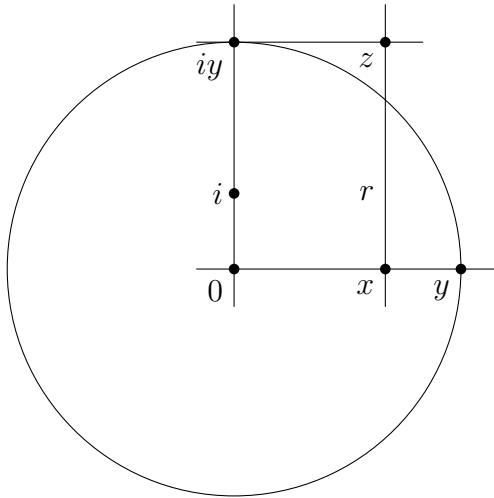
$$z \in C(S) \iff x, y \in C(S)$$

*Demostración.* Por doble implicación:

$\implies$ ) Supuesto que  $z \in C(S)$ , vemos que podemos construir  $x$  e  $y$  de la siguiente forma:

- Si  $z \in \mathbb{R}$ , tenemos ya construido  $x = z$  y sabemos que  $y = 0 \in C(S)$ .
- Si  $Re(z) = 0$ , sabemos que  $x = 0 \in C(S)$  y tenemos el punto  $z = iy$  que construiremos en el siguiente apartado.
- En otro caso, podemos considerar la recta  $01$  y trazar la recta perpendicular a ella que pasa por el punto  $z$ . Como la intersección de las dos rectas obtenemos el punto  $x$ . Ahora, si consideramos la recta  $0i$  y trazamos la recta perpendicular a ella que pasa por el punto  $z$ , obtenemos el punto  $iy$ . Para obtener  $y$ , lo que haremos será considerar la intersección de la recta  $01$  con la circunferencia de centro 0 y radio hasta  $iy$ . El procedimiento se ilustra en la Figura 1.6.

$\iff$ ) Supuesto que  $x, y \in C(S)$ , lo que haremos será considerar la recta perpendicular a la recta  $0x$  que pasa por el punto  $x$ , obteniendo la recta  $r$ . Posteriormente, consideraremos como  $iy$  la intersección de la recta  $0i$  con la circunferencia de centro 0 y radio hasta  $y$ . Posteriormente, trazamos la recta perpendicular a  $0i$  que pasa por  $iy$ , y obtenemos como  $z$  la intersección de esta última recta con la recta  $r$ . El procedimiento se ilustra en la Figura 1.7.

Figura 1.7: Obtención de  $z$  a partir de  $x$  e  $y$ .

□

**Proposición 1.13.** *El conjunto  $C(S)$  es un subcuerpo de  $\mathbb{C}$ . Además, es cerrado por conjugación, es decir:*

$$z \in C(S) \implies \bar{z} \in C(S)$$

*Demostración.* Si probamos que la suma de dos números reales constructibles es constructible, obtenemos por el Lema 1.12 que la suma de dos números complejos constructibles es constructible. Análogamente, si demostramos que el producto de dos números reales constructibles es constructible, tendremos que el producto de dos números constructibles es constructible. Para el inverso, si demostramos que todo conjugado de un número constructible es constructible, tendremos probado que los inversos de los números constructibles serán números constructibles, puesto que ya sabemos que el producto de números constructibles es constructible y:

$$z^{-1} = \frac{z\bar{z}}{|z|^2}$$

Por tanto, solo hemos de probar que  $C(S) \cap \mathbb{R}$  es un subcuerpo de  $\mathbb{R}$ . Sean por tanto  $r, r' \in C(S) \cap \mathbb{R}$ , veamos que entonces  $r' + r, r' - r \in C(S) \cap \mathbb{R}$ . Podemos suponer sin pérdida de generalidad que  $r, r' > 0$ , y lo que haremos será considerar los puntos  $r'$  y  $ir$  (que ya sabemos construir), considerar las rectas  $0r'$  y  $0(ir)$  y trazar en cada una de ellas las rectas perpendiculares que pasan por  $r'$  y por  $ir$ , respectivamente; como punto de intersección de dichas rectas obtendremos el punto  $z$ . Finalmente, debemos trazar la circunferencia de centro  $r'$  y radio hasta  $z$ , obteniendo como puntos de intersección con la recta  $0r'$  los puntos  $r' + r$  y  $r' - r$ .

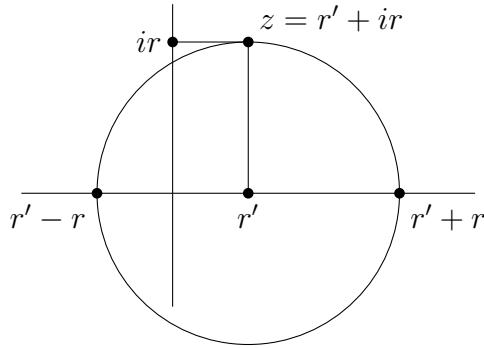
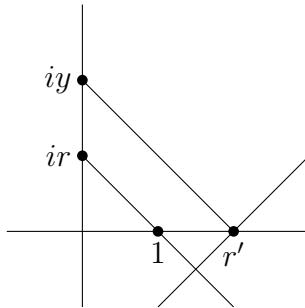


Figura 1.8: Obtención de  $r' + r$  y  $r' - r$  a partir de  $r$  y  $r'$ .

Por lo que  $r + r', r - r' \in C(S) \cap \mathbb{R}$ .

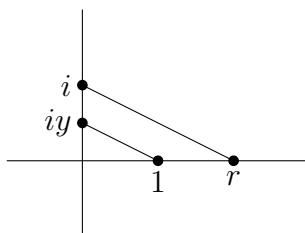
Bajo las mismas hipótesis, tratamos de probar que  $r \cdot r' \in C(S) \cap \mathbb{R}$ , supondremos de la misma forma que  $r, r' > 0$  y lo que faremos será considerar los puntos  $r'$ ,  $ir$ . Trazaremos la recta que une el punto  $1$  con  $ir$  y trazaremos la recta paralela a esta última que pasa por el punto  $r'$  (podemos hacerlo ya que podemos trazar la recta perpendicular a  $1(ir)$  que pasa por  $r'$  y a su vez la recta perpendicular a esta última que también pasa por  $r'$ ), obteniendo el punto  $iy$  de intersección con la recta  $0(ir)$ . De esta forma, hemos probado que el punto  $y$  es constructible.



Usando ahora que los triángulos dibujados son semejantes por tener ángulos iguales, tenemos entonces que:

$$\frac{r}{1} = \frac{y}{r'} \implies rr' = y \in C(S)$$

Finalmente, hemos de comprobar que si  $r \in C(S) \cap \mathbb{R}$ , entonces  $r^{-1} \in C(S) \cap \mathbb{R}$ . Al igual que antes, podemos suponer que  $r > 0$ , consideramos el punto  $r$  y las rectas  $0r$  y  $0i$ , y trazar las rectas  $ri$  y la paralela a esta última que pasa por el punto  $1$ , obteniendo el punto de intersección  $iy$  con la recta  $0i$ , con lo que el punto  $y$  es constructible.



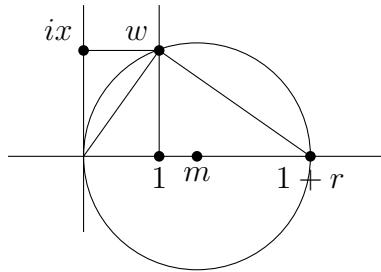
Ambos triángulos semejantes, luego:

$$\frac{1}{y} = \frac{r}{1} \implies yr = 1 \implies r^{-1} = y \in C(S) \cap \mathbb{R}$$

□

**Lema 1.14.** Si  $z \in C(S)$ , entonces  $\sqrt{z} \in C(S)$ .

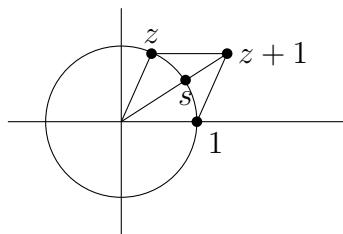
*Demostración.* Escribiendo  $z$  en forma polar, reducimos el problema al caso  $|z| = 1$ . Si tomamos  $r > 0$  con  $r \in C(S) \cap \mathbb{R}$ , veamos entonces que  $\sqrt{r} \in C(S) \cap \mathbb{R}$ . Para ello, consideramos el punto  $1 + r$  (anteriormente probamos que era constructible), trazamos el punto medio  $m$  entre  $0$  y  $1 + r$ , el punto  $1$  y la circunferencia de centro  $m$  y radio hasta  $r$ . Si trazamos la recta perpendicular a  $01$  que pasa por el punto  $1$  obtenemos  $w$ , como intersección de esta recta y de la circunferencia. Finalmente, tenemos que obtener  $ix$  como intersección de la recta  $0i$  y la perpendicular a  $0i$  que pasa por  $w$ , así como las rectas  $0w$  y  $w(1 + r)$ .



Resulta que los triángulos  $0, 1, w$  y  $w, 1, 1+r$  que hemos obtenido son semejantes, con lo que tenemos entonces que:

$$\frac{x}{1} = \frac{1+r-1}{x} \implies x^2 = r \implies \sqrt{r} = x \in C(S) \cap \mathbb{R}$$

Una vez hecha esta distinción, si tomamos un número complejo de módulo  $1$   $z = e^{i\theta}$ , tenemos que ver que si  $e^{i\theta} \in C(S) \cap \mathbb{R}$ , entonces  $e^{i\frac{\theta}{2}} \in C(S) \cap \mathbb{R}$ . Para ello, lo que faremos será considerar la circunferencia de centro  $0$  y radio hasta  $1$ , así como el cuarto punto que completa el paralelogramo de vértices  $z, 0, 1$ , que llamaremos  $z + 1$ . Finalmente, trazamos la recta que une  $0$  con  $1 + z$ , obteniendo un punto de intersección con la circunferencia, que es el punto  $e^{i\frac{\theta}{2}}$ .



□

**Ejercicio 1.3.3.** Sea  $F$  un subcuerpo de  $\mathbb{R}$ , diremos que  $(x, y) \in F \times F$  es un  $F$ -punto del plano. Una  $F$ -recta será la recta que une dos  $F$ -puntos del plano. Una  $F$ -circunferencia será la circunferencia determinada por dos  $F$ -puntos. Se pide demostrar:

- La intersección de dos  $F$ -rectas distintas es, si no vacía, un  $F$ -punto
- La intersección de una  $F$ -recta y una  $F$ -circunferencia o de dos  $F$ -circunferencias es, si no vacía,  $F(\sqrt{c})$ -puntos, para  $c > 0$ .

**Teorema 1.15.** *El menor subcuerpo de  $\mathbb{C}$  cerrado para conjugación y extracción de raíces cuadradas que contiene a  $S$  es  $C(S)$ .*

*Demostración.* Sea  $C'$  cualquier subcuerpo de  $\mathbb{C}$  cerrado para conjugación, raíces cuadradas y que contiene a  $S$ , queremos ver que  $C(S) \leq C'$ . Recordemos que teníamos que:

$$C(S) = \bigcup_{n \in \mathbb{N}} S_n$$

Por lo que basta demoststrar que  $S_n \subseteq C' \quad \forall n \in \mathbb{N}$ . Por inducción sobre  $n$ :

- **Para**  $n = 0$ . tenemos  $S_0 = S \subseteq C'$ .
- **Supuesto que**  $S_n \subseteq C'$ . tenemos que ver que  $S_{n+1} \subseteq C'$ . Dado un punto de  $S_{n+1}$ , este pertenece a  $X \cap Y$ , donde  $X, Y$  son elementos geométricos trazados a partir de  $S_n$ .

Por otra parte,  $X$  e  $Y$  son  $F$ -rectas o  $F$ -circunferencias, donde  $F = C' \cap \mathbb{R}$ . El Ejercicio 1.3.3 nos dice que las coordenadas del punto están en  $F(\sqrt{c})$ , con  $c > 0$  y como  $C'$  es estable para raíces cuadradas, tenemos entonces que las coordenadas del punto están en  $C'$ , de donde  $S_{n+1} \subseteq C'$ .

□

**Definición 1.16.** Sea  $F \leq K$  extensión, diremos que  $K$  es una torre por raíces cuadradas sobre  $F$  si  $K = F(u_1, \dots, u_t)$ , donde  $u_1^2 \in F$  y  $u_{i+1}^2 \in F(\overline{u_1, \dots, u_i})$  para  $i \in \{1, \dots, t-1\}$

**Notación.** Sea  $S \subseteq \mathbb{C}$ , denotamos:

$$\bar{S} = \{\bar{z} : z \in S\}$$

**Teorema 1.16.** *Sean  $S \subset \mathbb{C}$ ,  $F = \mathbb{Q}(S \cup \bar{S})$  y  $\mathcal{T}$  el conjunto de todas las torres por raíces cuadradas sobre  $F$  contenidas en  $\mathbb{C}$ , entonces:*

$$C(S) = \bigcup_{K \in \mathcal{T}} K$$

*Demostración.* Sea  $L = \bigcup_{K \in \mathcal{T}} K$ , tenemos que  $L$  es un subcuerpo de  $\mathbb{C}$ , ya que si  $0 \neq \alpha, \beta \in L$ , entonces existen  $K, E \in \mathcal{T}$  tales que  $\alpha \in K$  y  $\beta \in E$ . Como:

$$\begin{aligned} K &= F(u_1, \dots, u_t), \quad u_{i+1}^2 \in F(u_1, \dots, u_i), \quad i \in \{0, \dots, t-1\} \\ E &= F(v_1, \dots, v_s), \quad v_{i+1}^2 \in F(v_1, \dots, v_i), \quad i \in \{1, \dots, s-1\} \end{aligned}$$

Sea  $M$  el menor subcuerpo que contiene a  $K$  y  $E$ , es evidente que  $\alpha - \beta, \alpha\beta, \alpha^{-1} \in M$ . De donde:

$$M = F(u_1, \dots, u_t, v_1, \dots, v_s) \in \mathcal{T}$$

Una vez discutido que  $L$  es un subcuerpo, notemos que  $F \leq C(S)$  y que  $L \leq C(S)$  por la construcción de  $L$ . Finalmente, con vistas a aplicar el Teorema anterior, queremos ver que  $L$  contiene a  $S$  y que es cerrado para conjugación y para raíces cuadradas:

$S \subseteq L$ . Sea  $z \in L$ , queremos ver que  $\bar{z} \in L$ . Si  $z \in L$ , entonces  $z \in K = F(u_1, \dots, u_t)$ , de donde  $\bar{z} \in F(\bar{u}_1, \dots, \bar{u}_t)$ , ya que la conjugación es lineal, y tenemos que  $F(\bar{u}_1, \dots, \bar{u}_t) \in \mathcal{T}$ , de donde  $\bar{z} \in L$ .

Ahora, si tomamos un elemento de  $L$ , este estará en algún  $K, \dots$

□

**Corolario 1.16.1.**  $C(S)$  es una extensión algebraica de  $F = \mathbb{Q}(S \cup \bar{S})$ , de hecho, el grado de cada número en  $C(S)$  sobre  $F$  es una potencia de 2.

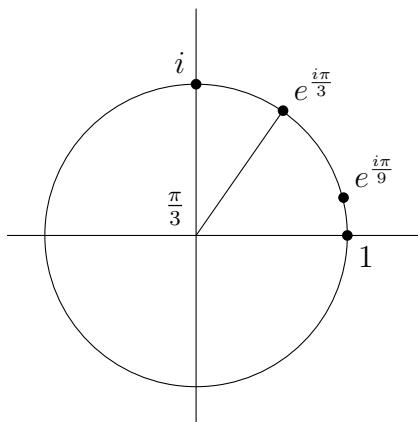
**Corolario 1.16.2.** Todo número constructible ( $F = \mathbb{Q}$ ) tiene grado sobre  $\mathbb{Q}$  una potencia de 2.

Y el recíproco de dicho corolario no es cierto, hay números complejos de grado 4 sobre  $\mathbb{Q}$  que no son constructibles. Tras ver la teoría de Galois se verá el contrarejemplo.

**Ejemplo.** Supongamos un cuadrado de lado  $l$  y una circunferencia de radio 1 centrada en 1. El círculo tiene área  $\pi$ . El área del cuadrado es  $l^2$ . Si  $l$  es constructible, entonces  $l^2$  es constructible. Si  $l^2 = \pi$ , entonces  $\pi$  sería constructible, luego sería algebraico, pero esto contradice el Teorema de Lindemann, que dice que  $\pi$  no es algebraico.

Dado un cubo de volumen 1, tampoco se puede construir un cubo de volumen mitad. Además, hay ciertos ángulos no se pueden trisecar, todo esto con regla y compás.

**Ejemplo.** El ángulo de  $60^\circ$  no se puede trisecar con regla y compás.



$$e^{i\pi/3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$$

es constructible. Nos preguntamos si  $e^{i\pi/9}$  también lo es. Si lo fuera, entonces sería algebraico, de donde su grado sería una potencia de 2. Vemos que:

$$e^{i\pi/9} = \cos \frac{\pi}{9} + i \sin \frac{\pi}{9}$$

de donde usando la fórmula del ángulo triple:

$$\cos(3\alpha) = 4\cos^3 \alpha - 3\cos \alpha \quad \forall \alpha \in \mathbb{R}$$

para  $\alpha = \pi/9$ , tenemos que:

$$\frac{1}{2} = 4\cos^3\left(\frac{\pi}{9}\right) - 3\cos\left(\frac{\pi}{9}\right)$$

Con lo que  $\cos(\pi/9)$  es raíz del polinomio

$$f = 8x^3 - 6x - 1 \in \mathbb{Q}[x]$$

como es de grado 3, que sea irreducible es equivalente a que no tenga ninguna raíz racional. Si  $r$  es una raíz de  $f$ , entonces  $2r$  es raíz de  $x^3 - 3x - 1$ . Si  $r \in \mathbb{Q}$ , entonces  $2r \in \mathbb{Q}$ , de donde<sup>6</sup>  $2r = \pm 1$ . Sin embargo, ni 1 ni -1 es raíz de  $x^3 - 3x - 1$ , con lo que  $f$  no tiene raíces reales, por lo que es irreducible sobre  $\mathbb{Q}$ , luego:

$$Irr\left(\cos\left(\frac{\pi}{9}\right), \mathbb{Q}\right) = \frac{f}{8}$$

De donde  $[\mathbb{Q}(\cos \frac{\pi}{9}) : \mathbb{Q}] = 3$  que no es potencia de 2, luego  $\cos(\pi/9)$  no es constructible, de donde  $e^{i\pi/9}$  tampoco lo es; es decir, el ángulo de  $60^\circ$  no se puede trisecar.

---

<sup>6</sup>Observando los coeficientes de  $x^3 - 3x - 1$  y la forma que tienen que tener las raíces racionales.

## 1.4. Homomorfismos de cuerpos

**Lema 1.17.** *Sea  $F$  un cuerpo y  $I$  un ideal suyo, entonces  $I = \{0\}$  o  $I = F$ .*

*Demostración.* Supuesto que  $I \neq \{0\}$ , existe por tanto  $a \in I \setminus \{0\}$ . Sea  $b \in F$ , tenemos que:

$$b = b \cdot a^{-1} \cdot a$$

Por lo que  $b \in I$ , de donde  $I = F$ .  $\square$

**Lema 1.18.** *Sea  $\sigma : F \rightarrow A$  un homomorfismo de anillos donde  $F$  es un cuerpo y  $A$  es no trivial, entonces  $\sigma$  es inyectivo y, por tanto,  $Im\sigma$  es un cuerpo isomorfo a  $F$  y subanillo de  $A$ .*

*Demostración.* Solo hemos de probar que  $\ker \sigma = \{0\}$ . Para ello,  $\ker \sigma$  es un ideal de  $F$  que no es  $F$  (ya que  $\sigma(1) = 1 \neq 0$ ), de donde  $\ker \sigma = \{0\}$ . Para ver que  $Im\sigma \cong F$ , basta aplicar el Primer Teorema de Isomorfía:

$$F = \frac{F}{\ker \sigma} \cong Im\sigma$$

Por ser  $\sigma$  un homomorfismo de anillos tenemos que  $Im\sigma$  es subanillo de  $A$ .  $\square$

**Definición 1.17** (Homomorfismo de cuerpos). *Sea  $F \xrightarrow{\sigma} K$  un homomorfismo de anillos entre cuerpos, diremos entonces que es un homomorfismo de cuerpos.*

*Observación.* Resulta sorprendente que exigir “buenas propiedades” a una aplicación entre anillos ya nos da una aplicación con “buenas propiedades” entre cuerpos, pero resulta que lo único que nos faltaba era que la aplicación se comporte bien con los inversos, propiedad que queda garantizada al exigir “buenas propiedades” sobre anillos:

$$1 = \sigma(1) = \sigma(\alpha\alpha^{-1}) = \sigma(\alpha)\sigma(\alpha^{-1}) \implies \sigma(\alpha^{-1}) = \sigma(\alpha)^{-1}$$

Como por el Lema anterior todo homomorfismo de cuerpos  $F \xrightarrow{\sigma} K$  es siempre inyectivo, tendremos siempre una copia de  $F$  dentro de  $K$ , que en ocasiones identificaremos con el propio  $F$ , viendo  $\sigma(F)$  como una copia isomorfa de  $F$ . Como  $\sigma(F) \leqslant K$  es una extensión de cuerpos, podemos ver  $K$  como un  $\sigma(F)$ -espacio vectorial. Además, si identificamos  $F$  con  $\sigma(F)$ , podremos ver  $K$  como un  $F$ -espacio vectorial.

**Definición 1.18.** Siempre que tengamos  $F \xrightarrow{\sigma} K$  y  $f \in F[x]$  dada por:

$$f = \sum_{i=0}^n f_i x^i, \quad f_i \in F \quad \forall i \in \{1, \dots, n\}$$

Definiremos:

$$f^\sigma = \sum_{i=0}^n \sigma(f_i) x^i \in K[x]$$

Se verifica que la correspondencia  $f \mapsto f^\sigma$  es un homomorfismo de anillos entre  $F[x]$  y  $K[x]$ , por la Propiedad Universal del anillo de polinomios.

**Ejemplo.** Sea  $f \in F[x]$ ,  $f$  no constante, sea  $p \in F[x]$  un factor irreducible de  $f$ , consideramos<sup>7</sup>:

$$K = \frac{F[x]}{\langle p \rangle}$$

como  $p$  es irreducible, tenemos que  $K$  es un cuerpo. Definimos  $\sigma : F \rightarrow K$  como:

$$\sigma(a) = a + \langle p \rangle \quad \forall a \in F$$

que es un homomorfismo de anillos como composición de la inclusión en  $F[x]$  con la proyección al cociente:

$$F \xhookrightarrow{\iota} F[x] \xrightarrow{\pi} \frac{F[x]}{\langle p \rangle}$$

Por lo que es un homomorfismo de cuerpos, con:

$$\sigma(F) = \{a + \langle p \rangle : a \in F\} \cong F$$

Sea  $\alpha = x + \langle p \rangle \in K$ , tenemos que:

$$p^\sigma(\alpha) = \sum_{i=0}^n (p_i + \langle p \rangle)(x + \langle p \rangle)^i = \sum_{i=0}^n p_i x^i + \langle p \rangle = p + \langle p \rangle = 0 + \langle p \rangle$$

Además:

$$\sigma(F)(\alpha) = K$$

$\subseteq$ ) Basta ver que  $K$  contiene a  $\sigma(F)$  y a  $\alpha$ .

$\supseteq$ ) Si tomamos un elemento de  $K$ , este será de la forma  $g + \langle p \rangle$  para cierta  $g \in F[x]$  dada por:

$$\sum_{i=0}^n g_i x^i, \quad g_i \in F, \quad \forall i \in \{1, \dots, n\}$$

Por lo que:

$$g + \langle p \rangle = \sum_{i=0}^n g_i x^i + \langle p \rangle = \sum_{i=0}^n (g_i + \langle p \rangle)(x + \langle p \rangle)^i \in \sigma(F)(\alpha)$$

El ejemplo anterior es de gran importancia, pues nos explica que dado cualquier cuerpo  $F$  y una ecuación polinómica que no sabemos resolver en  $F$  (o equivalentemente, un polinomio irreducible  $p$  de grado mayor<sup>8</sup> o igual que dos), podemos encontrar siempre un cuerpo más grande (que contiene una copia isomorfa de  $F$ ) en el que hayamos una solución de dicha ecuación (como el elemento  $x + \langle p \rangle$ ). Por ejemplo, si tomamos  $F = \mathbb{R}$  y  $p = x^2 + 1$ , obtenemos que  $K = \mathbb{C}$ .

---

<sup>7</sup>Donde  $\langle p \rangle$  es el ideal generado por  $p$ .

<sup>8</sup>Notemos que en un cuerpo siempre sabemos resolver una ecuación del tipo  $ax = b$ , las correspondientes a los polinomios de grado 1.

**Notación.** Siempre que estemos trabajando con un cuerpo  $F$  y digamos que “existe un homomorfismo  $F \xrightarrow{\sigma} K$ ”, lo que queremos decir en realidad es que existen otro cuerpo  $K$  y un homomorfismo de cuerpos entre ellos  $\sigma : F \rightarrow K$ , pero usaremos la primera expresión para abreviar.

**Lema 1.19.** *Si  $f \in F[x]$  es no constante y  $p$  es un factor irreducible de  $f$ , entonces existen  $F \xrightarrow{\sigma} K$  homomorfismo de cuerpos y  $\alpha \in K$  tales que:*

$$p^\sigma(\alpha) = 0 \quad y \quad K = \sigma(F)(\alpha)$$

Bajo estas condiciones, a menudo identificaremos  $F$  con  $\sigma(F)$  y en dicho caso, escribiremos  $K = F(\alpha)$ .

*Demostración.* La demostración se deduce del ejemplo anterior.  $\square$

**Proposición 1.20.** *Sea  $f \in F[x]$  con  $\deg f = n \geq 1$ , entonces existe un homomorfismo de cuerpos  $\sigma : F \rightarrow E$  tal que  $E$  es un cuerpo de descomposición de  $f^\sigma$ .*

*Demostración.* Suponemos sin pérdida de generalidad que  $f$  es mónico. Vamos a ver que existe  $F \xrightarrow{\sigma} L$  tal que  $f^\sigma$  se descompone completamente como producto de factores lineales en  $L[x]$ . Para ello, descomponemos  $f = gh$ , donde  $g \in F[x]$  es producto de polinomios lineales y  $h \in F[x]$  es un polinomio sin raíces en  $F$ . Por inducción sobre el grado de  $h$  (usando el segundo principio de inducción):

- Si  $\deg gh = 0$ , tomando  $L = F$  y  $\sigma = id_F$  se tiene.
- Supuesto que  $\deg gh > 0$  y la hipótesis de inducción, tomamos  $p$  un factor irreducible de  $h$ , por lo que podemos aplicar el Lema 1.19, con lo que existen  $F \xrightarrow{\tau} K$  y  $\alpha \in K$  tal que  $p^\tau(\alpha) = 0$  y  $K = \tau(F)(\alpha)$ . Observamos que  $h^\tau(\alpha) = 0$ .

El polinomio  $g$  que habíamos escogido será de la forma:

$$g = (x - \alpha_1) \cdot \dots \cdot (x - \alpha_t), \quad \alpha_1, \dots, \alpha_t \in F$$

Extraemos ahora los factores lineales de  $h^\tau$  en  $K[x]$  (sabemos que al menos  $s \geq 1$ , puesto que  $\alpha$  es raíz de  $h^\tau$ ):

$$h^\tau = (x - \beta_1) \cdot \dots \cdot (x - \beta_s)k, \quad k \in K[x], \beta_1, \dots, \beta_s \in K$$

Con uno de los  $\beta_i$  es  $\alpha$  y  $k$  sin raíces en  $K$  y de grado menor que el de  $h^\tau$ . En definitiva, tenemos que:

$$f^\tau = g^\tau h^\tau = (x - \tau(\alpha_1)) \cdot \dots \cdot (x - \tau(\alpha_s))(x - \beta_1) \cdot \dots \cdot (x - \beta_s)k, \quad \deg k < \deg h^\tau$$

Aplicando la hipótesis de inducción tomando  $k$  como  $h$ , existe un homomorfismo  $K \xrightarrow{\rho} L$  tal que  $k^\rho$  se descompone como producto de polinomios lineales en  $L[x]$ . En definitiva, tendremos que  $(f^\tau)^\rho$  se descompone como producto de polinomios lineales en  $L[x]$ . Si tomamos:

$$\sigma = \rho \tau : F \rightarrow L$$

tenemos que  $f^\sigma$  se descompone como producto de lineales en  $L[x]$ .

Una vez tenemos que existe  $\sigma : F \rightarrow L$  de forma que  $f^\sigma$  se descompone como producto de polinomios lineales en  $L[x]$ , si  $\gamma_1, \dots, \gamma_r \in L$  son las raíces de  $f^\sigma$ , podemos considerar  $E = \sigma(F)(\gamma_1, \dots, \gamma_r) \leqslant L$ , con lo que la restricción en codominio de  $\sigma$  a  $E$  nos da un homomorfismo, donde  $E$  es un cuerpo de descomposición de  $f^\sigma$ .  $\square$

**Definición 1.19.** Sea  $f \in F[x]$ , diremos que un homomorfismo de cuerpos  $\sigma : F \rightarrow E$  es un cuerpo de descomposición de  $f$  si  $E$  es un cuerpo de descomposición de  $f^\sigma$ , o equivalentemente, si:

- $f^\sigma$  se descompone en  $E[x]$  como producto de polinomios de grado 1, siendo  $\alpha_1, \dots, \alpha_t \in E$  todas sus raíces.
- $E = \sigma(F)(\alpha_1, \dots, \alpha_t)$ .

Respecto a esta última definición, debemos tener claro que antes llamábamos cuerpo de descomposición de  $f \in F[x]$  a una extensión  $F \leqslant K$  de forma que  $K$  cumplía ciertas propiedades relativas a  $f$ . Ahora, lo que hacemos es ver el homomorfismo  $F \xrightarrow{\sigma} K$  como una extensión de cuerpos, identificando  $F$  con  $\sigma(F)$ , por lo que al propio homomorfismo (que determina de qué forma  $K$  es extensión de  $F$ ) le llamamos ahora cuerpo de descomposición, si  $K$  cumple unas propiedades relativas a  $f^\sigma$ .

Sin embargo, no hemos cambiado el concepto, pues si tenemos  $F \leqslant K$  con  $K$  cuerpo de descomposición de  $f \in F[x]$  tenemos que  $\iota : F \hookrightarrow K$  es un cuerpo de descomposición de  $f$ . Hemos generalizado el concepto de cuerpo de descomposición.

A partir de la Proposición 1.20, para cualquier  $f \in F[x]$  tenemos garantizada siempre la existencia de un cuerpo de descomposición de  $f$ .

**Ejemplo.** Tomamos  $f = x^2 + x + 1 \in \mathbb{F}_2[x]$ , donde  $\mathbb{F}_2 = \{0, 1\}$  es el cuerpo que contiene dos elementos. Como  $f(0) = f(1) = 1 \neq 0$ , tenemos que  $f$  no tiene raíces en  $\mathbb{F}_2$ . Nuestro objetivo es buscar un cuerpo de descomposición suyo.

Observemos que como  $f$  es de grado 2 y no tiene raíces en  $\mathbb{F}_2$ ,  $f$  es irreducible, por lo que repitiendo el ejemplo anterior del que vienen el Lema y la Proposición, podemos tomar el cuerpo:

$$K = \frac{\mathbb{F}_2[x]}{\langle f \rangle}$$

y el homomorfismo de cuerpos:

$$\begin{aligned} \sigma : \quad \mathbb{F}_2 &\longrightarrow K \\ \sigma(y) &\longmapsto y + \langle f \rangle \end{aligned}$$

sabemos ya que:

$$f^\sigma(\alpha) = 0 \quad \text{con} \quad \alpha = x + \langle f \rangle$$

Si factorizamos  $f^\sigma$  (usando que  $\alpha^2 + \alpha + 1 = 0$ ):

$$f^\sigma = (x + \alpha)(x + \alpha^2)$$

tenemos que  $\sigma$  es un cuerpo de descomposición de  $F$ . Viendo que tenemos una copia isomorfa de  $\mathbb{F}_2$  dentro de  $K$ , identificamos  $\mathbb{F}_2$  con  $\sigma(\mathbb{F}_2)$ , y tenemos  $\mathbb{F}_2 \leqslant K$ , con lo que:

$$K = \mathbb{F}_2(\alpha), \quad \text{Irr}(\alpha, \mathbb{F}_2) = x^2 + x + 1$$

¿Cuántos elementos tiene  $K$ ?

En vista de que  $[K : \mathbb{F}_2] = 2$  y  $|\mathbb{F}_2| = 2$ , tenemos que  $|K| = 4$ . Para listarlos, sabemos ya que  $0, 1$  y  $\alpha$  son elementos distintos de  $K$ . Para buscar el cuarto elemento, como  $\deg \text{Irr}(\alpha, \mathbb{F}_2) = 2$ , sabemos que  $\{1, \alpha\}$  es una  $\mathbb{F}_2$ -base de  $K$ , por lo que  $1, \alpha$  son  $\mathbb{F}_2$ -linealmente independientes, lo que nos dice que  $1 + \alpha \in K$  es un elemento distinto de los tres que ya teníamos, puesto que:

- $1 + \alpha \neq 1$ , ya que  $\alpha \neq 0$ .
- $1 + \alpha \neq \alpha$ , ya que  $1 \neq 0$ .
- $1 + \alpha \neq 0$ , ya que si fuese  $1 + \alpha = 0$  tendríamos entonces que  $1$  y  $\alpha$  serían  $\mathbb{F}_2$ -linealmente dependientes.

A partir de la condición  $\alpha^2 + \alpha + 1 = 0$  vemos también que  $1 + \alpha = \alpha^2$ , por lo que podríamos haber descrito también  $K$  como:

$$K = \{0, 1, \alpha, \alpha^2\}$$

*Observación.* Si tenemos  $F \leq K$  una extensión de cuerpos con  $[K : F] = n$  y  $|F| = m$  tendremos entonces que  $|K| = m^n$ , ya que cada elemento de  $K$  queda únicamente determinado por la elección de  $n$  elementos de  $F$ , entre los cuales tenemos  $m$  para elegir.

**Ejemplo.** Al igual que en el ejemplo anterior, buscamos un cuerpo de descomposición de:

$$f = x^3 + x + 1 \in \mathbb{F}_2[x]$$

que sigue siendo irreducible sobre  $\mathbb{F}_2[x]$ , por ser de grado 3 y no tener raíces en  $\mathbb{F}_2[x]$ . De la misma forma, un cuerpo de descomposición de  $f$  es de la forma  $\mathbb{F}_2(a)$  con  $a$  en cierto cuerpo  $K$ , siendo  $a$  una raíz de  $f$ . Tratamos de factorizar  $f$  en  $\mathbb{F}_2(a)$ :

$$\begin{array}{r} x^3 + x + 1 \\ x^3 + ax^2 \\ \hline ax^2 + x + 1 \\ ax^2 + a^2x \\ \hline (a^2 + 1)x + 1 \\ (a^2 + 1)x + a^3 + a \\ \hline a^3 + a + 1 \end{array} \left| \begin{array}{c} x + a \\ x^2 + ax + (a^2 + 1) \end{array} \right.$$

Y tenemos que  $a^3 + a + 1 = 0$ . Buscamos ahora una raíz de  $x^2 + ax + (a^2 + 1)$ . Probamos con  $a^2$  (donde usamos que  $a^3 + a + 1 = 0$ ):

$$(a^2)^2 + aa^2 + (a^2 + 1) = a^4 + a^3 + a^2 + 1 = a^4 + a + a^2 = a(a^3 + a + 1) = 0$$

Dividimos ahora entre  $x + a^2$ :

$$\begin{array}{r} x^2 + ax + a^2 + 1 \\ x^2 + a^2x \\ \hline a^4x = a(a + 1)x + a^2 + 1 \\ a^4x + a^6 \\ \hline a^6 + a^2 + 1 \end{array} \left| \begin{array}{c} x + a^2 \\ x + a^4 \end{array} \right.$$

Y tenemos:

$$a^6 + a^2 + 1 = a^6 + a^2 + a^3 + a = a(a^5 + a + a^2 + 1) = a(a^5 + a^2 + a^3) = a^3(a^3 + 1 + a) = 0$$

En definitiva, la factorización de  $f$  en  $\mathbb{F}_2(a)$  es:

$$x^3 + x + 1 = (x + a)(x + a^2)(x + a^4)$$

con lo que  $\mathbb{F}_2(a)$  es un cuerpo de descomposición de  $f$ , con:

$$[\mathbb{F}_2(a) : \mathbb{F}_2] = \deg \text{Irr}(a, \mathbb{F}_2) = 3$$

por lo que ahora  $|\mathbb{F}_2(a)| = 2^3 = 8$ .

Podríamos haber estudiado también  $f = x^3 + x^2 + 1$ , obteniendo otro cuerpo de 8 elementos. Veremos luego que estos cuerpos obtenidos son isomorfos entre sí, e isomorfos con cualquier otro cuerpo que contenga 8 elementos, lo que nos permitirá notarlos a todos por  $\mathbb{F}_8$ .

**Lema 1.21.** *Sea  $F \xrightarrow{\sigma} K$  un homomorfismo,  $p \in F[x]$  irreducible y  $\alpha \in K$  una raíz de  $p^\sigma$ , entonces se tiene que:*

$$\begin{aligned} \sigma_\alpha : \quad & \frac{F[x]}{\langle p \rangle} &\longrightarrow & \sigma(F)(\alpha) \\ & g + \langle p \rangle &\longmapsto & g^\sigma(\alpha) \end{aligned}$$

es un isomorfismo de cuerpos.

*Demostración.* Podemos tomar:

$$\begin{aligned} \overline{\sigma_\alpha} : \quad & F[x] &\longrightarrow & \sigma(F)(\alpha) \\ & g &\longmapsto & g^\sigma(\alpha) \end{aligned}$$

En el Lema 1.19 vimos que  $g^\sigma(\alpha) \in \sigma(F)(\alpha)$  siempre que  $g \in F[x]$ , por lo que  $\overline{\sigma_\alpha}$  está bien definida ( $\text{Im } \overline{\sigma_\alpha} \subseteq \sigma(F)(\alpha)$ ), y además es un homomorfismo de cuerpos.

Como  $p^\sigma(\alpha) = 0$  tenemos que  $p \in \ker(\overline{\sigma_\alpha})$ , y como  $\overline{\sigma_\alpha}$  es un homomorfismo de cuerpos tenemos que  $\ker(\overline{\sigma_\alpha})$  es un ideal, que tiene que ser principal por ser  $F[x]$  un Dominio Euclídeo, luego existe  $f \in F[x]$  con  $\ker(\overline{\sigma_\alpha}) = \langle f \rangle$ , de donde ha de existir  $h \in F[x]$  con  $p = hf$ , pero como  $p$  es irreducible tiene que ser  $h \in \mathcal{U}(F[x])$ , de donde  $f = h^{-1}p$ , por lo que también  $\langle p \rangle = \langle f \rangle = \ker(\overline{\sigma_\alpha})$ .

Finalmente, observamos que  $\sigma(F) \subseteq \text{Im } \overline{\sigma_\alpha}$  así como que  $\alpha \in \text{Im } \overline{\sigma_\alpha}$  por ser  $x \in F[x]$ , de donde concluimos que  $\sigma(F)(\alpha) \subseteq \text{Im } \overline{\sigma_\alpha}$ . Si aplicamos ahora el Primer Teorema de Isomorfía para anillos, vemos que:

$$\frac{F[x]}{\langle p \rangle} = \frac{F[x]}{\ker(\overline{\sigma_\alpha})} \cong \text{Im } \overline{\sigma_\alpha} = \sigma(F)(\alpha)$$

□

**Definición 1.20.** Si tenemos dos homomorfismos de cuerpos:

$$\begin{array}{ccc} F & \xrightarrow{\tau} & E \\ & \searrow \sigma & \\ & & K \end{array}$$

Diremos que un homomorfismo de cuerpos  $\eta : K \rightarrow E$  es una  $\sigma$ -extensión de  $\tau$  si:

$$\eta\sigma = \tau$$

Y notaremos al conjunto de todas las  $\sigma$ -extensiones de  $\tau$  por:

$$Ex(\tau, \sigma) = \{\eta : K \rightarrow E \text{ con } \eta \text{ homomorfismo y } \eta\sigma = \tau\}$$

Notemos que todos estos hacen que el siguiente diagrama sea conmutativo:

$$\begin{array}{ccc} F & \xrightarrow{\tau} & E \\ & \searrow \sigma & \uparrow \eta \\ & & K \end{array}$$

Si  $F \leq K$  es una extensión de cuerpos y  $\sigma : F \hookrightarrow K$  es la aplicación inclusión, diremos simplemente que  $Ex(\tau, \sigma)$  es el conjunto de las extensiones de  $\tau$ .

**Proposición 1.22** (Extensión de homomorfismos). *Si tenemos dos homomorfismos de cuerpos:*

$$\begin{array}{ccc} F & \xrightarrow{\tau} & E \\ & \searrow \sigma & \\ & & K \end{array}$$

*Sean  $p \in F[x]$  irreducible y  $\alpha \in K$  con  $p^\sigma(\alpha) = 0$ . Si denotamos por  $\mathcal{R}$  al conjunto de todas las raíces de  $p^\tau$  en  $E$  y tenemos que  $K = \sigma(F)(\alpha)$ , tenemos entonces que la aplicación*

$$\begin{aligned} : Ex(\tau, \sigma) &\longrightarrow \mathcal{R} \\ \eta &\longmapsto \eta(\alpha) \end{aligned}$$

*es una biyección.*

*Demostración.* Veamos en primer lugar que dicha aplicación está bien definida. Para ello, sea  $\eta \in Ex(\tau, \sigma)$ :

$$p^\tau(\eta(\alpha)) = p^{\eta\sigma}(\eta(\alpha)) \stackrel{(*)}{=} \eta(p^\sigma(\alpha)) = \eta(0) = 0$$

donde en  $(*)$  hemos usado que si  $p$  es de la forma:

$$p = \sum_i p_i x^i, \quad p_i \in F$$

entonces:

$$p^{\eta\sigma}(\eta(\alpha)) = \sum_i \eta(\sigma(p_i))\eta(\alpha) = \sum_i \eta(\sigma(p_i)\alpha) = \eta\left(\sum_i \sigma(p_i)\alpha\right) = \eta(p^\sigma(\alpha))$$

Esto prueba que<sup>9</sup>  $\eta(\alpha) \in \mathcal{R}$ . Veamos ahora que la aplicación enunciada es sobreyectiva<sup>10</sup>. Para ello, sea  $\beta \in \mathcal{R}$ , buscamos una  $\sigma$ -extensión  $\eta$  de  $\tau$  de forma que  $\eta(\alpha) = \beta$ . Usando el Lema 1.21, obtenemos los isomorfismos:

$$\begin{aligned} \sigma_\alpha : \quad & \frac{F[x]}{\langle p \rangle} \longrightarrow \sigma(F)(\alpha) = K \\ & g + \langle p \rangle \longmapsto g^\sigma(\alpha) \\ \tau_\beta : \quad & \frac{F[x]}{\langle p \rangle} \longrightarrow \tau(F)(\beta) \leqslant E \\ & g + \langle p \rangle \longmapsto g^\tau(\beta) \end{aligned}$$

Si tomamos:

$$\eta = i \circ \tau_\beta \circ \sigma_\alpha^{-1}$$

donde  $i$  es la inclusión  $\tau(F)(\beta) \leqslant E$ , observamos que:

$$K \xrightarrow{\sigma_\alpha^{-1}} \frac{F[x]}{\langle p \rangle} \xrightarrow{\tau_\beta} \tau(F)(\beta) \xrightarrow{i} E$$

Comprobemos que  $\eta \in Ex(\tau, \sigma)$ , ya que si  $a \in F$ :

$$(\eta \circ \sigma)(a) = (i \circ \tau_\beta \circ \sigma_\alpha^{-1})(\sigma(a)) = (i \circ \tau_\beta)(\sigma_\alpha^{-1}(\sigma(a))) = (i \circ \tau_\beta)(a + \langle p \rangle) = i(\tau(a)) = \tau(a)$$

donde hemos aplicado que tanto  $\sigma_\alpha$  como  $\tau_\beta$  aplicado sobre constantes son iguales a  $\sigma$  y a  $\tau$ , respectivamente, lo que prueba que  $\eta \in Ex(\tau, \sigma)$ . Ahora:

$$\eta(\alpha) = (i \circ \tau_\beta)(\sigma_\alpha^{-1}(\alpha)) = (i \circ \tau_\beta)(x + \langle p \rangle) = i(\beta) = \beta$$

Falta probar que la aplicación es inyectiva. Para ello, sean  $\eta, \eta' \in Ex(\tau, \sigma)$  de forma que  $\eta(\alpha) = \eta'(\alpha)$ , entonces como  $\sigma(F) \leqslant K = \sigma(F)(\alpha)$  con  $\alpha$  algebraico sobre  $\sigma(F)$ , tenemos que  $\{1, \alpha, \alpha^2, \dots\}$  es un sistema de generadores de  $\sigma(F)(\alpha)$ , por lo que todo elemento de este cuerpo será de la forma:

$$\sum_i \sigma(a_i)\alpha^i \in \sigma(F)(\alpha), \quad a_i \in F$$

con lo que:

$$\eta\left(\sum_i \sigma(a_i)\alpha^i\right) = \sum_i \eta(\sigma(a_i))\eta(\alpha)^i \stackrel{(*)}{=} \sum_i \eta'(\sigma(a_i))\eta'(\alpha)^i = \eta'\left(\sum_i \sigma(a_i)\alpha^i\right)$$

donde en  $(*)$  usamos que  $\eta(\alpha) = \eta'(\alpha)$ , así como que  $\eta, \eta'$  son  $\sigma$ -extensiones de  $\tau$ , con lo que  $\eta \circ \sigma = \tau = \eta' \circ \sigma$ . En definitiva, tenemos que  $\eta = \eta'$ , al ser  $\eta(g) = \eta'(g)$  para todo  $g \in K$ , lo que nos dice que la aplicación es inyectiva.  $\square$

---

<sup>9</sup>Notemos que hemos probado además que  $Ex(\tau, \sigma) \neq \emptyset \implies \mathcal{R} \neq \emptyset$ .

<sup>10</sup>Con lo que tendremos  $\mathcal{R} \neq \emptyset \implies Ex(\tau, \sigma) \neq \emptyset$

Observemos que en esta última proposición hemos probado además que:

$$\mathcal{R} = \emptyset \iff Ex(\tau, \sigma) = \emptyset$$

**Lema 1.23.** *Sean tres homomorfismos entre cuerpos:*

$$\begin{array}{ccc} F & \xrightarrow{\tau} & L \\ \sigma_1 \downarrow & & \\ E_1 & \xrightarrow{\sigma_2} & E_2 \end{array}$$

Se verifica que:

$$Ex(\tau, \sigma_2 \sigma_1) = \biguplus_{\eta \in Ex(\tau, \sigma_1)} Ex(\eta, \sigma_2)$$

*Demostración.* Por doble inclusión:

$\subseteq$ ) Si tomamos  $\theta \in Ex(\tau, \sigma_2 \sigma_1)$ , tenemos entonces que:

$$\theta \sigma_2 \sigma_1 = \tau$$

Por lo que si tomamos  $\eta = \theta \sigma_2$ , tenemos que:

$$\begin{aligned} \eta \sigma_1 &= \theta \sigma_2 \sigma_1 = \tau \implies \eta \in Ex(\tau, \sigma_1) \\ \theta \sigma_2 &= \eta \implies \theta \in Ex(\eta, \sigma_2) \end{aligned}$$

$\supseteq$ ) Si  $\eta \in Ex(\tau, \sigma_1)$  y tomamos  $\theta \in Ex(\eta, \sigma_2)$ , tendremos entonces que:

$$\left. \begin{array}{l} \eta \sigma_1 = \tau \\ \theta \sigma_2 = \eta \end{array} \right\} \implies \theta \sigma_2 \sigma_1 = \tau \implies \theta \in Ex(\eta, \sigma_1 \sigma_2)$$

Hemos probado que

$$Ex(\tau, \sigma_2 \sigma_1) = \bigcup_{\eta \in Ex(\tau, \sigma_1)} Ex(\eta, \sigma_2)$$

Ahora, si  $\eta, \eta' \in Ex(\tau, \sigma_1)$  y tenemos que:

$$\theta \in Ex(\eta, \sigma_2) \cap Ex(\eta', \sigma_2) \implies \left\{ \begin{array}{l} \theta \sigma_2 = \eta \\ \theta \sigma_2 = \eta' \end{array} \right. \implies \eta = \eta'$$

por lo que la unión es disjunta.  $\square$

**Proposición 1.24.** *Sean dos homomorfismos de cuerpos:*

$$\begin{array}{ccc} F & \xrightarrow{\tau} & E \\ & \searrow \sigma & \\ & K & \end{array}$$

Si  $[K : \sigma(F)] < \infty$ , entonces  $|Ex(\tau, \sigma)| \leq [K : \sigma(F)]$ .

*Demostración.* Por inducción sobre  $n = [K : \sigma(F)]$  usando el segundo principio de inducción:

- Si  $n = 1$ , entonces  $\sigma(F) = K$ , por lo que  $\sigma$  es un isomorfismo, con lo que  $Ex(\tau, \sigma) = \{\tau\sigma^{-1}\}$ , ya que si  $\eta \in Ex(\tau, \sigma)$ , entonces:

$$\eta\sigma = \tau \implies \eta = \tau\sigma^{-1}$$

En definitiva,  $1 = |Ex(\tau, \sigma)| \leq [K : \sigma(F)] = 1$ .

- Supuesto que  $n > 1$  y la hipótesis de inducción, como  $[K : \sigma(F)] = n > 1$ , tenemos que existe  $\alpha \in K$  de forma que  $[\sigma(F)(\alpha) : \sigma(F)] > 1$ , con lo que el Lema de la Torre nos dice que  $[K : \sigma(F)(\alpha)] < n$ .

Sea ahora  $\iota : \sigma(F)(\alpha) \rightarrow K$  la inclusión en  $K$ , podemos tomar:

$$\sigma = \iota \circ \sigma'$$

con  $\sigma' : F \rightarrow \sigma(F)(\alpha)$  la restricción en codominio (o correstricción) de  $\sigma$ . Nos encontramos en la siguiente situación:

$$\begin{array}{ccc} F & \xrightarrow{\tau} & E \\ \sigma' \downarrow & \searrow \sigma & \\ \sigma(F)(\alpha) & \xrightarrow{\iota} & K \end{array}$$

Aplicando el Lema anterior, obtenemos:

$$Ex(\tau, \sigma) = \biguplus_{\eta \in Ex(\tau, \sigma')} Ex(\eta, \iota)$$

Con lo que:

$$|Ex(\tau, \sigma)| = \sum_{\eta \in Ex(\tau, \sigma')} |Ex(\eta, \iota)|$$

Sea  $\eta \in Ex(\tau, \sigma')$ , por hipótesis de inducción ( $[K : \sigma(F)(\alpha)] < n$ ) tenemos que:

$$|Ex(\eta, \iota)| \leq [K : \sigma(F)(\alpha)]$$

con lo que:

$$\begin{aligned} |Ex(\tau, \sigma)| &= \sum_{\eta \in Ex(\tau, \sigma')} |Ex(\eta, \iota)| \leq \sum_{\eta \in Ex(\tau, \sigma')} [K : \sigma(F)(\alpha)] \\ &= |Ex(\tau, \sigma')|[K : \sigma(F)(\alpha)] \end{aligned}$$

Sea  $p^\sigma = Irr(\alpha, \sigma(F))$ , la Proposición de extensión nos dice que si  $\mathcal{R}_\tau$  es el número de raíces de  $p^\tau$  en  $E$ , entonces:

$$|Ex(\tau, \sigma')| = |\mathcal{R}_\tau| \leq \deg p^\tau = [\sigma(F)(\alpha) : \sigma(F)]$$

Por lo que aplicando el Lema de la Torre:

$$|Ex(\tau, \sigma)| \leq [\sigma(F)(\alpha) : \sigma(F)][K : \sigma(F)(\alpha)] = [K : \sigma(F)]$$

□

**Ejercicio 1.4.1.** Si  $\Pi$  es el cuerpo primo de un cuerpo  $K$ , entonces el único homomorfismo de cuerpos  $\sigma : \Pi \rightarrow K$  es la inclusión.

Sea  $\sigma : \Pi \rightarrow K$  un homomorfismo de cuerpos, sea  $\iota : \Pi \rightarrow K$  el homomorfismo inclusión, vemos que:

- $\sigma(0) = 0 = \iota(0)$ .
- $\sigma(1) = 1 = \iota(1)$ .
- Si  $n \in \mathbb{N}$ , tenemos que:

$$\sigma \left( \sum_{k=1}^n 1 \right) = \sum_{k=1}^n \sigma(1) = \sum_{k=1}^n 1 = \sum_{k=1}^n \iota(1) = \iota \left( \sum_{k=1}^n 1 \right)$$

Distinguimos casos:

**Si**  $\text{car}(K) > 0$ . Tendremos entonces que existe un isomorfismo  $\Phi : \mathbb{Z}_p \rightarrow \Pi$  para  $p = \text{car}(K)$ . Si  $a \in \Pi$ , tenemos que existe  $b \in \mathbb{Z}_p$  de forma que:

$$a = \Phi(b) = \Phi \left( \sum_{k=1}^b 1 \right) = \sum_{k=1}^b \Phi(1) = \sum_{k=1}^b 1$$

por lo que  $\sigma(a) = \iota(a)$ , para todo  $a \in \Pi$ , luego  $\sigma = \iota$ .

**Si**  $\text{car}(K) = 0$ . Tendremos entonces que existe un isomorfismo  $\Phi : \mathbb{Q} \rightarrow \Pi$ . Si  $a \in \Pi$ , tenemos que existen  $z \in \mathbb{Z}, n \in \mathbb{N} \setminus \{0\}$  de forma que:

$$\begin{aligned} a &= \Phi \left( \frac{z}{n} \right) = \Phi(z)(\Phi(n))^{-1} = \Phi \left( sgn(z) \sum_{k=1}^{|z|} 1 \right) \left( \Phi \left( \sum_{k=1}^n 1 \right) \right)^{-1} \\ &= sgn(z) \left( \sum_{k=1}^{|z|} \Phi(1) \right) \left( \sum_{k=1}^n \Phi(1) \right)^{-1} = sgn(z) \left( \sum_{k=1}^{|z|} 1 \right) \left( \sum_{k=1}^n 1 \right)^{-1} \end{aligned}$$

por lo que  $\sigma(a) = \iota(a)$ , para todo  $a \in \Pi$ , de donde  $\sigma = \iota$ .

Mostramos a continuación un ejemplo básico de la proposición de extensión.

**Ejemplo.** ¿Cuántos homomorfismos de cuerpos hay de  $\mathbb{Q}(\sqrt[3]{2})$  en  $\mathbb{C}$ , y cuáles son?

Para responder a esta pregunta trataremos de reformularla en una que podamos responder usando la teoría de extensiones de homomorfismos. Sea  $\eta : \mathbb{Q}(\sqrt[3]{2}) \rightarrow \mathbb{C}$  un homomorfismo de cuerpos, si restringimos  $\eta$  al cuerpo primo de  $\mathbb{Q}(\sqrt[3]{2})$ , que es  $\mathbb{Q}$ , el Ejercicio 1.4.1 nos dice que entonces  $\eta|_{\mathbb{Q}}$  coincide con la aplicación inclusión  $\tau : \mathbb{Q} \hookrightarrow \mathbb{C}$ , es decir:

$$\iota \circ \eta = \tau$$

Si tomamos  $\sigma = \iota : \mathbb{Q} \rightarrow \mathbb{Q}(\sqrt[3]{2})$  la aplicación inclusión, estudiar cuántos homomorfismos de cuerpos hay de  $\mathbb{Q}(\sqrt[3]{2})$  en  $\mathbb{C}$  es equivalente a estudiar cuántas  $\sigma$ -extensiones de  $\tau$  hay.

$$\begin{array}{ccc} \mathbb{Q} & \xrightarrow{\tau} & \mathbb{C} \\ & \searrow \sigma & \uparrow \eta \\ & & \mathbb{Q}(\sqrt[3]{2}) \end{array}$$

Por lo que el problema se reduce a estudiar los elementos del conjunto  $Ex(\tau, \sigma)$ . Sabemos que:

$$\text{Irr}\left(\sqrt[3]{2}, \mathbb{Q}\right) = x^3 - 2$$

Cuyas raíces en  $\mathbb{C}$  son:

$$\mathcal{R} = \left\{ \sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2} \right\}$$

donde  $w$  es una raíz cónica primitiva de la unidad. La Proposición de extensión nos dice entonces que existen exactamente tres homomorfismos de  $\mathbb{Q}(\sqrt[3]{2})$  en  $\mathbb{C}$ . Les damos nombre a cada uno de ellos:

$$Ex(\tau, \sigma) = \{\eta_0, \eta_1, \eta_2\}$$

donde  $\eta_i$  está determinado (según la proposición de extensión) por:

$$\eta_j\left(\sqrt[3]{2}\right) = w^j\sqrt[3]{2}, \quad \forall j \in \{0, 1, 2\}$$

Como cada uno de los  $\eta_j$  es un homomorfismo definido sobre  $\mathbb{Q}(\sqrt[3]{2})$  con base  $\{1, \sqrt[3]{2}\}$ , es suficiente definirlos sobre 1 y sobre  $\sqrt[3]{2}$ , pero como  $\eta_j$  tiene que ser un homomorfismo de cuerpos, ha de cumplirse  $\eta_j(1) = 1$ , por lo que basta definirlo sobre  $\sqrt[3]{2}$ . Como ejemplo de esto último, observemos que podemos calcular:

$$\eta_2\left(\frac{\sqrt[3]{2} + (\sqrt[3]{2})^2}{27}\right) = \frac{\eta_2(\sqrt[3]{2}) + (\eta_2(\sqrt[3]{2}))^2}{\eta_2(27)} = \frac{w^2\sqrt[3]{2} + (w^2\sqrt[3]{2})^2}{27}$$

**Proposición 1.25.** *Sean dos homomorfismos de cuerpos:*

$$\begin{array}{ccc} F & \xrightarrow{\tau} & E \\ & \searrow \sigma & \\ & & K \end{array}$$

con  $\sigma$  un cuerpo de descomposición de  $f \in F[x]$ . Si  $f^\tau$  se descompone como producto de polinomios lineales en  $E[x]$ , entonces  $Ex(\tau, \sigma)$  es no vacío. Además, si  $f^\sigma$  tiene  $\deg f$  raíces distintas, entonces:

$$|Ex(\tau, \sigma)| = [K : \sigma(F)]$$

*Demostración.* La idea es similar a la de la Proposición 1.24, por inducción sobre  $n = [K : \sigma(F)]$ :

- Para  $n = 1$ , tenemos que  $K = \sigma(F)$ , con lo que  $\sigma$  es un isomorfismo y tendremos por tanto que  $Ex(\tau, \sigma) = \{\tau\sigma^{-1}\}$ .

- Supuesto que  $n > 1$  y la hipótesis de inducción, tenemos que  $f$  tiene un factor irreducible  $p \in F[x]$  de grado mayor o igual 1. Tomamos una raíz  $\alpha \in K$  de  $p^\sigma$ , de donde  $[K : \sigma(F)(\alpha)] < n$ . Si consideramos  $\sigma' : F \rightarrow \sigma(F)(\alpha)$  y la inclusión  $\iota : \sigma(F)(\alpha) \rightarrow K$ , tenemos que:

$$Ex(\tau, \sigma) = \biguplus_{\eta \in Ex(\tau, \sigma')} Ex(\eta, \iota)$$

con lo que:

$$|Ex(\tau, \sigma)| = \sum_{\eta \in Ex(\tau, \sigma')} |Ex(\eta, \iota)|$$

de la proposición de extensión deducimos que  $Ex(\tau, \sigma')$  tiene tantos elementos como raíces de  $p^\tau$  hay en  $E$ . Sin embargo, como  $f^\tau$  se factoriza como producto de polinomios de grado 1 en  $E[x]$  y  $p^\tau$  es un factor de  $f^\tau$ , en particular  $Ex(\tau, \sigma') \neq \emptyset$ , lo que nos permite tomar  $\eta \in Ex(\tau, \sigma')$ , y por hipótesis de inducción obtenemos que  $Ex(\eta, \iota)$  es no vacío, con lo que tampoco puede serlo  $Ex(\tau, \sigma)$ .

Además, si  $f^\sigma$  tiene  $\deg f$  raíces distintas, entonces  $p^\sigma$  tiene  $\deg p$  raíces distintas, de donde:

$$|Ex(\tau, \sigma')| = \mathcal{R}(p^\sigma) = \deg p^\sigma = [\sigma(F)(\alpha) : \sigma(F)]$$

Por hipótesis de inducción (como  $[K : \sigma(F)(\alpha)] < n$ ), para cada  $\eta \in Ex(\tau, \sigma')$  tenemos que  $|Ex(\eta, \iota)| = [K : \sigma(F)(\alpha)]$ , con lo que:

$$|Ex(\tau, \sigma)| = \sum_{\eta \in Ex(\tau, \sigma')} |Ex(\eta, \iota)| = [K : \sigma(F)(\alpha)][\sigma(F)(\alpha) : \sigma(F)] = [K : \sigma(F)]$$

□

**Ejemplo.** (Continuación del ejemplo anterior)

Sea  $K = \mathbb{Q}(\sqrt[3]{2}, w)$  con  $w$  una raíz cúbica primitiva de la unidad, si queremos calcular todos los homomorfismos de  $K$  en  $\mathbb{C}$ , lo que haremos será considerar las respectivas aplicaciones de inclusión  $\tau, \sigma_1$  y  $\sigma_2$ , con lo que tenemos:

$$\begin{array}{ccc} \mathbb{Q} & \xrightarrow{\tau} & \mathbb{C} \\ \sigma_1 \downarrow & \nearrow \eta_j & \uparrow \eta \\ \mathbb{Q}(\sqrt[3]{2}) & \xrightarrow{\sigma_2} & K \end{array}$$

Y queremos calcular  $Ex(\tau, \sigma_2 \sigma_1)$ . Para ello, trataremos de usar las aplicaciones  $\eta_j$  que ya conocemos, que cumplían:

$$\eta_j \left( \sqrt[3]{2} \right) = w^j \sqrt[3]{2} \quad \forall j \in \{0, 1, 2\}$$

Calcularemos para cada  $j$  todas las  $\sigma_2$ -extensiones de  $\eta_j$ , ya que:

$$Ex(\tau, \sigma_2 \sigma_1) = \biguplus_{\eta \in Ex(\tau, \sigma_1)} Ex(\eta, \sigma_2) = Ex(\eta_0, \sigma_2) \cup Ex(\eta_1, \sigma_2) \cup Ex(\eta_2, \sigma_2)$$

Para ello, necesitamos calcular el polinomio irreducible de  $w$  sobre  $\mathbb{Q}(\sqrt[3]{2})$  y calcular sus raíces en  $\mathbb{C}$ , cosa que ya hemos realizado en alguna ocasión:

$$\text{Irr}\left(w, \mathbb{Q}(\sqrt[3]{2})\right) = x^2 + x + 1 \quad \text{con raíces } w, w^2$$

Por tanto, tendremos 2 extensiones de  $\eta_j$  para cada  $j \in \{0, 1, 2\}$ :

$$\eta_{j,k}(w) = w^k \quad k \in \{1, 2\}$$

$$Ex(\tau, \sigma_2\sigma_1) = \{\eta_{j,k} : j \in \{0, 1, 2\}, k \in \{1, 2\}\}$$

determinadas por

$$\eta_{j,k}(\sqrt[3]{2}) = w^j \sqrt[3]{2}, \quad \eta_{j,k}(w) = w^k$$

Sabíamos que teníamos que obtener 6 extensiones, puesto que  $K$  es cuerpo de descomposición de  $x^3 - 2$ , con todas sus raíces distintas y que se descompone como producto de polinomios lineales en  $\mathbb{C}$ .

**Ejercicio 1.4.2.** Sean  $F \xrightarrow{\tau} E \xrightarrow{\rho} E$  homomorfismos de cuerpos. Sabemos que  $E$  es un  $\tau(F)$ -espacio vectorial, se verifica que:

$$\rho \text{ es } \tau(F)-\text{lineal} \iff \rho\tau = \tau$$

$\iff$ ) Sea  $y \in \tau(F)$  y  $z \in E$ , tenemos que existe  $x \in F$  de forma que  $\tau(x) = y$ , con lo que:

$$\rho(y \cdot z) = \rho(\tau(x) \cdot z) = \rho(\tau(x)) \cdot \rho(z) = \tau(x) \cdot \rho(z) = y \cdot \rho(z)$$

$\implies$ ) Supuesto que  $\rho$  es  $\tau(F)$ -lineal, tenemos que:

$$\rho(\tau(x)) = \rho(\tau(x) \cdot 1) = \tau(x) \cdot \rho(1) = \tau(x) \cdot 1 = \tau(x) \quad \forall x \in E$$

**Teorema 1.26** (Unicidad del cuerpo de descomposición).

Sean  $\tau : F \rightarrow E$  y  $\tau' : F \rightarrow E'$  dos cuerpos de descomposición de  $f \in F[x]$ . Entonces, existe un isomorfismo de cuerpos  $\eta : E \rightarrow E'$  tal que  $\eta\tau = \tau'$ .

*Demostración.* La Proposición 1.25 nos dice que como  $f^\tau$  y  $f^{\tau'}$  se descomponen como producto de polinomios lineales en  $E[x]$  y  $E'[x]$  de forma respectiva, entonces  $Ex(\tau, \tau')$  y  $Ex(\tau', \tau)$  son no vacíos, con lo que existen  $\eta : E \rightarrow E'$  y  $\eta' : E' \rightarrow E$  tales que

$$\eta'\tau' = \tau \quad \eta\tau = \tau'$$

si observamos que:

$$\eta\eta'\tau' = \tau'$$

el Ejercicio 1.4.2 nos dice que  $\eta\eta'$  es  $\tau'(F)$ -lineal. Ahora, como  $E'$  es de dimensión finita sobre  $\tau'(F)$  por ser  $E'$  cuerpo de descomposición de  $f^{\tau'}$ ; y como tenemos que  $\eta\eta' : E' \rightarrow E'$  es inyectiva, obtenemos automáticamente que  $\eta\eta'$  es biyectiva. De aquí deducimos que  $\eta$  es sobreyectiva, pero como era un homomorfismo de cuerpos, concluimos que  $\eta$  es biyectiva, con lo que  $\eta$  es un isomorfismo.  $\square$

**Ejercicio 1.4.3.** Sea  $\sigma : F \rightarrow E$  un homomorfismo de cuerpos tal que la extensión  $\sigma(F) \leqslant E$  es finita. Demostrar que existe un polinomio  $f \in F[x]$  y un homomorfismo de cuerpos  $\tau : E \rightarrow K$  tal que  $\tau\sigma : F \rightarrow K$  es cuerpo de descomposición de  $f$ .

Como la extensión  $\sigma(F) \leqslant E$  es finita, sabemos entonces que es algebraica y finitamente generada, con lo que existen  $\alpha_1, \dots, \alpha_n \in E$  algebraicos sobre  $\sigma(F)$  de forma que  $E = \sigma(F)(\alpha_1, \dots, \alpha_n)$ . Obtenemos para todo  $i \in \{1, \dots, n\}$ :

$$g_i = \text{Irr}(\alpha_i, \sigma(F))$$

con lo que  $g_i(\alpha_i) = 0 \quad \forall i \in \{1, \dots, n\}$ . Como  $\sigma : F \rightarrow \sigma(F)$  es un isomorfismo, para cada  $g_i$  existe un único polinomio  $f_i \in F[x]$  de forma que  $f_i^\sigma = g_i$ . Consideramos:

$$f = \prod_{i=1}^n f_i \implies f^\sigma = \prod_{i=1}^n f_i^\sigma = \prod_{i=1}^n g_i \in \sigma(F)[x]$$

Por la Proposición 1.20, sabemos que podemos encontrar  $\theta : \sigma(F) \rightarrow K$  cuerpo de descomposición de  $f^\sigma$ . Trataremos ahora de extender  $\theta$  a  $E$ . Para ello, si observamos que:

$$\begin{array}{ccc} \sigma(F) & \xrightarrow{\theta} & K \\ & \searrow \iota & \\ & & \sigma(F)(\alpha_1) \end{array}$$

y recordamos que  $g_1 \in \sigma(F)[x]$  es irreducible en  $\sigma(F)$ , la proposición de extensión nos dice que existe  $\eta_1 \in Ex(\theta, \iota)$  de forma que  $\eta_1(\alpha_1)$  es una raíz de  $g_1^\theta$  (y por tanto de  $(f^\sigma)^\theta$ ) en  $K$ . Supuesto ahora que:

$$\begin{array}{ccc} \sigma(F)(\alpha_1, \dots, \alpha_k) & \xrightarrow{\eta_k} & K \\ & \searrow \iota & \\ & & \sigma(F)(\alpha_1, \dots, \alpha_{k+1}) \end{array}$$

Si tomamos  $\text{Irr}(\alpha_{k+1}, \sigma(F)(\alpha_1, \dots, \alpha_k))$  (divisor de  $g_{k+1}$ ), la proposición de extensión nos garantiza la existencia de  $\eta_{k+1} \in Ex(\eta_k, \iota)$  de forma que  $\eta_{k+1}(\alpha_{k+1})$  es una raíz de  $g_{k+1}^{\eta_k}$ . Tomando ahora  $\tau = \eta_n$ , tenemos  $\tau : \sigma(F)(\alpha_1, \dots, \alpha_n) = E \rightarrow K$  de forma que  $(f^\sigma)^\tau$  se descompone como producto de polinomios lineales en  $K[x]$ , y si  $\mathcal{R}$  es el conjunto de raíces de  $(f^\sigma)^\tau$ ,  $K = \sigma(F)(\mathcal{R})$ , con lo que  $K$  es cuerpo de descomposición de  $(f^\sigma)^\tau$ .

## 1.5. Clasificación de los cuerpos finitos

**Proposición 1.27.** *Sea  $F$  un cuerpo finito de cardinal<sup>11</sup>  $q = p^n$  donde  $p = \text{car}(F)$ , entonces  $F$  es cuerpo de descomposición de  $x^q - x \in \mathbb{Z}_p[x]$ .*

---

<sup>11</sup>Sabemos que es así por el Ejercicio 1.

*Demostración.* Llamamos  $f = x^q - x$  y consideramos el grupo  $F^\times = F \setminus \{0\}$ , que tiene  $q - 1$  elementos. Por el Teorema de Lagrange para grupos tenemos que todo  $\alpha \in F^\times$  satisface que  $\alpha^{q-1} = 1$ , de donde  $\alpha^q = \alpha$ . Para 0 es trivial, con lo que:

$$\alpha^q = \alpha \quad \forall \alpha \in F$$

es decir, todo elemento de  $F$  es raíz de  $x^q - x$ . Como su polinomio derivado es  $qx^{q-1} - 1 \neq 0$ , tenemos entonces que  $x^q - x$  tiene exactamente  $q$  raíces distintas, que deben ser todos aquellos elementos de  $F$ . Como además  $\mathbb{Z}_p \leqslant F$  es el subcuerpo primo, tenemos que  $F$  es cuerpo de descomposición de  $f \in \mathbb{Z}_p[x]$ .  $\square$

**Ejercicio 1.5.1.** Sean  $a, b \in F$  con  $F$  un cuerpo de característica  $p > 0$ . Si  $q = p^n$ , comprobar que  $(a - b)^q = a^q - b^q$ .

Veamos en primer lugar que:

$$(a - b)^p = \sum_{k=0}^p \binom{p}{k} a^{p-k}(-b)^k = a^p - b^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} a^{p-k}(-b)^k \stackrel{(*)}{=} a^p - b^p$$

donde en  $(*)$  usamos que para  $1 < k < p - 1$  tenemos que  $\binom{p}{k}$  es múltiplo de  $p$ . Observemos ahora que:

$$(a - b)^{p^2} = ((a - b)^p)^p = (a^p - b^p)^p = a^{p^2} - b^{p^2}$$

Y por un procedimiento inductivo se termina probando que  $(a - b)^q = a^q - b^q$ .

**Teorema 1.28** (Clasificación de cuerpos finitos). *Para cada número primo  $p$  y para cada  $n \in \mathbb{N} \setminus \{0\}$  existe un único, salvo isomorfismos, cuerpo de cardinal  $p^n$ . Además, estos son los únicos cuerpos finitos.*

*Demostración.* Sea  $q = p^n$ , tomamos como  $F$  un cuerpo de descomposición del polinomio  $f = x^q - x \in \mathbb{Z}_p[x]$ . Sea  $S$  el conjunto de las raíces de  $f$  en  $F$ , veamos que  $S$  es un subcuerpo de  $F$ , puesto que:

- $1 \in S$ .
- Si  $a, b \in S$ :

$$\left. \begin{array}{l} a^q - a = 0 \\ b^q - b = 0 \end{array} \right\} \implies a^q b^q = ab \implies (ab)^q - ab = 0$$

con lo que  $ab \in S$ , y vemos ahora que:

$$(a - b)^q - (a - b) \stackrel{(*)}{=} a^q - b^q - (a - b) = a - b - (a - b) = 0$$

donde en  $(*)$  usamos el Ejercicio 1.5.1, con lo que también  $a - b \in S$ .

- Ahora, si  $a \in S \setminus \{0\}$ , tenemos que:

$$(a^{-1})^q = a^{-q} = (a^q)^{-1} = a^{-1} \implies (a^{-1})^q - a^{-1} = 0$$

por lo que  $a^{-1} \in S$ .

Como  $\mathbb{Z}_p \leqslant F$  es el cuerpo primo y  $S \leqslant F$ , ha de ser  $\mathbb{Z}_p \leqslant S$ . Finalmente, como  $F$  es un cuerpo de descomposición de  $f$ , ha de ser  $F = \mathbb{Z}_p(S) = S$ . Además, como el polinomio derivado no comparte raíces con  $f$ , tenemos que  $|F| = q$ .

Ahora, si tenemos dos cuerpos del mismo cardinal  $q$ , la Proposición 1.27 nos dice que ambos cuerpos son cuerpos de descomposición de  $x^q - x \in \mathbb{F}_p[x]$ , y aplicando el Teorema de unicidad del cuerpo de descomposición, tenemos que son isomorfos.

Sea ahora  $F$  cualquier cuerpo, tenemos por el Ejercicio 1 que este tiene cardinal  $p^n$ , por lo que tenemos el resultado por lo que acabamos de probar.  $\square$

**Notación.** Si  $F$  es un cuerpo de  $q = p^n$  elementos, lo notaremos por  $\mathbb{F}_q$ , y hablaremos “del” cuerpo de  $q$  elementos. Como todos los cuerpos de  $q$  elementos son isomorfos entre sí, usaremos  $\mathbb{F}_q$  como una etiqueta que hace referencia a cualquier cuerpo de  $q$  elementos.

**Ejemplo.** Sabemos ya que:

$$\frac{\mathbb{Z}[i]}{\langle 3 \rangle}, \quad \frac{\mathbb{F}_3[x]}{\langle x^2 + x + 2 \rangle}$$

son dos cuerpos de 9 elementos, con lo que el Teorema recién probado nos dice que ambos son isomorfos.

## 1.6. El grupo de automorfismos de una extensión

**Definición 1.21** (Grupo de automorfismos de un cuerpo). Sea  $K$  un cuerpo, consideramos el conjunto de todos los automorfismos de  $K$ :

$$\text{Aut}(K) = \{\sigma : K \rightarrow K \text{ homomorfismo de cuerpos biyectivo}\}$$

Se verifica que  $\text{Aut}(K)$  es un grupo con la operación composición de aplicaciones, que recibe el nombre de grupo de automorfismos de  $K$ .

Si  $F \leqslant K$  es una extensión de cuerpos, consideraremos también:

$$\text{Aut}_F(K) = \{\sigma \in \text{Aut}(K) : \sigma \text{ es } F\text{-lineal}\}$$

y se verifica que  $\text{Aut}_F(K)$  es un subgrupo de  $\text{Aut}(K)$ , que recibe el nombre de grupo de automorfismos de  $F \leqslant K$ .

**Ejercicio 1.6.1.** Si  $\Pi$  es el subcuerpo primo de  $K$ , entonces  $\text{Aut}_{\Pi}(K) = \text{Aut}(K)$ .

Basta probar la inclusión  $\supseteq$ ). Para ello, sea  $\sigma \in \text{Aut}(K)$ , si tomamos  $a \in \Pi$  y  $b \in K$ , tenemos que:

$$\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b) \stackrel{(*)}{=} \iota(a) \cdot \sigma(b) = a \cdot \sigma(b)$$

Donde en  $(*)$  hemos usado que  $\sigma|_{\Pi} = \iota$ , donde  $\iota : \Pi \rightarrow K$  es la aplicación inclusión, algo que probamos en el Ejercicio 1.4.1, con lo que  $\sigma \in \text{Aut}_{\Pi}(K)$ .

**Proposición 1.29.** Si  $F \leq K$  es finita, entonces  $|\text{Aut}_F(K)| \leq [K : F]$

*Demostración.* Si llamamos  $F \xrightarrow{\iota} K$  al homomorfismo inclusión, entonces:

$$\text{Aut}_F(K) = \text{Ex}(\iota, \iota)$$

$\subseteq$ ) Si  $\sigma \in \text{Aut}_F(K)$ , tenemos entonces que  $\sigma$  es  $F$ -lineal, y por el Ejercicio 1.4.2, tenemos entonces que  $\sigma \circ \iota = \iota$ , lo que nos dice que  $\sigma \in \text{Ex}(\iota, \iota)$ .

$\supseteq$ ) Si tomamos  $\sigma \in \text{Ex}(\iota, \iota)$  como es homomorfismo de cuerpos tenemos que es inyectivo, y la condición  $\sigma\iota = \iota$  nos dice por el Ejercicio 1.4.2 que  $\sigma$  es  $F$ -lineal. Como está definida entre dos espacios vectoriales de dimensión finita, ha de ser necesariamente sobreyectivo, con lo que  $\sigma \in \text{Aut}_F(K)$

Finalmente, la segunda proposición de extensión nos dice que:

$$|\text{Aut}_F(K)| = |\text{Ex}(\iota, \iota)| \leq [K : F]$$

□

**Notación.** En una situación como la de la Proposición anterior, es decir, siempre que tengamos  $F \leq K$  con  $\iota : F \rightarrow K$  el homomorfismo inclusión, llamaremos al conjunto  $\text{Ex}(\iota, \iota)$  extensiones de la inclusión.

**Proposición 1.30.** Si  $F \leq K$  es cuerpo de descomposición de  $f \in F[x]$ , entonces:

$$|\text{Aut}_F(K)| \leq [K : F]$$

y si todas las raíces de  $f$  en  $K$  son simples (es decir,  $f$  tiene  $\deg f$  raíces distintas), entonces:

$$|\text{Aut}_F(K)| = [K : F]$$

*Demostración.* Si  $F \leq K$  es un cuerpo de descomposición de  $f \in F[x]$ , tenemos entonces que si  $\alpha_1, \dots, \alpha_s$  son las raíces de  $f$  en  $K$  entonces  $K = F(\alpha_1, \dots, \alpha_s)$  es una extensión algebraica y finitamente generada, luego finita, de donde aplicando la Proposición anterior tenemos que  $|\text{Aut}_F(K)| \leq [K : F]$ .

Si ahora tenemos que todas las raíces de  $f$  en  $K$  son simples, aplicando la igualdad de la demostración anterior  $|\text{Aut}_F(K)| = |\text{Ex}(\iota, \iota)|$  para  $\iota : F \hookrightarrow K$  la aplicación inclusión, tenemos por la tercera Proposición de extensión que:

$$|\text{Aut}_F(K)| = |\text{Ex}(\iota, \iota)| = [K : F]$$

□

**Ejemplo.** Según un ejercicio ya visto, tenemos que:

$$\text{Aut}\left(\mathbb{Q}\left(\sqrt[3]{2}, w\right)\right) = \text{Aut}_{\mathbb{Q}}\left(\mathbb{Q}\left(\sqrt[3]{2}, w\right)\right)$$

con lo que la Proposición nos dice que:

$$\left|\text{Aut}_{\mathbb{Q}}\left(\mathbb{Q}\left(\sqrt[3]{2}, w\right)\right)\right| = 6$$

Por Álgebra II, tenemos que este grupo es isomorfo a  $C_6$  o a  $S_3$ , pero en ejemplos anteriores vimos que:

$$\text{Aut}\left(\mathbb{Q}\left(\sqrt[3]{2}, w\right)\right) = \{\eta_{j,k} : j \in \{0, 1, 2\}, k \in \{1, 2\}\}$$

donde:

$$\begin{cases} \eta_{j,k}(\sqrt[3]{2}) &= w^j \sqrt[3]{2} \\ \eta_{j,k}(w) &= w^k \end{cases}$$

resulta que tenemos un grupo no conmutativo:

$$\begin{aligned} \sqrt[3]{2} &\xrightarrow{\eta_{1,1}} w\sqrt[3]{2} \xrightarrow{\eta_{1,0}} w\sqrt[3]{2} \\ \sqrt[3]{2} &\xrightarrow{\eta_{1,0}} w\sqrt[3]{2} \xrightarrow{\eta_{1,1}} w^2\sqrt[3]{2} \end{aligned}$$

por lo que es isomorfo a  $S_3$ .

**Teorema 1.31.** *Sea  $\mathbb{F}_q$  un cuerpo finito con  $q = p^n$  elementos, entonces  $\text{Aut}(\mathbb{F}_q)$  es un grupo cíclico de orden  $n$ .*

*Demostración.* Sabemos por la Proposición 1.27 que  $\mathbb{F}_q$  es cuerpo de descomposición de  $x^q - x \in \mathbb{F}_q[x]$ , así como que las raíces de dicho polinomio son todas distintas (puesto que no comparte raíces con su polinomio derivado). Estamos en las condiciones de aplicar la Proposición 1.30, obteniendo que:

$$|\text{Aut}(\mathbb{F}_q)| = |\text{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)| = [\mathbb{F}_q : \mathbb{F}_p] = n$$

Sea  $\tau : \mathbb{F}_q \rightarrow \mathbb{F}_q$  la aplicación:

$$\tau(a) = a^p \quad \forall a \in \mathbb{F}_q$$

tenemos por el Ejercicio 1.5.1 que es un homomorfismo de cuerpos, luego un automorfismo (que recibe el nombre de automorfismo de Frobenius). Veamos que su orden es  $n$ . Para ello, sea  $m \in \mathbb{N} \setminus \{0\}$  de forma que:

$$\tau^m = id_{\mathbb{F}_q}$$

En el Ejercicio 1.7.10 vimos que  $\mathbb{F}_q^\times$  es cíclico y de orden  $q - 1$ . Tomamos  $a$  como su generador, que será de orden  $q - 1$ , lo que nos dice entonces que:

$$a = id_{\mathbb{F}_q}(a) = \tau^m(a) = a^{p^m}$$

Usando que el orden de  $a$  es  $p^n - 1$ , deducimos que  $p^m - 1 \geq p^n - 1$ , luego  $m \geq n$ , de donde el orden de  $\tau \in \text{Aut}(\mathbb{F}_q)$  es  $n$ , con lo que  $\text{Aut}(\mathbb{F}_q)$  ha de ser cíclico.  $\square$

## 1.7. Ejercicios

**Ejercicio 1.7.1.** Sea  $F \leq K$  una extensión de cuerpos de grado 2. Mostrar que, si la característica de  $F$  es distinta de dos, existe  $\beta \in K$  tal que  $\beta^2 \in F$  y  $K = F(\beta)$ .

Sea  $\alpha \in K \setminus F$ , tenemos que  $\alpha$  tiene grado 2 sobre  $K$ , puesto que si fuera de grado 1, entonces existe un polinómico mónico de grado 1  $x - a$  (con  $a \in F$ ) de forma que  $\alpha$  es raíz de dicho polinomio, con lo que ha de ser  $a = \alpha \notin F$ , contradicción. De esta forma,  $\deg \text{Irr}(\alpha, F) = 2$ , es decir, existen  $a, b \in F$  de forma que  $\alpha$  es raíz del polinomio:

$$x^2 + ax + b$$

Por lo que  $\alpha^2 + a \cdot \alpha + b = 0$ . Como la característica de  $F$  no es dos, tenemos que  $1 + 1 = 2 \neq 0$ , con lo que podemos considerar  $2^{-1}$ . Si tomamos:

$$\beta = \alpha + \frac{a}{2}$$

tenemos que:

$$\beta^2 = \left( \alpha + \frac{a}{2} \right)^2 = \alpha^2 + \alpha \cdot a + \frac{a^2}{4} = -b + \frac{a^2}{4} \in F$$

Y además  $\beta \notin F$ , pues  $\alpha = \beta - \frac{a}{2}$ . Como  $\beta \in K$ , es obvio que  $F(\beta) \leq K$ , y como  $[F(\beta) : F] = [K : F]$ , ha de ser  $K = F(\beta)$ .

**Ejercicio 1.7.2.** Calcular un cuerpo de descomposición de  $x^4 + 16 \in \mathbb{Q}[x]$ .

Tenemos que:

$$x^4 + 16 = 0 \iff x = \sqrt[4]{-16} = 2\sqrt[4]{-1}$$

Si recordamos que:

$$\sqrt[4]{-1} = \left\{ e^{\frac{i}{n}(\pi+2k\pi)} : k \in \{0, 1, 2, 3\} \right\} = \left\{ e^{\frac{i\pi}{4}}, e^{\frac{3i\pi}{4}}, e^{\frac{5i\pi}{4}}, e^{\frac{7i\pi}{4}} \right\}$$

con:

$$\begin{aligned} e^{\frac{i\pi}{4}} &= \cos\left(\frac{\pi}{4}\right) + i \sen\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2} \\ e^{\frac{3i\pi}{4}} &= \cos\left(\frac{3\pi}{4}\right) + i \sen\left(\frac{3\pi}{4}\right) = -\frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2} \\ e^{\frac{5i\pi}{4}} &= \cos\left(\frac{5\pi}{4}\right) + i \sen\left(\frac{5\pi}{4}\right) = -\frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2} \\ e^{\frac{7i\pi}{4}} &= \cos\left(\frac{7\pi}{4}\right) + i \sen\left(\frac{7\pi}{4}\right) = \frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2} \end{aligned}$$

Por lo que:

$$\sqrt[4]{-16} = \left\{ \sqrt{2} + i\sqrt{2}, -\sqrt{2} + i\sqrt{2}, -\sqrt{2} - i\sqrt{2}, \sqrt{2} - i\sqrt{2} \right\}$$

Con lo que  $\mathbb{Q}(\sqrt{2} + i\sqrt{2}, \sqrt{2} - i\sqrt{2})$  es un cuerpo de descomposición de  $x^4 + 16$ , que trataremos de probar que es igual a  $\mathbb{Q}(i, \sqrt{2})$ :

$\subseteq$ ) Es claro que  $\mathbb{Q}(\sqrt{2} + i\sqrt{2}, \sqrt{2} - i\sqrt{2}) \leq \mathbb{Q}(i, \sqrt{2})$ .

⊇) Vemos que:

$$\begin{aligned}\sqrt{2} &= \frac{\sqrt{2} + i\sqrt{2} + \sqrt{2} - i\sqrt{2}}{2} \in \mathbb{Q}(\sqrt{2} + i\sqrt{2}, \sqrt{2} - i\sqrt{2}) \\ i &= \frac{\sqrt{2} + i\sqrt{2} - \sqrt{2}}{\sqrt{2}} \in \mathbb{Q}(\sqrt{2} + i\sqrt{2}, \sqrt{2} - i\sqrt{2})\end{aligned}$$

En definitiva,  $\mathbb{Q}(i, \sqrt{2})$  es un cuerpo de descomposición de  $x^4 + 16$ .

**Ejercicio 1.7.3.** Razonar cuáles de los siguientes números complejos son algebraicos sobre  $\mathbb{Q}$ , suponiendo conocido que  $e$  y  $\pi$  son trascendentales:

$$\sqrt[5]{4}, (1 + \sqrt[5]{4})(1 - \sqrt[5]{16})^{-1}, \pi^2, e^2 - i, i\sqrt{i} + \sqrt{2}, \sqrt{1 - \sqrt[3]{2}}, \sqrt{\pi}, \sqrt{2}(\sqrt[3]{2} + \sqrt[5]{2})^{-1}.$$

Veamos cada caso:

- $\sqrt[5]{4}$  es algebraico sobre  $\mathbb{Q}$ , puesto que es raíz de  $x^5 - 4$ .
- $(1 + \sqrt[5]{4})(1 - \sqrt[5]{16})^{-1}$

En el apartado anterior hemos visto que  $[\mathbb{Q}(\sqrt[5]{4}) : \mathbb{Q}] \leq 5$ , con lo que la extensión  $\mathbb{Q} \leq \mathbb{Q}(\sqrt[5]{4})$  es finita, luego algebraica y finitamente generada, por lo que todo elemento de este último cuerpo será algebraico sobre  $\mathbb{Q}$ . Observemos que:

$$(1 + \sqrt[5]{4})(1 - \sqrt[5]{16})^{-1} = (1 + \sqrt[5]{4})(1 - \sqrt[5]{4}\sqrt[5]{4})^{-1} \in \mathbb{Q}(\sqrt[5]{4})$$

Por lo que es algebraico sobre  $\mathbb{Q}$ .

- $\pi^2$

Por reducción al absurdo, si fuera  $\pi^2$  algebraico sobre  $\mathbb{Q}$  tendríamos entonces que existe un polinomio:

$$f = \sum_{i=0}^n f_i x^i, \quad f_i \in \mathbb{Q} \quad \forall i \in \{0, \dots, n\}$$

de forma que  $f(\pi^2) = 0$ . En dicho caso, si tomamos:

$$h = \sum_{i=0}^n f_i x^{2i} \in \mathbb{Q}[x]$$

obtendríamos entonces que:

$$h(\pi) = \sum_{i=0}^n f_i \pi^{2i} = \sum_{i=0}^n f_i (\pi^2)^i = f(\pi^2) = 0$$

y esto es una contradicción con que  $\pi$  es trascendente.

■  $e^2 - i$ 

Por reducción al absurdo, si fuera  $e^2 - i \in \overline{\mathbb{Q}}$ , por ser  $i \in \overline{\mathbb{Q}}$  (es raíz de  $x^2 + 1$ ) tendríamos entonces que  $e^2 \in \overline{\mathbb{Q}}$ , de donde seríamos capaces de razonar que  $e \in \overline{\mathbb{Q}}$ , al igual que en el caso  $\pi^2$ , llegando a una contradicción, puesto que  $e$  es trascendente.

■  $i\sqrt{i} + \sqrt{2}$ 

Vemos que  $i\sqrt{i} + \sqrt{2} \in \mathbb{Q}(\sqrt{i}, \sqrt{2})$ , y aplicando el Lema de la Torre vemos que:

$$[\mathbb{Q}(\sqrt{i}, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{i}, \sqrt{2})] [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

con:

- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$  por ser  $x^2 - 2 = \text{Irr}(\sqrt{2}, \mathbb{Q})$ , irreducible por Eisenstein para  $p = 2$ .
- $[\mathbb{Q}(\sqrt{i}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] \leq 4$ , ya que  $x^4 + 1$  tiene a  $\sqrt{i}$  como raíz.

En definitiva, la extensión  $\mathbb{Q} \leq \mathbb{Q}(\sqrt{i}, \sqrt{2})$  es finita, luego algebraica, de donde el elemento  $i\sqrt{i} + \sqrt{2}$  es algebraico.

■  $\sqrt{1 - \sqrt[3]{2}}$ 

Buscamos un polinomio con coeficientes en  $\mathbb{Q}$  del que este elemento sea raíz. Para ello, lo que haremos será ver que este ha de cumplir que:

$$x^2 = 1 - \sqrt[3]{2} \implies x^2 - 1 = -\sqrt[3]{2}$$

De donde:

$$(x^2 - 1)^3 = x^6 - 3x^4 + 3x^2 - 1 = -2$$

Por lo que si tomamos  $f = x^6 - 3x^4 + 3x^2 + 1 \in \mathbb{Q}[x]$ , tenemos que  $\sqrt{1 - \sqrt[3]{2}}$  es raíz de  $f$ , con lo que es algebraico sobre  $\mathbb{Q}$ .

■  $\sqrt{\pi}$ ■  $\sqrt{2}(\sqrt[3]{2} + \sqrt[5]{2})^{-1}$ 

Por el Lema de la Torre, tenemos que:

$$\begin{aligned} & [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2}) : \mathbb{Q}] = \\ & [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2}) : \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})] [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})] [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \end{aligned}$$

Con:

- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ , ya que  $\text{Irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$  por Eisenstein para  $p = 2$ .
- $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})] \leq 3$  ya que  $x^3 - 2$  es un polinomio con  $\sqrt[3]{2}$  como raíz.
- $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2}) : \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})] \leq 5$ , ya que  $x^5 - 2$  es un polinomio con  $\sqrt[5]{2}$  como raíz.

En definitiva, la extensión  $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2})$  es finita, luego algebraica y finitamente generada. En particular, tenemos que:

$$\sqrt{2}\left(\sqrt[3]{2} + \sqrt[5]{2}\right)^{-1} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2})$$

Por lo que  $\sqrt{2}(\sqrt[3]{2} + \sqrt[5]{2})^{-1}$  es algebraico.

**Ejercicio 1.7.4.** Sea  $F \leqslant K$  una extensión de cuerpos,  $\alpha \in K$  y  $n$  natural no nulo. Demostrar que  $\alpha$  es algebraico sobre  $F$  si, y solo si,  $\alpha^n$  es algebraico sobre  $F$ .

$\Rightarrow$ ) Si  $\alpha$  es algebraico sobre  $F$  entonces la extensión  $F \leqslant F(\alpha)$  es algebraica, y tenemos que  $\alpha^n \in F(\alpha)$ , por lo que  $\alpha^n$  es algebraico sobre  $F$ .

$\Leftarrow$ ) Si  $\alpha^n$  es algebraico sobre  $F$ , entonces existe  $f \in F[x]$  de forma que  $f(\alpha^n) = 0$ . Si  $f$  se escribe como:

$$f = \sum_{i=1}^m f_i x^i \quad f_i \in F$$

tenemos entonces que:

$$f(\alpha^n) = \sum_{i=1}^m f_i (\alpha^n)^i = 0$$

Por tanto, si consideramos el polinomio:

$$g = \sum_{k=1}^m f_k x^{kn} \in F[x]$$

tendremos entonces:

$$g(\alpha) = \sum_{k=1}^m f_k \alpha^{kn} = \sum_{k=1}^m f_k (\alpha^n)^k = 0$$

Por lo que  $\alpha$  es algebraico sobre  $F$ .

**Ejercicio 1.7.5.** Sea  $F \leqslant K$  una extensión de cuerpos,  $\alpha \in K$  y  $\beta = 1 + \alpha^2 + \alpha^5$ . Demostrar que  $\alpha$  es algebraico sobre  $F$  si, y solo si,  $\beta$  es algebraico sobre  $F$ :

$\Rightarrow$ ) Si  $\alpha$  es algebraico sobre  $F$  entonces la extensión  $F \leqslant F(\alpha)$  es algebraica, y tenemos que:

$$\beta = 1 + \alpha^2 + \alpha^5 \in F(\alpha)$$

Por lo que  $\beta$  es algebraico sobre  $F$ .

$\Leftarrow$ ) Tenemos las extensiones  $F \leqslant F(\beta) \leqslant F(\alpha)$ . Como  $\beta$  es algebraico sobre  $F$  tenemos que la primera extensión es finita. Si observamos ahora que:

$$\beta = 1 + \alpha^2 + \alpha^5 \iff 1 - \beta + \alpha^2 + \alpha^5$$

Vemos que  $\alpha$  es algebraico sobre  $F(\beta)$ , pues es raíz del polinomio  $1 - \beta + x^2 + x^5 \in F(\beta)$ , por lo que la extensión  $F(\beta) \leqslant F(\alpha)$  es también finita. El Lema de la Torre nos dice entonces que  $F \leqslant F(\alpha)$  es finita, por lo que es algebraica, de donde  $\alpha$  es algebraico sobre  $F$ .

**Ejercicio 1.7.6.** Calcular  $\text{Irr}(\alpha, \mathbb{Q})$  para los siguientes valores de  $\alpha$ :

$$3 + \sqrt{2}, \sqrt{3} - \sqrt[4]{3}, \sqrt[3]{2} + \sqrt[3]{4}$$

a) Para  $\alpha = 3 + \sqrt{2}$ .

Es claro que  $\mathbb{Q}(\alpha) \leq \mathbb{Q}(\sqrt{2})$ , así como que:

$$\sqrt{2} = 3 + \sqrt{2} - 3 \in \mathbb{Q}(\alpha)$$

Por lo que  $\mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\alpha)$ . Como  $\text{Irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$  por Eisenstein para  $p = 2$ , tenemos que:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$

Por lo que basta encontrar un polinomio mónico de grado 2 del que  $\alpha$  sea raíz.

$$\alpha - 3 = \sqrt{2} \implies \alpha^2 - 6\alpha + 9 = (\alpha - 3)^2 = 2 \implies \alpha^2 - 6\alpha + 7 = 0$$

Por lo que  $\text{Irr}(\alpha, \mathbb{Q}) = x^2 - 6x + 7$ .

b) Para  $\alpha = \sqrt{3} - \sqrt[4]{3}$ .

Buscamos primero un polinomio del que  $\alpha$  sea raíz. Para ello:

$$\sqrt[4]{3} = \alpha - \sqrt{3} \implies \sqrt{3} = \alpha^2 + 3 - 2\alpha\sqrt{3} \iff \sqrt{3}(1 + 2\alpha) = \alpha^2 + 3$$

de donde elevando al cuadrado:

$$3(1 + 4\alpha^2 + 4\alpha) = \alpha^4 + 9 + 6\alpha^2$$

por lo que  $\alpha$  es raíz de:

$$f = x^4 - 6x^2 - 12x + 6$$

y vemos que  $f$  es irreducible por Eisenstein para  $p = 2$ , de donde tenemos que  $f = \text{Irr}(\alpha, \mathbb{Q})$ .

c) Para  $\alpha = \sqrt[3]{2} + \sqrt[3]{4}$ .

Si escribimos  $u = \sqrt[3]{2}$ , vemos que  $\alpha = u + u^2$ , de donde:

$$\alpha^3 = u^3 + 3u^2u^2 + 3uu^4 + u^6 = u^3(1 + 3u + 3u^2 + u^3) = 2(1 + 3\alpha + 2)$$

por lo que  $\alpha$  es raíz de:

$$f = x^3 - 6x - 6$$

que es irreducible por Eisenstein para  $p = 2$ , luego  $\text{Irr}(\alpha, \mathbb{Q}) = f$ .

**Ejercicio 1.7.7.** Calcular  $[E : \mathbb{Q}]$  y una base de  $E$  sobre  $\mathbb{Q}$  en los siguientes casos:

$$E = \mathbb{Q}(\sqrt{6}, i), \quad E = \mathbb{Q}(\sqrt[3]{5}, \sqrt{-2}), \quad E = \mathbb{Q}(\sqrt{18}, \sqrt[3]{4})$$

a) Para  $E = \mathbb{Q}(\sqrt{6}, i)$ .

Tenemos por el Lema de la Torre que:

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{6})] [\mathbb{Q}(\sqrt{6}) : \mathbb{Q}]$$

con:

- $[E : \mathbb{Q}(\sqrt{6})] = 2$ , ya que  $\text{Irr}(i, \mathbb{Q}(\sqrt{6})) = x^2 + 1$ , por ser de grado 2 y ser sus raíces complejas.
- $[\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = x^2 - 6$ , ya que es un polinomio de grado 2 y no tiene raíces en  $\mathbb{Q}$ , ya que sus posibles raíces son:

$$\text{Div}(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

y ninguna de ellas es raíz:

$$\begin{aligned} (-1)^2 - 6 &= 1^2 - 6 = -5 \neq 0 \\ (-2)^2 - 6 &= 2^2 - 6 = -2 \neq 0 \\ (-3)^2 - 6 &= 3^2 - 6 = 3 \neq 0 \\ (-6)^2 - 6 &= 6^2 - 6 = 30 \neq 0 \end{aligned}$$

b) Para  $E = \mathbb{Q}(\sqrt[3]{5}, \sqrt{-2})$ .

Tenemos por el Lema de la Torre que:

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{5})] [\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}]$$

con:

- $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$ , ya que  $\text{Irr}(\sqrt[3]{5}, \mathbb{Q}) = x^3 - 5$  por Eisenstein para  $p = 5$ .
- $[E : \mathbb{Q}(\sqrt[3]{5})] = 2$ , ya que  $\text{Irr}(\sqrt{-2}, \mathbb{Q}) = x^2 + 2$ , ya que es de grado 2 y no tiene raíces en  $\mathbb{Q}(\sqrt[3]{5}) \leq \mathbb{R}$ .

En definitiva,  $[E : \mathbb{Q}] = 6$ , y el Lema de la Torre nos dice que una base suya es:

$$\left\{ 1, \sqrt[3]{5}, w\sqrt[3]{5}, \sqrt{-2}, \sqrt{-2}\sqrt[3]{5}, w\sqrt{-2}\sqrt[3]{5} \right\}$$

con  $w$  una raíz cúbica primitiva de la unidad.

c) Para  $E = \mathbb{Q}(\sqrt{18}, \sqrt[3]{4})$ .

**Ejercicio 1.7.8.** Sea  $\alpha \in \mathbb{C}$  una raíz del polinomio  $x^3 + 3x + 1$ . Describir una base de  $\mathbb{Q}(\alpha)$  sobre  $\mathbb{Q}$  y calcular las coordenadas racionales con respecto de la misma de  $(1 + \alpha)(1 + \alpha + \alpha^2)^{-1}$ .

Como  $x^3 + 3x + 1$  es un polinomio de grado 3, este es irreducible en  $\mathbb{Q}[x]$  si y solo si no tiene raíces en  $\mathbb{Q}$ . Como las únicas candidatas a raíces de  $x^3 + 3x + 1$  en  $\mathbb{Q}$  son 1 y  $-1$  y ninguna de ellas es raíz, concluimos que el polinomio es irreducible en  $\mathbb{Q}[x]$ , por lo que  $\text{Irr}(\alpha, \mathbb{Q}) = x^3 + 3x + 1$ , de donde  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ . Sabemos también que

$\{1, \alpha, \alpha^2\}$  es una  $\mathbb{Q}$ -base de  $\mathbb{Q}(\alpha)$ .

Calculamos las coordenadas en  $\mathbb{Q}(\alpha)$  del número mencionado, conociendo que:

$$\alpha^3 + 3\alpha + 1 = 0$$

**Ejercicio 1.7.9.** Pongamos  $\mathbb{F}_4 = \mathbb{F}_2(a)$  con  $a^2 + a + 1 = 0$ . Comprobar que  $\mathbb{F}_{16}$  puede presentarse como  $\mathbb{F}_{16} = \mathbb{F}_2(b)$ , donde  $b^4 + b + 1 = 0$ . Determinar todos los homomorfismos de cuerpos  $\mathbb{F}_4 \rightarrow \mathbb{F}_{16}$  en función de  $a$  y  $b$ .

Tomamos  $x^4 + x + 1 \in \mathbb{F}_2[x]$ , y comprobamos que es irreducible para ello, comprobamos que no tiene raíces y que no puede escribirse como producto de dos polinomios irreducibles de grado 2. Como el único polinomio irreducible de grado 2 en  $\mathbb{F}_2[x]$  es  $x^2 + x + 1$ , basta ver que no es cuadrado del mismo. Como consecuencia:

$$\frac{\mathbb{F}_2[x]}{\langle x^4 + x + 1 \rangle}$$

es un cuerpo, que tiene dimensión 4 (el grado de  $x^4 + x + 1$ ) sobre  $\mathbb{F}_2$ , con lo que el cuerpo “es”  $\mathbb{F}_{16}$ . Tomamos  $b = x + \langle x^4 + x + 1 \rangle$  y se tiene.

Para ver ahora todos los homomorfismos de cuerpos, conocido:

$$p = \text{Irr}(a, \mathbb{F}_2) = x^2 + x + 1$$

$$\begin{array}{ccc} \mathbb{F}_2 & \xrightarrow{\iota} & \mathbb{F}_2(a) \\ & \searrow \iota & \downarrow \eta \\ & & \mathbb{F}_2(b) \end{array}$$

tenemos que hay tantos homomorfismos entre dichos cuerpos como raíces de  $p$ . La Propiedad de Extensión nos dice que los homomorfismos que me piden están parametrizados por las raíces de  $p$  en  $\mathbb{F}_2(b)$ .

Observemos que en este ejercicio (usando el ejercicio siguiente), cada  $\eta$  por restricción nos da un homomorfismo de grupos  $\eta : \mathbb{F}_2^\times(a) \rightarrow \mathbb{F}_2^\times(b)$  como los cardinales son 3 y 15 y 3 divide a 15, hay homomorfismos. Sabemos que  $\mathbb{F}_2(a) = \langle a \rangle$  por ser 3 primo. Ahora, no estamos seguros de si  $\mathbb{F}_2(b) = \langle b \rangle$ , para lo cual hemos de probar que  $O(b) = 15$ .

- $b^2 \neq 1$ , ya que  $b^2 + 1 = 0$ , ya que  $\{1, b, b^2, b^3\}$  es una  $\mathbb{F}_2$ -base de  $\mathbb{F}_{16}$ .
- $b^3 \neq 1$  por la misma razón.
- $b^4 = b + 1 \neq 1$ , ya que si no  $b = 0$ .
- $b^5 = b(b^4) = b(b + 1) = b^2 + b \neq 1$ , por la misma razón.

En definitiva,  $O(b) = 15$ , luego  $\mathbb{F}_{16}^\times = \langle b \rangle$ .

Buscando ahora homomorfismos de grupos, tenemos que llevar  $a$  en un elemento de orden 3. Ahora, los candidatos a elementos de orden 3 de  $\mathbb{F}_{16}^\times$  son los que generan un grupo de orden 5 y 10, es decir,  $b^5$  y  $b^{10}$ , y tenemos que comprobar que son raíces de  $x^2 + x + 1$ .

Finalmente, evalúo  $p$  en las candidatas para comprobar que sean raíces:

$$\begin{aligned} p(b^5) &= b^{10} + b^5 + 1 = (b^2 + b)^2 + b^2 + b + 1 = b^4 + b^2 + b^2 + b + 1 \\ &= b^4 + b + 1 = 0 \end{aligned}$$

Por el Automorfismo de Frobenius, la otra raíz es  $b^{10}$ . Sabemos que hay un  $\eta$  para cada raíz del polinomio, obteniendo  $\eta_i : \mathbb{F}_4 \rightarrow \mathbb{F}_{16}$ :

$$\eta_1(a) = b^5, \quad \eta_2(a) = b^{10}$$

**Ejercicio 1.7.10.** Demostrar que, si  $F$  es un cuerpo, entonces cualquier subgrupo finito de  $F^\times$  es cíclico. Deducimos que, en particular,  $\mathbb{F}_q^\times$  es un grupo cíclico de orden  $q - 1$ . (Pista: usar la descomposición cíclica de un grupo finito abeliano).

Sea  $G$  un subgrupo finito de  $F^\times$ , tomamos la descomposición cíclica de  $G$ :

$$G = C_1 \oplus \dots \oplus C_t$$

Con  $C_i$  cíclico para cada  $i \in \{1, \dots, t\}$ , con  $|C_{i+1}| \mid |C_i|$ . Sea  $m = |C_1|$ , para todo  $g \in G$  tenemos que  $g^m = 1$ . De esta forma, cada elemento de  $G$  es raíz de  $x^m - 1 \in F[x]$ , que a lo mucho tiene  $m$  raíces, con lo que  $|G| \leq m \leq |G|$ , de donde  $|G| = m$ , por lo que todos los grupos cíclicos en los que  $G$  se descompone son triviales salvo  $C_1$ , de donde  $G$  es cíclico.

*Observación.* Para  $\mathbb{F}_q$ ,  $\mathbb{F}_q^\times$  es un grupo cíclico de orden  $q - 1$ .

A cualquier generador  $a$  de  $\mathbb{F}_q^\times$  se le llama elemento primitivo de  $\mathbb{F}_q$ , por lo que:

$$\mathbb{F}_q = \{0, 1, a, \dots, a^{q-2}\}$$

Por lo que  $\mathbb{F}_q = \mathbb{F}_p(a)$ , con  $p = \text{car}(\mathbb{F}_q)$ .

**Ejercicio 1.7.11.** Demostrar que los anillos  $\frac{\mathbb{Z}[i]}{\langle 3 \rangle}$  y  $\frac{\mathbb{F}_3[x]}{\langle x^2 + x + 2 \rangle}$  son isomorfos sin necesidad de dar un isomorfismo concreto. ¿Serías capaz de darlo? ¿Y de calcularlos todos?

Tenemos que  $\frac{\mathbb{F}_3[x]}{\langle x^2 + x + 2 \rangle}$  es un cuerpo, porque  $\mathbb{F}_3[x]$  es un cuerpo y  $x^2 + x + 2$  es irreducible. Además, tiene dimensión 2 sobre un cuerpo de 3 elementos, por lo que tiene  $3^2 = 9$  elementos.

Por otra parte, 3 es irreducible en el DIP  $\mathbb{Z}[i]$ , ya que si  $3 = zw$ , entonces. Calculamos el módulo al cuadrado:

$$9 = |z|^2|w|^2$$

de donde haciendo cuentas deducimos que  $z$  o  $w$  son unidades, por lo que 3 es irreducible, de donde  $\frac{\mathbb{Z}[i]}{\langle 3 \rangle}$  es un cuerpo. Calculamos sus elementos, dividiendo cada clase de equivalencia entre 3, y obtenemos que su módulo al cuadrado es menor que 9, obteniendo 9 elementos que lo verifican, por lo que  $\frac{\mathbb{Z}[i]}{\langle 3 \rangle}$  es un cuerpo de 9 elementos.

Como son dos cuerpos del mismo cardinal, han de ser isomorfos.

**Ejercicio 1.7.12.** Se pide:

1. Comprobar que  $\sqrt{3} \in \mathbb{Q}(\sqrt{1+2\sqrt{3}})$ .

Llamamos  $\alpha = \sqrt{1+2\sqrt{3}}$  y calculamos:

$$\alpha^2 = 1 + 2\sqrt{3} \implies \sqrt{3} = \frac{\alpha^2 - 1}{2} \in \mathbb{Q}(\alpha)$$

De donde también deducimos que  $\mathbb{Q}(\sqrt{3}) \leq \mathbb{Q}(\alpha)$ .

2. Calcular  $\text{Irr}(\alpha, \mathbb{Q}(\sqrt{3}))$ .

Sabemos que  $\alpha$  es raíz de  $f = x^2 - 1 - 2\sqrt{3} \in \mathbb{Q}(\sqrt{3})[x]$ , con lo que:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] \leq 2$$

Supongamos que  $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] = 1$ , con lo que  $\alpha \in \mathbb{Q}(\sqrt{3})$ , de donde  $\alpha = a + b\sqrt{3}$  para ciertos  $a, b \in \mathbb{Q}$ . Si elevamos al cuadrado:

$$1 + 2\sqrt{3} = \alpha^2 = a^2 + 3b^2 + 2ab\sqrt{3}$$

Usando que  $\{1, \sqrt{3}\}$  es una base de  $\mathbb{Q}(\sqrt{3})$ , tenemos entonces que:

$$\begin{aligned} \left. \begin{array}{l} 1 = a^2 + 3b^2 \\ 2 = 2ab \end{array} \right\} &\implies \left. \begin{array}{l} b = \frac{1}{a} \\ 1 = a^2 + 3\frac{1}{a^2} \end{array} \right\} \implies a^2 = a^4 + 3 \\ &\implies a^2 = \frac{1 \pm \sqrt{1-12}}{2} \notin \mathbb{Q} \implies a \notin \mathbb{Q} \end{aligned}$$

Por lo que no es posible  $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] = 1$ , con lo que  $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{3})] = 2$ , de donde deducimos que:

$$\text{Irr}(\alpha, \mathbb{Q}(\sqrt{3})) = x^2 - 1 - 2\sqrt{3}$$

3. Calcular los homomorfismos de  $\mathbb{Q}(\alpha)$  en  $\mathbb{C}$ .

Queremos calcular los  $\eta$  que cumplen:

$$\begin{array}{ccc} \mathbb{Q} & \xrightarrow{\tau} & \mathbb{C} \\ & \searrow \iota & \uparrow \eta \\ & & \mathbb{Q}(\alpha) \end{array}$$

donde  $\tau, \iota$  son la inclusión, es decir, calcular  $\text{Ex}(\tau, \iota)$ .

No conocemos  $\text{Irr}(\alpha, \mathbb{Q})$ , pero hemos hecho el apartado 2, con lo que calculamos primero los homomorfismos de  $\mathbb{Q}(\sqrt{3})$  a  $\mathbb{C}$ , que son dos por la Proposición de extensión, determinados por:

$$\eta_j(\sqrt{3}) = (-1)^j \sqrt{3}, \quad \forall j \in \{0, 1\}$$

ya que  $\text{Irr}(\sqrt{3}, \mathbb{Q}) = x^2 - 3$ . Cada uno de ellos da lugar a 2 homomorfismos de  $\mathbb{Q}(\alpha)$  en  $\mathbb{C}$ . Las extensiones de  $\eta_0$ , digamos  $\eta_{0,k}$  con  $k \in \{0, 1\}$ , determinadas por:

$$\eta_{0,k}(\alpha) = (-1)^k \alpha \quad \forall k \in \{0, 1\}$$

Las extensiones de  $\eta_1$  vienen dadas por las raíces en  $\mathbb{C}$  de  $p^{\eta_1} = x^2 - 1 + 2\sqrt{3}$ , que son  $\pm\beta$ , con  $\beta = \sqrt{1 - 2\sqrt{3}}$ , con lo que tenemos  $\eta_{1,k}$  con  $k \in \{0, 1\}$  dadas por:

$$\eta_{1,k}(\beta) = (-1)^k \beta$$

4. Calcular  $\text{Irr}(\alpha, \mathbb{Q})$  y sus raíces en  $\mathbb{C}$ .

Sabemos ya que el grado es 4, el polinomio se obtiene elevando  $\alpha^2 = 1 + 2\sqrt{3}$  al cuadrado, y las raíces las sacamos por la biquadrática, que salen  $\alpha, -\alpha, \beta, -\beta$ .

**Ejercicio 1.7.13.** Sea  $\eta = e^{i\frac{2\pi}{5}} \in \mathbb{C}$ , ¿ $\text{Irr}(\eta + \bar{\eta}, \mathbb{Q})$ ? Llamando  $\alpha = \eta + \bar{\eta}$ , observamos que  $\alpha = \eta + \eta^4$ , y ahora:

$$\alpha^2 = \eta^2 + 2 + \eta^8 = \eta^2 + 2 + \eta^3$$

Y ahora como:

$$\eta^4 + \eta^3 + \eta^2 + \eta + 1 = 0$$

tenemos que:

$$\alpha^2 = \eta^2 + 2 + \eta^3 = 2 - 1 - \eta - \eta^4 = 1 - \alpha$$

Por lo que  $\alpha^2 + \alpha - 1 = 0$ , le calculamos las raíces:

$$\alpha = \frac{-1 \pm \sqrt{5}}{2} \notin \mathbb{Q}$$

Y como es de grado 2 ha de ser irreducible, con lo que:

$$\text{Irr}(\eta + \bar{\eta}, \mathbb{Q}) = x^2 + x + 1$$

Y el número  $\eta$  es constructible porque  $\eta + \bar{\eta}$  es 2 veces su parte real, y  $\sqrt{5}$  es constructible, luego su parte real es constructible. La parte imaginaria la obtenemos del Teorema de Pitágoras, como la raíz cuadrada de cierto número constructible.

Este ejercicio demuestra que el pentágono regular es constructible.

**Ejercicio 1.7.14.** Calcular  $\text{Irr}(\alpha, \mathbb{Q})$ , donde:

$$\alpha = \sqrt{\frac{3 + \sqrt{5}}{2}}$$

Buscamos el grado del polinomio:

$$\alpha^2 = \frac{3 + \sqrt{5}}{2}$$

Por lo que  $\mathbb{Q} \leqslant \mathbb{Q}(\alpha^2) \leqslant \mathbb{Q}(\alpha)$ , y sabemos que  $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{5})$ , con lo que tenemos  $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 2$ . Necesitamos ver si  $\alpha \in \mathbb{Q}(\sqrt{5})$ , ya que si despejamos  $\sqrt{5}$  de la igualdad anterior tenemos que  $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] \in \{1, 2\}$ .

Si  $\alpha \in \mathbb{Q}(\sqrt{5})$ , entonces (como  $\{1, \sqrt{5}\}$  es base) existen  $a, b \in \mathbb{Q}$  de forma que:

$$\alpha = a + b\sqrt{5}$$

de donde:

$$\frac{3 + \sqrt{5}}{2} = \alpha^2 = a^2 + 2ab\sqrt{5} + 5b^2$$

Como 1 y  $\sqrt{5}$  son linealmente independientes sobre  $\mathbb{Q}$ , han de ser iguales los coeficientes, con lo que:

$$\begin{cases} a^2 + 5b^2 = 3/2 \\ 2ab = 1/2 \end{cases}$$

Despejando:

$$a = \frac{1}{4b}$$

por lo que:

$$\frac{3}{2} = \frac{1}{16b^2} + 5b^2 \implies 3 = \frac{1}{8b^2} + 10b^2 \implies 24 = \frac{1}{b^2} + 80b^2 \implies 24b^2 = 1 + 80b^4$$

es decir:

$$80b^4 - 24b^2 + 1 = 0$$

Si  $b \in \mathbb{Q}$  entonces  $b^2 \in \mathbb{Q}$ , y tenemos que:

$$b^2 = \frac{24 \pm \sqrt{576 - 320}}{160} = \frac{24 \pm \sqrt{256}}{160} = \frac{24 \pm \sqrt{2^8}}{160} = \frac{24 \pm 16}{160} \in \mathbb{Q}$$

Y tenemos  $b^2 \in \{1/4, 1/20\}$ . Por lo que  $b$  puede ser  $\frac{1}{2} \in \mathbb{Q}$ , parece que no hay contradicción. ¿Es cierto que si  $b = 1/2$  entonces  $a = 1/2$ , se cumple?:

$$\sqrt{\frac{3 + \sqrt{5}}{2}} = \frac{1}{2} + \frac{\sqrt{5}}{2}$$

efectivamente:

$$\left(\frac{1 + \sqrt{5}}{2}\right)^2 = \frac{3 + \sqrt{5}}{2}$$

Con lo que efectivamente,  $\alpha \in \mathbb{Q}(\sqrt{5})$ , es decir:

$$\alpha = \sqrt{\frac{3 + \sqrt{5}}{2}} = \frac{1 + \sqrt{5}}{2}$$

Por lo que:

$$2\alpha = 1 + \sqrt{5} \implies 4\alpha^2 - 4\alpha + 1 = 5$$

de donde:

$$\alpha^2 - \alpha - 1 = 0$$

Por lo que  $\text{Irr}(\alpha, \mathbb{Q}) = x^2 - x - 1$ .

## 2. Extensiones de Galois

### 2.1. Extensiones de Galois

Del Capítulo anterior recordamos la Proposición 1.29, que nos servirá para comenzar este Capítulo:

Sea  $F \leq K$  una extensión finita, entonces  $|\text{Aut}_F(K)| \leq [K : F]$ .

Esto nos permite obtener grupos finitos de automorfismos a partir de extensiones finitas, y lo que haremos ahora será describir un procedimiento en sentido contrario.

**Ejemplo.** Si consideramos  $\text{Aut}(\mathbb{Q}(\sqrt[3]{2}))$ , sabemos que:

$$|\text{Aut}(\mathbb{Q}(\sqrt[3]{2}))| \leq 3$$

Y afirmamos que solo hay uno, ya que si observamos el diagrama:

$$\begin{array}{ccc} \mathbb{Q} & \xrightarrow{\iota} & \mathbb{Q}(\sqrt[3]{2}) \\ & \searrow & \uparrow \eta \\ & & \mathbb{Q}(\sqrt[3]{2}) \end{array}$$

tenemos que raíces de  $x^3 - 2$  en  $\mathbb{Q}(\sqrt[3]{2})$  solo hay 1. Sin embargo, anteriormente vimos que:

$$|\text{Aut}(\mathbb{Q}(\sqrt[3]{2}, w))| = 6$$

Por lo que la idea intuitiva es que faltan raíces en el cuerpo para poder tener todos los automorfismos.

**Notación.** Para no confundir la notación de “subgrupo” con la de “subcuerpo”, siempre que tengamos  $H$  un subgrupo de  $G$  lo notaremos por  $H < G$ .

**Definición 2.1.** Sea  $K$  un cuerpo y  $G < \text{Aut}(K)$  subgrupo, definimos el subcuerpo fijo de  $K$  bajo (la acción de)  $G$  como el conjunto:

$$K^G = \{a \in K : \sigma(a) = a \quad \forall \sigma \in G\}$$

*Observación.* Sea  $K$  un cuerpo y  $G < \text{Aut}(K)$ , tenemos que:

$$K^G \leq K$$

*Demostración.* Para probar que  $K^G$  es un subcuerpo de  $K$ :

- Es claro que  $1 \in K^G$ , ya que de hecho  $\sigma(1) = 1 \quad \forall \sigma \in \text{Aut}(K)$ .
- Si  $a, b \in K^G$ , tenemos entonces que  $\sigma(a) = a, \sigma(b) = b \quad \forall \sigma \in G$ , de donde:

$$\left. \begin{array}{l} \sigma(a - b) = \sigma(a) - \sigma(b) = a - b \\ \sigma(ab) = \sigma(a)\sigma(b) = ab \end{array} \right\} \implies a - b, ab \in K^G$$

- Finalmente, si  $a \in K^G$  tenemos entonces que:

$$\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1} \implies a^{-1} \in K^G$$

□

**Proposición 2.1** (Artin). *Si  $G$  es un subgrupo finito de  $\text{Aut}(K)$ , entonces*

$$[K : K^G] \leq |G|$$

*Demostración.* Sea  $n = |G|$ , será  $G = \{\sigma_1, \dots, \sigma_n\}$  y tomamos  $m$  (con  $m > n$ ) elementos de  $K$ ,  $\alpha_1, \dots, \alpha_m \in K$ , basta probar que estos son  $K^G$ -linealmente dependientes, para tener  $[K : K^G] \leq n$ . Para verlo, formamos la matriz:

$$A = (\sigma_j(\alpha_i))_{i,j} = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_m) & \sigma_2(\alpha_m) & \cdots & \sigma_n(\alpha_m) \end{pmatrix} \in M_{m \times n}(K)$$

cuyo rango es menor o igual que  $n$ , luego menor o igual que  $m$ , es decir, existe un vector

$$0 \neq v = (v_1, \dots, v_m) \in K^m$$

tal que  $vA = 0$ . Ahora, de entre todos los vectores que cumplen dichas condiciones, tomamos como  $v$  aquel con mínimo número de componentes no nulas y tal que alguna componente, digamos la  $l$ -ésima (con  $1 \leq l \leq m$ ), verifique que  $v_l \in K^G$ . Notemos que esto podemos conseguirlo siempre con  $v_l = 1$ , ya que como  $v \neq 0$  ha de existir  $1 \leq l \leq m$  con  $v_l \neq 0$ , y podemos dividir todas las componentes del vector  $v$  entre la  $l$ -ésima. Si escribimos la igualdad  $vA = 0$ , obtenemos las igualdades:

$$\sum_{i=1}^m v_i \sigma_j(\alpha_i) = 0 \quad \forall j \in \{1, \dots, n\}$$

Y observamos que para obtener la dependencia lineal de los  $\alpha_i$  falta ver que realmente los coeficientes  $v_i$  están en  $K^G$  (por ahora solo sabemos que están en  $K$ ). Para ello, supuesto que  $v_l \notin K^G$ , tendremos que  $v_l \neq \sigma_k(v_l)$  para cierto índice  $k \in \{1, \dots, n\}$ . Tomamos ahora cualquier  $\sigma \in G$  y definimos:

$$\sigma(v) = (\sigma(v_1), \dots, \sigma(v_n))$$

Si usamos esto para  $\sigma_k$ :

$$\sigma_k(v) = (\sigma_k(v_1), \dots, \sigma_k(v_m))$$

Podemos aplicar  $\sigma_k$  a las igualdades anteriores, con lo que:

$$\sum_{i=1}^m \sigma_k(v_i)\sigma_k(\sigma_j(\alpha_i)) = 0 \quad \forall j \in \{1, \dots, n\}$$

Observemos que:

$$G = \{\sigma_1, \dots, \sigma_n\} = \{\sigma_k\sigma_1, \dots, \sigma_k\sigma_n\}$$

$\supseteq$ ) Como  $G$  es un grupo tenemos que es cerrado para su operación.

$\subseteq$ ) Tenemos a la derecha  $n$  elementos distintos de  $G$ , y sabemos que son distintos porque si fuera  $\sigma_k\sigma_i = \sigma_k\sigma_j$  para ciertos  $i, j \in \{1, \dots, n\}$  con  $i \neq j$  tendríamos entonces que  $\sigma_i = \sigma_j$ , pero  $G$  tenía  $n$  elementos distintos.

Por lo que tenemos en realidad es:

$$\sum_{i=1}^m \sigma_k(v_i)\sigma_j(\alpha_i) = 0 \quad \forall j \in \{1, \dots, n\}$$

o equivalentemente:

$$\sigma_k(v)A = 0$$

Como  $vA = 0$  y  $\sigma_k(v)A = 0$ , tenemos que:

$$(v - \sigma_k(v))A = 0, \quad v - \sigma_k(v) \neq 0$$

ya que  $v_{l'} \neq \sigma_k(v_{l'})$ . Sin embargo, las componentes  $l$ -ésimas de los vectores eran iguales ( $v_l = \sigma_k(v_l)$ ), por lo que hemos obtenido un vector  $v - \sigma_k(v)$  que verifica que al multiplicarse por  $A$  se obtiene cero y con al menos una componente no nula menos que  $v$ , contradicción, que viene de suponer que  $v_{l'} \notin K^G$ , lo que nos dice que los coeficientes  $v_i$  estaban en  $K^G$ . Si en la igualdad:

$$\sum_{i=1}^m v_i \sigma_j(\alpha_i) = 0 \quad \forall j \in \{1, \dots, n\}$$

tomamos aquel índice  $j$  que verifica que  $\sigma_j = Id_K$ , tendremos entonces que:

$$\sum_{i=1}^m v_i \alpha_i = 0, \quad v_i \in K^G$$

lo que implica que  $\alpha_1, \dots, \alpha_m$  eran  $K^G$ -linealmente dependientes, por lo que:

$$[K : K^G] \leq n = |G|$$

□

**Lema 2.2.** *Para un cuerpo  $K$ , tenemos que:*

1. *Si  $H < G$  son subgrupos de  $\text{Aut}(K)$ , entonces  $K^H \geq K^G$ .*
2. *Si  $F \leq E$  son subcuerpos de  $K$ , entonces  $\text{Aut}_F(K) > \text{Aut}_E(K)$ .*

3. Si  $G < \text{Aut}(K)$ , entonces  $G < \text{Aut}_{K^G}(K)$ .

4. Si  $F \leqslant K$ , entonces  $F \leqslant F^{\text{Aut}_F(K)}$ .

*Demostración.* Demostramos cada uno de los apartados de forma muy sencilla:

1. Sea  $a \in K^G$ , tenemos que  $\sigma(a) = a \quad \forall \sigma \in G$ , en particular para los automorfismos de  $H$ , por lo que  $a \in K^H$ .
2. Sea  $\sigma \in \text{Aut}_E(K)$ , tenemos entonces que  $\sigma$  es  $E$ -lineal, pero como  $F \leqslant E$ , será  $\sigma \in \text{Aut}_F(K)$ .
3. Sea  $\sigma \in G < \text{Aut}(K)$ , si tomamos  $x \in K$  y  $y \in K^G$ , observamos que:

$$\sigma(y \cdot x) = \sigma(y) \cdot \sigma(x) = y \cdot \sigma(x)$$

Por lo que  $\sigma \in \text{Aut}_{K^G}(K)$ .

4. Sea  $x \in F$  y  $\sigma \in \text{Aut}_F(K)$ , entonces:

$$\sigma(x) = \sigma(x \cdot 1) = x \cdot \sigma(1) = x$$

Por lo que  $x \in F^{\text{Aut}_F(K)}$ .

□

**Teorema 2.3.** *Sea  $K$  un cuerpo, si  $G$  es un subgrupo finito de  $\text{Aut}(K)$ , entonces:*

$$[K : K^G] = |G| \quad y \quad G = \text{Aut}_{K^G}(K)$$

*Demostración.* El Lema de Artin nos dice que  $[K : K^G] \leqslant |G|$ . Para la otra desigualdad, el Lema anterior nos dice que  $G < \text{Aut}_{K^G}(K)$  y la Proposición 1.29 nos dice que  $|\text{Aut}_{K^G}(K)| \leqslant [K : K^G]$ , por lo que:

$$|G| \leqslant |\text{Aut}_{K^G}(K)| \leqslant [K : K^G]$$

de donde  $[K : K^G] = |G|$  y tendrá que ser  $|G| = |\text{Aut}_{K^G}(K)|$ , por lo que finalmente  $G = \text{Aut}_{K^G}(K)$ . □

**Ejemplo.** Sea  $K = \mathbb{Q}(\sqrt[3]{2}, w)$  con  $w$  una raíz cúbica primitiva de la unidad, sabemos ya que:

$$\text{Aut}(K) = \{\eta_{j,k} : j \in \{0, 1, 2\}, k \in \{1, 2\}\}$$

donde:

$$\eta_{j,k}(\sqrt[3]{2}) = w^j \sqrt[3]{2} \quad \eta_{j,k}(w) = w^k$$

Los subgrupos propios de  $\text{Aut}(K)$  (por el Teorema de Lagrange) son de orden 2 o 3, todos ellos cíclicos, por lo que tenemos que buscar elementos de orden 2 y 3. Son:

$$\langle \eta_{1,1} \rangle \cong \langle \eta_{2,1} \rangle, \quad \langle \eta_{0,2} \rangle \cong \langle \eta_{1,2} \rangle \cong \langle \eta_{2,2} \rangle$$

Que hemos obtenido ya que por ejemplo:

$$\begin{aligned}\sqrt[3]{2} &\xrightarrow{\eta_{0,2}} \sqrt[3]{2} \\ w &\mapsto w^2 \mapsto w^4 = w\end{aligned}$$

$$\begin{aligned}\sqrt[3]{2} &\xrightarrow{\eta_{1,2}} w\sqrt[3]{2} \xrightarrow{\eta_{1,2}} w^2w\sqrt[3]{2} = \sqrt[3]{2} \\ w &\mapsto w^2 \mapsto w\end{aligned}$$

Si el grupo fuera cíclico, tendríamos un único subgrupo por cada divisor, pero como hemos encontrado dos elementos distintos de orden 2 sabemos que no es cíclico.

$$\sqrt[3]{2} \xrightarrow{\eta_{1,1}} w\sqrt[3]{2} \xrightarrow{\eta_{1,1}} ww\sqrt[3]{2} = w^2\sqrt[3]{2} \neq \sqrt[3]{2}$$

hemos encontrado un elemento de orden que no es 2, por lo que ha de ser de orden 3 (puesto que no hay elementos de orden 6 al no ser cíclico). Para calcular el segundo elemento de orden 3 calculamos el cuadrado a  $\eta_{1,1}$ , obteniendo el  $\eta_{2,1}$ . Finalmente, tenemos el elemento  $\eta_{2,2}$ , que automáticamente sabemos que es de orden 2, puesto que es el que queda.

Buscamos ahora calcular  $K^{\langle \eta_{1,1} \rangle}$ , y sabemos que:

$$[K : K^{\langle \eta_{1,1} \rangle}] = |\langle \eta_{1,1} \rangle| = 3$$

Por lo que aplicando el Lema de la torre (sabiendo que  $[K : \mathbb{Q}] = 6$ ):

$$[K^{\langle \eta_{1,1} \rangle} : \mathbb{Q}] = 2$$

buscamos una extensión de grado 2 de  $\mathbb{Q}$  que esté dentro de  $\text{Aut}(K)$ . Heurísticamente, conocemos que  $[\mathbb{Q}(w) : \mathbb{Q}] = 2$ , con lo que buscamos razonar que  $K^{\langle \eta_{1,1} \rangle} = \mathbb{Q}(w)$ , comprobémoslo:

- Sabemos que  $\mathbb{Q} \leq K^{\langle \eta_{1,1} \rangle}$ , por ser  $\eta_{1,1}|_{\mathbb{Q}} = \iota$ .
- Como  $\eta_{1,1}(w) = w$ , tenemos que  $w \in K^{\langle \eta_{1,1} \rangle}$ .  
De estos dos puntos deducimos que  $\mathbb{Q}(w) \leq K^{\langle \eta_{1,1} \rangle}$ .
- Finalmente, como  $[K^{\langle \eta_{1,1} \rangle} : \mathbb{Q}] = 2 = [\mathbb{Q}(w) : \mathbb{Q}]$ , ha de ser  $\mathbb{Q}(w) = K^{\langle \eta_{1,1} \rangle}$ .

Si pensamos ahora en calcular  $K^{\langle \eta_{0,2} \rangle}, K^{\langle \eta_{1,2} \rangle}, K^{\langle \eta_{2,2} \rangle}$ , lo que haremos será buscar primero extensiones de grado 3 de  $\mathbb{Q}$ . Sabemos que los elementos  $\sqrt[3]{2}, w\sqrt[3]{2}$  y  $w^2\sqrt[3]{2}$  tienen grado 3 sobre  $\mathbb{Q}$ , y no será difícil comprobar que  $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(w\sqrt[3]{2})$  y  $\mathbb{Q}(w^2\sqrt[3]{2})$  son los subcuerpos que estábamos buscando.

**Definición 2.2** (Polinomio separable). Sea  $f \in F[x]$  con  $\deg f \geq 1$ , se dice que  $f$  es separable si todas sus raíces (en un cuerpo de descomposición de  $f$ ) son simples.

*Observación.* Las siguientes afirmaciones sobre  $f \in F[x]$  son equivalentes:

1.  $f$  es separable.

2.  $f$  tiene  $\deg f$  raíces distintas en su cuerpo de descomposición.
3.  $\text{mcd}(f, f') = 1$ .

*Demostración.*  $1 \iff 2$  es evidente, para  $2 \iff 3$ :

- $\iff$ ) Si  $\text{mcd}(f, f') = 1$  tenemos por la identidad de Bezout que si  $\alpha$  es una raíz de  $f$  entonces no puede ser también raíz de  $f'$ , ya que entonces tendríamos  $1 = 0$ , por lo que las raíces de  $f$  y  $f'$  son distintas, luego todas las raíces de  $f$  son simples.
- $\implies$ ) Si  $\text{mcd}(f, f') = 0$  entonces tendríamos que  $f' \mid f$ , de donde compartirían alguna raíz. Si fuera  $\text{mcd}(f, f')$  igual a un polinomio no constante, entonces  $f$  y  $f'$  compartirían las raíces de dicho polinomio.

□

**Ejemplo.** Para mostrar la abundancia de polinomios separables así como la existencia de polinomios no separables:

- Si  $F$  es un cuerpo con  $\text{car}(F) = 0$  y  $f$  es irreducible, entonces  $f$  es separable. Como  $\text{car}(F) = 0$  y  $\deg f \geq 1$ , tenemos al ser  $f$  no constante que  $f' \neq 0$ , y como  $f$  es irreducible tendremos que  $\text{mcd}(f, f') = 1$ , de donde  $f$  es separable.
- Sea  $f = x^q - x \in \mathbb{F}_p[x]$ , donde  $q = p^n$ , tenemos que  $f$  es separable. Como  $f' = qx^{q-1} - 1 = -1 \neq 0$ , tenemos que  $\text{mcd}(f, f') = 1$ , por lo que  $f$  es separable.
- Sea  $\mathbb{F}_p(t)$  el cuerpo de fracciones del anillo de polinomios  $\mathbb{F}_p[t]$ , si consideramos el polinomio:

$$f = x^p - t \in \mathbb{F}_p(t)[x]$$

tenemos que  $f$  es irreducible (por Eisenstein para  $t$ ) y que  $f' = 0$ , con lo que  $\text{mcd}(f, f') = f \neq 1$ , luego  $f$  no es separable.

**Definición 2.3** (Extensión separable). Una extensión algebraica  $F \leq K$  se dice separable si  $\text{Irr}(\alpha, F)$  es separable, para todo  $\alpha \in K$ .

*Observación.* Toda extensión algebraica en característica 0 es separable.

**Definición 2.4** (Extensión normal). Una extensión algebraica  $F \leq K$  se dice normal si  $\text{Irr}(\alpha, F)$  se factoriza como producto de polinomios lineales en  $K[x]$ , para todo  $\alpha \in K$ .

**Ejemplo.** Por ejemplo, la extensión  $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$  no es normal pero sí es separable.

*Observación.* Si  $F \leq K$  es una extensión normal y  $p \in F[x]$  es un polinomio mónico irreducible, entonces se verifica alguna de las dos siguientes afirmaciones:

- $p$  no tiene ninguna raíz en  $K$ .
- $p$  tiene todas sus raíces en  $K$ .

*Demostración.* Supongamos que  $\alpha \in K$  es una raíz de  $p$ . En dicho caso, como  $p$  es mónico e irreducible tenemos que  $p = \text{Irr}(\alpha, F)$ , y como la extensión es normal tendremos que  $p$  se descompone en  $K[x]$  como producto de polinomios de grado uno, por lo que debe tener todas sus raíces en  $K$ .  $\square$

**Teorema 2.4.** *Sea  $F \leqslant K$  una extensión de cuerpos. Son equivalentes:*

- i)  $K$  es cuerpo de descomposición de un  $f \in F[x]$  separable.
- ii)  $F \leqslant K$  es finita y  $F = K^{\text{Aut}_F(K)}$ .
- iii)  $F = K^G$  para un subgrupo finito  $G$  de  $\text{Aut}(K)$ .
- iv)  $F \leqslant K$  es finita, normal y separable.

*Demostración.* Veamos las equivalencias:

i)  $\implies$  ii) Como  $K$  es cuerpo de descomposición de cierto  $f \in F[x]$ , tenemos entonces que si  $\alpha_1, \dots, \alpha_s$  son las raíces de  $f$  entonces:

$$K = F(\alpha_1, \dots, \alpha_s)$$

Por lo que  $F \leqslant K$  es finitamente generada. Si observamos ahora la demostración del Teorema 1.10 observamos que solo usaba que los  $\alpha_i$  eran algebraicos, por lo que podemos concluir que  $F \leqslant K$  es finita.

Sabemos ya que  $F \leqslant F^{\text{Aut}_F(K)} \leqslant K^{\text{Aut}_F(K)}$ . Como  $F \leqslant K$  es finita tenemos entonces por la Proposición 1.29 que  $\text{Aut}_F(K)$  es un subgrupo finito de  $\text{Aut}(K)$ , de donde por el Teorema 2.3 tenemos que:

$$[K : K^{\text{Aut}_F(K)}] = |\text{Aut}_F(K)|$$

Finalmente, como  $K$  es cuerpo de descomposición de  $f \in F[x]$  separable, la Proposición 1.30 nos da la igualdad (\*):

$$[K : K^{\text{Aut}_F(K)}] = |\text{Aut}_F(K)| \stackrel{(*)}{=} [K : F]$$

y como tenemos  $F \leqslant K^{\text{Aut}_F(K)} \leqslant K$ , el Lema de la Torre nos dice que  $[K^{\text{Aut}_F(K)} : F] = 1$ , de donde  $F = K^{\text{Aut}_F(K)}$ .

ii)  $\implies$  iii) Si la extensión es finita, tenemos entonces que  $\text{Aut}_F(K)$  es un subgrupo finito de  $\text{Aut}(K)$ , con lo que tomando  $G = \text{Aut}_F(K)$  tenemos que  $F = K^G$ .

iii)  $\implies$  iv) Si  $F = K^G$  con  $G$  un subgrupo finito de  $\text{Aut}(K)$ , la Proposición de Artin nos dice que:

$$[K : F] = [K : K^G] \leqslant |G|$$

por lo que  $F \leqslant K$  es finita, luego también es algebraica.

Sean  $\alpha \in K$  y  $h = \text{Irr}(\alpha, F) \in F[x]$ , tenemos que probar que  $h$  se descompone en  $K[x]$  como producto de polinomios lineales que no comparten raíces entre sí. Como  $G$  actúa sobre  $K$ , podemos considerar la órbita de  $\alpha$  (considerando todos sus elementos distintos):

$$\text{Orb}(\alpha) = \{\alpha_1, \dots, \alpha_t\} \subseteq K$$

y podemos considerar el polinomio:

$$g = \prod_{i=1}^t (x - \alpha_i) = \sum_{j=0}^t a_j x^j \in K[x]$$

para ciertos  $a_0, \dots, a_t \in K$ . Veamos que  $a_j \in F$  para todo  $j \in \{1, \dots, t\}$ , usando que  $F = K^G$ . Dado  $\sigma \in G$ :

$$\prod_{i=1}^t (x - \sigma(\alpha_i)) = g^\sigma = \sum_{j=0}^t \sigma(a_j) x^j$$

y vemos que  $g = \prod_{i=1}^t (x - \sigma(\alpha_i))$ , puesto que al aplicar  $\sigma$  sobre los elementos de la órbita los permuta, con lo que de la igualdad de la derecha deducimos que  $\sigma(a_j) = a_j$ , para todo  $j \in \{1, \dots, t\}$ , con lo que tenemos  $a_j \in F$  para todo  $j \in \{1, \dots, t\}$ , luego  $g \in F[x]$ .

Por una parte  $g(\alpha) = 0$ , puesto que  $\alpha \in Orb(\alpha)$ . Como  $h = \text{Irr}(\alpha, F)$ , tenemos que  $h$  divide a  $g$ .

Por otra parte, cada  $\alpha_i$  es raíz de  $h$ , ya que si  $\alpha_i \in Orb(\alpha)$  tenemos que existe  $\sigma \in G$  de forma que  $\sigma(\alpha) = \alpha_i$ , de donde (usando en (\*) que  $h \in K^G[x]$ ):

$$h(\alpha_i) = h(\sigma(\alpha)) \stackrel{(*)}{=} \sigma(h(\alpha)) = \sigma(0) = 0$$

Como los elementos  $\alpha_i$  son distintos, tenemos que  $\deg h \geq t$ , pero como  $h$  divide a  $g$  y  $g$  es un polinomio mónico de grado  $t$ , tenemos que  $g = h$ . Hemos probado que  $\text{Irr}(\alpha, F)$  se descompone en  $K[x]$  como producto de polinomios de grado uno que no comparten raíces entre sí, para cada  $\alpha \in K$ . Es decir, hemos probado que  $F \leq K$  es una extensión normal y separable.

*iv)  $\Rightarrow i)$*  Como  $F \leq K$  es finita, tenemos entonces que existen  $\alpha_1, \dots, \alpha_s \in K$  algebraicos de forma que  $K = F(\alpha_1, \dots, \alpha_s)$ . Podemos por tanto considerar  $f_i = \text{Irr}(\alpha_i, F)$ , y tomamos como  $f$  el producto de los  $f_i$  eliminando repeticiones (es decir, multiplicamos todos los  $f_i$  distintos). Como la extensión es normal y separable, cada uno de los  $f_i$  se descompone como producto de polinomios de grado uno mónicos distintos, de donde  $f$  es un polinomio separable, por lo que  $K$  es un cuerpo de descomposición de  $f$ .

□

Este Teorema tiene consecuencias importantes relacionadas con lo que luego llamaremos “extensiones de Galois”, que será una extensión  $F \leq K$  que cumple alguno de los apartados anteriores, todos ellos equivalentes.

- El punto *i)* nos da una forma práctica de comprobar que una extensión es de Galois, para lo cual repetiremos de forma parecida la demostración *iv)  $\Rightarrow i)$* .
- El apartado *ii)* tiene que ver con lo que luego llamaremos “conexión de Galois”, que responde a la pregunta de qué le tiene que suceder a una extensión finita para estar en biyección con su grupo de Galois.

**Definición 2.5.** La órbita de  $\alpha \in K$  bajo la acción de  $G$  que ha aparecido en la demostración anterior,  $Orb(\alpha)$  se llama el conjunto de conjugados de  $\alpha$  bajo  $G$ .

Se trata de la generalización del concepto “conjugado” de un número complejo, pues basta considerar  $\mathbb{R} \leqslant \mathbb{C}$  y  $G = \{id_{\mathbb{C}}, \sigma\}$ , con  $\sigma : \mathbb{C} \rightarrow \mathbb{C}$  la aplicación conjugación.

**Definición 2.6** (Extensión de Galois). Una extensión  $F \leqslant K$  se dice que es de Galois si es finita, normal y separable.

El grupo  $\text{Aut}_F(K)$  recibe el nombre Grupo de Galois de la extensión.

Notemos que el grupo de Galois de una extensión  $F \leqslant K$  de Galois siempre es finito, porque  $F \leqslant K$  es finita por ser de Galois y en dicho caso  $|\text{Aut}_F(K)| \leqslant [K : F]$ .

**Corolario 2.4.1.** *En característica 0, si  $K$  es cuerpo de descomposición de  $f \in F[x]$ , entonces  $F \leqslant K$  es de Galois.*

*Demostración.* Consideramos la descomposición de  $f$  en irreducibles:

$$f = p_1^{n_1} \cdot \dots \cdot p_t^{n_t}$$

con  $p_i$  distintos. Observemos que  $K$  es cuerpo de descomposición de  $p_1 \cdot \dots \cdot p_t$ . Cada uno de los  $p_i$  es irreducible en  $\text{car}(F) = 0$ , por lo que cada  $p_i$  es separable. Como estos no pueden compartir raíces entre sí por ser irreducibles<sup>1</sup>, tendremos que  $p_1 \cdot \dots \cdot p_t$  es separable. Por el Teorema anterior, la extensión es finita, normal y separable.  $\square$

**Corolario 2.4.2.** *Si  $F \leqslant K$  es de Galois y  $F \leqslant E \leqslant K$  es una subextensión, entonces  $E \leqslant K$  es de Galois.*

*Demostración.* Como  $F \leqslant K$  es de Galois, entonces  $K$  es cuerpo de descomposición de cierto  $f \in F[x]$  separable, por lo que  $K$  es cuerpo de descomposición de  $f \in E[x]$ , que sigue siendo separable.  $\square$

**Ejemplo.** Si consideramos  $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[3]{2})$ , tenemos una extensión finita y separable pero que no es de Galois, porque no es normal. Sin embargo,  $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[3]{2}, w)$  sí que es de Galois. En consecuencia,  $\mathbb{Q}(\sqrt[3]{2}) \leqslant \mathbb{Q}(\sqrt[3]{2}, w)$  es de Galois.

Sabemos que  $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[3]{2})$  no es normal porque  $\text{Irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$  no se descompone como producto de polinomios lineales en  $\mathbb{Q}(\sqrt[3]{2})$ , ya que  $w\sqrt[3]{2}$  es una raíz del polinomio que no está en  $\mathbb{Q}(\sqrt[3]{2})$ .

**Corolario 2.4.3.** *Toda extensión de cuerpos finitos es de Galois.*

*Demostración.* Si tenemos una extensión  $F \leqslant E$  de cuerpos finitos de característica  $\text{car}(F) = p$ , tenemos entonces que:

$$\mathbb{F}_p \leqslant F \leqslant E$$

con  $\mathbb{F}_p \leqslant E$  de Galois, puesto que el polinomio  $x^q - x \in \mathbb{F}_p[x]$  con  $q = |E| = p^n$  es separable y  $E$  es un cuerpo de descomposición suyo.  $\square$

---

<sup>1</sup>Si  $p_i$  tiene alguna raíz en común con  $p_j$  entonces  $p_i$  dividiría a  $p_j$ , de donde deducimos que  $p_i = p_j$  por ser ambos irreducibles, pero eran polinomios distintos.

**Ejemplo.** Consideramos  $\mathbb{Q} \leqslant E = \mathbb{Q}(\sqrt[3]{5}, i\sqrt{5})$ , que es una extensión finita, con (por el Lema de la Torre)  $[E : \mathbb{Q}] = 6$ . Si esta extensión fuera de Galois, entonces la raíz  $w\sqrt[3]{5}$  de  $x^3 - 5 = \text{Irr}(\sqrt[3]{5}, \mathbb{Q})$  estaría en  $E$ , para  $w = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$ .

En dicho caso,  $i\sqrt{3} \in E$ , luego  $\mathbb{Q}(i\sqrt{3}, i\sqrt{5}) \leqslant E$ . Buscamos calcular:

$$[\mathbb{Q}(i\sqrt{3}, i\sqrt{5}) : \mathbb{Q}]$$

Sabemos que  $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$ , así como que  $[\mathbb{Q}(i\sqrt{5}, i\sqrt{3}) : \mathbb{Q}(i\sqrt{3})] \leqslant 2$ :

- Si  $[\mathbb{Q}(i\sqrt{5}, i\sqrt{3})] = 1$ , esto es porque  $i\sqrt{5} \in \mathbb{Q}(i\sqrt{3})$ . En dicho caso, tendríamos que:

$$i\sqrt{5} = a + bi\sqrt{3} \quad a, b \in \mathbb{Q}$$

de donde  $a = 0$ , con lo que  $i\sqrt{5} = bi\sqrt{3}$ , y elevando al cuadrado tendríamos que:

$$-5 = -3b^2$$

de donde  $b \in \mathbb{Q}$  es raíz de  $3x^2 - 5$ , pero:

**Opción 1.**  $3x^2 - 5$  es irreducible por Eisenstein (notemos que es primitivo).

**Opción 2.** Las posibles raíces racionales del polinomio enunciado son:

$$1, -1, 5, -5, \frac{1}{3}, \frac{-1}{3}, \frac{5}{3}, \frac{-5}{3}$$

y ninguna es raíz.

- Tenemos por tanto que  $[\mathbb{Q}(i\sqrt{5}, i\sqrt{3}) : \mathbb{Q}(i\sqrt{3})] = 2$ , y por el lema de la torre tenemos que  $[\mathbb{Q}(i\sqrt{3}, i\sqrt{5}) : \mathbb{Q}] = 4$ , de donde 4 divide a  $6 = [E : \mathbb{Q}]$ , contradicción que viene de suponer que la extensión es de Galois.

## 2.2. Teorema fundamental de la Teoría de Galois

**Notación.** Notaremos:

- Si  $F \leqslant K$  es una extensión y  $F \leqslant E \leqslant K$  se dice que  $E$  es una subextensión de  $F \leqslant K$ . Denotamos al conjunto de todas ellas por  $\text{Subex}(F \leqslant K)$ .
- Si  $G$  es un grupo, llamamos  $\text{Subgr}(G)$  al conjunto de todos sus subgrupos.
- Si  $H \in \text{Subgr}(G)$ , denotamos por  $(G : H)$  al índice de  $H$  en  $G$ .

Recordemos que si  $G$  es un grupo finito el Teorema de Lagrange nos decía que:

$$|G| = (G : H)|H|$$

**Definición 2.7.** Sean  $(A, \leqslant)$ ,  $(B, \leqslant)$  dos conjuntos ordenados, un anti-isomorfismo de conjuntos ordenados es una aplicación biyectiva  $f : A \rightarrow B$  de forma que:

$$a \leqslant a' \iff f(a) \geqslant f(a')$$

*Observación.* Si  $G$  es un grupo y  $F \leq K$  es una extensión de cuerpos, tenemos que  $(\text{Subgr}(G), <)$  y  $(\text{Subex}(F \leq K), \leq)$  son conjuntos ordenados, pues la relación indicada en cada conjunto es reflexiva, transitiva y antisimétrica.

**Teorema 2.5.** *Sea  $F \leq K$  una extensión de Galois con grupo de Galois  $G$ . La aplicación*

$$\begin{aligned} : \text{Subgr}(G) &\longrightarrow \text{Subex}(F \leq K) \\ H &\longmapsto K^H \end{aligned}$$

*es un anti-isomorfismo de conjuntos ordenados, cuya isomorfismo inverso es*

$$\begin{aligned} : \text{Subex}(F \leq K) &\longrightarrow \text{Subgr}(G) \\ E &\longmapsto \text{Aut}_E(K) \end{aligned}$$

*Si  $H_1 < H_2$  son subgrupos de  $G$  y  $E_2 \leq E_1$  son las subextensiones de  $F \leq K$  correspondientes a  $H_1$  y  $H_2$  por la anterior biyección, entonces:*

$$(H_2 : H_1) = [E_1 : E_2]$$

*Demostración.* Para ver que es un anti-isomorfismo, veamos que cada aplicación está bien definida y que una es la inversa de la otra:

- Sea  $H \in \text{Subgr}(G)$ , tenemos entonces que  $\{id_K\} < H < G$ , y el Lema 2.2 nos dice que:

$$K = K^{id_K} \geq K^H \geq K^G \stackrel{(*)}{=} F$$

donde en  $(*)$  hemos usado que como  $F \leq K$  es de Galois, tenemos el segundo punto del Teorema 2.4. Por tanto,  $K^H \in \text{Subex}(F \leq K)$ .

- Sea  $E \in \text{Subex}(F \leq K)$ , tenemos entonces que  $F \leq E \leq K$ , y el Lema 2.2 nos dice que:

$$G = \text{Aut}_F(K) > \text{Aut}_E(K) > \text{Aut}_K(K) = \{id_K\}$$

de donde  $\text{Aut}_E(K) \in \text{Subgr}(G)$ .

- Sea  $H \in \text{Subgr}(G)$ , si aplicamos las dos aplicaciones a  $H$  obtenemos:

$$H \longmapsto K^H \longmapsto \text{Aut}_{K^H}(K)$$

como  $F \leq K$  es de Galois tenemos que es una extensión finita, por lo que  $G$  es finito, y como  $H$  es un subgrupo finito de  $G$  podemos aplicar el Teorema 2.3, obteniendo que  $H = \text{Aut}_{K^H}(K)$ .

- Sea  $E \in \text{Subex}(F \leq K)$ , si aplicamos las dos aplicaciones a  $E$  obtenemos:

$$E \longmapsto \text{Aut}_E(K) \longmapsto K^{\text{Aut}_E(K)}$$

y como  $F \leq K$  es de Galois deducimos que  $E \leq K$  es también de Galois, pudiendo aplicar finalmente el segundo punto del Teorema 2.4, obteniendo que  $E = K^{\text{Aut}_E(K)}$ .

En consecuencia, la aplicación enunciada es un anti-isomorfismo de conjuntos ordenados.

Para la segunda parte, si  $H_1 < H_2$  son subgrupos de  $G$  y  $E_2 \leq E_1$  son las subextensiones de  $F \leq K$  correspondientes a dichos subgrupos (es decir,  $E_1 = K^{H_1}$  y  $E_2 = K^{H_2}$ ), aplicando el Teorema 2.3 en (\*) y el Lema de la Torre en (\*\*) tenemos entonces que:

$$|H_2| \stackrel{(*)}{=} [K : E_2] \stackrel{(**)}{=} [K : E_1][E_1 : E_2] \stackrel{(*)}{=} |H_1|[E_1 : E_2]$$

de donde:

$$[E_1 : E_2] = \frac{|H_2|}{|H_1|} = (H_2 : H_1)$$

□

**Definición 2.8** (Conexión de Galois). La biyección del Teorema anterior recibe el nombre “Conexión de Galois”.

**Ejemplo.** Si consideramos la extensión de Galois  $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}, w)$ , vimos anteriormente que  $\text{Aut}(\mathbb{Q}(\sqrt[3]{2}, w))$  tenía 6 elementos, y en un ejemplo anterior calculábamos  $\text{Subgr}(\text{Aut}(\mathbb{Q}(\sqrt[3]{2}, w)))$ , obteniendo 6 subgrupos.

Por la Conexión de Galois sabemos ahora que tenemos tantos subcuerpos de  $\mathbb{Q}(\sqrt[3]{2}, w)$  como subgrupos de  $\text{Aut}(\mathbb{Q}(\sqrt[3]{2}, w))$  (puesto que  $\mathbb{Q}$  es el subcuerpo primo de  $\mathbb{Q}(\sqrt[3]{2}, w)$ ).

**Ejemplo.** Sea  $\mathbb{F}_q = \mathbb{F}_{p^n}$ , nos preguntamos por los elementos de dicho cuerpo. La extensión  $\mathbb{F}_p \leq \mathbb{F}_{p^n}$  es de Galois por ser una extensión de cuerpos finitos, por lo que podemos tratar de usar la conexión de Galois. Más aún, habíamos visto que:

$$\text{Aut}(\mathbb{F}_{p^n}) = \text{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n}) = \langle \tau \rangle$$

cíclico de orden  $n$ , con  $\tau(\alpha) = \alpha^p$  el automorfismo de Frobenius. Los subgrupos están parametrizados por los divisores de  $n$ , con lo que:

$$\text{Subgr}(\text{Aut}(\mathbb{F}_{p^n})) = \{ \langle \tau^d \rangle : d \in \text{Div}(n) \}$$

Los subcuerpos de  $\mathbb{F}_{p^n}$  son, por la conexión de Galois:

$$\left\{ \mathbb{F}_{p^n}^{\langle \tau^d \rangle} : d \in \text{Div}(n) \right\}$$

Vamos a calcular:

$$\left[ \mathbb{F}_{p^n}^{\langle \tau^d \rangle} : \mathbb{F}_p \right] = (\langle \tau \rangle : \langle \tau^d \rangle) = d$$

Por lo que:

$$\left| \mathbb{F}_{p^n}^{\langle \tau^d \rangle} \right| = p^d$$

Y estos son todos.

Cada cuerpo de  $p^n$  elementos tiene un subcuerpo de cardinal  $p^d$  con  $d \in \text{Div}(n)$ . Por ejemplo, un cuerpo de 64 elementos tiene 4 subcuerpos (cada divisor de 6).

**Lema 2.6.** Sea  $F \leq K$  de Galois con grupo de Galois  $G$ , sea  $H \in \text{Subgr}(G)$  y  $E \in \text{Subex}(F \leq K)$  su correspondiente mediante la conexión de Galois. Si  $\sigma \in G$ , entonces  $\sigma H \sigma^{-1}$  y  $\sigma(E)$  son correspondientes por la conexión de Galois.

*Demostración.* De Álgebra II sabemos que si  $H \in \text{Subgr}(G)$  entonces para  $\sigma \in G$  tenemos  $\sigma H \sigma^{-1} \in \text{Subgr}(G)$ , vemos también que  $\sigma(E)$  es sigue siendo una subextensión de  $F \leq K$ , por lo que la pregunta está bien planteada.

Tenemos que  $E = K^H$  y queremos probar que  $\sigma(K^H) = K^{\sigma H \sigma^{-1}}$ . Tendremos:

$$\begin{aligned}\alpha \in K^{\sigma H \sigma^{-1}} &\iff \sigma \tau \sigma^{-1}(\alpha) = \alpha \quad \forall \tau \in H \iff \tau \sigma^{-1}(\alpha) = \sigma^{-1}(\alpha) \quad \forall \tau \in H \\ &\iff \sigma^{-1}(\alpha) \in K^H \iff \alpha \in \sigma(K^H)\end{aligned}$$

□

**Teorema 2.7.** Sea  $F \leq K$  de Galois y  $G$  su grupo de Galois, si  $H \in \text{Subgr}(G)$  y  $E \in \text{Subex}(F \leq K)$  es su correspondiente mediante la conexión de Galois entonces:

$$H \text{ es normal en } G \iff F \leq E \text{ es de Galois}$$

En cuyo caso,  $\text{Aut}_F(E) \cong G/H$ .

*Demostración.* Por doble implicación:

$\implies$ ) Si  $H \triangleleft G$  tenemos entonces que:

$$\sigma(E) = \sigma(K^H) = K^{\sigma H \sigma^{-1}} = K^H = E \quad \forall \sigma \in \text{Aut}_F(K)$$

Por lo que podemos definir la aplicación  $r : \text{Aut}_F(K) \rightarrow \text{Aut}_F(E)$  dada por:

$$r(\sigma) = \sigma|_E$$

y estará bien definida, pues  $\sigma(E) = E$  para cada  $\sigma \in \text{Aut}_F(K)$ . Es fácil ver que  $r$  es un homomorfismo de grupos. Observamos ahora que:

$$\ker(r) = \{\sigma \in \text{Aut}_F(K) : \sigma|_E = id_E\} = \text{Aut}_E(K) = H$$

Aplicando el Primer Teorema de Isomorfía para grupos obtenemos que:

$$G/H \cong \text{Im } r$$

y si observamos ahora que:

$$[E : F] = (G : H) = |\text{Im } r| \leq |\text{Aut}_F(E)| \leq [E : F]$$

Obtenemos que  $\text{Im } r = \text{Aut}_F(E)$ , por lo que  $r$  es sobreyectivo, tenemos ya que  $G/H \cong \text{Aut}_F(E)$ . Para ver que  $F \leq E$  es de Galois, trataremos de probar la tercera condición del Teorema 2.4, de la que conocemos ya la inclusión  $F \leq E^{\text{Aut}_F(E)}$ . Sea pues  $\alpha \in E^{\text{Aut}_F(E)}$ , vemos que:

$$\alpha = r(\sigma)(\alpha) = \sigma|_E(\alpha) = \alpha \quad \forall \sigma \in \text{Aut}_F(K)$$

por lo que  $\alpha \in K^{\text{Aut}_F(K)} = F$ , lo que nos da la otra inclusión, de donde  $F \leq E$  es de Galois.

$\iff$ ) Si  $F \leqslant E$  es de Galois tenemos entonces que  $E$  es cuerpo de descomposición de cierto polinomio  $f \in F[x]$  separable, que podemos suponer de la forma:

$$f = \prod_{i=1}^n (x - \alpha_i)$$

con  $E = F(\alpha_1, \dots, \alpha_n)$ , ya que si  $f$  no es mónico podemos dividir todos sus coeficientes entre el término líder, obteniendo un polinomio mónico con las mismas raíces. Sea  $\sigma \in \text{Aut}_F(K)$ , por ser  $f \in F[x]$  tenemos que:

$$f = f^\sigma = \prod_{i=1}^n (x - \sigma(\alpha_i))$$

por lo que será  $\sigma(\alpha_i) = \alpha_j \in E$ , en particular vemos que (usando una  $F$ -base de  $E$  en función de  $\alpha_i$ )  $\sigma(E) = E \quad \forall \sigma \in \text{Aut}_F(K)$ , por lo que:

$$K^H = E = \sigma(E) = \sigma(K^H) = K^{\sigma H \sigma^{-1}} \quad \forall \sigma \in \text{Aut}_F(K)$$

de donde  $H = \sigma H \sigma^{-1} \quad \forall \sigma \in \text{Aut}_F(K)$ , por lo que  $H \triangleleft \text{Aut}_F(K)$ .

□

**Ejemplo.** Consideramos  $f = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$ , y tomamos  $K$  el cuerpo de descomposición de  $f$ . Se pide calcular o describir todos los subcuerpos de  $K$ .

Observemos que  $\mathbb{Q} \leqslant K$  es de Galois por ser  $K$  cuerpo de descomposición de  $f$  en característica 0. Calculamos primero las raíces de  $f$ . Observamos que si  $s$  es una de ellas, entonces  $s^2$  es raíz de  $x^2 - 2x - 2$ . Así:

$$s^2 = \frac{2 \pm \sqrt{12}}{2} = 1 \pm \sqrt{3}$$

Obtenemos que las raíces de  $f$  son  $\alpha, -\alpha, \beta, -\beta$ , donde:

$$\alpha = \sqrt{\sqrt{3} + 1}, \quad \beta = i\sqrt{\sqrt{3} - 1}$$

Sabemos en este momento que  $K = \mathbb{Q}(\alpha, \beta)$ . Si vemos que:

$$\alpha\beta = i\sqrt{2}$$

Tenemos que  $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \alpha\beta) = \mathbb{Q}\left(\sqrt{\sqrt{3} + 1}, i\sqrt{2}\right)$ . Nos preguntamos si  $f$  es irreducible, y la respuesta es sí, por Eisenstein para  $p = 2$ . De aquí concluimos que  $f = \text{Irr}(\alpha, \mathbb{Q})$ , luego  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ .

Por otra parte,  $[\mathbb{Q}(\alpha, i\sqrt{2}) : \mathbb{Q}(\alpha)] = 2$ , ya que  $i\sqrt{2} \notin \mathbb{Q}(\alpha) \leqslant \mathbb{R}$ . Notemos que este argumento no podríamos haberlo hecho con  $\beta$ , ya que obtendríamos que  $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \in \{1, 2, 4\}$ , y no podemos distinguir entre 2 y 4. Sabemos ya seguro que  $f$  no es irreducible sobre  $\mathbb{Q}(\alpha)$ , pues si lo fuera tendríamos que  $f = \text{Irr}(\beta, \mathbb{Q}(\alpha))$ , de donde sería  $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 4$ .

En conclusión, tenemos por el Lema de la Torre que:

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, i\sqrt{2}) : \mathbb{Q}] = 8$$

Y como  $F \leq K$  es de Galois, el Teorema 2.5 nos dice que:

$$|\text{Aut}_{\mathbb{Q}}(K)| = 8$$

Buscamos los automorfismos por la propiedad de extensión, es decir, calculamos las extensiones de la inclusión  $\iota : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{Q}(\alpha, i\sqrt{2}) = K$  mediante la Proposición de extensión. Así, están determinadas por:

$$\eta_0(\alpha) = \alpha, \quad \eta_1(\alpha) = -\alpha, \quad \eta_2(\alpha) = \beta, \quad \eta_3(\alpha) = -\beta$$

Ahora,  $\text{Irr}(i\sqrt{2}, \mathbb{Q}) = x^2 + 2$ , con lo que cada uno de los anteriores se extienden a dos automorfismos  $K \rightarrow K$  determinados por:

$$\eta_{j,k} : \begin{cases} \alpha \mapsto \eta_j(\alpha) \\ \alpha\beta \mapsto (-1)^k \alpha\beta \end{cases} \quad \forall j \in \{0, 1, 2, 3\}, k \in \{0, 1\}$$

Por lo que:

$$\text{Aut}(K) = \{\eta_{j,k} : j \in \{0, 1, 2, 3\}, k \in \{0, 1\}\}$$

Si tratamos de calcular ahora todos los subgrupos de  $\text{Aut}(K)$ , conviene tener en mente todos los grupos de orden 8:

$$C_8, \quad C_4 \oplus C_2, \quad C_2 \oplus C_2 \oplus C_2, \quad D_4, \quad H = \{\pm 1, \pm i, \pm j, \pm k\}$$

Sabemos que  $\mathbb{Q}(i\sqrt{2}) \leq K$  con  $[K : \mathbb{Q}(i\sqrt{2})] = 4$  (ya que  $[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = 2$  y aplicamos el Lema de la Torre, sabiendo que  $[K : \mathbb{Q}] = 8$ ) que por la conexión de Galois corresponderá con un subgrupo de orden 4. Por lo que:

$$|\text{Aut}_{\mathbb{Q}(i\sqrt{2})}(K)| = 4$$

Y este es un subgrupo normal de  $\text{Aut}_{\mathbb{Q}}(K)$ , podemos verlo de dos formas distintas:

- $\mathbb{Q}(i\sqrt{2}) \leq K$  es de Galois.
- Tiene índice 2 sobre  $\text{Aut}(K)$ .

Más aún, sabemos que:

$$\text{Aut}_{\mathbb{Q}(i\sqrt{2})}(K) = \{\eta_{j,0} : j \in \{0, 1, 2, 3\}\}$$

ya que se debe cumplir que  $\alpha\beta \mapsto \alpha\beta$  y debe tener 4 elementos, los únicos 4 candidatos posibles. Veamos el orden de cada elemento:

$$\begin{array}{cccccccc} \eta_{0,0} & \eta_{1,0} & \eta_{2,0} & \eta_{3,0} & \eta_{0,1} & \eta_{1,1} & \eta_{1,2} & \eta_{1,3} \\ 1 & 2 & 2 & 2 & 2 & 2 & 4 & 4 \end{array}$$

Que por ejemplo calculamos el orden de  $\eta_{2,0}$  ya que:

$$\eta_{2,0}(\alpha) = \beta, \quad \eta_{2,0}^2(\alpha) = \eta_{2,0}(\beta) = \eta_{2,0}\left(\frac{\alpha\beta}{\alpha}\right) = \frac{\eta_{2,0}(\alpha\beta)}{\eta_{2,0}(\alpha)} = \frac{\alpha\beta}{\beta} = \alpha$$

Por lo que  $O(\eta_{2,0}) = 2$ . Como sabemos que el único grupo finito que tiene 5 subgrupos de orden 2 es  $D_4$ , tiene que ser  $\text{Aut}(K) \cong D_4$ .

Queremos calcular todos sus subgrupos, para así calcular todos los subcuerpos de  $K$  aplicando el Teorema 2.5.

Sabemos ya que  $\text{Aut}_{\mathbb{Q}(i\sqrt{2})}(K) = \langle \eta_{1,0}, \eta_{2,0} \rangle$ , y para terminar de hallar los subgrupos, nos falta por localizar otro subgrupo isomorfo al de Klein. Como  $\alpha = \sqrt{\sqrt{3} + 1} \in K$ , tenemos que  $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{3}) \leqslant K$  de Galois, por lo que tiene que corresponderse con un subgrupo de 4 elementos, que buscaremos cuál es. Probemos con el cíclico, tomamos  $\eta_{2,1}$  y:

$$\eta_{2,1}(\sqrt{3}) = \eta_{2,1}(\alpha^2 - 1) = (\eta_{2,1}(\alpha))^2 - 1 = \beta^2 - 1 = -\sqrt{3}$$

que no deja fijo al generador, por lo que buscamos otra expresión cuadrática que se corresponda con el cíclico.

Tomamos  $\mathbb{Q}(i\sqrt{6}) \leqslant K$ , que se tiene que corresponder con otro subgrupo de orden 4:

$$\eta_{2,1}(i\sqrt{6}) = \eta_{2,1}(\sqrt{3})\eta_{2,1}(i\sqrt{2}) = (-\sqrt{3})(-i\sqrt{2}) = i\sqrt{6}$$

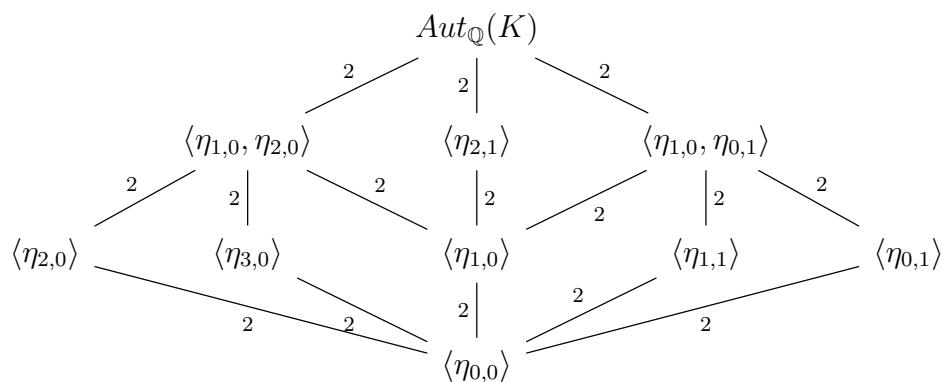
Por lo que  $\mathbb{Q} \leqslant \mathbb{Q}(i\sqrt{6})$  de grado 2, tenemos que:

$$\text{Aut}_{\mathbb{Q}(i\sqrt{6})}(K) = \langle \eta_{2,1} \rangle = \langle \eta_{3,1} \rangle$$

También sabemos por la conexión de Galois que:

$$K^{\langle \eta_{2,1} \rangle} = \mathbb{Q}(i\sqrt{6})$$

En resumen, tenemos que:



Y por la conexión de Galois podemos obtener:

- Los tres primeros lo sabíamos ya cuando nos pusimos a buscar el grupo cíclico y los dos isomorfos al de Klein.
- Observeos que  $\langle \eta_{1,0} \rangle$  es el mayor subgrupo contenido en la intersección  $\langle \eta_{1,0}, \eta_{2,0} \rangle$  y  $\langle \eta_{1,0}, \eta_{0,1} \rangle$ , por lo que obtenemos  $\mathbb{Q}(i\sqrt{2}, \sqrt{3})$ .
- Más aún, sabíamos ya que  $\mathbb{Q}(\alpha)$  era una extensión de grado 4, por lo que buscamos por qué automorfismo es estable, que es el  $\eta_{0,1}$ .

También lo podríamos haber visto porque:

$$\alpha \in K^{\langle \eta_{0,1} \rangle} \implies \mathbb{Q}(\alpha) \leq K^{\langle \eta_{0,1} \rangle}$$

con  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$  y  $[K^{\langle \eta_{1,0} \rangle} : \mathbb{Q}] = 4$ , por lo que han de ser iguales.

- La extensión  $\mathbb{Q}(\beta) \geq \mathbb{Q}$  también tiene grado 4, por lo que buscamos por cuál queda estable:

$$\eta_{1,1}(\beta) = \eta_{1,1}\left(\frac{\alpha\beta}{\alpha}\right) = \frac{\eta_{1,1}(\alpha\beta)}{\eta_{1,1}(\alpha)} = \frac{-\alpha\beta}{-\alpha} = \beta$$

Por lo que:

$$\beta \in K^{\langle \eta_{1,1} \rangle} \implies \mathbb{Q}(\beta) \leq K^{\langle \eta_{1,1} \rangle}$$

Ambas extensiones de grado 4, por lo que  $\mathbb{Q}(\beta)$  es el correspondiente a  $\langle \eta_{1,1} \rangle$  por la conexión de Galois.

- Para buscar las que nos faltan, buscaremos hacer cuentas con las raíces de polinomios (tiene que ver con la Teoría de Galois de las ecuaciones). Probemos a sumar  $\alpha$  con  $\beta$  y buscamos los fijos por  $\langle \eta_{3,0} \rangle$  y  $\langle \eta_{2,0} \rangle$ :

$$\eta_{2,0}(\alpha + \beta) = \eta_{2,0}(\alpha) + \eta_{2,0}(\beta) = \beta + \eta_{2,0}\left(\frac{\alpha\beta}{\alpha}\right) = \beta + \alpha$$

Por lo que:

$$\alpha + \beta \in K^{\langle \eta_{2,0} \rangle} \implies \mathbb{Q}(\alpha + \beta) \leq K^{\langle \eta_{2,0} \rangle}$$

Por la conexión de Galois, tenemos que:

$$\langle \eta_{2,0} \rangle \leq \text{Aut}_{\mathbb{Q}(\alpha+\beta)}(K) \implies \text{Aut}_{\mathbb{Q}(\alpha+\beta)}(K) \in \{\langle \eta_{2,0} \rangle, \langle \eta_{1,0}, \eta_{2,0} \rangle, \text{Aut}_{\mathbb{Q}}(K)\}$$

Y descartamos:

- No es el total, porque  $\alpha + \beta \notin \mathbb{Q}$ .
- No es el generado por los dosetas, ya que:

$$\eta_{1,0}(\alpha + \beta) = \eta_{1,0}(\alpha) + \eta_{1,0}(\beta) = -\alpha + \eta_{1,0}\left(\frac{\alpha\beta}{\alpha}\right) = -\alpha - \beta \neq \alpha + \beta$$

La única opción posible es que  $\text{Aut}_{\mathbb{Q}(\alpha+\beta)}(K) = \langle \eta_{2,0} \rangle$ . Por lo que tenemos ya otro subcuerpo de  $K$ .

- Buscamos ahora un elemento que quede fijo por  $\eta_{3,0}$ , sospechamos que podría ser  $\alpha - \beta$ , lo comprobamos y luego vemos que  $\alpha - \beta \notin \mathbb{Q}$ , por lo que el subgrupo no podría ser el total y falta comprobar que no queda fijo bien por  $\eta_{1,0}$  bien por  $\eta_{2,0}$ .

En definitiva, obtenemos:

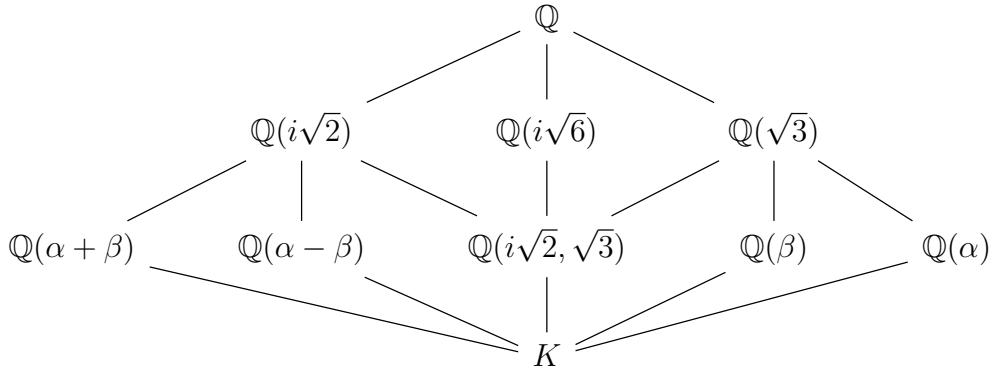


Figura 2.1: Todos los subcuerpos de  $K$ .

### 2.3. El Teorema Fundamental del Álgebra

Se tiene que  $\mathbb{C}$  es el cuerpo de descomposición de  $x^2 + 1 \in \mathbb{R}[x]$ , y  $[\mathbb{C} : \mathbb{R}] = 2$ , por lo que  $|\text{Aut}_{\mathbb{R}}(\mathbb{C})| = 2$ , que son:

$$\text{Aut}_{\mathbb{R}}(\mathbb{C}) = \{id, \sigma\}$$

con  $\sigma$  el automorfismo que conjuga cada número complejo.

Además, si  $f \in \mathbb{C}[x]$ ,  $\bar{f} \in \mathbb{C}[x]$  será el polinomio obtenido de  $f$  conjugando todos sus coeficientes.

**Teorema 2.8** (Fundamental del Álgebra). *Si  $f \in \mathbb{C}[x]$  no constante, entonces  $f$  tiene todas sus raíces<sup>2</sup> en  $\mathbb{C}$ .*

*Demostración.* Sea  $g = f\bar{f} \in \mathbb{R}[x]$ , y consideramos  $(x^2 + 1)g \in \mathbb{R}[x]$ , que es no constante. Sea  $K$  su cuerpo de descomposición, queremos probar que  $K = \mathbb{C}$ . Observemos que  $K$  contiene a  $\mathbb{C}$  por la Proposición de extensión:

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & K \\ & \searrow & \uparrow \\ & & \mathbb{C} \end{array}$$

Además, las tres extensiones que aparecen son de Galois. El Lema de la Torre nos dice que

$$|\text{Aut}_{\mathbb{R}}(K)| = [K : \mathbb{R}] = [K : \mathbb{C}][\mathbb{C} : \mathbb{R}] = [K : \mathbb{C}] \cdot 2$$

<sup>2</sup>O equivalentemente,  $\mathbb{C}$  es cuerpo de descomposición de  $f$ .

múltiplo de 2, por lo que  $G = \text{Aut}_{\mathbb{R}}(K)$  contiene un 2–subgrupo de Sylow,  $H$ . La conexión de Galois nos dice que  $[K^H : \mathbb{R}] = (G : H)$ , con  $(G : H)$  impar por ser  $H$  un 2–subgrupo de Sylow.

Sea  $\alpha \in K^H$ , consideramos  $\text{Irr}(\alpha, \mathbb{R})$ , que tiene grado impar por el Lema de la Torre (si su grado fuera par tendríamos entonces que  $(G : H)$  también sería par, ya que  $\mathbb{R} \leqslant K(\alpha) \leqslant K^H$ ), por lo que ha de tener una raíz real  $\beta \in \mathbb{R}$ , de donde  $\text{Irr}(\alpha, \mathbb{R})$  es divisible por  $(x - \beta)$ , pero como  $\text{Irr}(\alpha, \mathbb{R})$  es irreducible, este debe ser asociado a  $x - \beta$ , y los dos son mónicos, de donde  $\text{Irr}(\alpha, \mathbb{R}) = x - \beta$ , luego  $\beta = \alpha$  y tenemos por tanto que  $[K^H : \mathbb{R}] = 1$ , por lo que  $G = H$ , de donde  $G$  es un 2–grupo.

Así,  $\text{Aut}_{\mathbb{C}}(K)$  es un 2–grupo (por ser subgrupo de un 2–grupo,  $\text{Aut}_{\mathbb{R}}(K) > \text{Aut}_{\mathbb{C}}(K)$ ). Supongamos que  $|\text{Aut}_{\mathbb{C}}(K)| > 1$ . Como  $\text{Aut}_{\mathbb{C}}(K)$  es resoluble (por ser un  $p$ –grupo), tiene un subgrupo de índice 2,  $N$ . Por la conexión de Galois, tenemos que  $\mathbb{C} \leqslant K^N$  es una extensión de grado 2, por lo que  $K^N = \mathbb{C}(\beta)$  para  $\beta \in K^N$  con  $\text{Irr}(\beta, \mathbb{C})$  de grado 2. Si tratamos de obtener las raíces de este polinomio, obtenemos que  $\beta \in \mathbb{C}$ , porque cada número complejo tiene sus raíces cuadradas en  $\mathbb{C}$ , contradicción, puesto que teníamos que  $\beta \in K^N \setminus \mathbb{C}$ , por lo que tenemos que  $|\text{Aut}_{\mathbb{C}}(K)| = 1$ , de donde por la conexión de Galois,  $K = \mathbb{C}$ .  $\square$

**Corolario 2.8.1.** *Si  $f \in \mathbb{R}[x]$  es irreducible, entonces  $\deg f \in \{1, 2\}$ .*

*Demostración.* Sea  $f \in \mathbb{R}[x]$  irreducible con  $\deg f \geqslant 2$ , el Teorema Fundamental del Álgebra nos permite tomar  $\alpha \in \mathbb{C}$  una raíz suya, de donde  $\bar{\alpha}$  también será una raíz de  $f$ . Tenemos así que  $(x - \alpha)(x - \bar{\alpha})$  divide a  $f$ , pero como  $f$  es irreducible tiene que ser asociado a  $(x - \alpha)(x - \bar{\alpha})$ , por lo que  $\deg f = 2$ .  $\square$

**Ejercicio 2.3.1.** Sea  $\overline{\mathbb{Q}}$  la clausura algebraica de  $\mathbb{Q}$  en  $\mathbb{C}$ . Razonar que todo polinomio no constante  $f \in \overline{\mathbb{Q}}[x]$  tiene todas sus raíces en  $\overline{\mathbb{Q}}$ .

## 2.4. Ejercicios

**Ejercicio 2.4.1.** Tomemos  $f = (x^3 - 2)(x^2 - 3) \in \mathbb{Q}[x]$  y su el cuerpo de descomposición de  $f$  sobre  $\mathbb{Q}$ .

- Decidir razonadamente si  $i + \sqrt{3} \in K$ .

El cuerpo de descomposición es:

$$K = \mathbb{Q} \left( \pm \sqrt{3}, \sqrt[3]{2}, w \sqrt[3]{2}, w^2 \sqrt[3]{2} \right)$$

donde:

$$w = -\frac{1}{2} + i \frac{\sqrt{3}}{2}$$

Tenemos entonces que  $\sqrt{3} \in K$  así como que:

$$w = \frac{w \sqrt[3]{2}}{\sqrt[3]{2}} \in K$$

Por lo que  $i\sqrt{3} \in K$ , de donde:

$$i = \frac{i\sqrt{3}}{\sqrt{3}} \in K$$

Por tanto, tenemos que  $i + \sqrt{3} \in K$ .

2. Calcular razonadamente  $[K : \mathbb{Q}]$ . Sabemos ya que:

$$\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}, i) \leq K$$

Y la otra inclusión la vemos viendo que todos los elementos que definen  $K$  se expresan con operaciones con estos tres, con lo que:

$$K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}, i)$$

Con vistas al Lema de la Torre, vemos:

$$[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})] [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$$

Donde el segundo vale 3 por Eisenstein y el primero es menor o igual que 2, por lo que en total es menor o igual que 6. Si lo miramos de otra forma:

$$[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$$

Tenemos que el segundo vale 2 por Eisenstein y el primero es menor o igual que 3. En definitiva, tenemos que  $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}] = 6$ . Ahora:

$$[K : \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})] = 2$$

Ya que  $x^2 + 1$  es irreducible en  $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$ , al no tener raíces en dicho cuerpo. En definitiva, el Lema de la Torre nos dice que:

$$[K : \mathbb{Q}] = 12$$

3. Describir los elementos del grupo  $\text{Aut}(K)$ .

$F \leq K$  es de Galois por ser  $K$  cuerpo de descomposición de  $f$  con  $\text{car}(F) = 0$ , por lo que:

$$|\text{Aut}(K)| = [K : F] = 12$$

Usamos varias veces la Proposición de Extensión. Calculamos primero las extensiones de la inclusión a  $\mathbb{Q}(\sqrt{3}) \xrightarrow{\eta_j} K$ . Las mismas están en correspondencia biyectiva con las raíces de  $\text{Irr}(\sqrt{3}, \mathbb{Q}) = x^2 - 3$  en  $K$ . A saber, son dos determinadas por:

$$\eta_j(\sqrt{3}) = (-1)^j \sqrt{3} \quad j \in \{0, 1\}$$

Análogamente, con la misma Proposición tenemos que cada  $\eta_j$  se extienden a 3 homomorfismos  $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) \rightarrow K$ , ya que las raíces de  $x^3 - 2 \in \mathbb{Q}(\sqrt{3})[x]$

en  $K$  son tres, a saber,  $\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}$ . Obsérvese que  $x^3 - 2 \in \mathbb{Q}(\sqrt{3})[x]$  es irreducible porque:

$$3 = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})]$$

Así, obtengo  $\eta_{j,k} : \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) \rightarrow K$ , determinados por:

$$\begin{aligned}\eta_{j,k}(\sqrt[3]{2}) &= w^k \sqrt{2} \\ \eta_{j,k}(\sqrt{3}) &= (-1)^j \sqrt{3} \quad j \in \{0, 1\}, \quad k \in \{0, 1, 2\}\end{aligned}$$

De la misma manera, extendiendo cada  $\eta_{j,k}$  según las raíces de  $x^2 + 1$ , obtengo que:

$$\text{Aut}(K) = \{\eta_{j,k,l} : j, l \in \{0, 1\}, k \in \{0, 1, 2\}\}$$

donde cada uno de ellos está determinado por:

$$\begin{aligned}\eta_{j,k,l}(\sqrt{3}) &= (-1)^j \sqrt{3} \\ \eta_{j,k,l}(\sqrt[3]{2}) &= w^k \sqrt[3]{2} \\ \eta_{j,k,l}(i) &= (-1)^l i\end{aligned}$$

4. Describir los elementos de  $\text{Aut}_{\mathbb{Q}(i+\sqrt{3})}(K)$  y decidir si es un subgrupo normal de  $\text{Aut}(K)$ .

Tenemos que el subgrupo enunciado es el correspondiente a la extensión

$$\mathbb{Q} \leqslant \mathbb{Q}(i + \sqrt{3})$$

$\mathbb{Q}$  es correspondiente con  $G$  y  $\mathbb{Q}(i + \sqrt{3})$  es correspondiente con  $H$ . Como  $[\mathbb{Q}(i + \sqrt{3}) : \mathbb{Q}] = 4$ , tenemos por la conexión de Galois que  $|H| = 3$ , por lo que buscamos:

$$i + \sqrt{3} = \eta_{j,k,l}(i + \sqrt{3}) = (-1)^l i + (-1)^j \sqrt{3}$$

si y solo si  $l = 0 = j$ , obtenemos 3 automorfismos, que son los únicos posibles para  $H$ . En definitiva:

$$\text{Aut}_{\mathbb{Q}(i+\sqrt{3})}(K) = \{\eta_{0,k,0} : k \in \{0, 1, 2\}\}$$

Que es normal, porque la extensión  $\mathbb{Q} \leqslant \mathbb{Q}(i + \sqrt{3})$  es de Galois. Veamos esto último, pues:

$$\mathbb{Q}(i + \sqrt{3}) = \mathbb{Q}(i, \sqrt{3})$$

por lo que  $\mathbb{Q}(i + \sqrt{3})$  es cuerpo de descomposición de  $(x^2 + 1)(x^2 - 3)$ .

**Ejercicio 2.4.2.** Sea  $K$  cuerpo de descomposición de  $f = (x^2 + 3)(x^3 - 3)$ .

1. Calcular todos los subcuerpos de  $K$ .

Las raíces de  $f$  son:

$$i\sqrt{3}, -i\sqrt{3}, \sqrt[3]{3}, w\sqrt[3]{3}, w^2\sqrt[3]{3}$$

donde:

$$w = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

Por lo que  $K = \mathbb{Q}(i\sqrt{3}, -i\sqrt{3}, \sqrt[3]{3}, w\sqrt[3]{3}, w^2\sqrt[3]{3})$ . Sin embargo, veamos que:

$$K = \mathbb{Q}(i\sqrt{3}, \sqrt[3]{3})$$

- $\subseteq$ ) Vemos que cada una de las raíces de  $f$  podemos expresarla como el resultado de una cuenta por operaciones cerradas para cuerpos en función de elementos de  $\mathbb{Q}$ ,  $i\sqrt{3}$  y  $\sqrt[3]{3}$ , por lo que tenemos esta inclusión.
- $\supseteq$ ) Es obvia.

Por el Lema de la Torre tenemos que:

$$[K : \mathbb{Q}] = [\mathbb{Q}(i\sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}] = [\mathbb{Q}(i\sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{3})] [\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}]$$

donde vemos fácilmente que:

- $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ , ya que  $\text{Irr}(\sqrt[3]{3}, \mathbb{Q}) = x^3 - 3$ , al ser un polinomio de grado 3 sin raíces en  $\mathbb{Z}$  o bien por Eisenstein para  $p = 3$ .
- $[\mathbb{Q}(i\sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{3})] = 2$ , ya que  $\text{Irr}(i\sqrt{3} : \mathbb{Q}(\sqrt[3]{3})) = x^2 + 3$ , por ser un polinomio de grado 2 sin raíces en  $\mathbb{Q}(\sqrt[3]{3})$  (sus raíces son complejas).

Por lo que  $[K : \mathbb{Q}] = 6$ . Como  $\text{car}(\mathbb{Q}) = 0$  y  $K$  es cuerpo de descomposición de  $f \in \mathbb{Q}[x]$  tenemos que la extensión  $\mathbb{Q} \leq K$  es de Galois, por lo que:

$$|\text{Aut}(K)| = 6$$

Por lo que el grupo de Galois de la extensión será isomorfo a  $C_6$  o a  $D_3$ .

Calculamos los elementos de  $\text{Aut}(K)$ , aplicando para ello dos veces la proposición de Extensión. Calculamos en primer lugar las extensiones de la inclusión a  $\mathbb{Q}(\sqrt[3]{3}) \xrightarrow{\eta_j} K$ , que están en correspondencia biyectiva con las raíces de:

$$\text{Irr}(\sqrt[3]{3}, \mathbb{Q}) = x^3 - 3$$

a saber,  $\sqrt[3]{3}, w\sqrt[3]{3}, w^2\sqrt[3]{3}$ , por lo que las extensiones obtenidas son las determinadas por:

$$\eta_j(\sqrt[3]{3}) = w^j \sqrt[3]{3} \quad j \in \{0, 1, 2\}$$

Análogamente, para cada  $\eta_j$  tenemos 2 extensiones suyas en automorfismos  $K \rightarrow K$ , puesto que estas están a su vez en correspondencia biyectiva con las raíces de:

$$\text{Irr}(i\sqrt{3}, \mathbb{Q}(\sqrt[3]{3})) = x^2 + 3$$

Que son  $\pm i\sqrt{3}$ , por lo que obtenemos en total 6 automorfismos, que son los determinados por:

$$\begin{aligned}\eta_{j,k} \left( \sqrt[3]{3} \right) &= w^j \sqrt[3]{3} \\ \eta_{j,k} \left( i\sqrt{3} \right) &= (-1)^k i\sqrt{3} \quad j \in \{0, 1, 2\}, k \in \{0, 1\}\end{aligned}$$

De donde:

$$\text{Aut}(K) = \{\eta_{j,k} : j \in \{0, 1, 2\}, k \in \{0, 1\}\}$$

Calculamos ahora los órdenes de cada uno de los elementos:

- Observamos que  $\eta_{0,0} = i_K$ , por lo que su orden es 1.
- Para  $\eta_{1,0}$ :

$$\begin{aligned}\sqrt[3]{3} &\longmapsto w\sqrt[3]{3} \longmapsto w^2\sqrt[3]{3} \longmapsto w^3\sqrt[3]{3} = \sqrt[3]{3} \\ i\sqrt{3} &\longmapsto i\sqrt{3}\end{aligned}$$

Donde hemos usado que como  $\eta_{1,0}(i\sqrt{3}) = i\sqrt{3}$  ha de ser por tanto  $\eta_{1,0}(w) = w$ , ya que:

$$w = \frac{-1}{2} + \frac{i\sqrt{3}}{2}$$

Por lo que el orden de  $\eta_{1,0}$  es 3.

- Para  $\eta_{2,0}$ :

$$\begin{aligned}\sqrt[3]{3} &\longmapsto w^2\sqrt[3]{3} \longmapsto w^4\sqrt[3]{3} = w\sqrt[3]{3} \longmapsto w^3\sqrt[3]{3} = \sqrt[3]{3} \\ i\sqrt{3} &\longmapsto i\sqrt{3}\end{aligned}$$

donde hemos vuelto a usar que como  $\eta_{2,0}(i\sqrt{3}) = i\sqrt{3}$  entonces  $\eta_{2,0}(w) = w$ . En definitiva, el orden es 3.

- Para  $\eta_{0,1}$ :

$$\begin{aligned}\sqrt[3]{3} &\longmapsto \sqrt[3]{3} \\ i\sqrt{3} &\longmapsto -i\sqrt{3} \longmapsto i\sqrt{3}\end{aligned}$$

Por lo que su orden es 2.

- Para  $\eta_{1,1}$ :

$$\begin{aligned}\sqrt[3]{3} &\longmapsto w\sqrt[3]{3} = \left( \frac{-1}{2} + \frac{i\sqrt{3}}{2} \right) \sqrt[3]{3} \longmapsto \bar{w}w\sqrt[3]{3} = |w|^2\sqrt[3]{3} = \sqrt[3]{3} \\ i\sqrt{3} &\longmapsto -i\sqrt{3} \longmapsto i\sqrt{3}\end{aligned}$$

Por lo que su orden es 2.

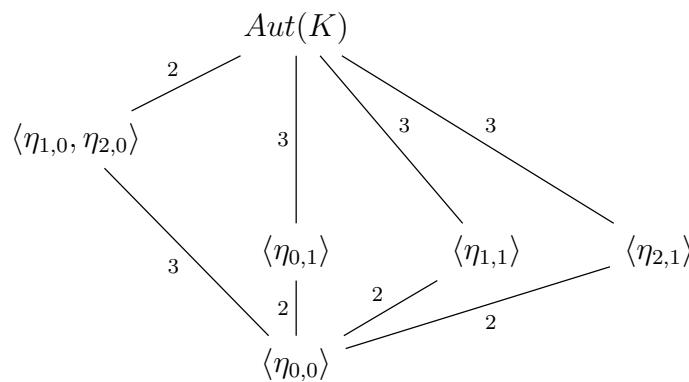
Tenemos por tanto:

$$\begin{array}{ccccccc} \eta_{0,0} & \eta_{1,0} & \eta_{2,0} & \eta_{0,1} & \eta_{1,1} & \eta_{2,1} \\ \hline 1 & 3 & 3 & 2 & 2 & \end{array}$$

Como  $C_6$  tiene 2 elementos de orden 6, descartamos automáticamente esta opción, por lo que tiene que ser  $|\text{Aut}(K)| \cong D_3$ , luego el orden del elemento que falta es 2.

$$\begin{array}{ccccccc} \eta_{0,0} & \eta_{1,0} & \eta_{2,0} & \eta_{0,1} & \eta_{1,1} & \eta_{2,1} \\ \hline 1 & 3 & 3 & 2 & 2 & 2 \end{array}$$

En este punto, es fácil conocer cada uno de los subgrupos de  $D_3$ :



Buscamos ahora identificar cada uno de los subgrupos no triviales de  $K$ , que sabemos que están en correspondencia biyectiva con los subgrupos no triviales de  $\text{Aut}(K)$ . En primer lugar observamos que ya conocemos dos subextensiones de  $\mathbb{Q} \leqslant K$ :

$$\mathbb{Q} \leqslant \mathbb{Q}\left(i\sqrt{3}\right), \quad \mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt[3]{3}\right)$$

La primera de grado 2 y la segunda de grado 3, por lo que sus respectivos subgrupos serán de orden 3 y 2, de forma respectiva. Como el único subgrupo de  $\text{Aut}(K)$  de orden 3 es  $\langle \eta_{1,0}, \eta_{2,0} \rangle$ , tenemos que este es el subgrupo correspondiente con  $\mathbb{Q}(i\sqrt{3})$ . Buscamos ahora qué subgrupo de  $\text{Aut}(K)$  se corresponde con  $\mathbb{Q}(\sqrt[3]{3})$ . Para ello, hemos de buscar el automorfismo  $\eta_{j,1}$  que deja fijo el elemento  $\sqrt[3]{3}$ . Esto es sencillo, pues el único que lo deja fijo es  $\eta_{0,1}$ . Es sencillo observar que también tenemos:

$$\mathbb{Q} \leqslant \mathbb{Q}\left(w\sqrt[3]{3}\right), \quad \mathbb{Q} \leqslant \mathbb{Q}\left(w^2\sqrt[3]{3}\right)$$

extensiones de grado 3, por lo que sus subgrupos correspondientes serán de grado 2. Veamos cuáles de ellos son:

- Para  $\mathbb{Q}(w^2\sqrt[3]{3})$ , veamos que  $\eta_{1,1}$  deja fijo a este elemento:

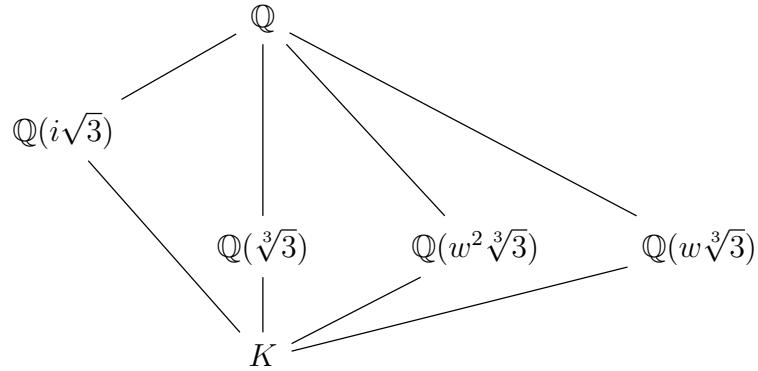
$$w^2\sqrt[3]{3} \mapsto \overline{w}w\sqrt[3]{3} = \overline{w}\sqrt[3]{3} = w^2\sqrt[3]{3}$$

Efectivamente.

- Para  $\mathbb{Q}(w\sqrt[3]{3})$ , veamos que  $\eta_{2,1}$  dejó fijo a dicho elemento:

$$w\sqrt[3]{3} \mapsto \overline{w}ww\sqrt[3]{3} = w\sqrt[3]{3}$$

En definitiva, los subcuerpos de  $K$  son:



- Demostrar que  $\mathbb{Q}(\sqrt[3]{3} + i\sqrt{3}) = K$ .

Para ello, veamos qué automorfismos  $\text{Aut}_{\mathbb{Q}}(K)$  dejan fijo al elemento  $\sqrt[3]{3}+i\sqrt{3}$ :

$$\begin{aligned} \sqrt[3]{3} + i\sqrt{3} &\xrightarrow{\eta_{1,0}} w\sqrt[3]{3} + i\sqrt{3} \\ \sqrt[3]{3} + i\sqrt{3} &\xrightarrow{\eta_{2,0}} w^2\sqrt[3]{3} + i\sqrt{3} \\ \sqrt[3]{3} + i\sqrt{3} &\xrightarrow{\eta_{0,1}} \sqrt[3]{3} - i\sqrt{3} \\ \sqrt[3]{3} + i\sqrt{3} &\xrightarrow{\eta_{1,1}} w\sqrt[3]{3} - i\sqrt{3} \\ \sqrt[3]{3} + i\sqrt{3} &\xrightarrow{\eta_{2,1}} w^2\sqrt[3]{3} - i\sqrt{3} \end{aligned}$$

Como vemos, ningún automorfismo salvo  $\eta_{0,0}$  deja fijo al elemento, por lo que:

$$\mathbb{Q}\left(\sqrt[3]{3} + i\sqrt{3}\right) \leq K^{\langle\eta_{1,1}\rangle} = K$$

Terminar el razonamiento.



# 3. Teoría de Galois de Ecuaciones

## 3.1. Grupo de Galois de un polinomio

A lo largo de este capítulo, consideraremos siempre polinomios mónicos, pues solo nos interesan las raíces de los polinomios.

**Definición 3.1.** Sea  $f \in F[x]$  no constante, mónico<sup>1</sup> y sean  $\alpha_1, \dots, \alpha_n$  sus raíces (repetidas tantas veces como indique su multiplicidad) en algún cuerpo de descomposición  $K$  de  $f$ . Se define el discriminante de  $f$  como:

$$\text{Disc}(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \in K$$

Resulta que  $\text{Disc}(f)$  se puede calcular a partir de los coeficientes del polinomio.

*Observación.* Vemos que  $f$  es separable  $\iff \text{Disc}(f) \neq 0$ .

**Notación.** Notaremos usualmente a la raíz del discriminante  $\text{Disc}(f)$  por:

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$$

**Notación.** Dado un conjunto  $S = \{\alpha_1, \dots, \alpha_n\}$ , denotaremos normalmente al grupo de permutaciones de dichos elementos por:

$$\text{Sim}(\alpha_1, \dots, \alpha_n)$$

Observemos que  $\text{Sim}(\alpha_1, \dots, \alpha_n) \cong S_n$ .

**Definición 3.2.** Si  $f \in F[x]$  es separable y  $K$  es su cuerpo de descomposición, diremos que  $\text{Aut}_F(K)$  es el grupo de Galois<sup>2</sup> de  $f$ .

Si  $f \in F[x]$  es separable y  $K$  es su cuerpo de descomposición, si consideramos  $\{\alpha_1, \dots, \alpha_n\}$  el conjunto de todas las raíces de  $f$  en  $K$ , podemos siempre definir un homomorfismo de grupos entre el grupo de Galois de  $f$  y el grupo de permutaciones de sus raíces:

$$\begin{aligned} \text{Aut}_F(K) &\longrightarrow \text{Sim}(\alpha_1, \dots, \alpha_n) \\ \sigma &\longmapsto \sigma|_{\{\alpha_1, \dots, \alpha_n\}} \end{aligned}$$

Tenemos que:

---

<sup>1</sup>Si no, su discriminante se define como cierto elemento de  $F$  multiplicado por la cantidad enunciada, pero no será relevante para nosotros.

<sup>2</sup>Observemos que por ser  $f$  separable y  $K$  cuerpo de descomposición suyo tenemos siempre por el Teorema 2.4 que la extensión  $F \leq K$  es de Galois.

- La aplicación está bien definida, pues si consideremos  $\sigma \in \text{Aut}_F(K)$ , tendremos siempre que  $\sigma^* = \sigma|_{\{\alpha_1, \dots, \alpha_n\}} \in \text{Sim}(\alpha_1, \dots, \alpha_n)$ , pues si  $\alpha_i$  es una raíz de  $f$  (para  $i \in \{1, \dots, n\}$ ) tendremos entonces que  $\sigma(\alpha_i)$  también es raíz de  $f$ :

$$f(\sigma(\alpha_i)) = \sum_{i=0}^n f_i(\sigma(\alpha_i))^i \stackrel{(*)}{=} \sigma \left( \sum_{i=0}^n f_i \alpha_i^i \right) = \sigma(f(\alpha_i)) = 0$$

donde en  $(*)$  hemos usado que  $\sigma \in \text{Aut}_F(K)$  y que  $f \in F[x]$ .

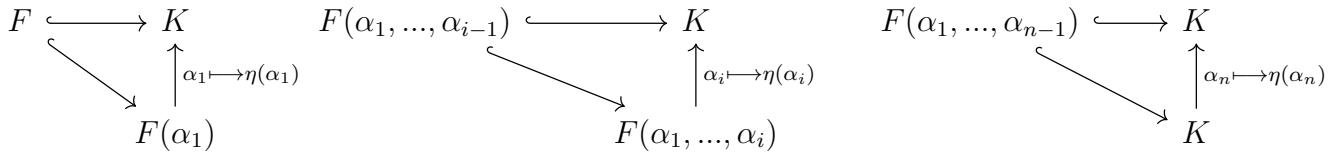
- La aplicación es un homeomorfismo, pues si  $\sigma, \tau \in \text{Aut}_F(K)$  tenemos entonces que:

$$(\sigma\tau)|_{\{\alpha_1, \dots, \alpha_n\}} = \sigma|_{\{\alpha_1, \dots, \alpha_n\}} \tau|_{\{\alpha_1, \dots, \alpha_n\}}$$

Además dicho homomorfismo de grupos es siempre inyectivo, pues la Proposición de Extensión nos dice que cada automorfismo del grupo de Galois queda únicamente determinado por la imagen de cada raíz de  $f$ , puesto que sabemos que el grupo de Galois de  $f$  coincide con las extensiones de la inclusión:

$$\text{Aut}_F(K) = \text{Ex}(\iota, \iota)$$

Si pensamos en la obtención de todos los elementos del grupo de Galois de  $f$  mediante el siguiente procedimiento:



observamos que cada uno de ellos queda determinado por cada una de las elecciones hechas sobre cada una de las imágenes de cada raíz. De esta forma, si tenemos que dos elementos  $\sigma, \tau \in \text{Aut}_F(K)$  coinciden en  $\{\alpha_1, \dots, \alpha_n\}$ , tendremos entonces que  $\sigma = \tau$ , lo que nos prueba la inyectividad del homomorfismo de grupos.

De esta forma, como  $\text{Sim}(\alpha_1, \dots, \alpha_n) \cong S_n$ , podemos ver siempre el grupo de Galois de  $f$  como subgrupo de  $S_n$ , aquel que permuta los índices de las raíces de  $f$ :

$$\alpha_i \xrightarrow{\sigma} \alpha_{\sigma(i)}$$

**Notación.** En vista de la relación existente entre  $\text{Aut}_F(K)$  (el grupo de Galois de cierto polinomio  $f \in F[x]$ ),  $\text{Sim}(\alpha_1, \dots, \alpha_n)$  (el grupo de permutaciones sobre sus raíces) y  $S_n$ , será habitual identificar  $\text{Sim}(\alpha_1, \dots, \alpha_n)$  con  $S_n$ , y ver  $\text{Aut}_F(K)$  directamente como subgrupo de  $S_n$ . Este uso de la notación no debe llevar a errores, pues simplemente es una forma más rápida de enunciar ciertas propiedades sobre  $\text{Aut}_F(K)$ .

*Observación.* Si tomamos  $\sigma \in \text{Aut}_F(K)$ , una vez visto que  $\sigma$  actuando sobre las raíces del polinomio  $f$  simplemente las permuta, vemos fácilmente que:

- $\sigma(\text{Disc}(f)) = \text{Disc}(f)$ .

- $\sigma(\Delta(f)) = \text{sgn}(\sigma)\Delta(f)$ .

**Proposición 3.1.** Sea  $f \in F[x]$  separable con grupo de Galois  $G = \text{Aut}_F(K)$ , entonces  $\text{Disc}(f) \in F$ . Además:

$$K^{G \cap A_n} = F(\Delta(f))$$

Por tanto,  $\Delta(f) \in F \iff G < A_n$ .

*Demostración.* Para ver que  $\text{Disc}(f) \in F$ , vimos en el primer punto de la observación superior que:

$$\sigma(\text{Disc}(f)) = \text{Disc}(f) \quad \forall \sigma \in G$$

Por lo que tenemos que  $\text{Disc}(f) \in K^G$ , pero como  $F \leqslant K$  es de Galois, tenemos que  $K^G = F$ .

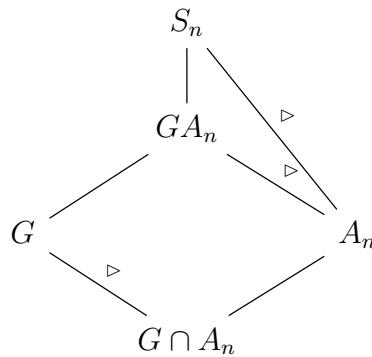
Para ver que  $K^{G \cap A_n} = F(\Delta(f))$ , en vista del segundo punto de la observación superior:

$$\sigma(\Delta(f)) = \text{sgn}(\sigma)\Delta(f) \quad \forall \sigma \in G$$

Tenemos que  $\Delta(f) \in K^{G \cap A_n}$ , y como todo elemento de  $G$  es  $F$ -lineal es claro que  $F(\Delta(f)) \leqslant K^{G \cap A_n}$ . Si estudiamos el índice de este subcuerpo de  $K$ , la conexión de Galois nos dice que:

$$[K^{G \cap A_n} : F] = (G : G \cap A_n) \stackrel{(*)}{\leqslant} (S_n : A_n) = 2$$

donde en (\*) hemos usado el Segundo Teorema de Isomorfía para grupos:



Por tanto, solo tenemos dos situaciones posibles ante  $F \leqslant F(\Delta(f)) \leqslant K^{G \cap A_n}$ :

$$F(\Delta(f)) = F \quad \text{o} \quad F(\Delta(f)) = K^{G \cap A_n}$$

- Si  $F(\Delta(f)) = F$ , tendremos entonces que  $\Delta(f) \in F$ , así como que:

$$\text{sgn}(\sigma)\Delta(f) = \sigma(\Delta(f)) = \Delta(f)\sigma(1) = \Delta(f) \quad \forall \sigma \in G$$

Por lo que  $G \leqslant A_n$ , de donde:

$$K^{G \cap A_n} = K^G = F = F(\Delta(f))$$

- Si  $F(\Delta(f)) = K^{G \cap A_n}$ , tendremos entonces que  $\Delta(f) \notin F$ , por lo que:

$$sgn(\sigma)\Delta(f) = \sigma(\Delta(f)) \neq \Delta(f) \quad \forall \sigma \in G$$

Por lo que  $sgn(\sigma) = -1$ , de donde  $G \not\leq A_n$ .

□

En relación al enunciado de la Proposición anterior, se suele hacer referencia a la condición “ $\Delta(f) \in F$ ” por “Disc( $f$ ) es un cuadrado en  $F$ ”.

**Ejercicio 3.1.1.** Sea  $f \in \mathbb{R}[x]$  mónico con  $\deg f = 3$ , discutir el número de raíces reales de  $f$  según el signo de Disc( $f$ ).

Distinguimos casos:

- Si Disc( $f$ ) = 0 tenemos entonces que  $f$  tiene alguna raíz múltiple, por lo que tienen que ser todas sus raíces reales.
- Si Disc( $f$ ) < 0, si fueran todas las raíces de  $f$  reales, digamos  $\alpha, \beta, \gamma \in \mathbb{R}$  tendríamos entonces que:

$$\text{Disc}(f) = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 > 0$$

contradicción, por lo que  $f$  debe tener alguna raíz compleja  $\alpha \in \mathbb{C}$ , por lo que  $\bar{\alpha} \in \mathbb{C}$  también es raíz y debe tener alguna raíz real.

- Si Disc( $f$ ) > 0, si  $\alpha \in \mathbb{C} \setminus \mathbb{R}$  fuera una raíz de  $f$  tendríamos entonces que  $\bar{\alpha}$  también sería una raíz de  $f$ , de donde si  $\beta \in \mathbb{R}$  es la última raíz de  $f$  tendríamos que:

$$\text{Disc}(f) = (\alpha - \bar{\alpha})^2(\alpha - \beta)^2(\bar{\alpha} - \beta)^2$$

supuesto que  $\alpha = a + ib$  para  $a, b \in \mathbb{R}$ , tenemos entonces que:

$$\bullet \quad \alpha - \bar{\alpha} = 2ib \implies (\alpha - \bar{\alpha})^2 = (2ib)^2 = -4b^2 < 0$$

• Por otra parte:

$$(\alpha - \beta)^2(\bar{\alpha} - \beta)^2 = ((\alpha - \beta)(\bar{\alpha} - \beta))^2$$

y tenemos que:

$$\begin{aligned} (\alpha - \beta)(\bar{\alpha} - \beta) &= ((a + ib) - \beta)((a - ib) - \beta) = ((a - \beta) + ib)((a - \beta) - ib) \\ &= (a - \beta)^2 + b^2 > 0 \end{aligned}$$

de donde Disc( $f$ ) < 0, contradicción, por lo que  $f$  tiene que tener en este caso 3 raíces reales.

**Ejemplo.** Consideramos  $f = x^n + \sum_{i=0}^{n-1} a_i x^i \in F[x]$  y sean  $\alpha_1, \dots, \alpha_n$  sus raíces (repetidas según multiplicidad), tenemos que:

$$f = \prod_{i=1}^n (x - \alpha_i)$$

Igualando coeficientes de igual grado, obtenemos las relaciones de Cardano-Vieta<sup>3</sup>. Por ejemplo, si  $n = 2$  se obtiene:

$$a_0 = \alpha_1 \alpha_2 \quad a_1 = -(\alpha_1 + \alpha_2)$$

Como  $\text{Disc}(f) = (\alpha_1 - \alpha_2)^2$ , tenemos que  $\text{Disc}(f) = a_1^2 - 4a_0$ .

Para  $n > 2$ , la cuenta no es tan sencilla, por lo que se prefiere usar un algoritmo para resolver el sistema de ecuaciones. En definitiva, se puede expresar  $\text{Disc}(f)$  en términos de los coeficientes de  $f$ . Para  $n = 3$ , la damos para  $f = x^3 + px + q$  (cúbica reducida<sup>4</sup>) es:

$$\text{Disc}(f) = -4p^3 - 27q^2$$

**Proposición 3.2.** *Sea  $f \in F[x]$  separable con grupo de Galois  $G$*

$$f \text{ es irreducible} \iff G \text{ actúa transitivamente sobre las raíces de } f$$

*En tal caso,  $\deg f$  divide a  $|G|$ .*

*Demostración.* Sea  $K$  el cuerpo de descomposición de  $f$ , tenemos que  $G = \text{Aut}_F(K)$ .

$\implies$  Si  $f$  es irreducible y  $\alpha, \beta \in K$  son raíces de  $f$ , podemos ( $f = \text{Irr}(\alpha, F)$ ) usar la Proposición de extensión, obteniendo  $\sigma : F(\alpha) \rightarrow K$  de forma que  $\sigma(\alpha) = \beta$ .

La tercera proposición de extensión nos dice que  $\sigma$  puede extenderse a un automorfismo  $\eta \in G$  y  $\eta(\alpha) = \sigma(\alpha) = \beta$ , por lo que la acción es transitiva.

$\iff$  Sea  $g$  un factor irreducible de  $f$  (ambos mónicos), tenemos que  $g$  no es constante, con lo que sus raíces son también de  $f$ . Sea  $\alpha \in K$  una raíz de  $g$ , tenemos que  $\sigma(\alpha)$  es raíz de  $g$  para todo  $\sigma \in G$ , y como  $G$  actúa transitivamente sobre las raíces de  $f$ , vemos que toda raíz de  $f$  también es de  $g$ , con lo que  $f = g$ , de donde  $f$  es irreducible.

Finalmente, para ver que  $\deg f$  divide a  $|G|$ , si  $\alpha$  es raíz de  $f$ , tenemos entonces  $[F(\alpha) : F] = \deg f$ , que divide a  $[K : F]$  por el Lema de la Torre, y  $|G| = [K : F]$ .  $\square$

**Corolario 3.2.1.** *Por tanto, a la hora de buscar el grupo de Galois de un polinomio irreducible, descartaremos automáticamente los subgrupos de  $S_n$  no transitivos.*

**Ejemplo.** Sea  $f \in F[x]$  separable e irreducible:

1. Si  $\deg f = 1$ , su grupo de Galois es la identidad, como único elemento de  $S_1$ .
2. Si  $\deg f = 2$ , el cuerpo de Galois de  $f$  tiene grado 1 o 2. Si  $f$  es irreducible, ha de ser de grado 2, con lo que su grupo de Galois es isomorfo a  $C_2$  (observemos que  $S_2 \cong C_2$ ).
3. Si  $\deg f = 3$ , la Proposición anterior nos dice que bien  $G \cong A_3$  o  $G \cong S_3$ . La Proposición 3.1 nos dice que tenemos el primer caso si  $\Delta(f) \in F$  y el segundo si  $\Delta(f) \notin F$ .

---

<sup>3</sup>Hay una teoría desarrollada sobre esto, siempre se obtienen funciones simétricas en las raíces del polinomio.

<sup>4</sup>Sin término cuadrático.

4. Si  $\deg f = 4$ , la Proposición anterior nos dice que  $G$  es isomorfo a un subgrupo transitivo de  $S_4$ .

**Ejemplo.** Sea  $f \in F[x]$  polinomio separable e irreducible de grado  $\deg f = 4$ , sean  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$  las raíces de  $f$  en un cuerpo de descomposición  $K$  de  $f$ , consideramos:

$$\begin{aligned}\beta_1 &= \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ \beta_2 &= \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ \beta_3 &= \alpha_1\alpha_4 + \alpha_2\alpha_3\end{aligned}$$

y definimos:

$$g = (x - \beta_1)(x - \beta_2)(x - \beta_3) \in K[x]$$

Veamos que en realidad  $g \in F[x]$ . Para ello, como  $F \leq K$  es de Galois, hemos de ver que el polinomio es fijo por todos los automorfismos del grupo de Galois de  $f$  (basta verlo para todas las permutaciones). Concluimos que  $g^\sigma = g \quad \forall \sigma \in G$ , con lo que  $g$  es una resolvente cónica de  $f$  (se verá).

Se puede ver por el algoritmo mencionado anteriormente que si  $f = x^4 + bx^3 + cx^2 + dx + e$ , entonces:

$$g = x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2$$

Consultamos si sus raíces son distintas:

$$\beta_2 - \beta_1 = (\alpha_2 - \alpha_3)(\alpha_4 - \alpha_1)$$

Por lo que  $\beta_2$  y  $\beta_1$  son distintas (análogo para el resto de las parejas), con lo que  $g$  es separable, luego  $E = F(\beta_1, \beta_2, \beta_3)$  es una extensión de Galois de  $F$ , con  $F \leq E \leq K$ , de donde el grupo de Galois de  $g$ ,  $N = \text{Aut}_E(K)$  es normal en  $G$ . Por lo que:

$$\text{Aut}_F(E) \cong \frac{G}{N}$$

Consideramos  $S : \text{Sim}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \rightarrow \text{Sim}(\beta_1, \beta_2, \beta_3)$  una aplicación de forma que:

$$S(\sigma)(\alpha_i\alpha_j + \alpha_k\alpha_l) = \alpha_{\sigma(i)}\alpha_{\sigma(j)} + \alpha_{\sigma(k)}\alpha_{\sigma(l)}$$

que es un homomorfismo de grupos y es sobreyectivo (ya que dada una trasposición en el grupo de la derecha, podemos encontrar un elemento en la izquierda cuya imagen vaya a él). Calculamos su núcleo:

$$\ker S = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Y sabemos que son todas porque el grupo de la derecha tiene 6 elementos y el de la izquierda 24; con lo que  $\ker S = V$  ( $r$  es la restricción, viene del teorema que habla sobre subgrupos normales). Donde  $N$  es el núcleo, ya que  $N$  es  $\text{Aut}_E(K)$ .

$$\begin{array}{ccccccc}
 1 & \longrightarrow & V & \longrightarrow & \text{Sim}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) & \xrightarrow{s} & \text{Sim}(\beta_1, \beta_2, \beta_3) \longrightarrow 1 \\
 & & \uparrow & & \curvearrowright & & \uparrow \\
 1 & \longrightarrow & N & \hookrightarrow & G & \xrightarrow{r} & \text{Aut}_F(E) \longrightarrow 1
 \end{array}$$

Donde los homomorfismos que suben son los que ven el dominio como cuerpo de descomposición y el otro contiene las raíces.

De aquí deducimos que:

$$N = V \cap G$$

Ya que tomamos  $\sigma \in G$  y lo vemos en  $\text{Aut}_F(E)$ , las raíces  $\beta$  las permutará, pero por otra parte,  $\sigma$  sabe actuar sobre  $\text{Sim}(\alpha_1, \dots, \alpha_4)$ , que las permuta, y teníamos que:

$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$$

- $\subseteq$ ) SI tomamos alguien de  $N$  tenemos que va a la permutación trivial en  $\text{Sim}(\beta)$ , pero estos están en  $V$ .
- $\supseteq$ ) Si alguien está en  $G \cap V$ , al aplicarle  $s$  caerá en  $V$ , y usamos ahora que el camino es comunitativo, obteniendo que está en el núcleo de  $r$ .

**Ejemplo.** Si tenemos  $f = x^4 + x + 1 \in \mathbb{Q}[x]$ , no tiene raíces en  $\mathbb{Q}$  (las únicas posibles son  $-1$  y  $1$ ). Como  $f \in \mathbb{Z}[x]$  y  $f$  es primitivo, reducimos módulo 2, obteniendo:

$$\bar{f} = x^4 + x + 1 \in \mathbb{Z}_2[x]$$

$\bar{f}$  no tiene raíces y si fuera irreducible, tendríamos entonces que es producto del único polinomio irreducible de  $\mathbb{Z}_2[x]$  que es  $x^2 + x + 1$ , pero no lo es, por lo que  $f$  es irreducible sobre  $\mathbb{Z}[x]$ , luego sobre  $\mathbb{Q}[x]$  también. Sea  $G$  el grupo de Galois de  $f$  sobre  $\mathbb{Q}$ , tenemos que  $G$  es un subgrupo transitivo de  $S_4$ , así como que  $|G|$  es un múltiplo de  $\deg f = 4$ . Los transitivos de  $S_4$  son:

- Los cíclicos de 4 elementos.
- Un Klein, de entre los 3 isomorfos a Klein uno es transitivo y dos no.

Como ejemplo de esto:

$$V = \{(1 2)(3 4), (1 3)(2 4), (1 4)(2 3), 1\}$$

es transitivo pero:

$$\{(1), (1 2), (3 4), (1 2)(3 4)\}$$

es isomorfo a Klein pero no es transitivo (desde 1 no podemos llegar a 3).

- De 8 elementos tenemos los diédricos, que hay varios.
- $A_4$ .

Anteriormente vimos que si  $f = x^4 + bx^3 + cx^2 + dx + e$  entonces su resolvente tenía el aspecto:

$$g = x^3 - cx^2 + (bd - 4e)x - b^2 + 4ce - d^2$$

Para nuestro  $f$  la resolvente cúbica es:

$$g = x^3 - 4x - 1$$

Si  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$  son raíces de  $f$  y  $\beta_1, \beta_2, \beta_3$  son las de  $g$ , teníamos entonces que:

$$\beta_2 - \beta_1 = (\alpha_2 - \alpha_3)(\alpha_4 - \alpha_1)$$

más otras dos relaciones. Usando estas, se demuestra que  $\text{Disc}(f) = \text{Disc}(g)$ . Además,  $g$  es una cónica reducida, y teníamos una fórmula para calcular  $\text{Disc}(g)$ , obteniendo que:

$$\text{Disc}(f) = \text{Disc}(g) = 229$$

Y tenemos que  $\sqrt{229} \notin \mathbb{Q}$ , ya que esto sucede si  $x^2 - 229 \in \mathbb{Q}[x]$  es irreducible, porque 229 es primo (se comprueba tratando de dividir entre primos hasta la parte entera de  $\sqrt{229}$ , que es 15). Como  $\sqrt{229} \notin \mathbb{Q}$ , tenemos que  $G \not\subseteq A_4$ , por lo que no puede ser el isomorfo a Klein ni  $A_4$ .

En estas condiciones, teníamos una subextensión:

$$\mathbb{Q} \leqslant E = \mathbb{Q}(\beta_1, \beta_2, \beta_3) \leqslant K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$$

Como  $\mathbb{Q} \leqslant K$  es de Galois, tenemos que  $E \leqslant K$  es de Galois, y la conexión nos dice que:

$$\text{Aut}_E(K) \triangleleft G$$

Veamos qué aspecto tiene  $\text{Aut}_E(K)$ , para reducir las opciones sobre  $G$ , de hecho:

$$\frac{G}{\text{Aut}_E(K)} \cong \text{Aut}_{\mathbb{Q}}(E)$$

Como  $g$  no tiene raíces (ya que las únicas posibles raíces son  $\pm 1$ ) y es de grado 3 tenemos que  $g$  es irreducible, por lo que  $|\text{Aut}_{\mathbb{Q}}(E)|$  es múltiplo de  $\deg g = 3$ , con lo que solo puede ser 3 o 6. Como el único posible grupo  $G$  que es divisible entre 3 es la opción  $G \cong S_4$ . Buscamos ahora  $\text{Aut}_E(K)$ , que ha de ser  $V$ .

Respecto al tema anterior ganamos que no es necesario calcular de forma explícita cada uno de los automorfismos.

## 3.2. Extensiones ciclotómicas

Para  $n \geqslant 1$ , a lo largo de este capítulo nos interesarán el polinomio  $x^n - 1 \in F[x]$ , para  $F \leqslant K$  cualquier extensión.

**Proposición 3.3.** *Si  $n \geqslant 1$  y consideramos como  $S$  el conjunto de todas las raíces de  $x^n - 1 \in F[x]$  en  $K$  para  $F \leqslant K$  cualquier extensión, tenemos que  $S$  es un subgrupo cíclico de  $K^\times$  cuyo orden es un divisor de  $n$ .*

*Demostración.* Sean  $\alpha, \beta \in S$ , tenemos que:

$$\alpha^n - 1 = 0 = \beta^n - 1 \implies \alpha^n = 1 = \beta^n$$

Y observamos ahora que:

$$(\alpha\beta^{-1})^n - 1 = (\alpha^n\beta^{-n}) - 1 = (1 \cdot 1) - 1 = 0$$

Por lo que  $\alpha\beta^{-1} \in S$ , de donde  $S$  es un subgrupo de  $K^\times$ . Sabemos que  $S$  es un subgrupo cíclico de  $K^\times$  por el Ejercicio 1.7.10. Además, su orden ha de dividir a  $n$ , pues todos los elementos tienen orden un divisor de  $n$ :  $\alpha^n = 1 \quad \forall \alpha \in S$ .  $\square$

El subgrupo cíclico de las raíces será de orden  $n$  si  $K$  contiene un cuerpo de descomposición de  $x^n - 1$  y si  $x^n - 1$  es separable, es decir, si  $n$  no es múltiplo de  $\text{car}(F)$ . En este contexto, llamamos a las raíces de  $x^n - 1$  raíces  $n$ -ésimas de la unidad, que es un grupo cíclico de orden  $n$  si  $x^n - 1$  es separable, por lo que lo supondremos en general. A sus generadores los llamamos raíces  $n$ -ésimas primitivas de la unidad.

**Ejemplo.** En característica cero, podemos suponer sin pérdida de generalidad que  $F = \mathbb{Q}$ , por lo que obtenemos las conocidas raíces  $n$ -ésimas primitivas de la unidad en  $\mathbb{C}$ .

En Álgebra I se vió que<sup>5</sup>  $|\mathcal{U}(\mathbb{Z}_n)| = \varphi(n)$ , sea  $\zeta$  una raíz  $n$ -ésima primitiva de la unidad, tenemos que el conjunto de todas las raíces  $n$ -ésimas de la unidad es:

$$\{\zeta^k : k \in \mathbb{Z}_n\}$$

Y las raíces  $n$ -ésimas primitivas de la unidad son:

$$\{\zeta^k : k \in \mathcal{U}(\mathbb{Z}_n)\}$$

De esta forma, el cuerpo de descomposición de  $x^n - 1 \in F[x]$  es  $F(\zeta)$ , que recibe el nombre  $n$ -ésima extensión ciclotómica de  $F$ , y como mucho es:

$$[F(\zeta) : F] \leq n - 1$$

Puesto que  $x^n - 1$  siempre tiene a 1 como raíz.

**Proposición 3.4.** *Sea  $x^n - 1 \in F[x]$  separable, tiene grupo de Galois  $G$  isomorfo a un subgrupo de  $\mathcal{U}(\mathbb{Z}_n)$ . Además,  $G$  es isomorfo a  $\mathcal{U}(\mathbb{Z}_n)$  si y solo si actúa transitivamente sobre las raíces  $n$ -ésimas primitivas de la unidad (sobre  $F$ ).*

*Demostración.* Sea  $\zeta$  una raíz primitiva de la unidad, tenemos que:

$$G = \text{Aut}_F(F(\zeta))$$

donde  $F(\zeta)$  es la  $n$ -ésima extensión ciclotómica de  $F$ . Habíamos visto que las raíces  $n$ -ésimas primitivas de la unidad son:

$$\{\zeta^k : k \in \mathcal{U}(\mathbb{Z}_n)\}$$

---

<sup>5</sup>Donde  $\varphi$  es la función de Euler.

Sea  $\sigma \in G$ , tenemos que  $\sigma(\zeta) = \zeta^k$  para cierto  $k \in \mathcal{U}(\mathbb{Z}_n)$ . Podemos definir

$$\begin{array}{ccc} : & G & \longrightarrow \mathcal{U}(\mathbb{Z}_n) \\ & \sigma & \longmapsto k \end{array}$$

donde se cumple que:

$$\sigma(\zeta) = \zeta^k$$

Si tomamos  $\sigma, \tau \in G$  de forma que  $\tau(\zeta) = \zeta^l$  con  $l \in \mathcal{U}(\mathbb{Z}_n)$ , tenemos que:

$$\sigma\tau(\zeta) = \sigma(\zeta^l) = \sigma(\zeta)^l = (\zeta^k)^l = \zeta^{kl}$$

Con lo que la aplicación considerada es un homomorfismo de grupos, que además es inyectivo por su definición. Tenemos pues que  $G$  es isomorfo a cierto subgrupo de  $\mathcal{U}(\mathbb{Z}_n)$ . Esta aplicación será sobreyectiva si para cada exponente tenemos un automorfismo, con lo que  $G$  actuará transitivamente sobre estas raíces.  $\square$

**Definición 3.3** (Polinomio ciclotómico). Sea  $F$  un cuerpo, definimos el  $n$ -ésimo polinomio ciclotómico como:

$$\phi_n = \prod_{k \in \mathcal{U}(\mathbb{Z}_n)} (x - \zeta^k)$$

con  $\zeta$  una raíz  $n$ -ésima primitiva de la unidad.

**Proposición 3.5.** *Se tiene que:*

$$x^n - 1 = \prod_{d \in \text{Div}(n)} \phi_d$$

*Demostración.* Consideramos como  $R_n$  el conjunto de todas las raíces de  $x^n - 1$  (es decir, el conjunto de todas las raíces  $n$ -ésimas de la unidad). Si consideramos también  $P_m$ , el conjunto de las raíces  $m$ -ésimas primitivas de la unidad, tenemos una partición de  $R_n$ :

$$R_n = \biguplus_{d \in \text{Div}(n)} P_d$$

Como:

$$x^n - 1 = \prod_{\alpha \in R_n} (x - \alpha)$$

y cada  $\alpha$  está en un cierto  $P_d$ , ha de estar en  $\phi_d$ , con lo que:

$$x^n - 1 = \prod_{\alpha \in R_n} (x - \alpha) = \prod_{d \in \text{Div}(n)} \phi_d$$

$\square$

**Proposición 3.6.** *Cada  $\phi_n$  tiene coeficientes en el subcuerpo primo de  $F$  y además, si  $\text{car}(F) = 0$ , tenemos que  $\phi_n \in \mathbb{Z}[x]$ .*

*Demostración.* Por inducción sobre  $n$ :

- Si  $n = 1$ , entonces  $\phi_1 = x - 1$  y se tiene la Proposición.

- Si  $n > 1$ , tenemos:

$$x^n - 1 = \phi_n \cdot \prod_{\substack{d \in \text{Div}(n) \\ d < n}} \phi_d$$

Por hipótesis de inducción, tenemos que el producto de la derecha está en el subcuerpo primo de  $F$ . Tenemos además que  $\phi_n$  es cociente de  $x^n - 1$  entre el producto de la derecha, con lo que  $\phi_n$  también ha de tener coeficientes en el subcuerpo primo de  $F$ .

Si  $\text{car}(F) = 0$ , sabemos por lo ya probado que  $\phi_n \in \mathbb{Q}[x]$ . Si expresamos sus coeficientes como fracciones irreducibles y tomamos  $a \in \mathbb{Z}$  el mínimo común múltiplo de sus denominadores, tenemos que  $a\phi_n \in \mathbb{Z}[x]$ , con todos sus coeficientes coprimos entre sí, luego  $a\phi_n$  es primitivo. Tenemos pues que:

$$a(x^n - 1) = a\phi_n \prod_{\substack{d \in \text{Div}(n) \\ d < n}} \phi_d$$

de nuevo por inducción, suponemos ahora que los polinomios  $\phi_d$  son primitivos (para  $n = 1$  es claro que  $\phi_1$  es primitivo). Por el Lema de Gauss, tenemos que:

$$\prod_{\substack{d \in \text{Div}(n) \\ d < n}} \phi_d$$

es primitivo y con coeficientes en  $\mathbb{Z}$ , si recordamos que  $a\phi_n$  es primitivo, de donde todo el producto es primitivo, es decir,  $a(x^n - 1)$  es primitivo, luego ha de ser  $a = 1$ .  $\square$

**Ejemplo.** En característica cero:

$$\phi_1 = x - 1, \quad \phi_2 = x + 1, \quad \phi_3 = x^2 + x + 1, \quad \phi_4 = x^2 + 1$$

Para  $\phi_6$  usamos la fórmula:

$$\phi_6 = \frac{x^6 - 1}{\phi_1 \phi_2 \phi_3} = x^2 - x + 1$$

**Teorema 3.7.** *Cada  $\phi_n \in \mathbb{Z}[x]$  es irreducible.*

*Demostración.* Sea  $f$  un factor irreducible de  $\phi_n$ . Tomamos  $\zeta$  una raíz compleja de  $f$  en la  $n$ -ésima extensión ciclotómica. Probemos que si  $p$  es primo y no divide a  $n$ , entonces  $\zeta^p$  es raíz de  $f$ . Por reducción al absurdo, tomamos  $g$  con:

$$\phi_n = fg \quad f, g \in \mathbb{Z}[x]$$

Y ha de cumplir  $g(\zeta^p) = 0$ . Resulta que  $\zeta$  es raíz de  $h = g(x^p) \in \mathbb{Z}[x]$ . De esta forma,  $f$  y  $h$  tienen una raíz común compleja, y la identidad de Bezout nos dice entonces que  $f$  y  $h$  no son coprimos. Como  $f$  es irreducible, ha de ser  $f \mid h$ . Como  $f$  es primitivo, tenemos que  $f \mid h$  en  $\mathbb{Z}[x]$ . Reducimos módulo  $p$ :

$$\overline{\phi_n} = \overline{f}\overline{g}$$

y tenemos:

$$\bar{h} = \overline{g(x^p)} \stackrel{(*)}{=} \overline{g(x)}^p = \bar{g}^p$$

donde (\*) es porque como  $f \mid h$  en  $\mathbb{Z}[x]$ , tenemos que  $\bar{f} \mid \bar{h}$ , pero como  $\bar{h} = \bar{g}^p$ . Como  $\mathbb{F}_p[x]$  es DFU, tenemos que  $\bar{f}$  y  $\bar{g}$  tienen algún factor común no constante. Deducimos que  $\overline{x^n - 1}$  tiene una raíz múltiple en su cuerpo de descomposición. Sin embargo,  $p$  no divide a  $n$ , por lo que:

$$\overline{x^n - 1} = x^n - 1$$

y este polinomio es separable, contradicción; por lo que para cada  $p$  primo que no divide a  $n$  tenemos que  $\zeta^p$  es raíz de  $f$ . Si tomamos  $n$  y lo factorizamos en primos, miramos los primos que no dividen a  $n$ , con lo que tomando estos primos nos movemos dentro de las unidades de  $\mathbb{Z}_n$ , con lo que en alguna cantidad finita de pasos rellenamos todas las unidades de  $\mathbb{Z}_n$ . Por lo que todas las raíces de  $\phi_n$  son raíces de  $f$ . Como  $f$  dividía a  $\phi_n$ ,  $f = \phi_n$ .  $\square$

Hemos visto ya que el  $n$ -ésimo polinomio ciclotómico  $\phi_n \in \mathbb{Z}[x]$  es irreducible.  $\mathbb{Q}(\zeta)$ , la  $n$ -ésima extensión ciclotómica con  $\zeta \in \mathbb{C}$  la raíz  $n$ -ésima primitiva de la unidad. Así,  $\text{Irr}(\zeta, \mathbb{Q}) = \phi_n$ . Sabemos que  $\text{Aut}(\mathbb{Q}(\zeta))$  actúa transitivamente sobre las raíces de  $\phi_n$ .

Esto significa que  $|\text{Aut}(\mathbb{Q}(\zeta))| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \phi_n = \varphi(n)$ . Además, tenemos que  $\text{Aut}(\mathbb{Q}(\zeta)) \cong \mathcal{U}(\mathbb{Z}_n)$ .

**Ejemplo.** Para  $n = 16$ :

$$\deg \phi_n = \varphi(16) = 8$$

Por lo que tenemos que:

$$\text{Aut}(\mathbb{Q}(\zeta)) \cong \mathcal{U}(\mathbb{Z}_{16})$$

### 3.3. Construcciones con regla y compás II

A lo largo de la sección, consideraremos siempre que  $S$  es un subconjunto de  $\mathbb{C}$  con  $\{0, 1\} \subseteq S$ . Además, consideraremos siempre también  $F = \mathbb{Q}(S \cup \bar{S})$ .

**Teorema 3.8.** *Sea  $z \in \mathbb{C}$ , tenemos que:*

$$\begin{aligned} z \text{ es constructible a partir de } S &\iff z \in K, \text{ donde } F \leqslant K \text{ es de Galois y} \\ &[K : F] = 2^k, \text{ para cierto } k \in \mathbb{N}. \end{aligned}$$

*Demostración.* Por doble implicación:

$\implies$ ) Sé que existe una torre de subcuerpos de  $\mathbb{C}$ :

$$F = F_0 \leqslant F_1 \leqslant \dots \leqslant F_s$$

tales que  $F_{i+1} = F(\alpha_{\alpha_i+1})$ , con  $\alpha_{i+1}^2 \in F_i$ , para todo  $i \in \{0, \dots, s-1\}$ ; con  $z \in F_s$ . Por inducción sobre  $s$ :

- Para  $s = 0$ , tenemos que  $F_s = F_0$ , por lo que tomamos  $K = F_0$ , que trivialmente es de Galois.
- Supongamos como hipótesis de inducción que existe una extensión de Galois  $F \leqslant E$  con grado una potencia de 2 y tal que  $F_{s-1} \leqslant E$ . Llamamos  $a_s = \alpha_s^2 \in F_{s-1}$ , y enumeramos los elementos:

$$\text{Aut}_F(E) = \{\sigma_0, \dots, \sigma_t\}$$

Y definimos el polinomio:

$$f = \prod_{j=0}^t (x^2 - \sigma_j(a_s))$$

Que resulta ser un polinomio con coeficientes en  $E$ , pero queda fijo por cualquier automorfismo de la extensión de Galois, por lo que en realidad tenemos que  $f \in F[x]$ .

Como  $F \leqslant E$  es de Galois, tenemos que  $E$  es cuerpo de descomposición de cierto  $g \in F[x]$ . Tomamos como  $K$  el cuerpo de descomposición de  $fg$ , por lo que  $F \leqslant K$  es de Galois. Definimos  $\alpha_{s+j}$  como la raíz de  $x^2 - \sigma_j(a_s)$ , para cada  $j \in \{0, \dots, t\}$ , por lo que  $\alpha_{s+j} \in K$ .

Tenemos que:

$$K = E(\alpha_s, \alpha_{s+1}, \dots, \alpha_{s+t})$$

Puesto que las raíces de  $g$  ya están en  $E$ . Como el grado de  $\alpha_{s+j}$  es 1 o 2 (al ser raíz de  $x^2 - \sigma_j(a_s)$ ), tenemos que  $F \leqslant K$  tiene grado una potencia de 2. Ahora, como  $F_s \leqslant K$ , tenemos que  $z \in F_s \leqslant K$ , para completar la inducción.

- $\Leftarrow$ ) Tomamos  $z \in K$  con  $F \leqslant K$  de Galois y  $[K : F]$  una potencia de 2. Tenemos por tanto que  $\text{Aut}_F(K)$  es un 2-grupo, luego es resoluble<sup>6</sup>. Podemos por tanto tomar una serie de composición suya, obteniendo:

$$\text{Aut}_F(K) = G_0 \geqslant G_1 \geqslant \dots \geqslant G_n = \{id\}$$

con factores de composición 2. La conexión de Galois nos transforma esta cadena en una cadena de extensiones de subcuerpos cuadráticas:

$$F = K_0 \leqslant K_1 \leqslant \dots \leqslant K_n = K \tag{3.1}$$

con  $[K_{i+1} : K_i] = 2$ , para cada  $i \in \{0, \dots, n-1\}$ , por lo que:

$$K_{i+1} = K_i(\beta_i) \quad \text{con} \quad \beta_i = \frac{-b_i \pm \sqrt{b_i^2 - 4c_i}}{2}$$

en el caso de que  $\text{Irr}(\beta_i, K_i) = x^2 + b_i x + c_i$ . De esta forma:

$$K_{i+1} = K_i \left( \sqrt{b_i^2 - 4c_i} \right)$$

Por tanto, tenemos que (3.1) es una torre por raíces cuadradas, con lo que  $z$  es constructible a partir de  $S$ .

---

<sup>6</sup>Por ser un  $p$ -grupo.

$n$	Es constructible
3	Sí
4	Sí
5	Sí
6	Sí
7	No
8	Sí
9	No
10	Sí
11	No
12	No
13	No
14	No
15	Sí
16	Sí
17	Sí

Tabla 3.1: Qué polígonos regulares son constructibles.

□

Sabemos que el heptágono no es constructible, puesto que  $\text{Irr}(\sqrt[7]{algo}, \mathbb{Q})$  es de grado 6, al ser  $\varphi(7) = 6$ , que no es una potencia de 2.

**Corolario 3.8.1.** *Un polígono regular de  $n$  lados es constructible (con regla y compás) si y solo si  $\varphi(n)$  es una potencia de 2.*

*Demostración.* Decir que un polígono regular de  $n$  lados es constructible es equivalente a decir que una raíz primitiva  $n$ -ésima de la unidad es constructible. Por tanto, hemos de ver que  $\zeta$  es constructible (como raíz primitiva  $n$ -ésima de la unidad) si y solo si existe  $\mathbb{Q} \leq K$  de forma que  $[K : \mathbb{Q}]$  es una potencia de 2.

Sabemos que  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ .

$\Rightarrow$ ) Si  $\zeta$  es constructible, existe una extensión de Galois  $\mathbb{Q} \leq K$  de grado 2 que contiene a  $\zeta$ , luego ha de contener a  $\mathbb{Q}(\zeta)$ :  $\mathbb{Q}(\zeta) \leq K$ , de donde por el Lema de la Torre ha de ser  $\varphi(n)$  una potencia de 2.

$\Leftarrow$ ) Si tomamos  $K = \mathbb{Q}(\zeta)$  se tiene.

□

De esta forma:

Si  $n$  es primo, tenemos que  $\varphi(n) = n - 1$ , que es una potencia de 2 si y solo si el primo es de la forma  $2^{algo} + 1$ . Haciendo la cuenta, tiene que ser:

$$n = 2^{2^m} + 1$$

- $m = 0, 3$
- $m = 1, 5$

- $m = 2, 17$
- $m = 3$ , algo
- $m = 4, 65$  mil y pico

Sin embargo, todavía no se ha encontrado un primo más de esta forma, los llamados primos de Fermat

### 3.4. Extensiones cíclicas

**Teorema 3.9.** *Sea  $x^n - a \in F[x]$  separable siendo  $K$  su cuerpo de descomposición. Entonces  $K$  contiene una raíz  $n$ -ésima primitiva de la unidad  $\zeta$  y  $K = F(\zeta, r)$  para cualquier raíz  $r$  de  $x^n - a$ .*

*Además, el grupo de Galois de la extensión  $F(\zeta) \leq K$  es cíclico de orden un divisor de  $n$ .*

*Demostración.* Si  $a = 0$ , si  $x^n$  es separable ha de ser  $n = 1$ , con lo que  $K = F$  y una raíz  $n$ -ésima primitiva de la unidad es 1, se trivializa el enunciado. Suponemos por tanto que  $a \neq 0$ , con lo que  $n$  puede ser cualquiera distinto de  $\text{car}(F)$ . Sea  $R$  el conjunto de las raíces en  $K$  de  $x^n - a$ , tenemos que  $|R| = n$ , puesto que  $x^n - a$  es separable. Además, si  $r, s \in R$ , tenemos que  $r^{-1}s \in K$  es una raíz  $n$ -ésima de la unidad.

Fijado  $r$ , entonces el conjunto  $\{r^{-1}s : s \in R\}$  contiene  $n$  raíces  $n$ -ésimas de la unidad, por lo que en dicho conjunto las tenemos todas, luego ha de contener al menos una raíz primitiva de la unidad, llamémosla  $\zeta \in K$ .

Para la segunda afirmación, tenemos que:

$$K = F(\zeta, r)$$

Puesto que  $\zeta$  genera  $\{r^{-1}s : s \in R\}$  y al multiplicar por  $s$  obtenemos  $r$ .

Para ver que el grupo de Galois es cíclico, representemos el grupo de manera sencilla. Para ello, tomamos  $\sigma \in \text{Aut}_{F(\zeta)}(K)$ . Como  $\sigma$  toma una raíz de  $x^n - a$ , la lleva en otra raíz y el conjunto de todas las raíces es:

$$R = \{r, \zeta r, \dots, \zeta^{n-1}r\}$$

Por lo que tendremos  $\sigma(r) = \zeta^j r$  para cierto  $j \in \mathbb{Z}_n$ . Si tuviéramos que  $\sigma(r) = \zeta^{j'} r$  para  $j' \neq j$ , como  $r$  es una raíz primitiva de la unidad tenemos entonces que  $j = j'$ , por lo que observamos una dependencia  $j \mapsto \sigma$ , que nos da una aplicación  $j : \text{Aut}_{F(\zeta)}(K) \rightarrow \mathbb{Z}^n$ . Podemos ver  $j$  como un homomorfismo de grupos, considerando  $\mathbb{Z}^n$  como grupo aditivo. Para ello, tomamos  $\sigma, \tau \in \text{Aut}_{F(\zeta)}(K)$  y tenemos que  $j(\sigma\tau) \in \mathbb{Z}_n$  está determinado por la condición:

$$(\sigma\tau)(r) = \zeta^{j(\sigma\tau)}r$$

Y tenemos que:

$$(\sigma\tau)(r) = \sigma(\tau(r)) = \sigma(\zeta^{j(\tau)}r) = \zeta^{j(\tau)}\sigma(r) = \zeta^{j(\tau)}\zeta^{j(\sigma)}r = \zeta^{j(\tau)+j(\sigma)}r$$

De donde  $j(\sigma\tau) = j(\sigma) + j(\tau)$ , por lo que  $j$  es un homomorfismo de grupos. Además tenemos que  $j$  es inyectivo, pues si  $j(\sigma) = 0$ , tendríamos por tanto que  $\sigma(r) = \zeta^0 r$ , de donde  $\sigma = id$ , por lo que  $\ker j = \{id\}$ . Tenemos por tanto que  $\text{Aut}_{F(\zeta)}(K)$  es isomorfo a un subgrupo de  $\mathbb{Z}_n$ , por lo que ha de ser cíclico y por el Teorema de Lagrange, de orden menor un divisor de  $n$ .  $\square$

**Corolario 3.9.1.** *Sea  $x^n - a \in F(\zeta)[x]$ , es irreducible si y solo si  $[K : F(\zeta)] = n$ .*

*Demostración.* Por doble implicación:

- $\Leftarrow)$  En este caso tenemos que  $j$  es sobreyectivo, por lo que  $j$  es un isomorfismo, de donde todo elemento de  $\mathbb{Z}_n$  proviene de un automorfismo, con lo que el conjunto  $R$  es transitivo.
- $\Rightarrow)$   $\square$

**Definición 3.4** (Extensiones cíclica). Una extensión  $F \leq K$  se dice cíclica si es de Galois y su grupo de Galois es cíclico.

*Observación.* Observemos que tanto las extensiones de cuerpos finitos como las extensiones como las del último Teorema son extensiones cíclicas:

- Ejemplo.**
- Si  $F$  contiene una raíz  $n$ -ésima primitiva de la unidad y  $x^n - a \in F[x]$  es separable, entonces para  $K$  un cuerpo de descomposición de  $x^n - a$  tenemos que  $F \leq K$  es cíclica.
  - Esto se debe a que el  $\zeta$  del Teorema está ya en  $F$ , y tenemos que  $\text{Aut}_F(K)$  es subgrupo de un grupo cíclico por el monomorfismo  $j$ .
  - Toda extensión de cuerpos finitos es cíclica.

**Lema 3.10** (de independencia de Dedekind). *Sean  $\sigma_1, \dots, \sigma_n : F \rightarrow E$  homomorfismos de cuerpos distintos. Tenemos entonces que  $\sigma_1, \dots, \sigma_n$  son linealmente independientes. Es decir, si  $\lambda_1, \dots, \lambda_n \in E$  es tal que:*

$$\lambda_1\sigma_1(x) + \dots + \lambda_n\sigma_n(x) = 0 \quad \forall x \in F \quad \Rightarrow \quad \lambda_1 = \dots = \lambda_n = 0$$

*Demostración.* Si  $n = 1$  es cierto. Suponemos que  $n > 1$  y razonamos por reducción al absurdo. Para ello, tomamos de entre todas las posibles elecciones de  $\lambda_1, \dots, \lambda_n$  aquella lista de ellos contengan  $m$  elementos no nulos. Reordenando, podemos suponer que:

$$\begin{aligned} \lambda_i &\neq 0 & \forall i \in \{1, \dots, m\} \\ \lambda_i &= 0 & \forall i > m \end{aligned}$$

Tenemos que  $m \geq 2$ . Como  $\sigma_1 \neq \sigma_m$ , existe  $y \in F$  de forma que  $\sigma_1(y) \neq \sigma_m(y)$ , de donde:

$$\lambda_1\sigma_1(yx) + \dots + \lambda_m\sigma_m(yx) = 0$$

Y obtenemos restando la cadena anterior con  $n = m$ :

$$\lambda_1(\sigma_1(y) - \sigma_m(y))\sigma_1(x) + \dots + \lambda_{m-1}(\sigma_{m-1}(y) - \sigma_m(y))\sigma_{m-1}(x) = 0 \quad \forall x \in F$$

Y tenemos que  $\sigma_m(y)$  no es cero, pero hemos llegado a una contradicción, pues tenemos  $\lambda_1, \dots, \lambda_{m-1}$  una lista de números menor.  $\square$

**Teorema 3.11.** *Sea  $F \leq K$  extensión cíclica tal que  $n = [K : F]$  no es múltiplo de  $\text{car}(F)$ . Si  $F$  contiene una raíz  $n$ -ésima primitiva de la unidad, entonces  $K$  es cuerpo de descomposición de un polinomio irreducible de la forma  $x^n - a \in F[x]$ . Además, si  $\alpha$  es una raíz de  $x^n - a$  entonces  $K = F(\alpha)$ .*

*Demostración.* El grupo de automorfismos debe ser cíclico de grado  $n$ , por lo que tendrá un generador  $\sigma \in \text{Aut}_F(K)$  de orden  $n$ . El Lema de independencia de Dedekind nos dice que ha de existir  $r \in K$  de forma que (si  $\zeta \in F$  es una raíz  $n$ -ésima primitiva de la unidad):

$$\beta := r + \zeta\sigma(r) + \dots + \zeta^{n-1}\sigma^{n-1}(r) \neq 0$$

Tendremos entonces que:

$$\zeta\sigma(\beta) = \beta$$

Por lo que:

$$\beta^n = \zeta^n\sigma(\beta)^n = \sigma(\beta)^n = \sigma(\beta^n)$$

como  $\sigma$  genera todo  $\text{Aut}_F(K)$  tenemos que  $a := \beta^n \in K^{\text{Aut}_F(K)} = F$ . Como  $\zeta^n = 1$ , tenemos que:

$$\beta, \zeta\beta, \dots, \zeta^{n-1}\beta$$

son todas raíces distintas de  $x^n - a$ , y tenemos  $n$ , de donde:

$$x^n - a = (x - \beta)(x - \zeta\beta)\dots(x - \zeta^{n-1}\beta)$$

Y como  $\zeta \in F$ , tenemos que  $F(\beta)$  es cuerpo de descomposición de  $x^n - a \in F[x]$ . Como el orden de  $\beta$  es menor o igual que  $n$ ,  $[F(\beta) : F] \leq n$ , y para conseguir la igualdad tenemos que:

$$\sigma^k(\beta) = \zeta^{-k}\beta$$

Por lo que la acción de  $\text{Aut}_F(K)$  sobre las raíces de  $x^n - a$  es transitiva, por lo que  $x^n - a$  es irreducible, de donde  $[F(\beta) : F] = n$ . Tenemos en definitiva que  $F(\beta) = K$ .  $\square$

**Ejemplo.** Si consideramos  $x^8 - 3 \in \mathbb{Q}[x]$ , si metemos una raíz octava primitiva de la unidad tenemos que su grupo de Galois es cíclico. Sea  $K \leq \mathbb{C}$  su cuerpo de descomposición, sabemos por el Teorema de ayer que  $K = \mathbb{Q}(\sqrt[8]{3}, \zeta)$ , con  $\zeta$  una raíz octava primitiva de la unidad. Esta podemos calcularla como una raíz cuadrada de  $i$ , que es una raíz cuarta de la unidad. Tomamos una de ellas:

$$\zeta = e^{i\frac{\pi}{4}} = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$$

Como el octavo polinomio ciclotómico tiene grado  $\varphi(8) = 4$ , tenemos que la extensión  $\mathbb{Q} \leq \mathbb{Q}(\zeta)$  es de grado 4. Si consideramos ahora  $\zeta + \bar{\zeta} \in \mathbb{Q}(\zeta)$ :

$$\zeta + \bar{\zeta} = 2\text{Re}(\zeta) = \sqrt{2} \in \mathbb{Q}(\zeta)$$

De donde  $\mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\zeta)$ , por lo que  $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta)$ .

Calculamos el grado de la extensión  $[K : \mathbb{Q}]$ , para saber el cardinal de  $\text{Aut}_F(K)$ . Por el Lema de la Torre:

$$[K : \mathbb{Q}] = \left[ \mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i) : \mathbb{Q}(\sqrt[8]{3}, \sqrt{2}) \right] \left[ \mathbb{Q}(\sqrt{2}, \sqrt[8]{3}) : \mathbb{Q}(\sqrt[8]{3}) \right] \left[ \mathbb{Q}(\sqrt[8]{3}) : \mathbb{Q} \right]$$

Donde el último grado es 8 por ser 3 primo y aplicar Eisenstein. La primera es 2 por ser  $i \notin \mathbb{R}$ . La segunda es 2 si y solo si  $\sqrt{2} \notin \mathbb{Q}(\sqrt[8]{3})$ .

Consideramos:

$$\mathbb{Q} \leqslant \mathbb{Q}(\sqrt{3}) \leqslant^2 \mathbb{Q}(\sqrt[4]{3}) \leqslant^2 \mathbb{Q}(\sqrt[8]{3})$$

Y como  $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[8]{3})$  es de grado 8, tienen que ser todas estas de grado 2. Veamos:

- $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$ , puesto que si esto fuera así,  $\sqrt{2} = a + b\sqrt{3}$ , elevamos al cuadrado y sale que  $\sqrt{3}$  es racional, que no es posible porque  $x^2 - 3$  es irreducible.
- $\sqrt{2} \notin \mathbb{Q}(\sqrt[4]{3})$ , usando que una  $\mathbb{Q}(\sqrt{3})$ -base es  $\{1, \sqrt[4]{3}\}$ , si  $\sqrt{2} \in \mathbb{Q}(\sqrt[4]{3})$  tendríamos entonces que  $\exists a, b \in \mathbb{Q}(\sqrt{3})$  de manera que:

$$\sqrt{2} = a + b\sqrt[4]{3}$$

Elevando al cuadrado:

$$2 = a^2 + 2ab\sqrt[4]{3} + b^2\sqrt{3} \implies \begin{cases} 2 = a^2 + b^2\sqrt{3} \\ 0 = 2ab \end{cases}$$

igualando coordenadas a coordenadas, por lo que:

- Si  $b = 0$ , entonces  $2 = a^2$ , de donde  $\sqrt{2} = a \in \mathbb{Q}(\sqrt{3})$ , pero ya habíamos visto que este caso no puede ser.
- Si  $a = 0$ , entonces  $2 = b^2\sqrt{3}$  para  $b = x + y\sqrt{3}$  con  $x, y \in \mathbb{Q}$ , luego:

$$2 = (x^2 + 2xy\sqrt{3} + 3y^2)\sqrt{3}$$

Y tenemos que  $\{1, \sqrt{3}\}$  es una  $\mathbb{Q}$ -base de  $\mathbb{Q}(\sqrt{3})$ , por lo que igualdando coordenadas:

$$0 = x^2 + 3y^2 \implies x = 0 = y$$

Luego  $b = 0 \implies 2 = 0$  contradicción, que viene de suponer que teníamos  $\sqrt{2} \in \mathbb{Q}(\sqrt[4]{3})$ .

- Intentamos ver ahora que  $\sqrt{2} \notin \mathbb{Q}(\sqrt[8]{3})$ . Por reducción al absurdo, si  $\sqrt{2} \in \mathbb{Q}(\sqrt[8]{3})$ , tenemos que  $\{1, \sqrt[8]{3}\}$  es una  $\mathbb{Q}(\sqrt[4]{3})$ -base, por lo que existirían  $c, d \in \mathbb{Q}(\sqrt[4]{3})$  de forma que:

$$\sqrt{2} = c + d\sqrt[8]{3}$$

con  $d \neq 0$ , por el apartado anterior. Elevando al cuadrado:

$$2 = c^2 + 2cd\sqrt[8]{3} + d^2\sqrt[4]{3}$$

Igualando coordenadas en la base obtenemos que ( $d \neq 0$ )  $c = 0$ , por lo que:

$$2 = d^4 \sqrt[4]{3}$$

Escribimos las coordenadas de  $d$ :

$$d = z + t \sqrt[4]{3} \quad z, t \in \mathbb{Q}(\sqrt{3})$$

De donde elevando al cuadrado:

$$2 = (z^2 + 2zt\sqrt[4]{3} + t^2\sqrt{3})\sqrt[4]{3}$$

Igualando coordenadas:

$$0 = z^2 + t^2\sqrt{3} \implies z = 0 = t$$

lo que nos lleva a una contradicción.

En definitiva,  $[K : \mathbb{Q}] = 32$ , de donde el grupo cíclico es de orden 8.

### 3.5. Ecuaciones resolubles por radicales

Las definiciones de este apartado dependen mucho del autor.

La siguiente definición generaliza el concepto de extensión por raíces cuadradas:

**Definición 3.5.** Una extensión de cuerpos  $F \leqslant E$  se llamará una extensión por radicales cuando existe una torre de cuerpos

$$F = E_0 \leqslant E_1 \leqslant \dots \leqslant E_t = E$$

tal que  $E_j = E_{j-1}(\alpha_j)$ , con  $\alpha_j^{n_j} \in E_{j-1}$ , para  $j \in \{1, \dots, t\}$ .

**Definición 3.6.** Un polinomio  $f \in F[x]$  se dice resoluble por radicales si existe una extensión por radicales  $F \leqslant E$  que contiene al cuerpo de descomposición de  $f$ .

**Supondremos** que siempre trabajaremos en  $\text{car}(F) = 0$ , para simplificar los enunciados siguientes. Es posible hacerlo para  $\text{car}(F) \neq 0$ , pero entonces los enunciados se complican.

**Definición 3.7.** Una extensión  $F \leqslant K$  es radical si  $K$  es cuerpo de descomposición de un polinomio  $x^n - a \in F[x]$  y  $F$  contiene una raíz  $n$ -ésima primitiva de la unidad.

Bajo estas condiciones, toda extensión radical es cíclica, y toda cíclica da una radical. Y como estamos en  $\text{car}(F) = 0$ , no hace falta hipótesis sobre que  $x^n - a$  sea separable.

**Definición 3.8.** Diremos que una extensión  $F \leqslant K$  es radical iterada si hay una torre de cuerpos

$$F = K_0 \leqslant K_1 \leqslant \dots \leqslant K_t = K$$

de forma que cada  $K_{i-1} \leqslant K_i$  es radical, para  $i \in \{1, \dots, t\}$ .

**Proposición 3.12.** Si  $F \leqslant E$  es una extensión de Galois, supongamos una extensión  $E \leqslant E(\alpha)$  para  $\alpha$  raíz de  $x^n - a \in E[x]$ ,  $a \neq 0$ . Entonces existe una extensión radical iterada  $E(\zeta) \leqslant K$  tal que  $F \leqslant K$  es de Galois y  $E(\alpha) \leqslant K$ , para  $\zeta$  una raíz  $n$ -ésima primitiva de la unidad.

*Demostración.* Consideramos:

$$f = \prod_{\sigma \in \text{Aut}_F(E)} (x^n - \sigma(a)) \in E[x]$$

Como  $f^\tau = f \quad \forall \tau \in \text{Aut}_F(E)$ , tenemos que en realidad  $f \in F[x]$ .  $E$  es cuerpo de descomposición de  $g \in F[x]$ . Sea  $K$  el cuerpo de descomposición de  $fg \in F[x]$ . Como  $f \in F[x]$ , es claro que  $E(\alpha) \leqslant K$ , al tomar  $\sigma = id$ .

Como  $x^n - a$  es un factor de  $f$ ,  $K$  ha de contener un cuerpo de descomposición de  $x^n - a$ ; por lo que podemos encontrar en  $K$  una raíz  $n$ -ésima primitiva de la unidad,  $\zeta$ . Si enumeramos los elementos de  $\text{Aut}_F(E)$ :

$$\text{Aut}_F(E) = \{\sigma_1, \dots, \sigma_s\}$$

con  $\sigma_1 = id_E$ . Tomando  $K_{-1} = E$  y  $K_0 = E(\zeta)$ , para cada  $i \in \{1, \dots, s\}$  tomamos  $K_i = K_{i-1}(\alpha_i)$ , con  $\alpha_i$  raíz de  $x^n - \sigma_i(a)$ .

De esta forma, cada  $K_{i-1} \leqslant K_i$  es radical para  $i \geqslant 1$ . Además,  $F \leqslant K$  es claramente de Galois.  $\square$

En cierto momento, usaremos la siguiente observación:

*Observación.* Sea  $F$  un cuerpo, dados  $\sigma_1 : F \rightarrow L_1$ ,  $\sigma_2 : F \rightarrow L_2$  dos homomorfismos de cuerpos tales que las extensiones  $\sigma_i(F) \leqslant L_i$  para  $i \in \{1, 2\}$  son finitas. Tomamos los polinomios  $f_1, f_2 \in F[x]$  tales que el cuerpo de descomposición de cada  $f_i^{\sigma_i}$  venga dado por  $\tau_i : L_i \rightarrow K_i$ , para  $i \in \{1, 2\}$ . Tenemos  $\tau : F \rightarrow E$ , cuerpo de descomposición de  $f_1 f_2$ .

La Tercera Proposición de Extensión obtenemos el diagrama de homomorfismos de cuerpos

$$\begin{array}{ccccc} F & \xrightarrow{\sigma_1} & L_1 & \xrightarrow{\tau_1} & K_1 \\ \downarrow \sigma_2 & \searrow & \downarrow \tau_2 & \nearrow \tau & \downarrow \eta_1 \\ L_2 & & K_2 & & E \\ \downarrow \tau_2 & & \downarrow \eta_2 & & \\ K_2 & \xrightarrow{\eta_2} & E & & \end{array}$$

de manera que (cada triángulo conmuta):

$$\tau = \eta_1 \tau_1 \sigma_1 = \eta_2 \tau_2 \sigma_2$$

De esta forma, como cada homomorfismo de cuerpos es inyectivo:

$$F \cong \text{Im } \tau = \tau(F) \leqslant \eta_i \tau_i(L_i) \leqslant E \quad \forall i \in \{1, 2\}$$

**Definición 3.9.** Una extensión  $F \leq K$  se dice radical si  $K$  es cuerpo de descomposición de un polinomio separable de la forma  $x^n - a \in F[x]$ .

Es decir, como  $\text{car}(F) = 0$ , es equivalente a decir que  $a \neq 0$ .

Más aún, se dice que es radical iterada si:

$$F = K_0 \leq K_1 \leq \dots \leq K_t = K$$

con  $K_{i-1} \leq K_i$  radical, para cada  $i \in \{1, \dots, t\}$  y  $F \leq K$  de Galois.

**Proposición 3.13.** Si  $F \leq E$  es de Galois y  $E \leq E(\alpha)$  para  $\alpha$  raíz de  $x^n - a \in E[x]$  con  $a \neq 0$ , entonces existe una extensión radical iterada  $E \leq K$  con  $E(\alpha) \leq K$  y  $F \leq K$  de Galois.

**Proposición 3.14.** Sea  $F \leq E$  una extensión por radicales, entonces existe una extensión radical iterada  $F \leq K$  tal que  $E \leq K$ .

*Demostración.* Suponemos pues que tenemos una torre:

$$F = E_0 \leq E_1 \leq \dots \leq E_t = E$$

tal que  $E_j = E_{j-1}(\alpha_j)$  con  $\alpha_j$  raíz de  $x^{n_j} - a_j \in E_{j-1}[x]$ ,  $j \in \{1, \dots, t\}$ . Razonamos por inducción sobre  $t \geq 0$ :

- Para  $t = 0$ , tomamos  $F = E = K$ .
- Para  $t > 0$ , por hipótesis de inducción tenemos que existe una extensión radical iterada

$$F = K_0 \leq K_1 \leq \dots \leq K_r$$

tal que  $E_{t-1} \leq K_r$ . Tomamos una  $F$ -extensión común de  $K_r$  y  $E_t$ , dentro de la cual esté  $K_r(\alpha_t)$ . Tenemos que  $E_t \leq K_r(\alpha_t)$ . Por la Proposición anterior aplicada a la extensión  $F \leq K_r$  de Galois, tenemos que existe una extensión radical iterada  $K_r \leq K$  tal que  $K_r(\alpha_t) \leq K$  y  $F \leq K$  es de Galois.

Tenemos una torre de cuerpos

$$K_r \leq K_{r+1} \leq \dots \leq K_s$$

con  $K_{i-1} \leq K_i$  radical para cada  $i \in \{r+1, \dots, s\}$ . Tenemos entonces que:

$$F = K_0 \leq K_1 \leq \dots \leq K_r \leq K_{r+1} \leq \dots \leq K_j = K$$

con cada  $K_{k-1} \leq K_k$  radical para  $k \in \{1, \dots, s\}$  y  $F \leq K$  de Galois. De aquí tenemos que  $F \leq K$  es radical iterada y  $E \leq K$ .

□

**Lema 3.15.** Toda extensión radical iterada tiene grupo de Galois resoluble.

*Demostración.* Veamos que si  $F \leq K$  es radical entonces  $\text{Aut}_F(K)$  es resoluble. Si  $F \leq K$  es radical entonces  $K$  es cuerpo de descomposición de  $x^n - a \in F[x]$  separable, por lo que contiene una raíz  $n$ -ésima primitiva de la unidad  $\zeta \in K$ . Tenemos por tanto:

$$F \leq F(\zeta) \leq K$$

Con  $F(\zeta) \leq K$  de Galois por ser  $F \leq K$  de Galois ( $F \leq K$  es radical) y  $F \leq F(\zeta)$  de Galois por ser una extensión ciclotómica (que siempre son de Galois). Usando ahora la conexión de Galois, tenemos entonces que:

$$\{id_K\} \triangleleft \text{Aut}_{F(\zeta)}(K) \triangleleft \text{Aut}_F(K)$$

y además:

$$\frac{\text{Aut}_F(K)}{\text{Aut}_{F(\zeta)}(K)} \cong \text{Aut}_F(F(\zeta))$$

Como  $\text{Aut}_F(F(\zeta))$  es el grupo de Galois de una extensión ciclotómica, tiene que ser abeliano, por lo que el factor  $\text{Aut}_{F(\zeta)}(K) \triangleleft \text{Aut}_F(K)$  da un cociente abeliano. Ahora, tenemos que  $\text{Aut}_{F(\zeta)}(K)$  es cíclico, luego el factor  $\{id_K\} \triangleleft \text{Aut}_{F(\zeta)}(K)$  también es abeliano. En definitiva, tenemos que  $\text{Aut}_F(K)$  es resoluble, ya que admite una serie de composición con factores simples abelianos.

Si ahora:

$$F = K_0 \leq K_1 \leq \dots \leq K_t = K$$

es radical iterada, tendremos entonces que  $F \leq K$  es de Galois por definición, así como que cada extensión intermedia es de Galois, por ser cuerpo de descomposición de un polinomio separable. Usando ahora la conexión de Galois, obtenemos una serie de grupos:

$$\text{Aut}_F(K) = \text{Aut}_{K_0}(K) \triangleright \text{Aut}_{K_1}(K) \triangleright \dots \triangleright \text{Aut}_{K_{t-1}}(K) \triangleright \{id_K\}$$

Veamos ahora que:

$$\frac{\text{Aut}_{K_{i-1}}(K)}{\text{Aut}_{K_i}(K)} \cong \text{Aut}_{K_{i-1}}(K_i)$$

con este resoluble, ya que la extensión  $K_{i-1} \leq K_i$  es de Galois, y hemos visto que estas tienen grupo de Galois resoluble. En definitiva, obtenemos que  $\text{Aut}_F(K)$  es resoluble.  $\square$

**Ejercicio 3.5.1.** Sea  $f \in F[x]$  y  $L$  cuerpo de descomposición de  $f \in F[x]$ , si  $F \leq E$  es una extensión, demostrar que para  $K$  cuerpo de descomposición de  $f \in E[x]$  se tiene que:

$$\text{Aut}_E(K) \text{ es isomorfo a un subgrupo de } \text{Aut}_F(L).$$

Es claro que  $L \leq K$ , como  $K$  está generado sobre  $F$  por las raíces de  $f$ , los generadores que necesitamos obtener para obtener  $K$  son los mismos. Si tomamos  $\sigma \in \text{Aut}_E(K)$ , lleva  $\alpha_i$  en  $\alpha_j$  y deja fijos a los elementos de  $L$ . Estamos llevando un elemento de  $L$  en otro de  $L$ . Se considera la aplicación restricción.

**Teorema 3.16** (Gran Teorema de Galois). *Sea  $f \in F[x]$ :*

$f$  es resoluble por radicales  $\iff$  el grupo de Galois de  $f$  es resoluble

*Demostración.* Sea  $L$  el cuerpo de descomposición de  $f$ :

$\implies$ ) Tenemos entonces una extensión por radicales  $E$  de  $f$  que contiene a todas sus raíces, por lo que tenemos la torre  $F \leq L \leq E$ . Por las Proposiciones anteriores, se ha visto que existe una extensión radical iterada de  $F$  tal que  $E \leq K$ , por lo que  $F \leq K$  es de Galois, y como  $F \leq L$  también es de Galois, sabemos por la conexión de Galois que  $\text{Aut}_F(K)$  contiene como subgrupo normal al grupo de Galois  $\text{Aut}_L(K)$ . Sabemos además que:

$$\text{Aut}_F(L) \cong \frac{\text{Aut}_F(K)}{\text{Aut}_L(K)}$$

Y en el Lema anterior vimos que  $\text{Aut}_F(K)$  es resoluble, por lo que  $\text{Aut}_F(L)$  es resoluble, que es el grupo de Galois de  $f$ .

$\iff$ ) Supuesto que  $\text{Aut}_F(L)$  es resoluble, tomamos  $n = [L : F]$  y consideramos  $K = L(\zeta)$  con  $\zeta$  una raíz  $n$ -ésima primitiva de la unidad. El Ejercicio anterior nos dice que  $\text{Aut}_{F(\zeta)}(K)$  es isomorfo a un subgrupo de  $\text{Aut}_F(L)$ . Como  $\text{Aut}_F(L)$  es resoluble, tendremos que  $\text{Aut}_{F(\zeta)}(K)$  es resoluble y sabemos que  $|\text{Aut}_{F(\zeta)}(K)|$  divide a  $n$  (por el Teorema de Lagrange). Usando la conexión de Galois, tenemos una serie de composición de  $\text{Aut}_{F(\zeta)}(K)$ :

$$\text{Aut}_{F(\zeta)}(K) = G_0 \triangleright G_1 \triangleright \dots \triangleright G_{t-1} \triangleright G_t = \{id_K\}$$

con  $\frac{G_{i-1}}{G_i}$  de cardinal  $p_i$  primo y esto nos da:

$$F(\zeta) = K^{G_0} \leq K^{G_1} \leq \dots \leq K^{G_{i-1}} \leq K^{G_t} = K$$

con  $p_i \mid n \quad \forall i$ , ya que el cardinal de cada uno de los factores invariantes dividen al cardinal del grupo del que son factores invariantes, por lo que cada primo divide a  $n$ .

Resulta que  $\zeta$  elevada a una potencia elevada nos da una raíz  $p_i$ -ésima de la unidad, por lo que cada  $K^{G_i}$  contiene una raíz  $p_i$ -ésima primitiva de la unidad. Como los cocientes son cíclicos, cada extensión  $K^{G_i}$  es cíclica, por lo que cada  $K^{G_i}$  es cuerpo de descomposición de cierto  $x^{p_i} - a_i \in K_{i-1}[x]$ .

Como  $K$  contiene todas las raíces de  $f$  y  $F(\zeta) \leq K$  es radical iterada será una extensión por radicales, con lo que  $f$  es resoluble por radicales.

□

## Consecuencias

- Si  $\deg f \leq 4$ , entonces  $f$  es resoluble por radicales.

Esto es porque el grupo de Galois de  $f$  está dentro de  $S_n$  con  $n \leq 4$  y estos grupos son resolubles.

- Si  $\deg f \geq 5$ , entonces  $f$  es resoluble por radicales dependiendo de su grupo de Galois.

Veremos que  $x^5 - 4x - 1 \in \mathbb{Q}[x]$  tiene grupo de Galois isomorfo a  $S_5$ , luego NO es resoluble por radicales.

### 3.6. Ecuación general de grado $n$

Recordamos que si  $F$  un cuerpo, consideramos  $F[x_1, \dots, x_n]$  el anillo de polinomios con  $n$  indeterminadas.

- recordamos que al alterar el orden de las indeterminadas obtenemos anillos isomorfos
- como  $F$  es un cuerpo,  $F[x_1]$  es un DFU, por lo que  $F[x_1, x_2]$  también,  $\dots$ ,  $F[x_1, \dots, x_n]$  es un DFU. En particular, un dominio de integridad.

Si aplicamos la construcción de cuerpo de fracciones a  $F[x_1, \dots, x_n]$ , obtenemos  $F(x_1, \dots, x_n)$ , el cuerpo de fracciones del dominio de integridad  $F[x_1, \dots, x_n]$ :

$$F(x_1, \dots, x_n) = \left\{ \frac{f}{g} : f, g \in F[x_1, \dots, x_n], g \neq 0 \right\}$$

Dada una permutación  $\sigma \in S_n$ , aplicando  $n$  veces la Propiedad Universal del anillo de polinomios, obtenemos un homomorfismo de anillos  $\bar{\sigma} : F[x_1, \dots, x_n] \rightarrow F[x_1, \dots, x_n]$  determinado por:

$$\begin{aligned}\bar{\sigma}(\alpha) &= \alpha \quad \forall \alpha \in F \\ \bar{\sigma}(x_i) &= x_{\sigma(i)} \quad \forall i \in \{1, \dots, n\}\end{aligned}$$

Que claramente es un isomorfismo, pues  $\bar{\sigma}^{-1}$  es su homomorfismo inverso. Usando la Propiedad Universal de  $F(x_1, \dots, x_n)$  para obtener un automorfismo de cuerpos  $\bar{\sigma} : F(x_1, \dots, x_n) \rightarrow F(x_1, \dots, x_n)$  dado por:

$$\bar{\sigma} \left( \frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)} \right) = \frac{f(x_{\sigma(1)}, \dots, x_{\sigma(n)})}{g(x_{\sigma(1)}, \dots, x_{\sigma(n)})}$$

Tenemos por tanto una aplicación  $S_n \rightarrow \text{Aut}_F(F(x_1, \dots, x_n))$  que es un homomorfismo de grupos inyectivo, cuya imagen denotaremos por  $G$ .

**Definición 3.10.** Al cuerpo  $E^G$  (donde  $E = F(x_1, \dots, x_n)$ ) lo llamamos cuerpo de las funciones simétricas racionales en  $x_1, \dots, x_n$  con coeficientes en  $F$ .

Tenemos que  $E^G \leqslant E$  es de Galois, por el Lema de Artin.

**Ejercicio 3.6.1.** Sea  $f \in F[x]$  separable, irreducible y de grado primo  $p$ , entonces su grupo de Galois contiene un  $p$ -ciclo.

Si es separable e irreducible,  $p$  divide al orden del grupo de Galois. Como es primo, entonces  $G$  ha de contener un elemento de orden  $p$ . Descomponemos el elemento como producto de ciclos disjuntos y su orden ha de ser el mínimo común múltiplo de todos los órdenes de los ciclos que aparecen en su descomposición. Si estos números tienen como mínimo común múltiplo un número primo, entonces el orden de todos los ciclos es  $p$ . En  $S_p$ , el primero que aparece ha gastado todos los símbolos, luego ha de ser un  $p$ -ciclo.

**Proposición 3.17.** Para cada  $k \in \{1, \dots, n\}$  escribimos:

$$S_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \dots x_{i_k} \in F[x_1, \dots, x_n]$$

Entonces  $E^G = F(s_1, \dots, s_n)$ :

*Demostración.* Recordamos que:

$$E = F(x_1, \dots, x_n)$$

Y consideramos:

$$f = (x - x_1) \dots (x - x_n) \in E[x]$$

Y si tomamos  $\bar{\sigma} \in G$  es claro que  $f^{\bar{\sigma}} = f$ , tenemos:

$$f = x^n - s_1 x^{n-1} + \dots + (-1)^n s_n$$

Y como cada  $s_k \in E^G$  tenemos que  $F(s_1, \dots, s_n) \leq E^G$ . Tenemos que  $E$  es cuerpo de descomposición de  $f$  sobre  $F(s_1, \dots, s_n)$ . Es claro que  $f$  es separable por su propia definición, con lo que la extensión  $F(s_1, \dots, s_n) \leq E$  es de Galois.

Además,  $G \leq \text{Aut}_{F(s_1, \dots, s_n)}(E)$ . Pero si  $\tau : F \rightarrow E$  es un automorfismo de cuerpos  $F(s_1, \dots, s_n)$ -lineal, entonces para cada  $i \in \{1, \dots, n\}$  tenemos que:

$$0 = \tau(0) = \tau(f(x_i)) = f(\tau(x_i))$$

Por lo que  $\tau$  permuta las indeterminadas  $x_i$ , que son los elementos de  $G$ , por lo que  $\tau \in G$ , de donde:

$$G = \text{Aut}_{F(s_1, \dots, s_n)}(E)$$

Y como  $F(s_1, \dots, s_n) \leq E$  es de Galois tenemos por la conexión de Galois que:

$$E^G = F(s_1, \dots, s_n)$$

□

Estos son los polinomios simétricos elementales, porque si les aplicamos una permutación se queda iguales.

Consideramos ahora:

$$g = x^n - \lambda_1 x^{n-1} + \dots + (-1)^n \lambda_n \in F(\lambda_1, \dots, \lambda_n)[x]$$

con  $\lambda_1, \dots, \lambda_n$  indeterminadas sobre  $F$ . La ecuación  $g = 0$  en  $x$  se llama ecuación general sobre  $F$  de grado  $n$ .

**Lema 3.18.** Si tomamos  $h \in F[\lambda_1, \dots, \lambda_n]$  con  $h \neq 0$ , tenemos entonces que:

$$h(s_1, \dots, s_n) \neq 0$$

*Demostración.* Llamamos  $s_0 := 1$ , y definimos:

$$s_n(x_1, \dots, x_{n-1}) := 0$$

Estas definiciones dan sentido a la fórmula recursiva:

$$s_k(x_1, \dots, x_n) = s_k(x_1, \dots, x_{n-1}) + s_{k-1}(x_1, \dots, x_{n-1})x_n, \quad k \in \{1, \dots, n\}$$

Por inducción sobre  $n$ :

- Para  $n = 1$ , tenemos que  $s_1 = x_1$ , y tenemos que  $h_1(x_1) \neq 0 \implies h_1(x_1) \neq 0$ .
- Para  $n > 1$ , razonamos por inducción al absurdo: supongamos que existe  $h \neq 0$  pero  $h(s_1, \dots, s_n) = 0$ . Entre todos éstos, tomamos:

$$0 \neq h = h_0 + h_1\lambda_n + \dots + h_m\lambda_n^m \quad \text{con} \quad h_i \in F[\lambda_1, \dots, \lambda_{n-1}]$$

de grado mínimo  $m$  en  $\lambda_n$ . Tenemos entonces que:

$$\begin{aligned} 0 &= h(s_1, \dots, s_n) \\ &= h_0(s_1, \dots, s_{n-1}) + h_1(s_1, \dots, s_{n-1})s_n + \dots + h_m(s_1, \dots, s_{n-1})s_n^m \end{aligned}$$

Evaluando en  $x_n = 0$ , obtenemos que  $s_n = 0$ , por lo que:

$$\begin{aligned} 0 &= h_0(s_1(x_1, \dots, x_{n-1}, 0), \dots, s_{n-1}(x_1, \dots, x_{n-1}, 0)) \\ &= h_0(s_1(x_1, \dots, x_{n-1}), \dots, s_{n-1}(x_1, \dots, x_{n-1})) \end{aligned}$$

La hipótesis de inducción nos dice que  $h_0(\lambda_1, \dots, \lambda_{n-1}) = 0$ , y sacando factor común  $\lambda_n$  de la definición de  $h$ :

$$h = (h_1 + h_2\lambda_n + \dots + h_m\lambda_n^{m-1})\lambda_n$$

Evaluando en  $(s_1, \dots, s_{n-1})$  obtengo

$$0 = (h_1(s_1, \dots, s_{n-1}) + h_2(s_1, \dots, s_{n-1})s_n + \dots + h_m(s_1, \dots, s_{n-1})s_n^{m-1})s_n$$

y como  $s_n \neq 0$ , tenemos que:

$$0 = h_1(s_1, \dots, s_{n-1}) + h_2(s_1, \dots, s_{n-1})s_n + \dots + h_m(s_1, \dots, s_{n-1})s_n^{m-1}$$

de donde obtendríamos que  $h_1 + h_2\lambda_n + \dots + h_m\lambda_n^{m-1}$  se anula a  $(s_1, \dots, s_n)$ , con grado menor que  $h$ , lo que nos lleva a una contradicción.

□

**Proposición 3.19.** *El polinomio:*

$$g = x^n - \lambda_1 x^{n-1} + \dots + (-1)^n \lambda_n \in F(\lambda_1, \dots, \lambda_n)[x]$$

*es irreducible, separable y su grupo de Galois es isomorfo a  $S_n$ .*

*Demostración.* Tomamos  $\varepsilon : F[\lambda_1, \dots, \lambda_n] \rightarrow F(s_1, \dots, s_n)$  el anillo de polinomios determinado por  $\varepsilon(\alpha) = \alpha \quad \forall \alpha \in F$  y  $\varepsilon(\lambda_i) = s_i \quad i \in \{1, \dots, n\}$ , tenemos que  $\ker \varepsilon = \{0\}$  por el Lema anterior. La propiedad universal del cuerpo de fracciones  $F(\lambda_1, \dots, \lambda_n)$  nos da un homomorfismo de cuerpos

$$\bar{\varepsilon} : F(\lambda_1, \dots, \lambda_n) \rightarrow F(s_1, \dots, s_n)$$

que extiende a  $\varepsilon$ . Tenemos que  $\bar{\varepsilon}$  es  $F$ -lineal y es un isomorfismo de cuerpos. Cardano-Vietta nos dice que  $g^{\bar{\varepsilon}} = f$ . Tenemos que  $E = F(x_1, \dots, x_n)$  es cuerpo de descomposición de  $f$ , por lo que al aplicar el isomorfismo  $\bar{\varepsilon}$  tenemos que la co-restricción:

$$\bar{\varepsilon} : F(\lambda_1, \dots, \lambda_n) \rightarrow E$$

da un cuerpo de descomposición de  $g \in F(\lambda_1, \dots, \lambda_n)[x]$ . El grupo de Galois de  $g$  es isomorfo al de  $f$ ,  $G$ , que es isomorfo a  $S_n$ .

Tenemos además que  $g$  es separable, porque  $f$  lo es. Como su grupo de Galois es transitivo ( $S_n$  es transitivo sobre  $1, \dots, n$ ) tenemos que el grupo de Galois de  $f$  es transitivo, luego  $f$  es irreducible.  $\square$

**Teorema 3.20** (de Abel-Ruffini). *Si  $\text{car}(F) = 0$  y  $n \geq 5$ , entonces  $g$  no es resoluble por radicales.*

*Demostración.* El grupo de Galois de  $g$  es isomorfo a  $S_n$  con  $n \geq 5$ , que no es resoluble, por lo que  $f$  no puede ser resoluble por radicales.  $\square$

## 3.7. Resolución de las ecuaciones de grado hasta 4

Tendremos siempre que  $F$  será un cuerpo cualesquiera, y tengamos en cuenta que basta estudiar los polinomios mónicos.

### 3.7.1. Cuadrática

Tendremos  $f = x^2 + bx + c \in F[x]$ . Si  $\text{car}(F) \neq 2$ , podemos escribir:

$$f = \left( x + \frac{b}{2} \right)^2 + c - \frac{b^2}{4}$$

y ahora extendiendo  $F$  de forma adecuada:  $F \leq K$ , conseguimos escribir en  $K$  despejando  $x$ :

$$x + \frac{b}{2} = \pm \sqrt{\frac{b^2}{4} - c} = \pm \sqrt{\frac{b^2 - 4c}{4}} = \pm \frac{\sqrt{b^2 - 4c}}{2}$$

de donde:

$$x = -\frac{b}{2} \pm \frac{\sqrt{b^2 - 4c}}{2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

Por lo que la ecuación cuadrática es resoluble por radicales para cualquier cuerpo  $F$  con  $\text{car}(F) \neq 2$ .

### 3.7.2. Cúbica

Tendremos  $f = x^3 + bx^2 + cx + d \in F[x]$ . Si<sup>7</sup>  $\text{car}(F) \notin \{2, 3\}$ , podemos escribir:

$$g(x) = f\left(x - \frac{b}{3}\right) = x^3 + px + q$$

para ciertos  $p, q \in F$ . El polinomio  $g$  recibe el nombre cúbica reducida de  $f$ . Sea  $K$  una extensión de  $F$  donde están las raíces de  $f$  y una raíz cúbica primitiva de la unidad<sup>8</sup>  $\omega$ . Sean  $\alpha_1, \alpha_2, \alpha_3 \in K$  las raíces de  $g$ . Tenemos por las ecuaciones de Cardano-Vietta:

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

tomamos ahora:

$$\begin{aligned}\beta &:= \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \\ \gamma &:= \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3\end{aligned}$$

Sumando vemos que ( $\omega$  es raíz de  $x^2 + x + 1$ ):

$$\beta + \gamma = 3\alpha_1 + 0 + 0 = 3\alpha_1$$

Multiplicamos ahora  $\beta$  por  $\gamma$ , obteniendo (usando propiedades de  $\omega$ ):

$$\begin{aligned}\beta\gamma &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_2\alpha_3 - \alpha_1\alpha_3 \\ &= \cancel{(\alpha_1 + \alpha_2 + \alpha_3)^2}^0 - 3(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3) = -3p\end{aligned}$$

De las condiciones  $\beta + \gamma = 3\alpha_1$  y  $\beta\gamma = -3p$  obtenemos una ecuación cuadrática a resolver. Llamamos para simplificar:

$$u = \frac{\beta}{3}, \quad v = \frac{\gamma}{3}$$

tenemos que:

$$\alpha_1 = u + v$$

y observamos ahora que:

$$u^3 + v^3 + (3uv + p)(u + v) + q = (u + v)^3 + p(u + v) + q = g(u + v) = g(\alpha_1) = 0$$

y usando ahora que  $uv = -p/3$ , tenemos que:

$$0 = u^3 + v^3 + q \implies \begin{cases} u^3 + v^3 = -q \\ u^3v^3 = \frac{-p^3}{27} \end{cases}$$

Si tomamos:

$$h(z) = (z - u^3)(z - v^3) = z^2 + qz - \frac{p^3}{27}$$

---

<sup>7</sup>Distinta de 3 para el truco siguiente y distinta de 2 para poder aplicar luego la resolución de cuadráticas.

<sup>8</sup>Aquí también necesitamos que  $\text{car}(F) \neq 3$ , para que  $x^3 - 1$  sea separable.

El sistema de ecuaciones es equivalente a  $h(z) = 0$ , obteniendo las soluciones  $u^3$  y  $v^3$ . Si tomamos raíces cúbicas en un cuerpo que extienda al nuestro obtenemos 6 posibles valores de  $u$  y  $v$ . Sabemos ahora que  $\alpha_1$  es suma de dos valores de forma que estos son raíces cúbicas, puesto que no hemos supuesto nada a  $\alpha_1$  distinto que a  $\alpha_2$  y  $\alpha_3$ .

Elegimos entre aquellas parejas de  $u$  y  $v$  las que verifican  $3uv = -p$  (ya que  $3uv = \beta\gamma$ ).

**Ejemplo.** Tomamos  $f = x^3 - 6x^2 - 9x + 2 \in \mathbb{Q}[x]$ .

Calculamos primero su cónica reducida:

$$g(x) = f\left(x - \frac{-6}{3}\right) = f(x+2) = x^3 - 21x - 32$$

Consideramos ahora:

$$h(z) = z^2 - 32z + 343$$

Y las raíces de la resolvente cuadrática de la reducida cónica en  $\mathbb{C}$  son  $u^3 = 16 + i\sqrt{87}$ ,  $v^3 = 16 - i\sqrt{87}$ .

Extraemos las raíces cúbicas, obteniendo:

$$\begin{aligned} u_k &= e^{ik2\pi/3} \sqrt[3]{6 + i\sqrt{87}}, \quad k = 0, 1, 2 \\ v_k &= e^{ik2\pi/3} \sqrt[3]{16 - i\sqrt{87}}, \quad k = 0, 1, 2 \end{aligned}$$

Hemos de elegir de acuerdo con la condición  $3uv = -p = 21$ , lo que nos da:

$$u_0v_0 = u_1v_2 = u_2v_1 = 7$$

Por tanto, las raíces de la cónica reducida son:

$$\begin{aligned} u_0 + v_0 &= \sqrt[3]{16 + i\sqrt{87}} + \sqrt[3]{16 - i\sqrt{87}} \\ u_1 + v_2 &= e^{i2\pi/3} \sqrt[3]{16 + i\sqrt{87}} + e^{i4\pi/3} \sqrt[3]{16 - i\sqrt{87}} \\ u_2 + v_1 &= e^{i4\pi/3} \sqrt[3]{16 + i\sqrt{87}} + e^{i2\pi/3} \sqrt[3]{16 - i\sqrt{87}} \end{aligned}$$

Las raíces para  $f$  es sumar 2 a cada una de ellas.

### 3.7.3. Cuártica

Consideramos ahora  $f = x^4 + bx^3 + cx^2 + dx + e \in F[x]$  con  $\text{car}(F) \notin \{2, 3\}$ . El primer paso es reducir la ecuación con la resolvente cónica:

$$g = f\left(x - \frac{b}{4}\right) = x^4 + px^2 + qx + r$$

Llamaremos  $\beta_1, \beta_2, \beta_3, \beta_4$  a las raíces de  $g$  en una extensión adecuada. Por las relaciones de Cardano-Vietta:

$$\beta_1 + \beta_2 + \beta_3 + \beta_4 = 0$$

Tomamos ahora las expresiones (se han obtenido pensando en la primera y luego aplicando permutaciones sobre los índices):

$$\begin{aligned}\rho_1 &= -(\beta_1 + \beta_2)(\beta_3 + \beta_4) \\ \rho_2 &= -(\beta_1 + \beta_3)(\beta_2 + \beta_4) \\ \rho_3 &= -(\beta_1 + \beta_4)(\beta_2 + \beta_3)\end{aligned}$$

De esta forma, independientemente del grupo de Galois de  $f$ , tenemos que el polinomio:

$$h(x) = (x - \rho_1)(x - \rho_2)(x - \rho_3)$$

tiene coeficientes en  $F$ . De hecho, calculando con ingenio, se obtiene que:

$$h(x) = x^3 + 2px^2 + (p^2 - 4r)x - q^2$$

Y este es un polinomio del que ya sabemos calcular sus raíces. Falta ver cómo relacionar  $\rho_1, \rho_2, \rho_3$  con  $\beta_1, \beta_2, \beta_3, \beta_4$ . Observamos por ejemplo que:

$$\beta_3 + \beta_4 = \beta_1 + \beta_2$$

de donde:

$$\rho_1^2 = (\beta_1 + \beta_2)^2 \implies \beta_1 + \beta_2 = \sqrt{\rho_1}$$

Y así obtenemos:

$$\begin{cases} \beta_1 + \beta_2 = \sqrt{\rho_1} & \beta_3 + \beta_4 = -\sqrt{\rho_1} \\ \beta_1 + \beta_3 = \sqrt{\rho_2} & \beta_2 + \beta_4 = -\sqrt{\rho_2} \\ \beta_1 + \beta_4 = \sqrt{\rho_3} & \beta_2 + \beta_3 = -\sqrt{\rho_3} \end{cases}$$

donde elegimos los signos de acuerdo con  $\sqrt{\rho_1}\sqrt{\rho_2}\sqrt{\rho_3} = -q$ . Sumando de 3 en 3 las igualdades adecuadas obtenemos:

$$\begin{aligned}\beta_1 &= \frac{1}{2}(\sqrt{\rho_1} + \sqrt{\rho_2} + \sqrt{\rho_3}) \\ \beta_2 &= \frac{1}{2}(\sqrt{\rho_1} - \sqrt{\rho_2} + \sqrt{\rho_3}) \\ \beta_3 &= \frac{1}{2}(-\sqrt{\rho_1} + \sqrt{\rho_2} - \sqrt{\rho_3}) \\ \beta_4 &= \frac{1}{2}(-\sqrt{\rho_1} - \sqrt{\rho_2} - \sqrt{\rho_3})\end{aligned}$$

Sumando  $b/4$  a cada una de ellas obtenemos las raíces de  $f$ .

Ahora, si consideramos  $3 \in \mathbb{F}_5$  y nos preguntamos por  $\sqrt{3}$  probando vemos que no está en  $\mathbb{F}_5$ ; por lo que la raíz estará en  $\mathbb{F}_5(\sqrt{3}) = \mathbb{F}_{25}$ .

Un poquillo de como resolver ecuaciones en cuerpos finitos.

Vimos que si teníamos  $f \in F[x]$  separable, irreducible y de grado primo  $p$  entonces el grupo de Galois contiene un ciclo de orden  $p$ .

**Ejercicio 3.7.1.** Sea  $f \in \mathbb{Q}[x]$  irreducible de grado primo  $p$ . Se pide demostrar que si  $f$  tiene exactamente 2 raíces complejas no reales entonces su grupo de Galois es  $S_p$ .

Si tomamos  $\alpha_1, \dots, \alpha_{p-2} \in \mathbb{R}$ ;  $\alpha, \bar{\alpha} \in \mathbb{C} \setminus \mathbb{R}$  las raíces de  $f$  tenemos que el cuerpo de descomposición de  $f$  es:

$$\mathbb{Q}(\alpha_1, \dots, \alpha_{p-2})(\alpha, \bar{\alpha}) \leqslant \mathbb{C}$$

Además, tenemos que la conjugación compleja deja fijo el cuerpo de descomposición de  $f$ . Visto como permutaciones tenemos que es una trasposición, por lo que el grupo de Galois de  $f$  visto como subgrupo de  $S_p$  contiene una trasposición.

Por el ejercicio mencionado antes tenemos que el grupo de Galois de  $f$  contiene además un ciclo de orden  $p$ . Como estos dos elementos generan  $S_p$  ha de ser el grupo de Galois igual a  $S_p$ .

**Ejercicio 3.7.2.** Sea  $f = x^5 - 4x - 1 \in \mathbb{Q}[x]$ , veamos que el grupo de Galois de  $f$  es isomorfo a  $S_5$ .

Como  $f \in \mathbb{Z}[x]$ , tenemos que  $f$  es irreducible si y solo si  $f \in \mathbb{Z}[x]$  es irreducible. Reducimos módulo 3, obteniendo:

$$\bar{f} = x^5 - x - 1 \in \mathbb{Z}_3[x]$$

que no tiene raíces en  $\mathbb{Z}_3$ . Los posibles factores de grado 2 son todos aquellos de grado 2 irreducibles:

$$x^2 + 1, \quad x^2 + 2x + 2, \quad , x^2 + x + 2$$

con la división euclíadiana vemos que al dividir  $f$  entre estos ningún resto sale nulo, por lo que  $f$  tiene que ser irreducible en  $\mathbb{Z}_3[x]$ , por ser de grado 5 y no tener factores ni de grado 1 (no tiene raíces) ni de grado 2. Por tanto,  $f \in \mathbb{Z}[x]$  es irreducible.

Veamos ahora cuántas raíces en  $\mathbb{R}$  tiene  $f$ . Para ello:

$$f' = 5x^4 - 4$$

imponiendo  $f' = 0$  y quedándonos con las reales obtenemos como puntos críticos  $\pm\sqrt{\frac{4}{5}}$ . Evaluando como en bachiller:

$$f(-2) = -25 < 0, \quad f(-1) = 2 > 0, \quad f(0) = -1 < 0$$

Vemos que  $f$  tiene que tener 3 raíces reales, ya que tiene 2, las raíces complejas van en parejas y por la derivada sabemos que  $f$  no puede tener más de 3 raíces reales.

El último ejercicio nos dice que el grupo de Galois de  $f$  es  $S_5$ , que no es resoluble, por lo que  $f$  no es resoluble por radicales, por el gran Teorema de Galois.

**Ejercicio 3.7.3.** Sea  $f = x^n - a \in F[x]$  separable y  $K$  su cuerpo de descomposición. Fijado  $\zeta \in K$  una raíz  $n$ -ésima primitiva de la unidad, fijamos  $\sqrt[n]{a} \in K$ . Sea  $\sigma \in \text{Aut}_F(K)$ , denotamos por  $j(\sigma), k(\sigma) \in \mathbb{Z}_n$  a los elementos determinados por

$$\sigma(\sqrt[n]{a}) = \zeta^{j(\sigma)} \sqrt[n]{a}, \quad \sigma(\zeta) = \zeta^{k(\sigma)}$$

con  $k(\sigma) \in \mathcal{U}(\mathbb{Z}_n)$ . Comprobar que la aplicación<sup>9</sup>  $\text{Aut}_F(K) \rightarrow GL_2(\mathbb{Z}_n)$  dada por:

$$\sigma \mapsto \begin{pmatrix} 1 & 0 \\ j(\sigma) & k(\sigma) \end{pmatrix}$$

es un homomorfismo inyectivo de grupos.

Vemos que la aplicación está bien definida, pues:

$$\det \begin{pmatrix} 1 & 0 \\ j(\sigma) & k(\sigma) \end{pmatrix} = k(\sigma) \in \mathcal{U}(\mathbb{Z}_n)$$

Si tomamos  $\sigma$  de forma que su matriz es la identidad tenemos por la definición de  $j(\sigma)$  y de  $k(\sigma)$  que  $\sigma = id$ . Se comprueba fácil que es un homomorfismo. Por tanto,  $|\text{Aut}_F(K)|$  es un divisor de  $|GL_2(\mathbb{Z}_n)| = n \times \varphi(n)$ . Y tenemos que alcanza el máximo si  $f$  es irreducible sobre  $F$ .

Se llaman grupos holomorfos, los de las matrices triangulares.

### 3.8. Cuerpos finitos

**Teorema 3.21.** *Tomamos (para  $q = p^k$ )  $\mathbb{F}_q \leqslant \mathbb{F}_{q^n}$  una extensión de cuerpos finitos. Entonces  $\text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$  es cíclico generado por  $\phi$ , donde:*

$$\phi(\alpha) = \alpha^q \quad \forall \alpha \in \mathbb{F}_{q^n}$$

Además,  $\mathbb{F}_{q^n}$  es cuerpo de descomposición de  $x^{qn} - x \in \mathbb{F}_q[x]$ .

*Demostración.* Con  $q = p^k$  con  $p$  primo y  $k \geqslant 1$ , tenemos la extensión:

$$\mathbb{F}_p \leqslant \mathbb{F}_{p^k} \leqslant \mathbb{F}_{p^{kn}}$$

y son las tres extensiones de Galois. El automorfismo de Frobenius  $\tau$  nos permite describir:

$$\text{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^{kn}}) = \langle \tau \rangle$$

donde  $\tau : \mathbb{F}_{p^{kn}} \rightarrow \mathbb{F}_{p^{kn}}$ , donde:

$$\tau(\alpha) = \alpha^p \quad \forall \alpha \in \mathbb{F}_{p^{kn}}$$

Como  $\text{Aut}_{\mathbb{F}_{p^k}}(\mathbb{F}_{p^{kn}})$  es un subgrpo de  $G = \text{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^{kn}})$  este último cíclico tenemos que el primero es cíclico.

Si buscamos ahora su generador, como todas las extensiones son de Galois calcular el orden del grupo equivale a calcular el grado de la extensión. Si observamos de esta forma que:

$$[\mathbb{F}_{p^{kn}} : \mathbb{F}_{p^k}] = n \implies |\text{Aut}_{\mathbb{F}_{p^k}}(\mathbb{F}_{p^{kn}})| = n$$

---

<sup>9</sup>Si se recuerda la demostración de que una matriz es invertible si y solo si su determinante es no nulo se puede hacer también considerando los coeficientes solo sobre un anillo comutativo.

tenemos entonces en vista de  $\tau$  y del orden del grupo que un generador suyo es  $\tau^k$ . Llamamos  $\phi = \tau^k$ , y calculamos:

$$\phi(\alpha) = (\tau^k)(\alpha) = \alpha^{p^k} = \alpha^q$$

Finalmente, como  $\mathbb{F}_p^{kn}$  es cuerpo de descomposición de  $x^{p^{kn}} - x = x^{q^n} - x \in \mathbb{F}_p[x]$  tenemos entonces que  $\mathbb{F}_{q^n}$  es cuerpo de descomposición de  $x^{q^n} - x \in \mathbb{F}_q[x]$ .  $\square$

**Notación.** En vistas el Teorema anterior, bajo sus mismas hipótesis, llamaremos a  $\phi$  automorfismo de Frobenius de la extensión  $\mathbb{F}_q \leqslant \mathbb{F}_{q^n}$ .

**Teorema 3.22.** *Si  $f \in \mathbb{F}_q[x]$  es un polinomio irreducible de grado  $n$ , entonces su cuerpo de descomposición es  $\mathbb{F}_{q^n}$ . Además, si  $\alpha \in \mathbb{F}_{q^n}$  es una raíz de  $f$ , entonces el resto de sus raíces son*

$$\alpha^q, \dots, \alpha^{q^{n-1}}$$

*Demostración.*  $f$  tiene una raíz en alguna extensión de grado  $n$  de  $\mathbb{F}_q$ , por ejemplo  $\frac{\mathbb{F}_q[x]}{\langle f \rangle}$ . Así, tomamos:

$$\mathbb{F}_{q^n} = \frac{\mathbb{F}_q[x]}{\langle f \rangle}$$

Y como la extensión  $\mathbb{F}_q \leqslant \mathbb{F}_{q^n}$  es de Galois, tenemos que  $f$  es separable y que todas sus raíces están en  $\mathbb{F}_{q^n}$ . Si  $\alpha$  es una raíz de  $f$  en  $\mathbb{F}_{q^n}$ , entonces:

$$\alpha^{q^k} = \phi(\alpha)^k \quad \forall k \in \{1, \dots, n\}$$

son raíces de  $f$ , gracias al grupo de Galois. Además, como tenemos  $n$ , son todas sus raíces.  $\square$

Si observamos ahora que cada uno de estos  $f$  que montamos es un factor irreducible del polinomio  $x^{q^n} - x \in \mathbb{F}_q[x]$ .

**Teorema 3.23.** *Un polinomio irreducible  $f \in \mathbb{F}_q[x]$  de grado  $n$  divide a  $x^{q^m} - x \in \mathbb{F}_q[x]$  si, y solo si,  $n$  divide a  $m$ .*

*Como consecuencia,  $x^{q^m} - x \in \mathbb{F}_q[x]$  es producto de todos los polinomios irreducibles en  $\mathbb{F}_q[x]$  cuyo grado divide a  $m$ .*

*Demostración.* Por doble implicación:

$\implies$ ) Supongamos que  $f$  es irreducible y que divide a  $x^{q^m} - x \in \mathbb{F}_q[x]$ . Tomamos sendos cuerpos de descomposición sobre  $\mathbb{F}_q$ :  $\mathbb{F}_{q^n} \leqslant \mathbb{F}_{q^m}$ , de donde  $n \mid m$  por el Lema de la Torre.

$\Leftarrow$ ) Si  $f$  es irreducible y  $n \mid m$  tenemos entonces que  $\mathbb{F}_{q^n} \leqslant \mathbb{F}_{q^m}$  (tomamos  $\mathbb{F}_{q^m}$  y por la conexión de Galois encontramos  $\mathbb{F}_{p^n}$ , ya que el grupo de Galois es cíclico). Ahora, los elementos de  $\mathbb{F}_{q^m}$  son las raíces de  $x^{q^m} - x \in \mathbb{F}_q[x]$ .  $n$  de ellas serán las raíces de  $f$ , y como todas las raíces son de  $x^{q^m} - x$  tenemos entonces que  $f$  divide a este.

La consecuencia viene del Teorema de factorización y por el si y solo si.  $\square$

**Ejemplo.** Factoricemos  $x^{16} + x \in \mathbb{F}_2[x]$  como producto de irreducibles.

Vemos que  $16 = 2^4$ , por lo que según el Teorema, para cada divisor de 4 buscamos divisores de dicho grado:

- De grado 1:  $x, x - 1$
- De grado 2:  $x^2 + x + 1$ .
- De grado 4 sabemos que quedan 3 posibles, que tenemos que buscar sin raíces y distintos de  $(x^2 + x + 1)^2 = x^4 + x^2 + 1$ .

$$x^4 + x + 1, \quad x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1$$

Y la factorización es:

$$x^{16} + x = x(x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$$

En esta última factorización vemos que  $\mathbb{F}_{16}$  puede presentarse de 3 formas distintas sobre  $\mathbb{F}_2$ , tomando  $\mathbb{F}_{16} = \mathbb{F}_2(a)$  con  $a$  raíz de cualquiera de los 3 polinomios de grado 4. Para cada polinomio tendremos una presentación posible. Es decir:

- Si tomamos  $f = x^4 + x + 1 \in \mathbb{F}_2[x]$ , tenemos que su cuerpo de descomposición es  $\mathbb{F}_{16}$ , y podemos dar el cuerpo como  $\mathbb{F}_2(\alpha)$ , con  $\alpha^4 + \alpha + 1 = 0$ . Además, las demás raíces de  $f$  son  $\alpha^2, \alpha^4$  y  $\alpha^8$
- Si tomamos  $g = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$ , queremos calcular ahora las raíces de  $g$  en  $\mathbb{F}_{16}$  en función de  $\alpha$ .

En primer lugar, sabemos que todas las raíces de  $g$  están en  $\mathbb{F}_{16}$ , porque la extensión  $\mathbb{F}_2 \leqslant \mathbb{F}_{16}$  es de Galois y en las extensiones de Galois bastaba encontrar una solución en  $\mathbb{F}_{16}$  de  $g$  (irreducible) para tenerlas todas.

Además, por uno de los últimos teoremas sabemos que si encontramos una de ellas el resto vienen dadas por elevar al cuadrado repetidas veces dicha raíz.

Sabemos que  $\mathbb{F}_{16}$  tiene que tener una raíz de  $g$  porque  $\mathbb{F}_{16}$  consiste en exclusivamente las raíces de  $x^{16} + x \in \mathbb{F}_2[x]$ , que según la descomposición en factores irreducibles nos dice que todas las raíces de  $x^4 + x^3 + 1$  son también raíces de  $x^{16} + x$ .

Para calcular sus raíces, calculemos el orden de  $\alpha$  en el grupo multiplicativo  $\mathbb{F}_{16}^\times$ . Los posibles órdenes de sus elementos son 1, 3, 5 y 15:

- Sabemos que  $O(\alpha) \neq 1$ , ya que  $\alpha \neq 1$  porque 1 no es raíz de  $f$ .
- Sabemos que  $\{1, \alpha, \alpha^2, \alpha^3\}$  es una  $\mathbb{F}_2$ -base de  $\mathbb{F}_{16}$ , por lo que  $\alpha$  y  $\alpha^3$  son linealmente independientes, luego no puede ser  $O(\alpha) = 3$ .
- Vemos ahora que  $\alpha^5 = \alpha\alpha^4 = \alpha(\alpha + 1) = \alpha^2 + \alpha \neq 1$ , ya que 1,  $\alpha$  y  $\alpha^2$  son  $\mathbb{F}_2$ -linealmente independientes, luego ha de ser  $O(\alpha) \neq 5$ .

Concluimos que ha de ser  $O(\alpha) = 15$ , por lo que:

$$\mathbb{F}_{16} = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{14}\}$$

Observamos primero que las raíces de  $f$  y de  $g$  han de ser distintas, porque  $f$  y  $g$  son dos polinomios irreducibles distintos. Por tanto, las raíces de  $g$  no son  $\alpha, \alpha^2, \alpha^4, \alpha^8$ . Tampoco pueden ser 0 ni 1, por lo que nos quedan 8 posibles candidatos a raíz.

Buscamos heurísticamente generadores de  $\mathbb{F}_{16}^\times$  (ya que hemos obtenido  $\mathbb{F}_{16}$  por  $\alpha$ , que era raíz de  $f$ ), por lo que creemos que  $\alpha^7$  (la primera potencia de  $\alpha$  que genera todo el grupo cíclico) es un candidato a raíz de  $g$ . Lo comprobamos (pensando que  $\alpha^{15} = 1$ ):

$$\begin{aligned} g(\alpha^7) &= (\alpha^7)^4 + (\alpha^7)^3 + 1 = \alpha^{28} + \alpha^{21} + 1 = \alpha^{13} + \alpha^6 + 1 = (\alpha^4)^3\alpha + \alpha^4\alpha^2 + 1 \\ &= (\alpha + 1)^3\alpha + (\alpha + 1)\alpha^2 + 1 = (\alpha^3 + \alpha^2 + \alpha + 1)\alpha + \alpha^3 + \alpha^2 + 1 \\ &= \alpha + 1 + \alpha^3 + \alpha^2 + \alpha + \alpha^3 + \alpha^2 + 1 = 0 \end{aligned}$$

En efecto,  $\alpha^7$  es una raíz de  $g$ . Ahora:

- Elevamos  $\alpha^7$  al cuadrado varias veces.
- Vemos elevar al cuadrado como automorfismo de Frobenius, que restringido a  $\mathbb{F}_{16}^\times$  es un automorfismo de grupos, por lo que lleva generadores en generadores, obteniendo que las raíces de  $g$  son:

$$\alpha^7, \alpha^{11}, \alpha^{13} \text{ y } \alpha^{14}$$

- Nos falta clasificar 6 raíces, 2 de  $k = x^2 + x + 1$  y 4 de  $h = x^4 + x^3 + x^2 + x + 1$ .

Tomamos la potencia más pequeña de  $\alpha$  que no hayamos clasificado:

$$k(\alpha^3) = \alpha^6 + \alpha^3 + 1 = (\alpha + 1)\alpha^2 + \alpha^3 + 1 = \alpha^3 + \alpha^2 + \alpha^3 + 1 = \alpha^2 + 1 \neq 0$$

donde  $\alpha^2 + 1 \neq 0$  porque 1 y  $\alpha^2$  son  $\mathbb{F}_2$ -linealmente independientes, por lo que  $\alpha^3$  es raíz de  $h$  y obtenemos todas sus raíces elevando  $\alpha^3$  al cuadrado, obteniendo:

$$\alpha^3, \alpha^6, \alpha^{12} \text{ y } \alpha^9$$

Las que quedan son  $\alpha^5$  y  $\alpha^{10}$ , que han de ser raíces de  $k$ .

Podríamos haberlo hecho también pensando también en que  $\alpha^5$  tiene orden 3 y  $\alpha^3$  tiene orden 5 sobre  $\mathbb{F}_{16}^\times$ . Como  $x^2 + x + 1$  tiene cuerpo de descomposición  $\mathbb{F}_4$ , tendremos un elemento  $\alpha^2 + \alpha + 1 = 0$  con orden 3 en  $\mathbb{F}_4^\times$ , por lo que viendo la extensión  $\mathbb{F}_4 \leq \mathbb{F}_{16}$  obtendremos finalmente que las raíces de  $k$  son las de orden 3.



## 4. Ejercicios

**Ejercicio 1.** Sea  $F$  cuerpo de descomposición de  $f = x^3 + x + 1 \in \mathbb{F}_2[x]$  y  $\alpha \in F$  raíz de  $f$ . Razonar que  $F = \mathbb{F}_2(\alpha)$ . Resolver en  $F$  las soluciones de las ecuaciones en función de  $\alpha$ :

$$x^3 + x + 1 = 0, \quad x^3 + x^2 + 1 = 0, \quad x^2 + x + 1 = 0$$

### Solución.

Para ver que  $F = \mathbb{F}_2(\alpha)$  basta ver que  $f$  es irreducible, por lo que entonces  $F \leq \mathbb{F}_2(\alpha)$  será de Galois y lo tenemos. Comprobamos que  $f$  es irreducible, ya que se tiene  $f(0) = f(1) = 1 \neq 0$ , y  $\deg f = 3$ .

Como  $\alpha$  es raíz de  $f$  y  $\mathbb{F}_2 \leq F$  es de Galois, entonces todas las raíces de  $f$ , que son,  $\alpha, \alpha^2, \alpha^4 \in F$ , tenemos entonces que  $F = \mathbb{F}_2(\alpha)$ . Puede razonarse también por el orden de los cuerpos, ambos es 8.

1. Las soluciones de la primera ecuación son trivialmente  $\alpha, \alpha^2$  y  $\alpha^4$ .
2. Para la segunda, vamos a repetir un argumento análogo al último ejemplo, es decir, resolver la ecuación en  $\mathbb{F}_8$ , y ya hemos descartado 5 raíces (3+2). Como  $\mathbb{F}_8^\times$  tiene por generador  $\alpha$ , las raíces de  $x^3 + x^2 + 1$  son  $\alpha^3, \alpha^5$  y  $\alpha^6$ .

Esto lo sabemos viendo la factorización de  $x^8 + x \in \mathbb{F}_2[x]$  como el producto:

$$x^8 + x = x(x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

3. Para la ecuación  $x^2 + x + 1 = 0$ , veamos que no tiene solución en  $\mathbb{F}_8$ , ya que:
  - Como hemos gastado todas las raíces, tendría que ser una de ellas y ...
  - El polinomio no está en la factorización de  $x^8 + x$ .
  - Si tuviera solución podríamos tener entonces:

$$\mathbb{F}_2 \leq \mathbb{F}_4 \leq \mathbb{F}_8$$

Pero no puede ser  $\mathbb{F}_{2^2} \leq \mathbb{F}_{2^3}$ , ya que  $2 \nmid 3$ .

**Ejercicio 2.** Consideramos  $f = x^3 + x + 1 \in \mathbb{F}_4[x]$  y tomamos  $K$  cuerpo de descomposición de  $f$ . Sea  $\alpha \in K$  una raíz de  $f$ , veamos que  $K = \mathbb{F}_4(\alpha)$ .

Para ello, usaremos que  $\mathbb{F}_4 \leq K$  es de Galois (puesto que son cuerpos finitos), como  $f$  es irreducible en  $\mathbb{F}_4[x]$ , por varios motivos tenemos que  $K = \mathbb{F}_4(\alpha)$ . Sabemos que  $f$  es irreducible en  $\mathbb{F}_4[x]$  porque no tiene raíces en  $\mathbb{F}_4$ :

- Una opción es tomar  $\mathbb{F}_4 = \{0, 1, \gamma, \gamma + 1\}$  y comprobarlo.
- Otra es por reducción al absurdo, suponer que sí, que  $\gamma \in \mathbb{F}_4$  es una raíz de  $f$ . Vemos claramente que  $\gamma \notin \mathbb{F}_2$ , puesto que  $f$  es irreducible en  $\mathbb{F}_2$ . De esta forma, observamos que  $\mathbb{F}_4 \leqslant \mathbb{F}_2(\gamma)$ , con lo que  $g = \text{Irr}(\gamma, \mathbb{F}_2) = x^2 + x + 1 \in \mathbb{F}_2[x]$ . Tenemos que  $g(\gamma) = 0 = f(\gamma)$ , con  $g, f \in \mathbb{F}_2[x]$ , por lo que (por definición de  $\text{Irr}(\gamma, \mathbb{F}_2)$ )  $g \mid f$ , pero ambos son irreducibles, por lo que hemos llegado a una contradicción.

Por tanto, como  $[K : \mathbb{F}_4] = 3$  y  $|\mathbb{F}_4| = 4$ , tenemos que  $|K| = 4^3 = (2^2)^3 = 64$ .

Nos preguntamos ahora cómo resolver las ecuaciones:

$$x^3 + x + 1 = 0, \quad x^3 + x^2 + 1 = 0, \quad x^2 + x + 1 = 0$$

**Si no nos acordamos del ejercicio anterior.** Como una solución es  $\alpha$  y consideramos el homomorfismo de Frobenius de la extensión (elevar a 4), tenemos entonces que sus raíces en  $K$  son  $\alpha, \alpha^4$  y  $\alpha^{16}$ .

**Si nos acordamos del ejercicio de ayer.** Habíamos resuelto la ecuación en  $\mathbb{F}_2$ , y es claro que  $F = \mathbb{F}_2(\alpha) \leqslant K$ , con  $|\mathbb{F}_2(\alpha)| = 8$ . Las soluciones que encontrábamos eran  $\alpha, \alpha^2$  y  $\alpha^4$  en  $F \leqslant K$ .

Parece que no coinciden. Sin embargo,  $\alpha^{16} = \alpha^2$ , porque  $\alpha^7 = 1$ .

De la misma forma y usando el ejercicio anterior, tenemos que las soluciones de la segunda ecuación son  $\alpha^3, \alpha^5$  y  $\alpha^6$ .

**Si no nos acordamos.** Podríamos haber pensado en considerar  $\mathbb{F}_2(\alpha) \leqslant K$  y resolver  $f$  en  $\mathbb{F}_2(\alpha)$ , que es lo que hicimos en el ejercicio anterior.

Para la última ecuación, tomamos  $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$ , de donde  $\gamma$  es solución de  $x^2 + x + 1 = 0$ , ya que es el único polinomio irreducible de grado 2 sobre  $\mathbb{F}_2[x]$ .

Finalmente, se nos pide hacer una base de  $K$  sobre  $\mathbb{F}_2$  usando  $\alpha$  y  $\gamma$ .

Para ello, lo que haremos es ver que:

$$\mathbb{F}_2 \leqslant F \leqslant K$$

con  $\{1, \gamma\}$  una base de  $\mathbb{F}_2 \leqslant F$  y  $\{1, \alpha, \alpha^2\}$  una base de  $F \leqslant K$ . Si repasamos la demostración del Lema de la Torre, tenemos que:

$$\{1, \alpha, \alpha^2, \gamma, \gamma\alpha, \gamma\alpha^2\}$$

es una base de  $\mathbb{F}_2 \leqslant K$ .

¿Cuál es el orden multiplicativo de  $\gamma\alpha$ ? ¿Es un elemento primitivo de  $K$  sobre  $\mathbb{F}_2$ ?

**Ejercicio 3.** ¿Cuántos polinomios irreducibles de grado 6 hay en  $\mathbb{F}_2[x]$ ?

Usando Álgebra III, estos polinomios aparecen en la descomposición del polinomio  $x^{64} - x$  en irreducibles ( $64 = 2^6$ , con  $\text{Div}(6) = \{1, 2, 3, 6\}$ )

$$x^{64} - x = x(x+1)(x^2+x+1)(x^3+x+1)(x^3+x^2+1) \prod \text{polinomios grado 6}$$

Como la suma de los grados tiene que ser 64, el último polinomio (el producto) tiene grado:

$$64 - 10 = 54, \quad \frac{54}{6} = 9$$

Por lo que hay 9 polinomios irreducibles de grado 6 en  $\mathbb{F}_2[x]$ .

**Ejercicio 4.** Calcular el cardinal del grupo de Galois sobre  $\mathbb{Q}$  del polinomio  $f = (x^3 + x + 1)(x^2 + 1)$ .

Sea  $K$  el cuerpo de descomposición de  $f \in \mathbb{Q}[x]$ . Las raíces del segundo están claras pero las del primero no (sabemos calcularlas pero es una cuesta llena de pinchos). Del primero sabemos que bien tiene 3 raíces reales o bien 1 raíz real y 2 complejas. Sea  $g$  la función  $g(x) = x^3 + x + 1$ , tenemos que:

$$g'(x) = 3x^2 + 1 > 0$$

Por lo que  $g$  es estrictamente creciente, por lo que solo tiene una raíz real. Será por tanto:

$$K = \mathbb{Q}(i, -i, r, \alpha, \bar{\alpha}) = \mathbb{Q}(i, r, \alpha)$$

donde  $r \in \mathbb{R}$ ,  $\alpha \in \mathbb{C} \setminus \mathbb{R}$  con  $r, \alpha$  raíces de  $x^3 + x + 1$ . Como  $\mathbb{Q} \leqslant K$  es de Galois, nos piden  $|\text{Aut}_{\mathbb{Q}}(K)| = [K : \mathbb{Q}]$ . Por el Lema de la Torre:

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = [K : \mathbb{Q}(i)] \cdot 2$$

Para calcular  $[K : \mathbb{Q}(i)]$  vamos a usar que las raíces de  $x^3 + x + 1$  están en  $K$ . ¿Es cierto que  $K$  es cuerpo de descomposición de  $g = x^3 + x + 1 \in \mathbb{Q}(i)[x]$ ? En efecto, si  $g$  fuera irreducible en  $\mathbb{Q}(i)$  entonces a partir del discriminante de  $g$  (si está en  $\mathbb{Q}$  o no) tendríamos que  $[K : \mathbb{Q}(i)]$  es el cardinal bien de  $A_3$  o de  $S_3$ .

Para ver que  $g$  es irreducible en  $\mathbb{Q}(i)[x]$  veamos que no tiene raíces en  $\mathbb{Q}(i)$ :

- Si  $r$  es raíz de  $g$  en  $\mathbb{Q}(i)$ , entonces  $r \in \mathbb{Q}$ , por lo que es raíz de  $x^3 + x + 1$ , pero  $x^3 + x + 1$  es irreducible en  $\mathbb{Q}$ .
- Si  $\alpha \in \mathbb{Q}(i)$ , como  $\alpha \notin \mathbb{Q}$ , tendremos entonces que  $\alpha$  tiene grado 2 sobre  $\mathbb{Q}$ , es decir, que  $\text{Irr}(\alpha, \mathbb{Q})$  tiene grado 2, y teníamos que  $\alpha$  era raíz de  $g$ , por lo que  $\text{Irr}(\alpha, \mathbb{Q}) \mid g$ , pero  $g$  es irreducible, lo que lleva a una contradicción.
- Como  $\alpha \notin \mathbb{Q}(i)$  tenemos entonces que  $\bar{\alpha} \notin \mathbb{Q}(i)$ .

De aquí tenemos que  $g$  es irreducible en  $\mathbb{Q}(i)$ , por lo que su grupo de Galois será bien  $A_3$  o  $S_3$ , en función del discriminante:

$$\text{Disc}(g) = -31$$

Por lo que:

$$\Delta = \sqrt{\text{Disc}(g)} = i\sqrt{31} \notin \mathbb{Q}(i)$$

Ya que si  $i\sqrt{31} \in \mathbb{Q}(i)$  tendríamos entonces que  $\sqrt{31} \in \mathbb{Q}(i)$ , pero  $\sqrt{31} \in \mathbb{R} \setminus \mathbb{Q}$ , ya que 31 es primo ( $x^2 - 31$  es irreducible por Eisenstein para  $p = 31$ ).

En definitiva, como  $\Delta \notin \mathbb{Q}(i)$  tenemos entonces que  $\text{Aut}_{\mathbb{Q}(i)}(K) \cong S_3$ , con  $|S_3| = 6$ , de donde:

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 6 \cdot 2 = 12$$

Describir cuál es el grupo  $\text{Aut}_{\mathbb{Q}}(K)$ .

La conexión de Galois nos dice que hay un subgrupo normal, puesto que su índice es 2.

Usamos el Teorema de extensión, por lo que estará  $\eta_0, \eta_1, \eta_2$ :

$$r \xrightarrow{\eta_0} r, \quad r \xrightarrow{\eta_1} \alpha, \quad r \xrightarrow{\eta_2} \bar{\alpha}$$

Cada uno de estos lo extendemos llevando  $i$  a  $i$  o a  $-i$ . El último paso parece más difícil.

**Ejercicio 5.** Calcular el grupo de Galois de  $f = (x^2 + x + 1)(x^2 - 3) \in \mathbb{Q}[x]$ .

Sea  $K$  el cuerpo de descomposición de  $f$ , tenemos que:

$$K = \mathbb{Q}\left(w, \sqrt{3}\right), \quad w \text{ una raíz cúbica primitiva de la unidad}$$

Por el Lema de la Torre:

$$[K : \mathbb{Q}] = \left[K : \mathbb{Q}\left(\sqrt{3}\right)\right] \left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = 2 \cdot 2 = 4$$

Por lo que:

$$|\text{Aut}(K)| = [K : \mathbb{Q}] = 4$$

Calculamos sus elementos, por la Proposición de extensión. Calculamos primero los homomorfismos de cuerpos  $\mathbb{Q}(\sqrt{3}) \rightarrow K$ , que son  $\eta_j$  con  $j \in \{0, 1\}$ , con:

$$\eta_j\left(\sqrt{3}\right) = (-1)^j \sqrt{3}, \quad j \in \{0, 1\}$$

Extendemos cada uno de estos homomorfismos, cada uno de ellos se extiende a dos homomorfismos  $K \rightarrow K$ , que son  $\eta_{j,k}$ , donde:

$$\eta_{j,k}\left(\sqrt{3}\right) = (-1)^j \sqrt{3}, \quad \eta_{j,k}(w) = w^k, \quad j \in \{0, 1\}, \quad k \in \{1, 2\}$$

Como  $\eta_{1,1}$  y  $\eta_{1,2}$  tienen orden 2 tenemos que el grupo es isomorfo a  $C_2 \oplus C_2$ .

**Ejercicio 6.** Calcular el grupo de Galois de  $g = (x^2 + x + 1)(x^2 + 3) \in \mathbb{Q}[x]$ .

Sea  $K$  el cuerpo de descomposición de  $g$ , si tomamos como raíz cúbica primitiva de la unidad:

$$w = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$$

Tendremos ahora que:

$$K = \mathbb{Q}(i\sqrt{3})$$

Con lo que  $|\text{Aut}_{\mathbb{Q}}(K)| = [K : \mathbb{Q}] = 2$ , isomorfo a  $C_2$ . Sus elementos son  $\eta_j$ , donde:

$$\eta_j(i\sqrt{3}) = (-1)^j i\sqrt{3} \quad j \in \{0, 1\}$$

**Ejercicio 7.** Sea  $f = x^3 - 3x + 1 \in \mathbb{Q}[x]$  y  $\alpha$  cualquier raíz real de  $f$ . Demostrar que el cuerpo de descomposición de  $f$  sobre  $\mathbb{Q}$  es  $\mathbb{Q}(\alpha)$ .

Veamos que  $f$  es irreducible, puesto que es de grado 3 y sus únicas posibles raíces en  $\mathbb{Q}$  son  $\pm 1$ , y no lo son; luego  $f$  es irreducible. De aquí deducimos que el grupo de Galois de la extensión  $\mathbb{Q} \leq K$  es un subgrupo transitivo de  $S_3$ , luego es  $A_3$  o  $S_3$ .

Calculamos ahora:

$$\text{Disc}(f) = -4(-3)^3 - 27 = 81 = 9^2 \implies \Delta = \sqrt{\text{Disc}(f)} = 9 \in \mathbb{Q}$$

por lo que el grupo de Galois de  $f$  es  $A_3$ , de donde:

$$[K : \mathbb{Q}] = |A_3| = 3$$

por lo que por el Lema de la Torre tenemos que  $\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq K$ , por lo que  $\mathbb{Q}(\alpha) = K$ , ya que  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$  por ser  $f = \text{Irr}(\alpha, \mathbb{Q})$  con  $\text{grd}(f) = 3$ .

**Ejercicio 8.** Sea  $K$  el cuerpo de descomposición de  $f = (x^2 + 3)(x^3 - 3) \in \mathbb{Q}[x]$ . Calcular todos los subcuerpos de  $K$ . Demostrar que  $\mathbb{Q}(\sqrt[3]{3} + i\sqrt{3}) = K$ .

Las raíces de  $f$  son:

$$\pm i\sqrt{3}, \quad \sqrt[3]{3}, \quad w\sqrt[3]{3}, \quad w^2\sqrt[3]{3}, \quad w = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$$

con lo que  $K = \mathbb{Q}(i\sqrt{3}, \sqrt[3]{3}, w\sqrt[3]{3}, w^2\sqrt[3]{3})$ . Como  $w \in \mathbb{Q}(i\sqrt{3})$ , tenemos pues que:

$$K = \mathbb{Q}(i\sqrt{3}, \sqrt[3]{3})$$

y usando el Lema de la Torre obtenemos que:

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{3})] [\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 2 \cdot 3 = 6$$

Donde usamos:

- $\text{Irr}(\sqrt[3]{3}, \mathbb{Q}) = x^3 - 3$  por Eisenstein.
- $\text{Irr}(i\sqrt{3}, \mathbb{Q}(\sqrt[3]{3})) = x^2 + 3$ , ya que sus raíces son complejas.

Aplicamos la proposición de extensión, primero a  $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[3]{3})$  para determinar los homomorfismos de cuerpos  $\mathbb{Q}(\sqrt[3]{3}) \rightarrow K$ , que están en biyección con las raíces de  $\text{Irr}(\sqrt[3]{3}, \mathbb{Q}) = x^3 - 3$  en  $K$ . Así, aquellos son  $\eta_j : \mathbb{Q}(\sqrt[3]{3}) \rightarrow K$  determinados por:

$$\eta_j(\sqrt[3]{3}) = w^j \sqrt[3]{3}, \quad j \in \{0, 1, 2\}$$

Aplicando de nuevo la proposición citada a la extensión  $\mathbb{Q}(\sqrt[3]{3}) \leqslant K = \mathbb{Q}(\sqrt[3]{3})(i\sqrt{3})$ , puesto que  $\text{Irr}(i\sqrt{3}, \mathbb{Q}(\sqrt[3]{3})) = x^2 + 3$ , obtenemos los homomorfismos  $\eta_{j,k} : K \rightarrow K$  determinados por:

$$\eta_{j,k}(\sqrt[3]{3}) = w^j \sqrt[3]{3}, \quad \eta_{j,k} = (-1)^k \sqrt{3}, \quad j \in \{0, 1, 2\}, \quad k \in \{0, 1\}$$

De esta forma:

$$\text{Aut}(K) = \{\eta_{j,k} : j = 0, 1, 2, \quad k = 0, 1\}$$

Calculamos los órdenes de los elementos:

$$\begin{array}{ccccccc} \eta_{0,0} & \eta_{0,1} & \eta_{1,0} & \eta_{1,1} & \eta_{2,0} & \eta_{2,1} \\ \hline 1 & 2 & 3 & 2 & 3 & 2 \end{array}$$

Por ejemplo:

$$\begin{aligned} \eta_{1,1}(\eta_{1,1}(\sqrt[3]{3})) &= \eta_{1,1}(w\sqrt[3]{3}) = \eta_{1,1}(w)\eta_{1,1}(\sqrt[3]{3}) = \bar{w}w\sqrt[3]{3} = \sqrt[3]{3} \\ \eta_{1,1}(\eta_{1,1}(i\sqrt{3})) &= \eta_{1,1}(-i\sqrt{3}) = i\sqrt{3} \end{aligned}$$

Y ya sabemos en este punto los subgrupos que tenemos de  $\text{Aut}(K)$ .

- Usando la conexión de Galois,  $K^{\langle \eta_{1,0} \rangle}$  ha de ser una extensión de grado 2 de  $\mathbb{Q}$ . Como  $i\sqrt{3} \in K^{\langle \eta_{1,0} \rangle}$ :

$$\eta_{1,0}(i\sqrt{3}) = i\sqrt{3}$$

resulta que  $\mathbb{Q}(i\sqrt{3}) \leqslant K^{\langle \eta_{1,0} \rangle}$  con  $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$ , por lo que:

$$\mathbb{Q}(i\sqrt{3}) = K^{\langle \eta_{1,0} \rangle}$$

- Observemos que  $\eta_{0,1}(\sqrt[3]{3}) = \sqrt[3]{3}$ , de donde se deduce que  $\mathbb{Q}(\sqrt[3]{3}) \leqslant K^{\langle \eta_{0,1} \rangle}$  con:

$$[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$$

por lo que  $\mathbb{Q}(\sqrt[3]{3}) = K^{\langle \eta_{0,1} \rangle}$ .

- Si vemos que:

$$\eta_{1,1}(w\sqrt[3]{3}) = \eta_{1,1}(w)\eta_{1,1}(\sqrt[3]{3}) = \bar{w}w\sqrt[3]{3} = \sqrt[3]{3}$$

no es fijo, probamos ahora con:

$$\eta_{2,1}(w\sqrt[3]{3}) = \eta_{2,1}(w)\eta_{2,1}(\sqrt[3]{3}) = \eta_{2,1}(w)w^2\sqrt[3]{3} = w^2w^2\sqrt[3]{3} = w\sqrt[3]{3}$$

Y concluimos que  $\mathbb{Q}(w\sqrt[3]{3}) = K^{\langle \eta_{2,1} \rangle}$ .

- De forma análoga, observaremos que:

$$\mathbb{Q} \left( w^2 \sqrt[3]{3} \right) = K^{\langle \eta_{1,1} \rangle}$$

Para ver que:

$$K = \mathbb{Q} \left( \sqrt[3]{3} + i\sqrt{3} \right)$$

Obviamente tenemos que  $E = \mathbb{Q} \left( \sqrt[3]{3} + i\sqrt{3} \right) \leqslant K = \mathbb{Q} \left( \sqrt[3]{3} + i\sqrt{3} \right)$ . Para ver la igualdad, la estrategia que seguimos es ver que este subcuerpo no es ninguno de los ya mencionados, que son todos los posibles, descartando trivialmente  $\mathbb{Q}$ , por lo que tendrá que ser igual a  $K$ .

- Como  $\mathbb{Q} \left( \sqrt[3]{3} \right) \leqslant \mathbb{R}$  este tampoco puede ser, al igual que  $\mathbb{Q}$ .
- Para  $\mathbb{Q} \left( w\sqrt[3]{3} \right) = K^{\langle \eta_{2,1} \rangle}$ :

$$\eta_{2,1} \left( \sqrt[3]{3} + i\sqrt{3} \right) = \eta_{2,1} \left( \sqrt[3]{3} \right) + \eta_{2,1} \left( i\sqrt{3} \right) = w^2 \sqrt[3]{3} - i\sqrt{3}$$

Si fuese  $E = \mathbb{Q} \left( w\sqrt[3]{3} \right)$  entonces tendríamos que:

$$\sqrt[3]{3} + i\sqrt{3} = w^2 \sqrt[3]{3} - i\sqrt{3}$$

Y comparando partes reales (recordemos que  $w^2 = \bar{w}$ ), obtenemos:

$$\sqrt[3]{3} = -\frac{1}{2} \sqrt[3]{3}$$

lo que es una contradicción.

- De forma análoga se descartan todos.

**Ejercicio 9.** Sean  $\sqrt{2}, \sqrt[3]{2} \in \mathbb{R}$ :

1. Calcular razonadamente  $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$ .

Sale 6.

2. Decidir razonadamente si  $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, i\sqrt{3})$  es una extensión de Galois de  $\mathbb{Q}$ .

Vamos a tratar de ver si  $K$  es cuerpo de descomposición de un polinomio. Candidato a  $f$  para que  $K$  sea cuerpo de descomposición de  $f$ :

$$f = (x^2 - 2)(x^3 - 2)$$

así metemos las dos primeras, y el cuerpo de descomposición de  $f$   $E$  debe contener también las raíces cúbicas primitivas de la unidad, entre ellas:

$$w = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

Y tenemos así que  $E = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, w)$  y tenemos que  $\mathbb{Q} \leqslant E$  es de Galois, por ser un cuerpo de descomposición de un polinomio en característica 0. En vista de la forma de  $w$ , tenemos que  $E = K$ , por lo que  $\mathbb{Q} \leqslant K$  es de Galois.

3. Calcular  $\text{Aut}(K)$  definiendo explícitamente todos sus elementos.

Buscamos primero  $[K : \mathbb{Q}]$ , que por el Lema de la Torre:

$$[K : \mathbb{Q}] = \left[ K : \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \right] \left[ \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \right] = 2 \cdot 6 = 12$$

Y aplicamos ahora en reiteradas ocasiones la Proposición de extensión, para hallar todos los elementos de  $\text{Aut}(K)$ , obteniendo:

$$\begin{aligned} \eta_{j,k,l}(\sqrt{2}) &= (-1)^j \sqrt{2} \\ \eta_{j,k,l}(\sqrt[3]{2}) &= w^k \sqrt[3]{2} \\ \eta_{j,k,l}(i\sqrt{3}) &= (-1)^l i\sqrt{3} \\ j &\in \{0, 1\}, \quad k \in \{0, 1, 2\}, \quad l \in \{0, 1\} \end{aligned}$$

con todos estos números en  $K$ , el polinomio  $x^2 - 2$  es irreducible sobre  $\mathbb{Q}$ , el polinomio  $x^3 - 2$  es irreducible sobre  $\mathbb{Q}(\sqrt{2})$  por el apartado 2.

4. Calcular razonadamente el grado del polinomio

$$f = \text{Irr}(\sqrt{2} + \sqrt[3]{2}, \mathbb{Q})$$

Como  $\deg \text{Irr}(\alpha, \mathbb{Q}) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = (\text{Aut}_{\mathbb{Q}}(K) : \text{Aut}_{\mathbb{Q}(\alpha)}(K)) = \frac{|\text{Aut}_{\mathbb{Q}}(K)|}{|\text{Aut}_{\mathbb{Q}(\alpha)}(K)|}$ . Vemos que:

$$\text{Aut}_{\mathbb{Q}(\alpha)}(K) \supseteq \{\eta_{0,0,0}, \eta_{0,0,1}\}$$

ya que estos elementos dejan fijo el elemento  $\sqrt{2} + \sqrt[3]{2}$ . Veamos ahora que  $\alpha$  no se queda fijo por el resto de automorfismos:

$$\eta_{j,k,l}(\alpha) = \eta_{j,k,l}(\sqrt{2}) + \eta_{j,k,l}(\sqrt[3]{2}) = (-1)^j \sqrt{2} + w^k \sqrt[3]{2}$$

Tendremos que  $\eta_{j,k,l}(\alpha) = \alpha$  si y solo si:

$$\sqrt{2} + (-1)^{j+1} \sqrt{2} = (w^k - 1) \sqrt[3]{2}$$

como el de la izquierda es un número real, tiene que ser  $w^k - 1 \in \mathbb{R}$ , y esto sucede si y solo si  $k = 0$ . Por tanto tenemos que:

$$\sqrt{2} + (-1)^{j+1} \sqrt{2} = 0$$

de donde tiene que ser  $j + 1$  impar con  $j \in \{0, 1\}$ , luego tiene que ser  $j = 0$ . Así tenemos que:

$$\text{Aut}_{\mathbb{Q}(\alpha)}(K) = \{\eta_{0,0,0}, \eta_{0,0,1}\}$$

Por lo que:

$$\deg \text{Irr}(\alpha, \mathbb{Q}) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{|\text{Aut}_{\mathbb{Q}}(K)|}{|\text{Aut}_{\mathbb{Q}(\alpha)}(K)|} = \frac{12}{2} = 6$$

5. Decidir razonadamente quién es el grupo de Galois de  $f$ . ¿Es  $f$  resoluble por radicales? ¿Son las raíces complejas de este polinomio construibles por regla y compás?

Es de orden 12 porque  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[2]{2}, \sqrt[3]{2})$ . Otra forma de verlo es tomando  $E$  el cuerpo de descomposición de  $f$ ,  $\mathbb{Q} \leq K$  es de Galois y si la extensión contiene una raíz las tiene todas, por lo que  $\mathbb{Q}(\alpha) \leq E \leq K$ . Como es un cuerpo de descomposición, tendremos que  $\mathbb{Q} \leq E$  es de Galois. Si un polinomio irreducible tiene una raíz en  $E$  tiene que tenerlas todas, como por ejemplo  $x^3 - 2$ . Tiene que ser  $E = K$ .

Como todo grupo de orden 12 es resoluble tenemos que  $f$  es resoluble por radicales, por ser su grupo de Galois resoluble.

Una raíz es del grado de  $\deg \text{Irr}(\alpha, \mathbb{Q}) = 6$ , y todas estas tienen el mismo grado, que no es potencia de 2, por lo que ninguna de las raíces es constructible.

**Ejercicio 10.** Sea  $K$  el cuerpo de descomposición de  $f = x^6 - 3 \in \mathbb{Q}[x]$ .

- a) Calcular  $[K : \mathbb{Q}]$ .

Sea  $w$  una raíz sexta primitiva de la unidad, tenemos por un Teorema que  $K = \mathbb{Q}(\sqrt[6]{3}, w)$ . Podemos calcular el  $w$  con razones trigonométricas o con el sexto polinomio ciclotómico, que tiene grado 2:

$$\phi_6 = \frac{x^6 - 1}{\phi_1 \phi_2 \phi_3} = \frac{x^6 - 1}{(x - 1)(x + 1)(x^2 + x + 1)}$$

Dividimos:

$$x^6 - 1 = (x - 1)(x + 1)(4 + x^2 + 1) = (x^2 - 1)(x^4 + x^2 + 1) = \phi_1 \phi_2 \phi_3 (x^2 - x + 1)$$

Si lo hacemos por otra parte:

$$\phi_6 = (x - w)(x - w^5) = (x - w)(x - \bar{w}) = x^2 - 2Re w + 1$$

tenemos que usar por tanto trigonometría, con  $\cos(30^\circ) = 1/2$ . De aquí:

$$w = \frac{1 \pm \sqrt{-3}}{2} = \frac{1}{2} \pm i \frac{\sqrt{3}}{2}$$

tomamos  $w = \frac{1}{2} + i \frac{\sqrt{3}}{2}$ . Y obtenemos así que:

$$K = \mathbb{Q}(\sqrt[6]{3}, w) = \mathbb{Q}(\sqrt[6]{3}, i\sqrt{3})$$

Por el Lema de la Torre obtenemos fácilmente que  $[K : \mathbb{Q}] = 2 \cdot 6 = 12$ .

- b) Demostrar que  $i + \sqrt{3} \in K$ .

Tenemos que:

$$\sqrt{3} = (\sqrt[6]{3})^3 \in K$$

Por lo que:

$$i = \frac{i\sqrt{3}}{\sqrt{3}} \in K$$

de donde  $i + \sqrt{3} \in K$ .

c) Calcular, definiendo explícitamente todos sus elementos, el grupo  $G = \text{Aut}_{\mathbb{Q}(i+\sqrt[6]{3})}(K)$ .

Del apartado anterior vemos que  $K = \mathbb{Q}(\sqrt[6]{3}, i)$ , y aplicando la Proposición de extensión vemos que:

$$\text{Aut}(K) = \{\sigma_{j,k} : j \in \{0, \dots, 5\}, k \in \{0, 1\}\}$$

donde:

$$\sigma_{j,k}(\sqrt[6]{3}) = w^j \sqrt[6]{3}, \quad \sigma_{j,k}(i) = (-1)^k i$$

Tenemos que:

$$|G| = (G : \{\sigma_{0,0}\}) = [K : \mathbb{Q}(i + \sqrt{3})] = \frac{[K : \mathbb{Q}]}{[\mathbb{Q}(i + \sqrt{3}) : \mathbb{Q}]}$$

y como:

$$[\mathbb{Q}(i + \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}] = 4$$

tenemos entonces que:

$$|G| = 3$$

Será:

$$G \supseteq \{\sigma_{0,0}, \sigma_{2,0}, \sigma_{4,0}\}$$

ya que:

$$\sigma_{2,0}(\sqrt{3} + i) = \sigma_{2,0}\left(\left(\sqrt[6]{3}\right)^3\right) + \sigma_{2,0}(i) = w^6\left(\sqrt[6]{3}\right)^3 + i = i + \sqrt{3}$$

y como tenemos 3 será pues  $G = \{\sigma_{0,0}, \sigma_{2,0}, \sigma_{4,0}\}$ .

d) ¿Es  $G$  un subgrupo normal del grupo de Galois de  $f$ ?

Como  $\mathbb{Q} \leq \mathbb{Q}(i + \sqrt{3})$  es de Galois por ser cuerpo de descomposición de un polinomio tenemos que el grupo es normal.

**Ejercicio 11.** Calcular el número de polinomios irreducibles mónicos de grado hasta 3 en  $\mathbb{F}_5[x]$ .

- De grado 1 tenemos todos los irreducibles mónicos de grado 1:

$$x, \quad x - 1, \quad x - 2, \quad x - 3, \quad x - 4$$

- Para los de grado 2 sabemos que van a aparecer en la descomposición del polinomio  $x^{25} - x$ , y sabemos que ya tenemos 5, nos queda grado 20 y polinomios de grado 2 serán 10.
- Para los de grado 3, sabemos que van a aparecer en la descomposición del polinomio  $x^{125} - x$ , y sabemos que 2 no divide a 3, por lo que tenemos 5 y nos queda 120 entre 3, obteniendo 40.

Así, hay 55 polinomios mónicos irreducibles de grado hasta 3.

**Ejercicio 12.** En  $\mathbb{F}_{81} = \mathbb{F}_3(a)$  con  $a$  un elemento primitivo, describir todos los subcuerpos de  $\mathbb{F}_{81}$ .

Sabemos que  $81 = 3^4$  y que cada divisor del exponente nos da un cuerpo, por lo que tenemos  $3^1, 3^2$  y  $3^4$ .

Sabemos que  $\mathbb{F}_{81}^\times$  es un grupo cíclico de orden 80:

$$\mathbb{F}_{81}^\times = \{1, a, \dots, a^{79}\}$$

Por lo que:

$$\mathbb{F}_{81} = \{1, a, \dots, a^{80}\}$$

Un cuerpo de 9 elementos seguro que existe, buscamos un elemento que se exprese en términos de  $a$  para expresar  $\mathbb{F}_9$ , es decir, buscar un elemento de orden 8. Como:

$$(a^{10})^8 = a^{80} = 1$$

Tenemos que  $a^{10}$  tiene orden 8, por lo que:

$$\mathbb{F}_9 = \mathbb{F}_3(a^{10})$$

Cada subcuerpo de  $\mathbb{F}_{81}$  es subgrupo (quitando el 0) de  $\mathbb{F}_{81}^\times$ , pero hay más subgrupos de este que subcuerpos.

**Ejercicio 13.** ¿Cuántos subcuerpos tiene  $\mathbb{F}_{256}$ ?

Tenemos que  $256 = 2^8$ , con  $\text{Div}(8) = \{1, 2, 4, 8\}$ .

**Ejercicio 14.** Sea  $F = \mathbb{F}_3(a)$  con  $a^3 + a - 1 = 0$ :

1. Calcular el cardinal de  $F$ .

Tenemos que  $f = x^3 + x - 1$  no es irreducible, lo factorizamos:

$$x^3 + x - 1 = (x + 1)(x^2 - x - 1)$$

y como  $a$  es raíz de  $f$  tenemos que:

- Bien es raíz de  $x + 1$ , es decir,  $a = -1$ , con lo que  $F = \mathbb{F}_3(-1) = \mathbb{F}_3$ .
- Bien  $a^2 - a - 1 = 0$ , de donde  $[F : \mathbb{F}_3] = 2$ , con lo que  $|F| = 9$ .

2. Calcular el grado de  $\text{Irr}(a^2, \mathbb{F}_3)$ .

Tenemos que:

$$a^2 - a - 1 = 0 \implies a^2 = a + 1 \notin \mathbb{F}_3$$

ya que  $\{1, a\}$  es una  $\mathbb{F}_3$ -base de  $F$ . Por tanto,  $\text{Irr}(a, \mathbb{F}_3)$  tiene que tener grado 2.

3. Calcular  $\text{Irr}(a^2, \mathbb{F}_3)$ .

Buscamos en los 3 polinomios mónicos irreducibles de  $\mathbb{F}_3[x]$ , buscando dónde es  $a^2$  raíz, y podemos descartar  $x^2 - x - 1$ , por ser  $a$  raíz suya.

- Probamos en  $a^2 + 1$ :

$$(a^2)^2 + 1 = (a + 1)^2 + 1 = a^2 + 2a + 1 + 1 = a + 1 + 2a + 2 = 3a + 3 = 0$$

Hemos tenido suerte, por lo que  $\text{Irr}(a^2, \mathbb{F}_3) = x^2 + 1$ .