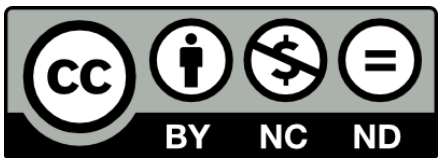
# Álgebra III


**Los Del DGIIM**, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada



# Álgebra III

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán

Granada, 2025

# Índice general


**1. Extensiones de cuerpos y raíces de polinomios** **5**
- 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

**2. Extensiones de Galois** **73**
- 2.1. Extensiones de Galois . . . 73
- 2.2. Teorema fundamental de la Teoría de Galois . . . 82
- 2.3. El Teorema Fundamental del Álgebra . . . 90
- 2.4. Ejercicios . . . 91

**3. Teoría de Galois de Ecuaciones** **99**
- 3.1. Grupo de Galois de un polinomio . . . 99
  - 3.1.1. Estructura de $S_n$ . . . 104
  - 3.1.2. Ejercicios . . . 111
- 3.2. Extensiones ciclotómicas . . . 111
- 3.3. Construcciones con regla y compás II . . . 118
- 3.4. Extensiones cíclicas . . . 122
- 3.5. Ecuaciones resolubles por radicales . . . 127
- 3.6. Ecuación general de grado $n$ . . . 133
- 3.7. Resolución de ecuaciones de grado hasta 4 . . . 136
  - 3.7.1. Cuadrática . . . 136
  - 3.7.2. Cúbica . . . 137
  - 3.7.3. Cuártica . . . 139
- 3.8. Cuerpos finitos . . . 141

**4. Ejercicios** **147**

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 <u>conmutativo</u> cuando esta sí lo es.

**Definición 1.1** (Cuerpo)**.** Un cuerpo es un anillo conmutativo $A$ 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 conmutativo $A$ 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*

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

*Además, $Im\chi$ es el menor subanillo de $A$.*

*Demostración.* Tenemos que probar:

**Unicidad.** Sean $\chi, \varphi : \mathbb{Z} \to A$ 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** $0 \leqslant s \leqslant k$ , vemos que:

$$\chi(k+1) = \chi(k) + \chi(1) = \varphi(k) + \varphi(1) = \varphi(k+1)$$
$$\chi(-(k+1)) = -\chi(k+1) = -\varphi(k+1) = \varphi(-(k+1))$$

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

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

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

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

**Minimalidad.** Para ver que $Im\chi$ es el menor subanillo contenido en $A$, vimos ya en Álgebra I que $Im\chi$ 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:

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

Por lo que $Im\chi \subseteq S$, de donde todo subanillo de $A$ contiene a $Im\chi$ 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

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

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 cumplan 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. □

**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[1], 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.

[1]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.

$\Longleftarrow$) 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 $\chi : \mathbb{Z} \to K$, 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[2] 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 $F \leqslant K$ 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 $F \leqslant K$ una extensión de cuerpos, decimos que una aplicación $\sigma : K \to K$ es $F-$lineal si verifica que:

$$\sigma(x + y) = \sigma(x) + \sigma(y) \qquad \forall x, y \in K$$
$$\sigma(a \cdot x) = a \cdot \sigma(x) \qquad \forall a \in F, \forall x \in K$$

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

$$[K : F]$$

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

**Ejemplo.** Como ejemplos a destacar:

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

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

[2]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 $\mathbb{R} \overset{f}{\cong} \mathbb{Q}^n$, 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 $n \geqslant 1$.

Sea $K$ un cuerpo finito, este no podrá tener característica cero, porque entonces seríamos capaces de obtener una cantidad infinita de elemetos 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:

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

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

Haremos próximamente una clasificacion 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 $F \leqslant K$ 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 $S = \{s_1, \ldots, s_t\}$, simplificaremos la notación y escribiremos $F(s_1, \ldots, s_t)$.
- Si $K = F(\alpha_1, \ldots, \alpha_t)$ para ciertos elementos $\alpha_1, \ldots, \alpha_t \in K$, diremos entonces que $F \leqslant K$ 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 $F \leqslant K$ es una extensión de cuerpos, no es lo mismo que $F \leqslant K$ sea finita o que sea finitamente generada:

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

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

  $\supseteq$) Es claro que $K$ contiene a $F$ y a $u_1, \ldots, u_n$, por lo que debemos tener $F(u_1, \ldots, u_n) \leqslant K$, por definición de $F(u_1, \ldots, u_n)$.

  $\subseteq$) Como $\{u_1, \ldots, u_n\}$ es una $F-$base de $K$, todo elemento $g \in K$ puede escribirse como:

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

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

- No toda extensión finitamente generada es finita. Veremos que a veces no se cumple esta propiedad y otras veces sí:
  - La extensión $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt{2}\right)$ es una extensión finita y claramente es finitamente generada.
  - La extensión $\mathbb{R} \leqslant \mathbb{R}(i)$ es una extensión finitamente generada pero no es finita (veremos que $\mathbb{R}(i) = \mathbb{C}$).

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

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

*Demostración.* Veámoslo:

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

$\subseteq$) Si demostramos que $Q = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$ es un cuerpo, entonces tenemos esta inclusión, ya que $\mathbb{Q}\left(\sqrt{2}\right)$ es el menor subcuerpo de $\mathbb{R}$ que contiene a $\sqrt{2}$. Es evidente que $Q$ es un anillo conmutativo. 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:

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

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:

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

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

□

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

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

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

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

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

**Definición 1.9** (Cuerpo de descomposición)**.** Sea $K \leqslant E$ 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 $\alpha_1, \ldots, \alpha_t \in E$ todas las raíces de $f$.
- $E = K(\alpha_1, \ldots, \alpha_t)$.

Diremos entonces que $E$ es un cuerpo de descomposición[3] 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 $\mathbb{Q}(i) = \mathbb{Q}(i, -i)$.

  $\subseteq$) Trivial.

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

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

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

**Ejercicio 1.1.1.** Si tenemos $F \leqslant K$ una extensión de cuerpos y $S, T \subseteq K$, demostrar que:
$$F(S \cup T) = F(S)(T)$$

*Demostración.* Veámoslo por doble inclusión:

$\subseteq$) $F(S \cup T)$ 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 $F(S \cup T) \subseteq F(S)(T)$.

$\supseteq$) 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, $F(S)(T) \subseteq F(S \cup T)$.

□

[3] o de escisión.

[4] Fundamentado por el Teorema Fundalmental 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 $r \geqslant 0$, el conjunto de todos los números complejos que satisfacen (para $n \in \mathbb{N}$):*

$$z^n = r$$

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

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

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

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

$$\left( \sqrt[n]{r} e^{i\frac{2\pi k}{n}} \right)^n = \left( \sqrt[n]{r} \right)^n \cdot \left( e^{i\frac{2\pi k}{n}} \right)^n = r \cdot e^{i2\pi k} = r(\cos(2\pi k) + i \operatorname{sen}(2\pi k)) = r$$

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

$$z = |z|(\cos(\theta) + i \operatorname{sen}(\theta))$$

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

$$r = z^n = |z|^n(\cos(\theta) + i \operatorname{sen}(\theta))^n \overset{(*)}{=} |z|^n(\cos(n\theta) + i \operatorname{sen}(n\theta))$$

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

$$\left.\begin{array}{l} r = |z|^n \cos(n\theta) \\ 0 = |z|^n \operatorname{sen}(n\theta) \end{array}\right\} \iff n\theta = 2\pi k \iff \theta = \frac{2\pi k}{n}$$

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

□

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

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

**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:

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

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:

$$R = \left\{1, w, w^2, \ldots, w^{n-1}\right\}$$

□

**Definición 1.10.** Sea $r \in \mathbb{Z}$ con $r \geqslant 0$ 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 compleja de $r$ que genera todas las raíces complejas $n-$ésimas de $r$.
Equivalentemente, si $w$ tiene orden multiplicativo $n$.

Próximamente veremos una generalización del estudio de las raíces $n-$ésimas de la unidad.

**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:

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

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

*Demostración.* Por doble inclusión:

$\subseteq$) Como $\mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$ 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 $\mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$.

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

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

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

□

**Ejemplo.** Tomamos $f = x^n - 1 \in \mathbb{Q}[x]$ con $n \geqslant 1$ 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 $F \leqslant K$ 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 $F \leqslant K$ una extensión de cuerpos y $\alpha \in K$ un elemento algebraico sobre $F$. Tenemos entonces que existe un único polinomio mónico*[5] *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 $F \leqslant F(\alpha)$ tiene grado $degf$, siendo $\{1, \alpha, \dots, \alpha^{degf-1}\}$ una $F-$base de $F(\alpha)$.*

*Demostración.* Definimos la aplicación "evaluación en $\alpha$"

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

que es un homomorfismo de anillos por la Propiedad Universal del Anillo de Polinomios, aplicado a la incusión $\iota : F \to K$ y al elemento $\alpha \in K$. Por tanto, su núcleo

[5] El coeficiente líder es 1.

$\ker e_\alpha$ 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:

- 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:

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

  dado por:

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

  Donde $Ime_\alpha$ 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

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

  nos dice que $Ime_\alpha$ 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 $a \in Ime_\alpha$, luego $F \leqslant Ime_\alpha$.
  - Si consideramos ahora el polinomio identidad $h = x \in F[x]$, tenemos que: $e_\alpha(h) = h(\alpha) = \alpha$, por lo que $\alpha \in Ime_\alpha$.

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

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

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 $Ime_\alpha \subseteq F(\alpha)$ que nos faltaba. En definitiva:

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

- Para ver que $\mathcal{B} = \{1, \alpha, \dots, \alpha^{degf-1}\}$ 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:

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

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 $degg \geqslant degf$, entonces usando que $F[x]$ es DE, podemos encontrar $q, r \in F[x]$ de forma que:

$$g = fq + r \qquad \text{con} \qquad degr < degf$$

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:

$$g(x) = \sum_{i=1}^{degf-1} f_i x^i \qquad f_i \in F$$

Luego $B = \{1 + \langle f \rangle, x + \langle f \rangle, \dots, x^{degf-1} + \langle f \rangle\}$ 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 $F \leqslant K$ 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 $\mathrm{Irr}(\alpha, F)$.

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

Si $F \leqslant K$ es una extensión de cuerpos y $\alpha \in K$, para buscar $\mathrm{Irr}(\alpha, F)$ 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 $g = h \operatorname{Irr}(\alpha, F)$ 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 $\operatorname{Irr}(\alpha, F)$, puesto que la condición $g(\alpha) = 0$ implica que $\operatorname{Irr}(\alpha, F)$ divide a $g$.

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

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

  $$x^3 - 1 = (x - 1)\left(x^2 + x + 1\right)$$

  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 $Irr\left(e^{\frac{2\pi i}{3}}, \mathbb{Q}\right) = x^2 + x + 1$.

  Una $\mathbb{Q}-$base de $\mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right)$ es $\left\{1, e^{\frac{2\pi i}{3}}\right\}$, 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 $F \leqslant K$ extensión y $\alpha \in K$ de grado 2 sobre $F$. Demostrar que $F(\alpha)$ es un cuerpo de descomposición de $Irr(\alpha, F)$.

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

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

puesto que sabemos que $Irr(\alpha, F)$ es un polinomio mónico. Por la propia definición de $Irr(\alpha, F)$, sabemos que $\alpha$ es raíz de este polinomio, por lo que el Teorema de

Ruffini nos dice que $Irr(\alpha, F)$ es divisible entre $(x-\alpha)$ en $K[x]$, luego se cumple que:

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

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

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

Deducimos que $a = -\alpha-\beta$, por lo que $\beta = -(\alpha+a) \in F(\alpha)$. En definitiva, acabamos de ver que $Irr(\alpha, F)$ 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 $Irr(\alpha, F)$.

**Ejercicio 1.1.3.** Calcular $Irr\left(w, \mathbb{Q}\left(\sqrt[3]{2}\right)\right)$, 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 $\mathbb{Q}\left(\sqrt[3]{2}\right)[x]$, por ser de grado 2 y ser sus dos raíces complejas (son $w$ y $w^2$). En definitiva, hemos probado que:

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

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

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:

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

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

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

## 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 $F \leqslant K \leqslant L$ es una extensión de cuerpos, entonces:*

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

*Además,* $[L : F] = [L : K][K : F]$.

*Demostración.* Por doble implicación:

$\Longrightarrow$) Notemos que $K$ es un $F-$subespacio vectorial de $L$, del que suponíamos ser un $F-$espacio vectorial de dimensión finita, por lo que $F \leqslant K$ será también una extensión finita. Como $F \subseteq K$, si tomamos $\{\alpha_1, \ldots, \alpha_t\}$ 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 $K \leqslant L$ también es finita, ya que basta mirar los escalares de $F$ como si fueran escalares de $K$.

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

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

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

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

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

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

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

  de donde:

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

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

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

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

Para la fórmula entre las dimensiones, si $F \leqslant K$ o $K \leqslant L$ no fuera finita, tendríamos entonces que $F \leqslant L$ 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 "$\Longleftarrow$)" 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:

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

tenemos la fórmula demostrada. □

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

$$F_1 \leqslant F_2 \leqslant \ldots \leqslant F_s$$

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 $\mathbb{Q}\left(w, \sqrt[3]{2}\right)$ era un cuerpo de descomposición de $x^3 - 2 \in \mathbb{Q}[x]$. Queremos calcular:

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

Calculemos mediante una torre:

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

Sabemos ya que:

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

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

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

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

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

En definitiva:

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

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

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

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

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

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

de donde:

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

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

$$\mathbb{Q}\left(\sqrt{5},\sqrt{-2}\right)\leqslant\mathbb{Q}(\alpha)\leqslant\mathbb{Q}\left(\sqrt{5},\sqrt{-2}\right)$$

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

$$\mathbb{Q}\leqslant\mathbb{Q}\left(\sqrt{5}\right)\leqslant\mathbb{Q}\left(\sqrt{5}\right)\left(\sqrt{-2}\right)=\mathbb{Q}\left(\sqrt{5}+\sqrt{-2}\right)$$

por el Lema de la Torre:

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

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:

$$\left[\mathbb{Q}(\sqrt{5}+\sqrt{-2}):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{5}\right):\mathbb{Q}\right]\left[\mathbb{Q}\left(\sqrt{5}\right)\left(\sqrt{-2}\right):\mathbb{Q}\left(\sqrt{5}\right)\right]=2\cdot2=4$$

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

*Demostración.* Por doble implicación:

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

$\Longleftarrow$) Sea $L$ un cuerpo en las condiciones del enunciado, tenemos entonces que como $F \leqslant L$ es finita y $F \leqslant F(\alpha) \leqslant L$ entonces (usando el Lema de la Torre) $F \leqslant F(\alpha)$ es finita, luego el conjunto $\{\alpha^n : n \geqslant 0\}$ no puede ser $F-$linealmente independiente, si no que tiene que existir $m \in \mathbb{N}$ con $m \geqslant 1$ de forma que $\alpha^m$ dependa linealmente de $1, \alpha, \ldots, \alpha^{m-1}$, es decir, existen $a_0, \ldots, a_{m-1} \in F$ 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 $F \leqslant K$ 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 $F \leqslant K$ una extensión de cuerpos, por doble implicación:

$\Longrightarrow$) Tomamos $\{u_1, \ldots, u_t\}$ una $F-$base de $K$, tenemos entonces que $K = F(u_1, \ldots, u_t)$. Además, si $\alpha \in K$, tenemos entonces que $F \leqslant F(\alpha) \leqslant K$ con $F \leqslant K$ finita, por lo que por el Lema de la Torre tenemos que $F \leqslant F(\alpha)$ es finita. Tomando $L = F(\alpha)$ y aplicando la Proposición anterior tenemos que $\alpha$ es algebraico sobre $F$.

$\Longleftarrow$) Suponemos que $K = F(\alpha_1, \ldots, \alpha_n)$ y que $\alpha_i$ es algebraico sobre $F$ para todo $i \in \{1, \ldots, n\}$. Por el lema de la torre y la Proposición 1.7, tenemos:

$$F \leqslant F(\alpha_1) \leqslant \ldots \leqslant F(\alpha_1, ..., \alpha_n)$$

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

□

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

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

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

*Entonces, $\Lambda$ es un subcuerpo de $K$ y la extensión $F \leqslant \Lambda$ 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 $F \leqslant F(\alpha, \beta)$ 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 $F \leqslant F(\alpha)$ 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 $F \leqslant K$ es algebraico. □

**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 $\left[\overline{\mathbb{Q}} : \mathbb{Q}\right] = \infty$, puesto que para todo $n \in \mathbb{N}$ podemos considerar $\mathbb{Q}\left(\sqrt[n]{2}\right) \leqslant \overline{\mathbb{Q}}$ y $\left[\mathbb{Q}\left(\sqrt[n]{2}\right) : \mathbb{Q}\right] = n$, que lo sabemos porque:

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

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

### 1.2.1. Ejercicios

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

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

$$\alpha - \sqrt{2} = i \Longrightarrow \alpha^2 + 2 - 2\alpha\sqrt{2} = -1 \Longrightarrow \sqrt{2} = \frac{\alpha^2 + 3}{2\alpha} \in \mathbb{Q}(\alpha)$$

$$\alpha - i = \sqrt{2} \Longrightarrow \alpha^2 - 1 - 2\alpha i = 2 \Longrightarrow i = \frac{\alpha^2 - 3}{2\alpha} \in \mathbb{Q}(\alpha)$$

Tenemos entonces que $\mathbb{Q}(\sqrt{2}, i) \leqslant \mathbb{Q}(\alpha)$, 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 $Irr(\alpha, \mathbb{Q})$. Para ello:

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

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:

$$\alpha - \sqrt{2} = i\sqrt{3} \Longrightarrow \alpha^2 + 2 - 2\alpha\sqrt{2} = -3 \Longrightarrow \sqrt{2} = \frac{\alpha^2 + 5}{2\alpha} \in \mathbb{Q}(\alpha)$$
$$\alpha - i\sqrt{3} = \sqrt{2} \Longrightarrow \alpha^2 - 3 - 2\alpha i\sqrt{3} = 2 \Longrightarrow i\sqrt{3} = \frac{\alpha^2 - 5}{2\alpha} \in \mathbb{Q}(\alpha)$$

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:

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

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:

$$e^{i\frac{\pi}{4}} = \cos\frac{\pi}{4} + i\,\mathrm{sen}\,\frac{\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

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:

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

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

$$\sqrt{2} \in K \Longrightarrow \mathbb{Q}(\sqrt{2}) \leqslant K$$
$$i\sqrt{2} \in K \Longrightarrow i \in K \Longrightarrow \mathbb{Q}(\sqrt{2}, i) \leqslant K$$

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 $\mathrm{Irr}(\alpha, \mathbb{Q})$.

a) Para el primero:

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

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 $x^3-2 = Irr(\sqrt[3]{2},\mathbb{Q})$, 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 $f = \mathrm{Irr}(1+\sqrt[3]{2},\mathbb{Q})$. Calcular las raíces complejas de $f$ y un cuerpo de descomposición suyo.

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

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

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

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

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:

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

Con lo que tomando $f = x^3-3x^2+3x-3 \in \mathbb{Q}[x]$ tenemos que $f = Irr(\alpha,\mathbb{Q})$. 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:

$$e^{\frac{2\pi i}{3}} = \cos\left(\frac{2\pi}{3}\right) + i\,\text{sen}\left(\frac{2\pi}{3}\right) = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$$
$$e^{\frac{4\pi i}{3}} = \cos\left(\frac{4\pi}{3}\right) + i\,\text{sen}\left(\frac{4\pi}{3}\right) = \frac{-1}{2} - i\frac{\sqrt{3}}{2}$$

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

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

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

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

y se verifica que es igual a:

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

## 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

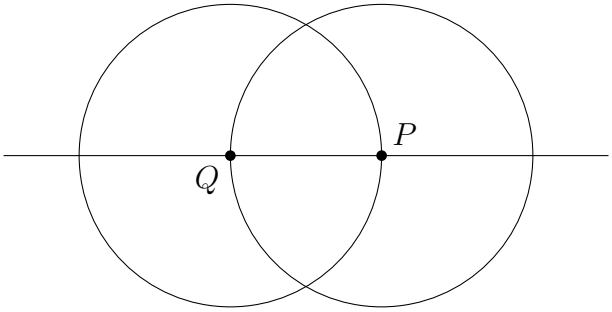



Figura 1.1: Prueba gráfica de que $S \subseteq S^c$.

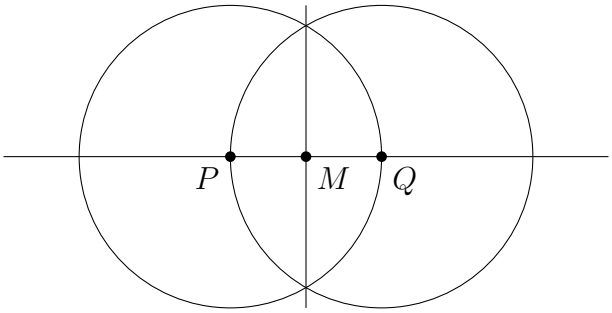



Figura 1.2: Construcción de la mediatriz.

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.

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

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

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 mediatriz, 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

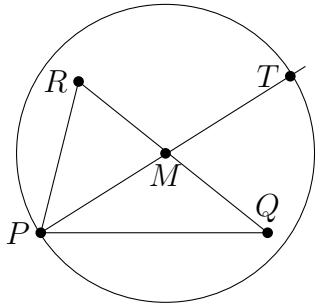



Figura 1.3: Completar el cuarto punto de un paralelogramo.

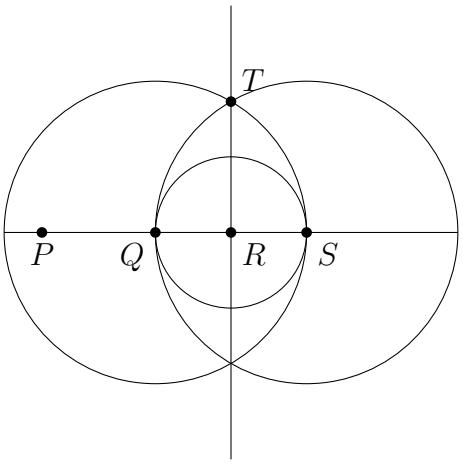



Figura 1.4: Trazar recta perpendicular por $R$.

$Q$, 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 $R$:

**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.

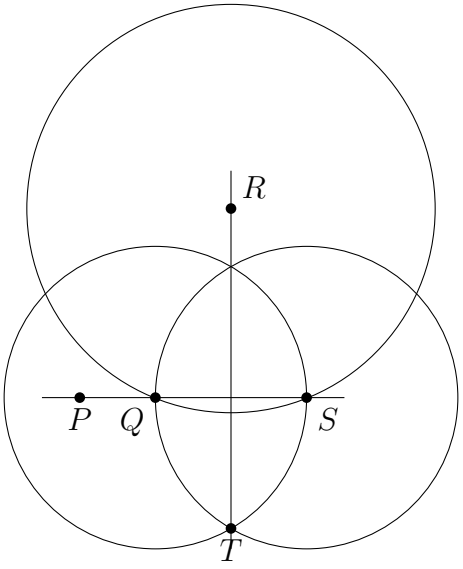


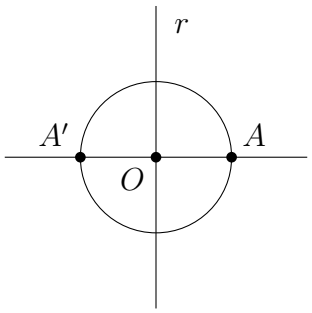

Figura 1.5: Trazar recta parpendicular por $R$.

□

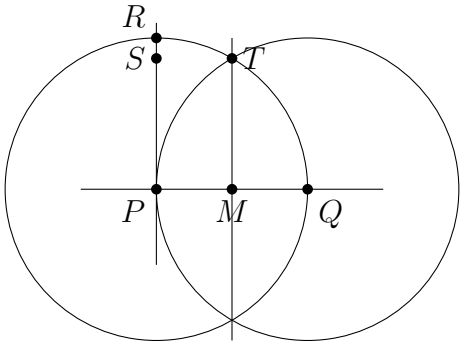
A partir del lema anterior, ya no será necesario recurrir a dichas construcciones cada vez que tengamos dos puntos $P$ y $Q$ que determinan una recta y queramos construir una recta perpendicular a ella que pase por un tercer punto $R$.

**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 mediatriz, 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. 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:

$\Longrightarrow$) 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

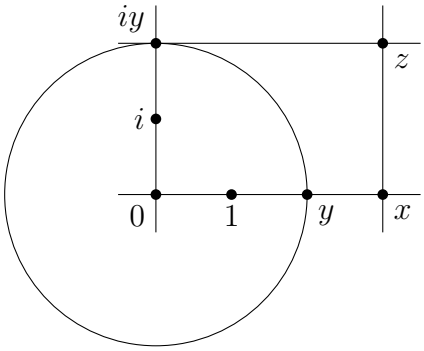



Figura 1.6: Obtención de $x$, $y$ a partir de $z$.

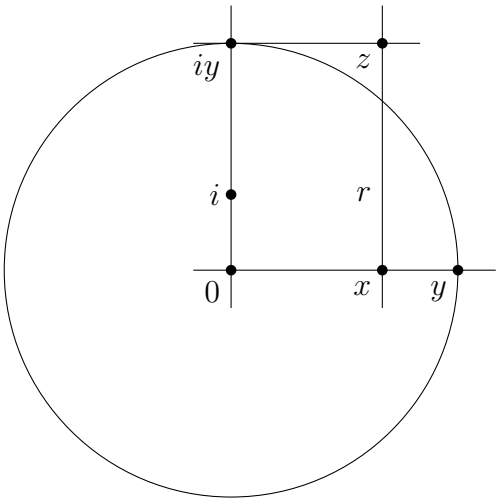



Figura 1.7: Obtención de $z$ a partir de $x$ e $y$.

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.

$\Longleftarrow$) 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 ilusta en la Figura 1.7.

□

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

$$z \in C(S) \Longrightarrow \overline{z} \in C(S)$$

*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 construcible. Para el inverso, si demostramos que todo conjugado de un número construcible 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:

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

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 $r' - r$.

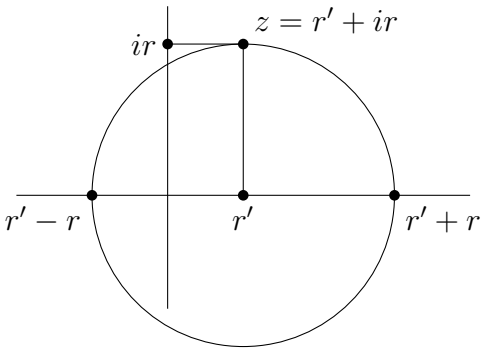
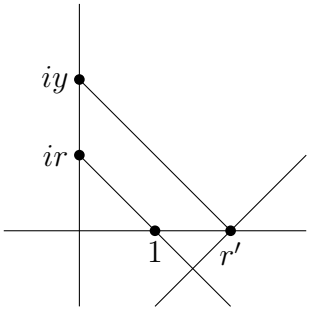



Figura 1.8: Obtención de $r' + r$ y $r' - r$ a partir de $r$ y $r'$.

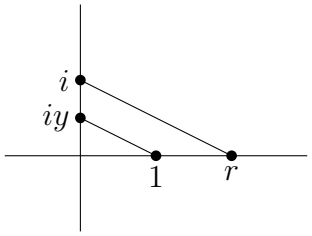
Por lo que $r + r', r - r' \in C(S) \cap \mathbb{R}$.
Bajo las mismas hipótesis, tratamos de probar que $r \cdot r' \in C(S) \cap \mathbb{R}$, supondremos de la misma forma que $r, r' > 0$ y lo que haremos será considerar los puntos $r'$, $ir$. Trazaremos la recta que une el punto 1 con $ir$ y trazaremos 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:

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

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.



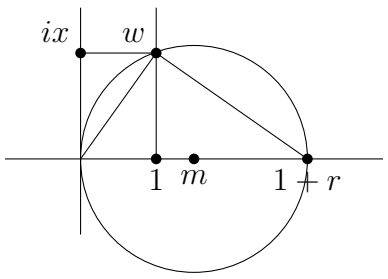

Ambos triángulos semejantes, luego:

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

□

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

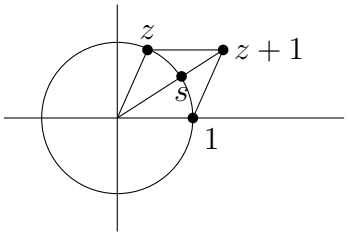
*Demostración.* Escribiendo $z$ en forma polar, reducimos el problema al caso $|z| = 1$. Si tomamos $r > 0$ con $r \in C(S) \cap \mathbb{R}$, veamos entonces que $\sqrt{r} \in C(S) \cap \mathbb{R}$. Para ello, consideramos el punto $1 + r$ (anteriormente probamos que era constructible), trazamos el punto 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:

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

Una vez hecha esta distinción, si tomamos un número complejo de módulo 1 $z = e^{i\theta}$, tenemos que ver que si $e^{i\theta} \in C(S)$, entonces $e^{i\frac{\theta}{2}} \in C(S)$. Para ello, lo que haremos 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 $C(S) \leqslant C'$. Recordemos que teníamos que:

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

Por lo que basta demostrar 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 pertence 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 $F \leqslant K$ extensión, diremos que $K$ es una torre por raíces cuadradas sobre $F$ si $K = F(u_1, \ldots, u_t)$, donde $u_1^2 \in F$ y $u_{i+1}^2 \in F(\overline{u_1, \ldots, u_i})$ para $i \in \{1, \ldots, t-1\}$

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

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

**Teorema 1.16.** *Sean $\{0,1\} \subseteq S \subseteq \mathbb{C}$, $F = \mathbb{Q}(S \cup \overline{S})$ 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:

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

Si tomamos:

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

Queda claro que $K \leqslant M$, $E \leqslant M$, por lo que es evidente que $\alpha - \beta, \alpha\beta, \alpha^{-1} \in M$.

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

Sea $z \in L$, queremos ver que $\overline{z} \in L$. Si $z \in L$, entonces $z \in K = F(u_1, \ldots, u_t)$, de donde $\overline{z} \in F(\overline{u_1}, \ldots, \overline{u_t})$, ya que $F$ es cerrado por conjugación, y tenemos que $F(\overline{u_1}, \ldots, \overline{u_t}) \in \mathcal{T}$, de donde $\overline{z} \in L$. Obviamete $L$ es cerrado por raíces cuadradas. Como $C(S)$ era el menor subcuerpo de $\mathbb{C}$ que contiene a $S$ y que es cerrado para conjugación y raíces cuadradas concluimos que $C(S) = L$. □

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

*Demostración.* Si $\alpha \in C(S)$, tenemos por el Teorema anterior que existe una torre por raíces cuadradas $F \leqslant K$ tal que $\alpha \in K$. Como $F(\alpha) \leqslant K$, deducimos del Lema de la Torre que $F \leqslant F(\alpha)$ es finita y que $[F(\alpha) : F]$ es un divisor de $[K : F]$. Como este último número es una potencia de dos por ser $F \leqslant K$ una torre por raíces cuadradas, tenemos que $[F(\alpha) : F]$ tiene que ser una potencia de 2. □

**Definición 1.17.** Un número complejo $z$ se dice constructible si lo es a partir de $\{0, 1\}$.

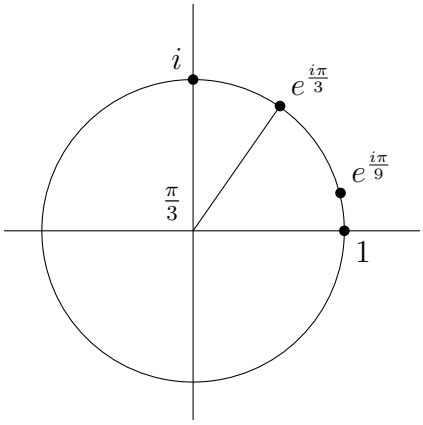
**Corolario 1.16.2.** *Todo número constructible ($F = \mathbb{Q}$) es algebraico y tiene grado sobre $\mathbb{Q}$ una potencia de 2.*

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 contraejemplo.

**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 $60^{\text{o}}$ no se puede trisecar con regla y compás.




El elemento:

$$e^{\frac{i\pi}{3}} = \frac{1}{2} + i\frac{\sqrt{3}}{2} \in \mathbb{Q}\left(i, \sqrt{3}\right)$$

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

$$e^{\frac{i\pi}{9}} = \cos\frac{\pi}{9} + i\,\text{sen}\,\frac{\pi}{9}$$

de donde usando la fórmula del ángulo triple:

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

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[6] $2r = \pm 1$. 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 $[\mathbb{Q}\left(\cos\frac{\pi}{9}\right) : \mathbb{Q}] = 3$ que no es potencia de 2, luego $\cos\left(\frac{\pi}{9}\right)$ no es constructible, de donde $e^{\frac{i\pi}{9}}$ tampoco lo es; es decir, el ángulo de $60^{\text{o}}$ no se puede trisecar.

[6] 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 $I = F$. □

**Lema 1.18.** *Sea $\sigma : F \to A$ 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 $A$. □

**Definición 1.18** (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:

$$1 = \sigma(1) = \sigma\left(\alpha\alpha^{-1}\right) = \sigma(\alpha)\sigma\left(\alpha^{-1}\right) \Longrightarrow \sigma\left(\alpha^{-1}\right) = \sigma(\alpha)^{-1}$$

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

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

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[7]:

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

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

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

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:

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

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[8] 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 $K = \mathbb{C}$.

[7] Donde $\langle p \rangle$ es el ideal generado por $p$.

[8] 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 $\sigma : F \to K$, 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:*

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

*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. □

**Proposición 1.20.** *Sea $f \in F[x]$ con $degf = n \geqslant 1$, entonces existe un homomorfismo de cuerpos $\sigma : F \to E$ 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 $degh = 0$, tomando $L = F$ y $\sigma = id_F$ se tiene.
- Supuesto que $degh > 0$ 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:

  $$g = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_t), \qquad \alpha_1, \ldots, \alpha_t \in F$$

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

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

  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:

  $$f^\tau = g^\tau h^\tau = (x - \tau(\alpha_1)) \cdot \ldots \cdot (x - \tau(\alpha_s))(x - \beta_1) \cdot \ldots \cdot (x - \beta_s)k, \qquad degk < degh^\tau$$

  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:

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

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

Una vez tenemos que existe $\sigma : F \to L$ 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 $f^\sigma$. □

**Definición 1.20.** Sea $f \in F[x]$, diremos que un homomorfismo de cuerpos $\sigma : F \to E$ 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:

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

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:

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

¿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 $deg\,\mathrm{Irr}(\alpha, \mathbb{F}_2) = 2$, 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 $F \leqslant K$ una extensión de cuerpos con $[K : F] = n$ y $|F| = m$ tendremos entonces que $|K| = m^n$, ya que cada elemento de $K$ queda unívocamente 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 descomopsición 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 $\mathbb{F}_2(a)$:

$$\begin{array}{rcrcrcr|l}
x^3 & + & & + & x & + & 1 & x + a \\
x^3 & + & ax^2 & & & & & \hline
 & & ax^2 & + & x & + & 1 & x^2 + ax + (a^2 + 1) \\
 & & ax^2 & + & a^2x & & & \\
\hline
 & & & & (a^2 + 1)x & + & 1 & \\
 & & & & (a^2 + 1)x & + & a^3 + a & \\
\hline
 & & & & & & a^3 + a + 1 &
\end{array}$$

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 $a^3 + a + 1 = 0$):

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

Dividimos ahora entre $x + a^2$:

$$\begin{array}{rcrcrcr|l}
x^2 & + & & & ax & + & a^2 + 1 & x + a^2 \\
x^2 & + & & & a^2x & & & \hline
a^4x & = & a(a + 1)x & + & a^2 + 1 & & & x + a^4 \\
 & & & & a^4x & + & a^6 & \\
\hline
 & & & & & & a^6 + a^2 + 1 &
\end{array}$$

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:

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

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:*

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

*es un isomorfismo de cuerpos.*

*Demostración.* Podemos tomar:

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

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

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

□

**Definición 1.21.** Si tenemos dos homomorfismos de cuerpos:

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

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

$$\eta\sigma = \tau$$

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

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

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

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

Si $F \leqslant K$ 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*

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

*es una biyección.*

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

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

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

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

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[9] $\eta(\alpha) \in \mathcal{R}$. Veamos ahora que la aplicación enunciada es sobreyectiva[10]. 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:

$$\begin{array}{rccc} \sigma_\alpha: & \dfrac{F[x]}{\langle p\rangle} & \longrightarrow & \sigma(F)(\alpha) = K \\ & g + \langle p\rangle & \longmapsto & g^\sigma(\alpha) \end{array}$$

$$\begin{array}{rccc} \tau_\beta: & \dfrac{F[x]}{\langle p\rangle} & \longrightarrow & \tau(F)(\beta) \leqslant E \\ & g + \langle p\rangle & \longmapsto & g^\tau(\beta) \end{array}$$

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 $\{1, \alpha, \alpha^2, \ldots\}$ es un sistema de generadores de $\sigma(F)(\alpha)$, por lo que todo elemento de este cuerpo será de la forma:

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

con lo que:

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

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. □

[9] Notemos que hemos probado además que $Ex(\tau, \sigma) \neq \emptyset \Longrightarrow \mathcal{R} \neq \emptyset$.

[10] Con lo que tendremos $\mathcal{R} \neq \emptyset \Longrightarrow Ex(\tau, \sigma) \neq \emptyset$

Obsevemos 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:*

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

*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:

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

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

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

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:

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

por lo que la unión es disjunta. □

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

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

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

*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:

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

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

- 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 $\iota : \sigma(F)(\alpha) \to K$ la inclusión en $K$, podemos tomar:

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

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

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

  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:

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

  con lo que:

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

  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:

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

  Por lo que aplicando el Lema de la Torre:

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

□

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

Sea $\sigma : \Pi \to K$ un homomorfismo de cuerpos, sea $\iota : \Pi \to K$ 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 $\Phi : \mathbb{Z}_p \to \Pi$ 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 $\Phi : \mathbb{Q} \to \Pi$. 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 $\sigma = \iota$.

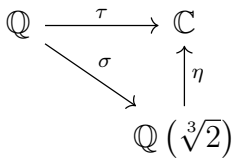
Mostramos a continuación un ejemplo básico de la proposición de extensión.

**Ejemplo.** ¿Cuántos homomorfismos de cuerpos hay de $\mathbb{Q}\left(\sqrt[3]{2}\right)$ 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 $\eta : \mathbb{Q}\left(\sqrt[3]{2}\right) \to \mathbb{C}$ un homomorfismo de cuerpos, si restringimos $\eta$ al cuerpo primo de $\mathbb{Q}\left(\sqrt[3]{2}\right)$, que es $\mathbb{Q}$, el Ejercicio 1.4.1 nos dice que entonces $\eta\big|_{\mathbb{Q}}$ coincide con la aplicación inclusión $\tau : \mathbb{Q} \hookrightarrow \mathbb{C}$, es decir:

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

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




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

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

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

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

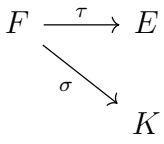
donde $\eta_i$ está determinado (según la proposición de extensión) por:

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

Como cada uno de los $\eta_j$ es un homomorfismo definido sobre $\mathbb{Q}\left(\sqrt[3]{2}\right)$ con base $\left\{1, \sqrt[3]{2}\right\}$, es suficiente definirlos sobre 1 y sobre $\sqrt[3]{2}$, pero como $\eta_j$ tiene que ser un homomorfimo 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:

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

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




*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 $\sigma' : F \to \sigma(F)(\alpha)$ y la inclusión $\iota : \sigma(F)(\alpha) \to K$, 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 $degf$ raíces distintas, entonces $p^\sigma$ tiene $degp$ raíces distintas, de donde:

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

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

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

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

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

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 $\mathbb{Q}\left(\sqrt[3]{2}\right)$ y calcular sus raíces en $\mathbb{C}$, cosa que ya hemos realizado en alguna ocasión:

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

Por tanto, tendremos 2 $\sigma_2$ extensiones de $\eta_j$ para cada $j \in \{0, 1, 2\}$:

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

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

determinadas por

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

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:

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

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

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

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

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

**Teorema 1.26** (Unicidad del cuerpo de descomposición)**.**
*Sean $\tau : F \to E$ y $\tau' : F \to E'$ dos cuerpos de descomposición de $f \in F[x]$. Entonces, existe un isomorfismo de cuerpos $\eta : E \to E'$ 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 $\eta : E \to E'$ y $\eta' : E' \to E$ tales que

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

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 $\eta\eta' : E' \to E'$ 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. □

**Ejercicio 1.4.3.** Sea $\sigma : F \to E$ 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 $\tau : E \to K$ tal que $\tau\sigma : F \to K$ 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 $\alpha_1, \ldots, \alpha_n \in E$ algebraicos sobre $\sigma(F)$ de forma que $E = \sigma(F)(\alpha_1, \ldots, \alpha_n)$. Obtenemos para todo $i \in \{1, \ldots, n\}$:

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

con lo que $g_i(\alpha_i) = 0 \quad \forall i \in \{1, \ldots, n\}$. Como $\sigma : F \to \sigma(F)$ 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:

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

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

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

y recordamos que $g_1 \in \sigma(F)[x]$ es irreducible en $\sigma(F)$, la proposición de extensión nos dice que existe 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:

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

Si tomamos $\mathrm{Irr}(\alpha_{k+1}, \sigma(F)(\alpha_1, \ldots, \alpha_k))$ (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 $\tau : \sigma(F)(\alpha_1, \ldots, \alpha_n) = E \to K$ 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*[11] *$q = p^n$ donde $p = \mathrm{car}(F)$, entonces $F$ es cuerpo de descomposición de $x^q - x \in \mathbb{Z}_p[x]$.*

[11] 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:

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

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 $f \in \mathbb{Z}_p[x]$. □

**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:

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

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 $a, b \in S$:

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

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

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

  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:

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

  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. □

**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:

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

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

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

Se verifica que $\mathrm{Aut}(K)$ 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:

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

y se verifica que $\mathrm{Aut}_F(K)$ es un subgrupo de $\mathrm{Aut}(K)$, 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 $\mathrm{Aut}_\Pi(K) = \mathrm{Aut}(K)$.

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

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

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

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

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

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

$\subseteq$) Si $\sigma \in \operatorname{Aut}_F(K)$, 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 $\sigma \in Ex(\iota, \iota)$.

$\supseteq$) Si tomamos $\sigma \in Ex(\iota, \iota)$ 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 $\sigma \in \operatorname{Aut}_F(K)$

Finalmente, la segunda proposición de extensión nos dice que:

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

□

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

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

$$|\operatorname{Aut}_F(K)| \leqslant [K : F]$$

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

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

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

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

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

□

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

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

con lo que la Proposición nos dice que:

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

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

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

donde:

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

resulta que tenemos un grupo no conmutativo:

$$\sqrt[3]{2} \overset{\eta_{1,1}}{\longmapsto} w\sqrt[3]{2} \overset{\eta_{1,0}}{\longmapsto} w\sqrt[3]{2}$$
$$\sqrt[3]{2} \overset{\eta_{1,0}}{\longmapsto} w\sqrt[3]{2} \overset{\eta_{1,1}}{\longmapsto} w^2\sqrt[3]{2}$$

por lo que es isomorfo a $S_3$.

**Teorema 1.31.** *Sea $\mathbb{F}_q$ un cuerpo finito con $q = p^n$ elementos, entonces $Aut(\mathbb{F}_q)$ 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:

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

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

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

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 $p^m - 1 \geqslant p^n - 1$, luego $m \geqslant n$, de donde el orden de $\tau \in \mathrm{Aut}(\mathbb{F}_q)$ es $n$, con lo que $\mathrm{Aut}(\mathbb{F}_q)$ ha de ser cíclico. □

## 1.7. Ejercicios

**Ejercicio 1.7.1.** Sea $F \leqslant K$ 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, $deg\,\mathrm{Irr}(\alpha, F) = 2$, 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 $F(\beta) \leqslant K$, 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:

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

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:

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

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

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

$\supseteq$) Vemos que:

$$\sqrt{2} = \frac{\sqrt{2}+i\sqrt{2}+\sqrt{2}-i\sqrt{2}}{2} \in \mathbb{Q}\left(\sqrt{2}+i\sqrt{2}, \sqrt{2}-i\sqrt{2}\right)$$
$$i = \frac{\sqrt{2}+i\sqrt{2}-\sqrt{2}}{\sqrt{2}} \in \mathbb{Q}\left(\sqrt{2}+i\sqrt{2}, \sqrt{2}-i\sqrt{2}\right)$$

En definitiva, $\mathbb{Q}\left(i, \sqrt{2}\right)$ 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 trascendentes:

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

Veamos cada caso:

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

  En el apartado anterior hemos visto que $[\mathbb{Q}\left(\sqrt[5]{4}\right) : \mathbb{Q}] \leqslant 5$, con lo que la extensión $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt[5]{4}\right)$ es finita, luego algebraica y finitamente generada, por lo que todo elemento de este último cuerpo será algebraico sobre $\mathbb{Q}$. Observemos que:
  $$(1+\sqrt[5]{4})\left(1-\sqrt[5]{16}\right)^{-1} = (1+\sqrt[5]{4})\left(1-\sqrt[5]{4}\sqrt[5]{4}\right)^{-1} \in \mathbb{Q}(\sqrt[5]{4})$$
  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:
  $$f = \sum_{i=0}^{n} f_i x^i, \qquad f_i \in \mathbb{Q} \quad \forall i \in \{0, \dots, n\}$$
  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 $i\sqrt{i} + \sqrt{2} \in \mathbb{Q}\left(\sqrt{i}, \sqrt{2}\right)$, y aplicando el Lema de la Torre vemos que:

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

  con:

  - $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$ por ser $x^2 - 2 = \text{Irr}\left(\sqrt{2}, \mathbb{Q}\right)$, irreducible por Eisenstein para $p = 2$.
  - $\left[\mathbb{Q}\left(\sqrt{i}, \sqrt{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] \leqslant 4$, ya que $x^4 + 1$ tiene a $\sqrt{i}$ como raíz.

  En definitiva, la extensión $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt{i}, \sqrt{2}\right)$ 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:

  $$x^2 = 1 - \sqrt[3]{2} \Longrightarrow x^2 - 1 = -\sqrt[3]{2}$$

  De donde:

  $$\left(x^2 - 1\right)^3 = x^6 - 3x^4 + 3x^2 - 1 = -2$$

  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 $\mathbb{Q}$.

- $\sqrt{\pi}$

  Si fuera $\sqrt{\pi}$ un número algebraico tendríamos entonces que la extensión $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt{\pi}\right)$ sería finita, y como tenemos:

  $$\mathbb{Q} \leqslant \mathbb{Q}(\pi) \leqslant \mathbb{Q}\left(\sqrt{\pi}\right)$$

  ya que $\pi = \left(\sqrt{\pi}\right)^2$, tendremos entonces por el Lema de la Torre que la extensión $\mathbb{Q} \leqslant \mathbb{Q}(\pi)$ es finita, luego algebraica, por lo que $\pi$ sería algebraico, contradicción que viene de suponer que $\sqrt{\pi}$ es un número algebraico.

- $\sqrt{2}(\sqrt[3]{2} + \sqrt[5]{2})^{-1}$

  Por el Lema de la Torre, tenemos que:

  $$\left[\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2}\right) : \mathbb{Q}\right] =$$
  $$\left[\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2}\right) : \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right) : \mathbb{Q}(\sqrt{2})\right]\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right]$$

  Con:

- $\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=2$, ya que $\mathrm{Irr}(\sqrt{2},\mathbb{Q})=x^2-2$ por Eisenstein para $p=2$.
- $\left[\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right):\mathbb{Q}\left(\sqrt{2}\right)\right]\leqslant 3$ ya que $x^3-2$ es un polinomio con $\sqrt[3]{2}$ como raíz.
- $\left[\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2},\sqrt[5]{2}\right):\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right)\right]\leqslant 5$, ya que $x^5-2$ es un polinomio con $\sqrt[5]{2}$ como raíz.

En definitiva, la extensión $\mathbb{Q}\leqslant\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2},\sqrt[5]{2}\right)$ es finita, luego algebraica y finitamente generada. En particular, tenemos que:

$$\sqrt{2}\left(\sqrt[3]{2}+\sqrt[5]{2}\right)^{-1}\in\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2},\sqrt[5]{2}\right)$$

Por lo que $\sqrt{2}\left(\sqrt[3]{2}+\sqrt[5]{2}\right)^{-1}$ 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 $F$.

$\Longrightarrow$) 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 $F$.

$\Longleftarrow$) 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:

$$f=\sum_{i=1}^{m}f_ix^i\qquad f_i\in F$$

tenemos entonces que:

$$f(\alpha^n)=\sum_{i=1}^{m}f_i(\alpha^n)^i=0$$

Por tanto, si consideramos el polinomio:

$$g=\sum_{k=1}^{m}f_ix^{in}\in F[x]$$

tendremos entonces:

$$g(\alpha)=\sum_{k=1}^{m}f_i\alpha^{in}=\sum_{k=1}^{m}f_i(\alpha^n)^i=0$$

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 $F$:

$\Longrightarrow$) 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 $F$.

$\Longleftarrow$) 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:

$$\beta = 1 + \alpha^2 + \alpha^5 \quad \Longleftrightarrow \quad 1 - \beta + \alpha^2 + \alpha^5$$

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 $\mathrm{Irr}(\alpha, \mathbb{Q})$ 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 $\mathbb{Q}(\alpha) \leqslant \mathbb{Q}\left(\sqrt{2}\right)$, así como que:

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

Por lo que $\mathbb{Q}\left(\sqrt{2}\right) \leqslant \mathbb{Q}(\alpha)$. Como $\mathrm{Irr}\left(\sqrt{2}, \mathbb{Q}\right) = x^2 - 2$ por Eisenstein para $p = 2$, tenemos que:

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

Por lo que basta encontrar un polinomio mónico de grado 2 del que $\alpha$ sea raíz.

$$\alpha - 3 = \sqrt{2} \Longrightarrow \alpha^2 - 6\alpha + 9 = (\alpha - 3)^2 = 2 \Longrightarrow \alpha^2 - 6\alpha + 7 = 0$$

Por lo que $\mathrm{Irr}(\alpha, \mathbb{Q}) = x^2 - 6x + 7$.

b) Para $\alpha = \sqrt{3} - \sqrt[4]{3}$.

Buscamos primero un polinomio del que $\alpha$ sea raíz. Para ello:

$$\sqrt[4]{3} = \alpha - \sqrt{3} \quad \Longrightarrow \quad \sqrt{3} = \alpha^2 + 3 - 2\alpha\sqrt{3} \quad \Longleftrightarrow \quad \sqrt{3}(1 + 2\alpha) = \alpha^2 + 3$$

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 $f = \mathrm{Irr}(\alpha, \mathbb{Q})$.

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 $\mathrm{Irr}(\alpha, \mathbb{Q}) = f$.

**Ejercicio 1.7.7.** Calcular $[E:\mathbb{Q}]$ y una base de $E$ sobre $\mathbb{Q}$ en los siguientes casos:

$$E=\mathbb{Q}\left(\sqrt{6},i\right), \qquad E=\mathbb{Q}\left(\sqrt[3]{5},\sqrt{-2}\right), \qquad E=\mathbb{Q}\left(\sqrt{18},\sqrt[3]{4}\right)$$

a) Para $E=\mathbb{Q}\left(\sqrt{6},i\right)$.

Tenemos por el Lema de la Torre que:

$$[E:\mathbb{Q}]=\left[E:\mathbb{Q}\left(\sqrt{6}\right)\right]\left[\mathbb{Q}\left(\sqrt{6}\right):\mathbb{Q}\right]$$

con:

- $\left[E:\mathbb{Q}\left(\sqrt{6}\right)\right]=2$, ya que $\operatorname{Irr}\left(i,\mathbb{Q}\left(\sqrt{6}\right)\right)=x^2+1$, por ser de grado 2 y ser sus raíces complejas.
- $\left[\mathbb{Q}\left(\sqrt{6}\right):\mathbb{Q}\right]=x^2-6$, ya que es un polinomio de grado 2 y no tiene raíces en $\mathbb{Q}$, ya que sus posibles raíces son:

  $$Div(6)=\{\pm1,\pm2,\pm3,\pm6\}$$

  y ninguna de ellas es raíz:

  $$\begin{gathered}(-1)^2-6=1^2-6=-5\neq0\\(-2)^2-6=2^2-6=-2\neq0\\(-3)^2-6=3^2-6=3\neq0\\(-6)^2-6=6^2-6=30\neq0\end{gathered}$$

b) Para $E=\mathbb{Q}\left(\sqrt[3]{5},\sqrt{-2}\right)$.

Tenemos por el Lema de la Torre que:

$$[E:\mathbb{Q}]=\left[E:\mathbb{Q}\left(\sqrt[3]{5}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{5}\right):\mathbb{Q}\right]$$

con:

- $\left[\mathbb{Q}\left(\sqrt[3]{5}\right):\mathbb{Q}\right]=3$, ya que $\operatorname{Irr}\left(\sqrt[3]{5},\mathbb{Q}\right)=x^3-5$ por Eisenstein para $p=5$.
- $\left[E:\mathbb{Q}\left(\sqrt[3]{5}\right)\right]=2$, ya que $\operatorname{Irr}\left(\sqrt{-2},\mathbb{Q}\right)=x^2+2$, ya que es de grado 2 y no tiene raíces en $\mathbb{Q}\left(\sqrt[3]{5}\right)\leqslant\mathbb{R}$.

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 $E=\mathbb{Q}\left(\sqrt{18},\sqrt[3]{4}\right)$.

Tenemos por el Lema de la Torre que:

$$[E:\mathbb{Q}]=\left[E:\mathbb{Q}\left(\sqrt[3]{4}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{4}\right):\mathbb{Q}\right]$$

con:

- $\left[\mathbb{Q}\left(\sqrt[3]{4}\right):\mathbb{Q}\right]=3$, ya que $\mathrm{Irr}\left(\sqrt[3]{4},\mathbb{Q}\right)=x^3-4$, es irreducible por ser de grado 3 y no tener raíces en $\mathbb{Q}$, ya que sus posibles raíces son:

$$Div(4)=\{\pm 1,\pm 2,\pm 4\}$$

y ninguna de ellas es raíz:

$$\begin{gathered}(1)^3-4=-3\neq 0\\(-1)^3-4=-5\neq 0\\(2)^3-4=4\neq 0\\(-2)^3-4=-12\neq 0\\(4)^3-4=60\neq 0\\(-4)^3-4=-68\neq 0\end{gathered}$$

- $\left[E:\mathbb{Q}\left(\sqrt[3]{4}\right)\right]\leqslant 2$, ya que $x^2-18$ es un polinomio mónico de grado 2 del que $\sqrt{18}$ es raíz, pero no sabemos si es irreducible sobre $\mathbb{Q}\left(\sqrt[3]{4}\right)$, por lo que podría ser $\left[E:\mathbb{Q}\left(\sqrt[3]{4}\right)\right]=1$.

En definitiva, tenemos que $[E:\mathbb{Q}]\leqslant 6$ y es múltiplo de 3. Si aplicamos ahora el Lema de la Torre de la otra forma tenemos que:

$$[E:\mathbb{Q}]=\left[E:\mathbb{Q}\left(\sqrt{18}\right)\right]\left[\mathbb{Q}\left(\sqrt{18}\right):\mathbb{Q}\right]$$

con:

- $\left[\mathbb{Q}\left(\sqrt{18}\right):\mathbb{Q}\right]=2$, ya que $\mathrm{Irr}\left(\sqrt{18},\mathbb{Q}\right)=x^2-18$, es irreducible por Eisenstein para $p=2$.
- $\left[E:\mathbb{Q}\left(\sqrt{18}\right)\right]\leqslant 3$, ya que $x^3-4$ es un polinomio mónico de gardo 3 del que $\sqrt[3]{4}$ es raíz, pero al igual que antes no sabemos si es irreducible o no.

Finalmente, vemos que $[E:\mathbb{Q}]$ es menor o igual que 6 y múltiplo de 2 y de 3, por lo que tiene que ser $[E:\mathbb{Q}]=6$.

**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 $\mathrm{Irr}(\alpha,\mathbb{Q})=x^3+3x+1$, 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:

$$\alpha^3+3\alpha+1=0$$

Calculamos primero las coordenadas de $(1+\alpha+\alpha^2)^{-1}$, que son los números racionales $a, b, c \in \mathbb{Q}$ que cumplen:

$$(1+\alpha+\alpha^2)(a+b\alpha+c\alpha^2) = 1$$

Calculamos entonces $a, b$ y $c$ imponiendo dicha condición:

$$\begin{aligned}(1+\alpha+\alpha^2)(a+b\alpha+c\alpha^2) &= a+b\alpha+c\alpha^2+a\alpha+b\alpha^2+c\alpha^3+a\alpha^2+b\alpha^3+c\alpha^4\\ &= a+\alpha(a+b)+\alpha^2(a+b+c)+\alpha^3(b+c)+c\alpha^4\end{aligned}$$

Usamos ahora que $\alpha^3+3\alpha+1=0$, con lo que:

$$\alpha^3 = -3\alpha-1, \qquad \alpha^4 = \alpha\alpha^3 = -3\alpha^2-\alpha$$

de aquí tenemos que:

$$\begin{aligned}(1+\alpha+\alpha^2)(a+b\alpha+c\alpha^2) &= a+\alpha(a+b)+\alpha^2(a+b+c)+(-3\alpha-1)(b+c)-3c\alpha^2-c\alpha\\ &= (a-b-c)+\alpha(a-2b-4c)+\alpha^2(a+b-2c)\end{aligned}$$

Y como queríamos que el producto fuese igual a 1 imponemos entonces que:

$$\begin{cases} a-b-c &= 1\\ a-2b-4c &= 0\\ a+b-2c &= 0\end{cases}$$

Si resolvemos el sistema obtenemos:

$$a = \frac{8}{7}, \qquad b = \frac{-2}{7}, \qquad c = \frac{3}{7}$$

Seguimos calculando las coordenadas del elemento enunciado:

$$\begin{aligned}(1+\alpha)(1+\alpha+\alpha^2)^{-1} &= (1+\alpha)(a+b\alpha+c\alpha^2)\\ &= a+b\alpha+c\alpha^2+a\alpha+b\alpha^2+c\alpha^3\\ &= a+\alpha(a+b)+\alpha^2(b+c)+c\alpha^3\\ &= a+\alpha(a+b)+\alpha^2(b+c)+c(-3\alpha-1)\\ &= (a-c)+\alpha(a+b-3c)+\alpha^2(b+c)\end{aligned}$$

Por lo que obtenemos que sus coordenadas son:

$$\begin{aligned}a-c &= \frac{8}{7}-\frac{3}{7} = \frac{5}{7}\\ a+b-3c &= \frac{8}{7}-\frac{2}{7}-\frac{9}{7} = \frac{-3}{7}\\ b+c &= \frac{-2}{7}+\frac{3}{7} = \frac{1}{7}\end{aligned}$$

**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 $\mathbb{F}_4 \to \mathbb{F}_{16}$ en función de $a$ y $b$.

Cuando decimos que $\mathbb{F}_4 = \mathbb{F}_2(a)$ con $a^2+a+1 = 0$ decimos que como $x^2+x+1 \in \mathbb{F}_2[x]$ es irreducible tenemos entonces que existe un homomorfismo $\sigma : \mathbb{F}_2 \to K$ y $a \in K$ de forma que $K = \sigma(\mathbb{F}_2)(a)$ (notemos que $\sigma(\mathbb{F}_2) = \mathbb{F}_2$ para cualquier homomorfismo de cuerpos $\sigma : \mathbb{F}_2 \to E$) y $a^2 + a + 1 = 0$.

Para ver que $\mathbb{F}_{16} = \mathbb{F}_2(b)$ con $b^4 + b + 1 = 0$, lo que hacemos es ver primero que el polinomio $f = x^4 + x + 1 \in \mathbb{F}_2[x]$ es irreducible, ya que:

- Como $f$ no tiene raíces en $\mathbb{F}_2$ tenemos que no puede tener factores de grado 1, por lo que tampoco puede tenerlos de grado 3.
- El único factor de grado 2 que puede tener $f$ es el único polinomio irreducible de grado 2 en $\mathbb{F}_2[x]$, que es $x^2 + x + 1$, pero esto solo puede suceder si $f = (x^2 + x + 1)^2$, y tenemos que:

  $$(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq f$$

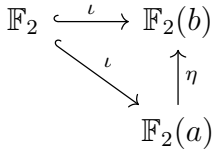
  Por lo que $f$ tampoco tiene factores de grado 2, luego $f$ es irreducible.

Como $f$ es irreducible, existe un homomorfismo de cuerpos $\sigma : \mathbb{F}_2 \to K$ y $b \in K$ de forma que $b^4 + b + 1 = 0$ y $K = \mathbb{F}_2(b)$. Como:

$$\operatorname{Irr}(b, \mathbb{F}_2) = x^4 + x + 1$$

tenemos entonces que $[K : \mathbb{F}_2] = 4$. Como $\mathbb{F}_2$ tiene 2 elementos, vemos entonces que $|K| = 2^4 = 16$, llamamos $\mathbb{F}_{16} = K$.

Para ver el número de homomorfismos de cuerpos $\eta : \mathbb{F}_4 \to \mathbb{F}_{16}$ que hay, como $\mathbb{F}_2 \leqslant \mathbb{F}_4$ y $\mathbb{F}_2 \leqslant \mathbb{F}_{16}$, si consideramos las inclusiones en cada extensión vemos que el problema de calcular todos los homomorfismos es equivalente al problema de calcular todas las extensiones de la inclusión.




Para ello, como $\operatorname{Irr}(a, \mathbb{F}_2) = x^2 + x + 1 \in \mathbb{F}_2[x]$ y $\mathbb{F}_4 = \mathbb{F}_2(a)$, tendremos tantas extensiones de la inclusión como raíces tenga el polinomio $x^2 + x + 1$ en $\mathbb{F}_2(b)$.

Observemos que en este ejercicio (usando el ejercicio siguiente), cada $\eta$ por restricción nos da un homomorfismo de grupos $\eta : \mathbb{F}_2^\times(a) \to \mathbb{F}_2^\times(b)$ 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 $\eta_i : \mathbb{F}_4 \to \mathbb{F}_{16}$:

$$\eta_1(a) = b^5, \qquad \eta_2(a) = b^{10}$$

**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 $G$:

$$G = C_1 \oplus \ldots \oplus C_t$$

Con $C_i$ cíclico para cada $i \in \{1, \ldots, t\}$, 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 $|G| \leqslant m \leqslant |G|$, 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:

$$\mathbb{F}_q = \{0, 1, a, \ldots, a^{q-2}\}$$

Por lo que $\mathbb{F}_q = \mathbb{F}_p(a)$, con $p = \mathrm{car}(\mathbb{F}_q)$.

**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 elemento, 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 $\sqrt{3} \in \mathbb{Q}\left(\sqrt{1+2\sqrt{3}}\right)$.

   Llamamos $\alpha = \sqrt{1+2\sqrt{3}}$ y calculamos:

   $$\alpha^2 = 1 + 2\sqrt{3} \quad \Longrightarrow \quad \sqrt{3} = \frac{\alpha^2 - 1}{2} \in \mathbb{Q}(\alpha)$$

   De donde también deducimos que $\mathbb{Q}(\sqrt{3}) \leqslant \mathbb{Q}(\alpha)$.

2. Calcular $Irr\left(\alpha, \mathbb{Q}\left(\sqrt{3}\right)\right)$.

   Sabemos que $\alpha$ es raíz de $f = x^2 - 1 - 2\sqrt{3} \in \mathbb{Q}\left(\sqrt{3}\right)[x]$, con lo que:

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

   Supongamos que $\left[\mathbb{Q}(\alpha) : \mathbb{Q}\left(\sqrt{3}\right)\right] = 1$, con lo que $\alpha \in \mathbb{Q}\left(\sqrt{3}\right)$, 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 $\mathbb{Q}\left(\sqrt{3}\right)$, tenemos entonces que:

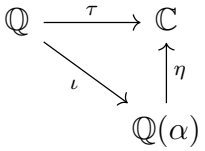
   $$\left.\begin{array}{l} 1 = a^2 + 3b^2 \\ 2 = 2ab \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} b = \frac{1}{a} \\ 1 = a^2 + 3\frac{1}{a^2} \end{array}\right\} \Longrightarrow a^2 = a^4 + 3$$
   $$\Longrightarrow a^2 = \frac{1 \pm \sqrt{1-12}}{2} \notin \mathbb{Q} \Longrightarrow a \notin \mathbb{Q}$$

   Por lo que no es posible $\left[\mathbb{Q}(\alpha) : \mathbb{Q}\left(\sqrt{3}\right)\right] = 1$, con lo que $\left[\mathbb{Q}(\alpha) : \mathbb{Q}\left(\sqrt{3}\right)\right] = 2$, de donde deducimos que:

   $$Irr\left(\alpha, \mathbb{Q}\left(\sqrt{3}\right)\right) = x^2 - 1 - 2\sqrt{3}$$

3. Calcular los homomofismos de $\mathbb{Q}(\alpha)$ en $\mathbb{C}$.

   Queremos calcular los $\eta$ que cumplen:

donde $\tau, \iota$ son la inclusión, es decir, calcular $Ex(\tau, \iota)$.

No conocemos $Irr(\alpha, \mathbb{Q})$, 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:

$$\eta_j(\sqrt{3}) = (-1)^j\sqrt{3}, \qquad \forall j \in \{0,1\}$$

ya que $Irr\left(\sqrt{3}, \mathbb{Q}\right) = x^2 - 3$. 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:

$$\eta_{0,k}(\alpha) = (-1)^k\alpha \qquad \forall k \in \{0,1\}$$

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 $Irr(\alpha, \mathbb{Q})$ 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 bicuadrática, que salen $\alpha, -\alpha, \beta, -\beta$.

**Ejercicio 1.7.13.** Sea $\eta = e^{i\frac{2\pi}{5}} \in \mathbb{C}$, ¿$Irr(\eta + \overline{\eta}, \mathbb{Q})$?. Llamando $\alpha = \eta + \overline{\eta}$, 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:

$$Irr(\eta + \overline{\eta}, \mathbb{Q}) = x^2 + x + 1$$

Y el número $\eta$ es constructible porque $\eta + \overline{\eta}$ 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 demustra que el pentágono regular es constructible.

**Ejercicio 1.7.14.** Calcular $\mathrm{Irr}(\alpha, \mathbb{Q})$, 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 $\mathbb{Q}(\alpha^2) = \mathbb{Q}\left(\sqrt{5}\right)$, con lo que tenemos $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 2$. Necesitamos ver si $\alpha \in \mathbb{Q}\left(\sqrt{5}\right)$, 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:

$$\frac{3}{2} = \frac{1}{16b^2} + 5b^2 \Longrightarrow 3 = \frac{1}{8b^2} + 10b^2 \Longrightarrow 24 = \frac{1}{b^2} + 80b^2 \Longrightarrow 24b^2 = 1 + 80b^4$$

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, $\alpha \in \mathbb{Q}\left(\sqrt{5}\right)$, es decir:

$$\alpha = \sqrt{\frac{3+\sqrt{5}}{2}} = \frac{1+\sqrt{5}}{2}$$

Por lo que:

$$2\alpha = 1 + \sqrt{5} \Longrightarrow 4\alpha^2 - 4\alpha + 1 = 5$$

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:

$$\text{Sea } F \leqslant K \text{ una extensión finita, entonces } |\operatorname{Aut}_F(K)| \leqslant [K:F].$$

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 $\operatorname{Aut}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)\right)$, sabemos que:

$$\left|\operatorname{Aut}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)\right)\right| \leqslant 3$$

Y afirmamos que solo hay uno, ya que si observamos el diagrama:

$$\begin{array}{ccc} \mathbb{Q} & \xrightarrow{\iota} & \mathbb{Q}\left(\sqrt[3]{2}\right) \\ & \searrow^{\iota} & \uparrow{\scriptstyle \eta} \\ & & \mathbb{Q}\left(\sqrt[3]{2}\right) \end{array}$$

tenemos que raíces de $x^3 - 2$ en $\mathbb{Q}\left(\sqrt[3]{2}\right)$ solo hay 1. Sin embargo, anteriormente vimos que:

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

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 $G < \operatorname{Aut}(K)$ 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 $G < \operatorname{Aut}(K)$, tenemos que:

$$K^G \leqslant K$$

*Demostración.* Para probar que $K^G$ es un subcuerpo de $K$:

- Es claro que $1 \in K^G$, ya que de hecho $\sigma(1) = 1 \quad \forall \sigma \in \mathrm{Aut}(K)$.
- Si $a, b \in K^G$, tenemos entonces que $\sigma(a) = a, \sigma(b) = b \quad \forall \sigma \in G$, de donde:

$$\left.\begin{array}{r} \sigma(a-b) = \sigma(a) - \sigma(b) = a - b \\ \sigma(ab) = \sigma(a)\sigma(b) = ab \end{array}\right\} \quad \Longrightarrow \quad a - b, ab \in K^G$$

- Finalmente, si $a \in K^G$ tenemos entonces que:

$$\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1} \quad \Longrightarrow \quad a^{-1} \in K^G$$

□

**Proposición 2.1** (Artin)**.** *Si $G$ es un subgrupo finito de* $\mathrm{Aut}(K)$*, entonces.*

$$\left[K : K^G\right] \leqslant |G|$$

*Demostración.* Sea $n = |G|$, será $G = \{\sigma_1, \ldots, \sigma_n\}$ y tomamos $m$ (con $m > n$) elementos de $K$, $\alpha_1, \ldots, \alpha_m \in K$, basta probar que estos son $K^G-$linealmente dependientes, para tener $[K : K^G] \leqslant n$. 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

$$0 \neq v = (v_1, \ldots, v_m) \in K^m$$

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 $1 \leqslant l \leqslant m$), 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 $1 \leqslant l \leqslant m$ 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:

$$\sum_{i=1}^{m} v_i \sigma_j(\alpha_i) = 0 \qquad \forall j \in \{1, \ldots, n\}$$

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 $k \in \{1, \ldots, n\}$. Tomamos ahora cualquier $\sigma \in G$ y definimos:

$$\sigma(v) = (\sigma(v_1), \ldots, \sigma(v_n))$$

Si usamos esto para $\sigma_k$:

$$\sigma_k(v) = (\sigma_k(v_1), \ldots, \sigma_k(v_m))$$

Podemos aplicar $\sigma_k$ a las igualdades anteriores, con lo que:

$$\sum_{i=1}^{m} \sigma_k(v_i)\sigma_k(\sigma_j(\alpha_i)) = 0 \qquad \forall j \in \{1, \dots, n\}$$

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 disintos 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:

$$\sum_{i=1}^{m} \sigma_k(v_i)\sigma_j(\alpha_i) = 0 \qquad \forall j \in \{1, \dots, n\}$$

o equivalentemente:

$$\sigma_k(v)A = 0$$

Como $vA = 0$ y $\sigma_k(v)A = 0$, tenemos que:

$$(v - \sigma_k(v))A = 0, \qquad v - \sigma_k(v) \neq 0$$

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:

$$\sum_{i=1}^{m} v_i\sigma_j(\alpha_i) = 0 \qquad \forall j \in \{1, \dots, n\}$$

tomamos aquel índice $j$ que verifica que $\sigma_j = Id_K$, tendremos entonces que:

$$\sum_{i=1}^{m} v_i\alpha_i = 0, \qquad v_i \in K^G$$

lo que implica que $\alpha_1, \dots, \alpha_m$ eran $K^G-$linealmente dependientes, por lo que:

$$[K : K^G] \leqslant n = |G|$$

□

**Lema 2.2.** *Para un cuerpo $K$, tenemos que:*

1. *Si $H < G$ son subgrupos de $\mathrm{Aut}(K)$, entonces $K^H \geqslant K^G$.*
2. *Si $F \leqslant E$ son subcuerpos de $K$, entonces $\mathrm{Aut}_F(K) > \mathrm{Aut}_E(K)$.*

3. *Si* $G < \mathrm{Aut}(K)$*, entonces* $G < \mathrm{Aut}_{K^G}(K)$.

4. *Si* $F \leqslant K$*, entonces* $F \leqslant F^{\mathrm{Aut}_F(K)}$.

*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 $\sigma \in \mathrm{Aut}_E(K)$, tenemos entonces que $\sigma$ es $E-$lineal, pero como $F \leqslant E$, será $\sigma \in \mathrm{Aut}_F(K)$.

3. Sea $\sigma \in G < \mathrm{Aut}(K)$, 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 $\sigma \in \mathrm{Aut}_{K^G}(K)$.

4. Sea $x \in F$ y $\sigma \in \mathrm{Aut}_F(K)$, entonces:

$$\sigma(x) = \sigma(x \cdot 1) = x \cdot \sigma(1) = x$$

   Por lo que $x \in F^{\mathrm{Aut}_F(K)}$.

□

**Teorema 2.3.** *Sea* $K$ *un cuerpo, si* $G$ *es un subgrupo finito de* $\mathrm{Aut}(K)$*, entonces:*

$$[K : K^G] = |G| \qquad y \qquad G = \mathrm{Aut}_{K^G}(K)$$

*Demostración.* El Lema de Artin nos dice que $[K : K^G] \leqslant |G|$. Para la otra desigualdad, el Lema anterior nos dice que $G < \mathrm{Aut}_{K^G}(K)$ y la Proposición 1.29 nos dice que $|\,\mathrm{Aut}_{K^G}(K)| \leqslant [K : K^G]$, por lo que:

$$|G| \leqslant |\,\mathrm{Aut}_{K^G}(K)| \leqslant [K : K^G]$$

de donde $[K : K^G] = |G|$ y tendrá que ser $|G| = |\,\mathrm{Aut}_{K^G}(K)|$, por lo que finalmente $G = \mathrm{Aut}_{K^G}(K)$. □

**Ejemplo.** Sea $K = \mathbb{Q}\left(\sqrt[3]{2}, w\right)$ con $w$ una raíz cúbica primitiva de la unidad, sabemos ya que:

$$\mathrm{Aut}(K) = \{\eta_{j,k} : j \in \{0,1,2\}, k \in \{1,2\}\}$$

donde:

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

Los subgrupos propios de $\mathrm{Aut}(K)$ (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:

$$\langle \eta_{1,1} \rangle \cong \langle \eta_{2,1} \rangle, \qquad \langle \eta_{0,2} \rangle \cong \langle \eta_{1,2} \rangle \cong \langle \eta_{2,2} \rangle$$

Que hemos obtenido ya que por ejemplo:

$$\begin{aligned}&\sqrt[3]{2} \overset{\eta_{0,2}}{\longmapsto} \sqrt[3]{2}\\ &w \longmapsto w^2 \longmapsto w^4 = w\end{aligned}$$

$$\begin{aligned}&\sqrt[3]{2} \overset{\eta_{1,2}}{\longmapsto} w\sqrt[3]{2} \overset{\eta_{1,2}}{\longmapsto} w^2 w\sqrt[3]{2} = \sqrt[3]{2}\\ &w \longmapsto w^2 \longmapsto w\end{aligned}$$

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.

$$\sqrt[3]{2} \overset{\eta_{1,1}}{\longmapsto} w\sqrt[3]{2} \overset{\eta_{1,1}}{\longmapsto} ww\sqrt[3]{2} = w^2\sqrt[3]{2} \neq \sqrt[3]{2}$$

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:

$$\left[K : K^{\langle \eta_{1,1} \rangle}\right] = |\langle \eta_{1,1} \rangle| = 3$$

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 $\mathrm{Aut}(K)$. 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 $\mathbb{Q} \leqslant K^{\langle \eta_{1,1} \rangle}$, por ser $\eta_{1,1}\big|_{\mathbb{Q}} = \iota$.
- Como $\eta_{1,1}(w) = w$, tenemos que $w \in K^{\langle \eta_{1,1} \rangle}$.
  De estos dos puntos deducimos que $\mathbb{Q}(w) \leqslant K^{\langle \eta_{1,1} \rangle}$.
- 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 $deg f \geqslant 1$, 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 $degf$ raíces distintas en su cuerpo de descomposición.

3. $\mathrm{mcd}(f, f') = 1$.

*Demostración.* $1 \iff 2$ es evidente, para $2 \iff 3$:

$\Longleftarrow$) Si $\mathrm{mcd}(f, f') = 1$ 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.

$\Longrightarrow$) Si $\mathrm{mcd}(f, f') = 0$ entonces tendríamos que $f' \mid f$, de donde compartirían alguna raíz. Si fuera $\mathrm{mcd}(f, f')$ 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 $\mathrm{car}(F) = 0$ y $f$ es irreducible, entonces $f$ es separable.

  Como $car(F) = 0$ y $degf \geqslant 1$, tenemos al ser $f$ no constante que $f' \neq 0$, y como $f$ es irreducible tendremos que $\mathrm{mcd}(f, f') = 1$, 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 $\mathrm{mcd}(f, f') = 1$, 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 $\mathrm{mcd}(f, f') = f \neq 1$, luego $f$ no es separable.

**Definición 2.3** (Extensión separable)**.** Una extensión algebraica $F \leqslant K$ se dice separable si $\mathrm{Irr}(\alpha, F)$ es separable, para todo $\alpha \in K$.

*Observación.* Toda extensión algebraica en característica 0 es separable.

**Definición 2.4** (Extensión normal)**.** Una extensión algebraica $F \leqslant K$ se dice normal si $\mathrm{Irr}(\alpha, F)$ se factoriza como producto de polinomios lineales en $K[x]$, para todo $\alpha \in K$.

**Ejemplo.** Por ejemplo, la extensión $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[3]{2})$ no es normal pero sí es separable.

*Observación.* Si $F \leqslant K$ 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 $p = \mathrm{Irr}(\alpha, F)$, 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 $K$. □

**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 $F = K^{\mathrm{Aut}_F(K)}$.*

*iii)* *$F = K^G$ para un subgrupo finito $G$ de $\mathrm{Aut}(K)$.*

*iv)* *$F \leqslant K$ es finita, normal y separable.*

*Demostración.* Veamos las equivalencias:

*i)* $\Longrightarrow$ *ii)* Como $K$ es cuerpo de descomposición de cierto $f \in F[x]$, tenemos entonces que si $\alpha_1, \ldots, \alpha_s$ son las raíces de $f$ entonces:

$$K = F(\alpha_1, \ldots, \alpha_s)$$

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 $F \leqslant F^{\mathrm{Aut}_F(K)} \leqslant K^{\mathrm{Aut}_F(K)}$. Como $F \leqslant K$ es finita tenemos entonces por la Proposición 1.29 que $\mathrm{Aut}_F(K)$ es un subgrupo finito de $\mathrm{Aut}(K)$, de donde por el Teorema 2.3 tenemos que:

$$\left[K : K^{\mathrm{Aut}_F(K)}\right] = |\,\mathrm{Aut}_F(K)|$$

Finalmente, como $K$ es cuerpo de descomposición de $f \in F[x]$ separable, la Proposición 1.30 nos da la igualdad $(*)$:

$$\left[K : K^{\mathrm{Aut}_F(K)}\right] = |\,\mathrm{Aut}_F(K)| \overset{(*)}{=} [K : F]$$

y como tenemos $F \leqslant K^{\mathrm{Aut}_F(K)} \leqslant K$, el Lema de la Torre nos dice que $[K^{\mathrm{Aut}_F(K)} : F] = 1$, de donde $F = K^{\mathrm{Aut}_F(K)}$.

*ii)* $\Longrightarrow$ *iii)* Si la extensión es finita, tenemos entonces que $\mathrm{Aut}_F(K)$ es un subgrupo finito de $\mathrm{Aut}(K)$, con lo que tomando $G = \mathrm{Aut}_F(K)$ tenemos que $F = K^G$.

*iii)* $\Longrightarrow$ *iv)* Si $F = K^G$ con $G$ un subgrupo finito de $\mathrm{Aut}(K)$, 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 $h = \mathrm{Irr}(\alpha, F) \in F[x]$, 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):

$$Orb(\alpha) = \{\alpha_1, \ldots, \alpha_t\} \subseteq K$$

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 $a_0, \ldots, a_t \in K$. Veamos que $a_j \in F$ para todo $j \in \{1, \ldots, t\}$, 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 $j \in \{1, \ldots, t\}$, con lo que tenemos tenemos $a_j \in F$ para todo $j \in \{1, \ldots, t\}$, luego $g \in F[x]$.

Por una parte $g(\alpha) = 0$, puesto que $\alpha \in Orb(\alpha)$. Como $h = \mathrm{Irr}(\alpha, F)$, 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 $h \in K^G[x]$):

$$h(\alpha_i) = h(\sigma(\alpha)) \overset{(*)}{=} \sigma(h(\alpha)) = \sigma(0) = 0$$

Como los elementos $\alpha_i$ son distintos, tenemos que $degh \geqslant t$, pero como $h$ divide a $g$ y $g$ es un polinomio mónico de grado $t$, tenemos que $g = h$. Hemos probado que $\mathrm{Irr}(\alpha, F)$ 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 $F \leqslant K$ es una extensión normal y separable.

$iv) \Longrightarrow i)$ Como $F \leqslant K$ es finita, tenemos entonces que existen $\alpha_1, \ldots, \alpha_s \in K$ algebraicos de forma que $K = F(\alpha_1, \ldots, \alpha_s)$. Podemos por tanto considerar $f_i = \mathrm{Irr}(\alpha_i, F)$, 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 $F \leqslant K$ 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 $iv) \Longrightarrow i)$.
- 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 $\sigma : \mathbb{C} \to \mathbb{C}$ 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 $\mathrm{Aut}_F(K)$ 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 $|\mathrm{Aut}_F(K)| \leqslant [K : F]$.

**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:

$$f = p_1^{n_1} \cdot \ldots \cdot p_t^{n_t}$$

con $p_i$ distintos. Obsevemos que $K$ es cuerpo de descomposición de $p_1 \cdot \ldots \cdot p_t$. Cada uno de los $p_i$ es irreducible en $\mathrm{car}(F) = 0$, por lo que cada $p_i$ es separable. Como estos no pueden compartir raíces entre sí por ser irreducibles[1], tendremos que $p_1 \cdot \ldots \cdot p_t$ es separable. Por el Teorema anterior, la extensión es finita, normal y separable. □

**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. □

**Ejemplo.** Si consideramos $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt[3]{2}\right)$, tenemos una extensión finita y separable pero que no es de Galois, porque no es normal. Sin embargo, $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt[3]{2}, w\right)$ sí que es de Galois. En consecuencia, $\mathbb{Q}(\sqrt[3]{2}) \leqslant \mathbb{Q}\left(\sqrt[3]{2}, w\right)$ es de Galois.

Sabemos que $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt[3]{2}\right)$ no es normal porque $\mathrm{Irr}\left(\sqrt[3]{2}, \mathbb{Q}\right) = x^3 - 2$ no se descompone como producto de polinomios lineales en $\mathbb{Q}\left(\sqrt[3]{2}\right)$, ya que $w\sqrt[3]{2}$ es una raíz del polinomio que no está en $\mathbb{Q}\left(\sqrt[3]{2}\right)$.

**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 $car(F) = p$, tenemos entonces que:

$$\mathbb{F}_p \leqslant F \leqslant E$$

con $\mathbb{F}_p \leqslant E$ de Galois, puesto que el polinomio $x^q - x \in \mathbb{F}_q[x]$ con $q = |E| = p^n$ es separable y $E$ es un cuerpo de descomposición suyo. □

[1]Si $p_i$ tiene alguna raíz en común con $p_j$ entones $p_i$ dividiría a $p_j$, de donde deducimos que $p_i = p_j$ por ser ambos irreducibles, pero eran polinomios distintos.

**Ejemplo.** Consideramos $\mathbb{Q} \leqslant E = \mathbb{Q}\left(\sqrt[3]{5}, i\sqrt{5}\right)$, 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 $x^3 - 5 = \mathrm{Irr}(\sqrt[3]{5}, \mathbb{Q})$ estaría en $E$, para $w = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$.

En dicho caso, $i\sqrt{3} \in E$, luego $\mathbb{Q}\left(i\sqrt{3}, i\sqrt{5}\right) \leqslant E$. Buscamos calcular:

$$\left[\mathbb{Q}\left(i\sqrt{3}, i\sqrt{5}\right) : \mathbb{Q}\right]$$

Sabemos que $\left[\mathbb{Q}\left(i\sqrt{3}\right) : \mathbb{Q}\right] = 2$, así como que $\left[\mathbb{Q}\left(i\sqrt{5}, i\sqrt{3}\right) : \mathbb{Q}\left(i\sqrt{3}\right)\right] \leqslant 2$:

- Si $\left[\mathbb{Q}\left(i\sqrt{5}, i\sqrt{3}\right)\right] = 1$, esto es porque $i\sqrt{5} \in \mathbb{Q}\left(i\sqrt{3}\right)$. En dicho caso, tendríamos que:
$$i\sqrt{5} = a + bi\sqrt{3} \qquad a, b \in \mathbb{Q}$$
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 $\left[\mathbb{Q}\left(i\sqrt{5}, i\sqrt{3}\right) : \mathbb{Q}\left(i\sqrt{3}\right)\right] = 2$, y por el lema de la torre tenemos que $\left[\mathbb{Q}\left(i\sqrt{3}, i\sqrt{5}\right) : \mathbb{Q}\right] = 4$, 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 $\mathrm{Subex}(F \leqslant K)$.
- Si $G$ es un grupo, llamamos $\mathrm{Subgr}(G)$ al conjunto de todos sus subgrupos.
- Si $H \in \mathrm{Subgr}(G)$, 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 $f : A \to B$ de forma que:

$$a \leqslant a' \iff f(a) \geqslant f(a')$$

*Observación.* Si $G$ es un grupo y $F \leqslant K$ es una extensión de cuerpos, tenemos que $(\mathrm{Subgr}(G), <)$ y $(\mathrm{Subex}(F \leqslant K), \leqslant)$ son conjuntos ordenados, pues la relación indicada en cada conjunto es reflexiva, transitiva y antisimétrica.

**Teorema 2.5.** *Sea $F \leqslant K$ una extensión de Galois con grupo de Galois $G$. La aplicación*

$$\begin{array}{rccc} : & \mathrm{Subgr}(G) & \longrightarrow & \mathrm{Subex}(F \leqslant K) \\ & H & \longmapsto & K^H \end{array}$$

*es un anti-isomorfismo de conjuntos ordenados, cuya isomorfismo inverso es*

$$\begin{array}{rccc} : & \mathrm{Subex}(F \leqslant K) & \longrightarrow & \mathrm{Subgr}(G) \\ & E & \longmapsto & \mathrm{Aut}_E(K) \end{array}$$

*Si $H_1 < H_2$ son subgrupos de $G$ y $E_2 \leqslant E_1$ son las subextensiones de $F \leqslant K$ 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 $H \in \mathrm{Subgr}(G)$, tenemos entonces que $\{id_K\} < H < G$, y el Lema 2.2 nos dice que:

  $$K = K^{id_K} \geqslant K^H \geqslant K^G \overset{(*)}{=} F$$

  donde en $(*)$ hemos usado que como $F \leqslant K$ es de Galois, tenemos el segundo punto del Teorema 2.4. Por tanto, $K^H \in \mathrm{Subex}(F \leqslant K)$.

- Sea $E \in \mathrm{Subex}(F \leqslant K)$, tenemos entonces que $F \leqslant E \leqslant K$, y el Lema 2.2 nos dice que:

  $$G = \mathrm{Aut}_F(K) > \mathrm{Aut}_E(K) > \mathrm{Aut}_K(K) = \{id_K\}$$

  de donde $\mathrm{Aut}_E(K) \in \mathrm{Subgr}(G)$.

- Sea $H \in \mathrm{Subgr}(G)$, si aplicamos las dos aplicaciones a $H$ obtenemos:

  $$H \longmapsto K^H \longmapsto \mathrm{Aut}_{K^H}(K)$$

  como $F \leqslant K$ 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 $H = \mathrm{Aut}_{K^H}(K)$.

- Sea $E \in \mathrm{Subex}(F \leqslant K)$, si aplicamos las dos aplicaciones a $E$ obtenemos:

  $$E \longmapsto \mathrm{Aut}_E(K) \longmapsto K^{\mathrm{Aut}_E(K)}$$

  y como $F \leqslant K$ es de Galois deducimos que $E \leqslant K$ es también de Galois, pudiendo aplicar finalmente el segundo punto del Teorema 2.4, obteniendo que $E = K^{\mathrm{Aut}_E(K)}$.

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 $E_2 \leqslant E_1$ son las subextensiones de $F \leqslant K$ 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:

$$|H_2| \overset{(*)}{=} [K : E_2] \overset{(**)}{=} [K : E_1][E_1 : E_2] \overset{(*)}{=} |H_1|[E_1 : E_2]$$

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 $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt[3]{2}, w\right)$, vimos anteriormente que $\mathrm{Aut}\left(\mathbb{Q}\left(\sqrt[3]{2}, w\right)\right)$ tenía 6 elementos, y en un ejemplo anterior calculábamos $\mathrm{Subgr}(\mathrm{Aut}\left(\mathbb{Q}\left(\sqrt[3]{2}, w\right)\right))$, obteniendo 6 subgrupos.

Por la Conexión de Galois sabemos ahora que tenemos tantos subcuerpos de $\mathbb{Q}\left(\sqrt[3]{2}, w\right)$ como subgrupos de $\mathrm{Aut}\left(\mathbb{Q}\left(\sqrt[3]{2}, w\right)\right)$ (puesto que $\mathbb{Q}$ es el subcuerpo primo de $\mathbb{Q}\left(\sqrt[3]{2}, w\right)$).

**Ejemplo.** Sea $\mathbb{F}_q = \mathbb{F}_{p^n}$, nos preguntamos por los elementos de dicho cuerpo. La extensión $\mathbb{F}_p \leqslant \mathbb{F}_{p^n}$ 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:

$$\mathrm{Aut}(\mathbb{F}_{p^n}) = \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n}) = \langle \tau \rangle$$

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:

$$\mathrm{Subgr}(\mathrm{Aut}(\mathbb{F}_{p^n})) = \left\{ \langle \tau^d \rangle : d \in Div(n) \right\}$$

Los subcuerpos de $\mathbb{F}_{p^n}$ son, por la conexión de Galois:

$$\left\{ \mathbb{F}_{p^n}^{\langle \tau^d \rangle} : d \in Div(n) \right\}$$

Vamos a calcular:

$$\left[ \mathbb{F}_{p^n}^{\langle \tau^d \rangle} : \mathbb{F}_p \right] = \left( \langle \tau \rangle : \langle \tau^d \rangle \right) = d$$

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 $d \in Div(n)$.
Por ejemplo, un cuerpo de 64 elementos tiene 4 subcuerpos (cada divisor de 6).

**Lema 2.6.** *Sea $F \leqslant K$ de Galois con grupo de Galois $G$, sea $H \in \mathrm{Subgr}(G)$ y $E \in \mathrm{Subex}(F \leqslant K)$ 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 $H \in \mathrm{Subgr}(G)$ entonces para $\sigma \in G$ tenemos $\sigma H \sigma^{-1} \in \mathrm{Subgr}(G)$, vemos también que $\sigma(E)$ es sigue siendo una subextensión de $F \leqslant K$, 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 $F \leqslant K$ de Galois y $G$ su grupo de Galois, si $H \in \mathrm{Subgr}(G)$ y $E \in \mathrm{Subex}(F \leqslant K)$ es su correspondiente mediante la conexión de Galois entonces:*

$$H \text{ es normal en } G \iff F \leqslant E \text{ es de Galois}$$

*En cuyo caso,* $\mathrm{Aut}_F(E) \cong G/H$.

*Demostración.* Por doble implicación:

$\Longrightarrow$) Si $H \lhd G$ tenemos entonces que:

$$\sigma(E) = \sigma(K^H) = K^{\sigma H \sigma^{-1}} = K^H = E \qquad \forall \sigma \in \mathrm{Aut}_F(K)$$

Por lo que podemos definir la aplicación $r : \mathrm{Aut}_F(K) \to \mathrm{Aut}_F(E)$ dada por:

$$r(\sigma) = \sigma\big|_E$$

y estará bien definida, pues $\sigma(E) = E$ para cada $\sigma \in \mathrm{Aut}_F(K)$. Es fácil ver que $r$ es un homomorfismo de grupos. Observamos ahora que:

$$\ker(r) = \left\{\sigma \in \mathrm{Aut}_F(K) : \sigma\big|_E = id_E\right\} = \mathrm{Aut}_E(K) = H$$

Aplicando el Primer Teorema de Isomorfía para grupos obtenemos que:

$$G/H \cong Imr$$

y si observamos ahora que:

$$[E : F] = (G : H) = |Imr| \leqslant |\mathrm{Aut}_F(E)| \leqslant [E : F]$$

Obtenemos que $Imr = \mathrm{Aut}_F(E)$, por lo que $r$ es sobreyectivo, tenemos ya que $G/H \cong \mathrm{Aut}_F(E)$. Para ver que $F \leqslant E$ es de Galois, trataremos de probar la tercera condición del Teorema 2.4, de la que conocemos ya la inclusión $F \leqslant E^{\mathrm{Aut}_F(E)}$. Sea pues $\alpha \in E^{\mathrm{Aut}_F(E)}$, vemos que:

$$\alpha = r(\sigma)(\alpha) = \sigma\big|_E(\alpha) = \alpha \qquad \forall \sigma \in \mathrm{Aut}_F(K)$$

por lo que $\alpha \in K^{\mathrm{Aut}_F(K)} = F$, lo que nos da la otra inclusión, de donde $F \leqslant E$ es de Galois.

$\Longleftarrow$) 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 $E = F(\alpha_1, \ldots, \alpha_n)$, 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 $\sigma \in \mathrm{Aut}_F(K)$, 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 $\alpha_i$) $\sigma(E) = E \quad \forall \sigma \in \mathrm{Aut}_F(K)$, por lo que:

$$K^H = E = \sigma(E) = \sigma(K^H) = K^{\sigma H \sigma^{-1}} \qquad \forall \sigma \in \mathrm{Aut}_F(K)$$

de donde $H = \sigma H \sigma^{-1} \quad \forall \sigma \in \mathrm{Aut}_F(K)$, por lo que $H \lhd \mathrm{Aut}_F(K)$.

□

**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:

$$\alpha = \sqrt{\sqrt{3} + 1}, \qquad \beta = i\sqrt{\sqrt{3} - 1}$$

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 $f = \mathrm{Irr}(\alpha, \mathbb{Q})$, luego $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

Por otra parte, $\left[\mathbb{Q}\left(\alpha, i\sqrt{2}\right) : \mathbb{Q}(\alpha)\right] = 2$, 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 $f = \mathrm{Irr}(\beta, \mathbb{Q}(\alpha))$, de donde sería $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 4$.

En conclusión, tenemos por el Lema de la Torre que:

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = \left[\mathbb{Q}\left(\alpha, i\sqrt{2}\right):\mathbb{Q}\right] = 8$$

Y como $F \leqslant K$ es de Galois, el Teorema 2.5 nos dice que:

$$|\operatorname{Aut}_{\mathbb{Q}}(K)| = 8$$

Buscamos los automorfismos por la propiedad de extensión, es decir, calculamos las extensiones de la inclusión $\iota : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{Q}\left(\alpha, i\sqrt{2}\right) = K$ mediante la Proposición de extensión. Así, están determinadas por:

$$\eta_0(\alpha) = \alpha, \qquad \eta_1(\alpha) = -\alpha, \qquad \eta_2(\alpha) = \beta, \qquad \eta_3(\alpha) = -\beta$$

Ahora, $\operatorname{Irr}(i\sqrt{2},\mathbb{Q}) = x^2+2$, con lo que cada uno de los anteriores se extienden a dos automorfismos $K \to K$ determinados por:

$$\eta_{j,k} : \begin{cases} \alpha \longmapsto \eta_j(\alpha) \\ \alpha\beta \longmapsto (-1)^k \alpha\beta \end{cases} \qquad \forall j \in \{0,1,2,3\}, k \in \{0,1\}$$

Por lo que:

$$\operatorname{Aut}(K) = \{\eta_{j,k} : j \in \{0,1,2,3\}, k \in \{0,1\}\}$$

Si tratamos de calcular ahora todos los subgrupos de $\operatorname{Aut}(K)$, conviene tener en mente todos los grupos de orden 8:

$$C_8, \qquad C_4 \oplus C_2, \qquad C_2 \oplus C_2 \oplus C_2, \qquad D_4, \qquad H = \{\pm 1, \pm i, \pm j, \pm k\}$$

Sabemos que $\mathbb{Q}\left(i\sqrt{2}\right) \leqslant K$ con $\left[K : \mathbb{Q}\left(i\sqrt{2}\right)\right] = 4$ (ya que $\left[\mathbb{Q}\left(i\sqrt{2}\right):\mathbb{Q}\right] = 2$ 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:

$$\left|\operatorname{Aut}_{\mathbb{Q}\left(i\sqrt{2}\right)}(K)\right| = 4$$

Y este es un subgrupo normal de $\operatorname{Aut}_{\mathbb{Q}}(K)$, podemos verlo de dos formas distintas:

- $\mathbb{Q}\left(i\sqrt{2}\right) \leqslant K$ es de Galois.
- Tiene índice 2 sobre $\operatorname{Aut}(K)$.

Más aún, sabemos que:

$$\operatorname{Aut}_{\mathbb{Q}\left(i\sqrt{2}\right)}(K) = \{\eta_{j,0} : j \in \{0,1,2,3\}\}$$

ya que se debe cumplir que $\alpha\beta \longmapsto \alpha\beta$ y debe tener 4 elementos, los únicos 4 candidatos posibles. Veamos el orden de cada elemento:

| $\eta_{0,0}$ | $\eta_{1,0}$ | $\eta_{2,0}$ | $\eta_{3,0}$ | $\eta_{0,1}$ | $\eta_{1,1}$ | $\eta_{1,2}$ | $\eta_{1,3}$ |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 2 | 2 | 2 | 2 | 4 | 4 |

Que por ejemplo calculamos el orden de $\eta_{2,0}$ ya que:

$$\eta_{2,0}(\alpha) = \beta, \qquad \eta_{2,0}^2(\alpha) = \eta_{2,0}(\beta) = \eta_{2,0}\left(\frac{\alpha\beta}{\alpha}\right) = \frac{\eta_{2,0}(\alpha\beta)}{\eta_{2,0}(\alpha)} = \frac{\alpha\beta}{\beta} = \alpha$$

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 $\mathrm{Aut}(K) \cong D_4$.

Queremos calcular todos sus subgrupos, para así calcular todos los subcuerpos de $K$ aplicando el Teorema 2.5.

Sabemos ya que $\mathrm{Aut}_{\mathbb{Q}\left(i\sqrt{2}\right)}(K) = \langle \eta_{1,0}, \eta_{2,0} \rangle$, 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:

$$\eta_{2,1}\left(\sqrt{3}\right) = \eta_{2,1}(\alpha^2 - 1) = \left(\eta_{2,1}(\alpha)\right)^2 - 1 = \beta^2 - 1 = -\sqrt{3}$$

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:

$$\eta_{2,1}(i\sqrt{6}) = \eta_{2,1}(\sqrt{3})\eta_{2,1}(i\sqrt{2}) = (-\sqrt{3})(-i\sqrt{2}) = i\sqrt{6}$$

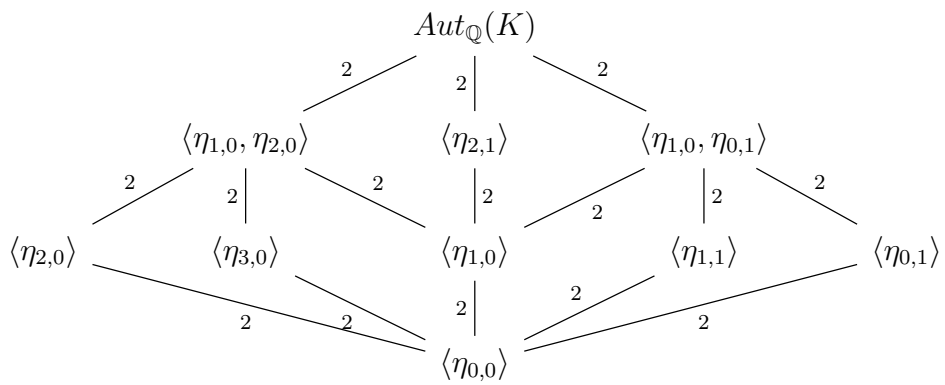
Por lo que $\mathbb{Q} \leqslant \mathbb{Q}(i\sqrt{6})$ de grado 2, tenemos que:

$$\mathrm{Aut}_{\mathbb{Q}\left(i\sqrt{6}\right)}(K) = \langle \eta_{2,1} \rangle = \langle \eta_{3,1} \rangle$$

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:

  $$\alpha \in K^{\langle \eta_{0,1} \rangle} \Longrightarrow \mathbb{Q}(\alpha) \leqslant K^{\langle \eta_{0,1} \rangle}$$

  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 $\mathbb{Q}(\beta) \geqslant \mathbb{Q}$ 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:

  $$\beta \in K^{\langle \eta_{1,1} \rangle} \Longrightarrow \mathbb{Q}(\beta) \leqslant K^{\langle \eta_{1,1} \rangle}$$

  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:

  $$\alpha + \beta \in K^{\langle \eta_{2,0} \rangle} \Longrightarrow \mathbb{Q}(\alpha + \beta) \leqslant K^{\langle \eta_{2,0} \rangle}$$

  Por la conexión de Galois, tenemos que:

  $$\langle \eta_{2,0} \rangle \leqslant \mathrm{Aut}_{\mathbb{Q}(\alpha+\beta)}(K) \Longrightarrow \mathrm{Aut}_{\mathbb{Q}(\alpha+\beta)}(K) \in \{\langle \eta_{2,0} \rangle, \langle \eta_{1,0}, \eta_{2,0} \rangle, \mathrm{Aut}_{\mathbb{Q}}(K)\}$$

  Y descartamos:

  - No es el total, porque $\alpha + \beta \notin \mathbb{Q}$.
  - No es el generado por los dos etas, 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 $\mathrm{Aut}_{(\alpha+\beta)}(K) = \langle \eta_{2,0} \rangle$. 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:

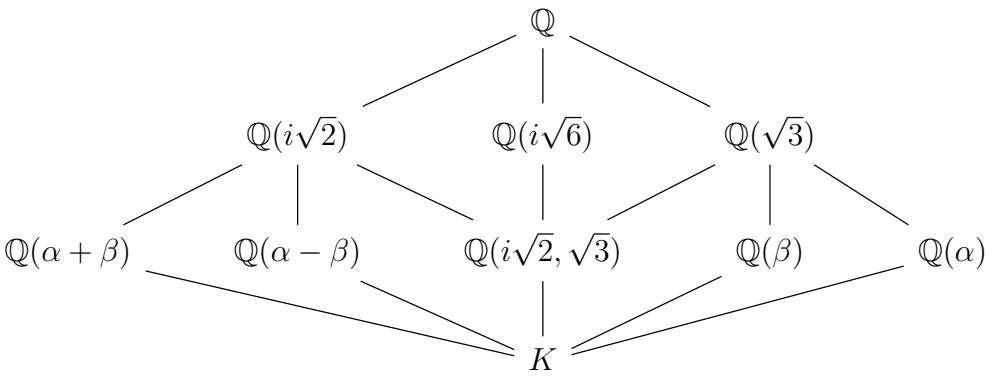



Figura 2.1: Todos los subcuerpos de $K$.

## 2.3. El Teorema Fundamental del Álgebra

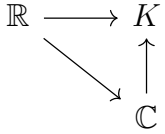
Se tiene que $\mathbb{C}$ es el cuerpo de descomposición de $x^2+1 \in \mathbb{R}[x]$, y $[\mathbb{C}:\mathbb{R}]=2$, por lo que $|\operatorname{Aut}_{\mathbb{R}}(\mathbb{C})|=2$, que son:

$$\operatorname{Aut}_{\mathbb{R}}(\mathbb{C})=\{id,\sigma\}$$

con $\sigma$ el automorfismo que conjuga cada número complejo.
Además, si $f \in \mathbb{C}[x]$, $\overline{f} \in \mathbb{C}[x]$ 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*[2] *en $\mathbb{C}$.*

*Demostración.* Sea $g=f\overline{f} \in \mathbb{R}[x]$, 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:




Además, las tres extensiones que aparecen son de Galois. El Lema de la Torre nos dice que

$$|\operatorname{Aut}_{\mathbb{R}}(K)|=[K:\mathbb{R}]=[K:\mathbb{C}][\mathbb{C}:\mathbb{R}]=[K:\mathbb{C}]\cdot 2$$

[2] O equivalentemente, $\mathbb{C}$ es cuerpo de descomposición de $f$.

múltiplo de 2, por lo que $G = \mathrm{Aut}_{\mathbb{R}}(K)$ 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 $\mathrm{Irr}(\alpha, \mathbb{R})$, 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 $\mathrm{Irr}(\alpha, \mathbb{R})$ es divisible por $(x - \beta)$, pero como $\mathrm{Irr}(\alpha, \mathbb{R})$ es irreducible, este debe ser asociado a $x - \beta$, y los dos son mónicos, de donde $\mathrm{Irr}(\alpha, \mathbb{R}) = x - \beta$, 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, $\mathrm{Aut}_{\mathbb{C}}(K)$ es un 2−grupo (por ser subgrupo de un 2−grupo, $\mathrm{Aut}_{\mathbb{R}}(K) > \mathrm{Aut}_{\mathbb{C}}(K)$). Supongamos que $|\mathrm{Aut}_{\mathbb{C}}(K)| > 1$. Como $\mathrm{Aut}_{\mathbb{C}}(K)$ 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 $\mathrm{Irr}(\beta, \mathbb{C})$ 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 $|\mathrm{Aut}_{\mathbb{C}}(K)| = 1$, de donde por la conexión de Galois, $K = \mathbb{C}$. □

**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 $\overline{\alpha}$ también será una raíz de $f$. Tenemos así que $(x - \alpha)(x - \overline{\alpha})$ divide a $f$, pero como $f$ es irreducible tiene que ser asociado a $(x - \alpha)(x - \overline{\alpha})$, por lo que $\deg f = 2$. □

**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 $\overline{\mathbb{Q}}$.

Sea $f \in \overline{\mathbb{Q}}[x]$ un polinomio no constante, $f$ será de la forma:

$$f = \sum_{i=0}^{n} a_i x^i$$

con $a_0, a_1, \ldots, a_n \in \overline{\mathbb{Q}}$ todos estos algebraicos, por lo que la extensión $\mathbb{Q} \leqslant \mathbb{Q}(a_0, a_1, \ldots, a_n)$ será finita. Sea $\alpha$ una raíz de $f$, tenemos que $\alpha$ es algebraico sobre $\mathbb{Q}(a_0, a_1, \ldots, a_n)$, por lo que tenemos que la extensión:

$$\mathbb{Q} \leqslant \mathbb{Q}(a_0, a_1, \ldots, a_n, \alpha)$$

es finita, luego es algebraica, de donde $\mathbb{Q}(a_0, a_1, \ldots, a_n, \alpha) \leqslant \overline{\mathbb{Q}}$, por lo que en particular $\alpha \in \overline{\mathbb{Q}}$.

## 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 $\mathbb{Q}$.

1. 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:

   $$\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}, i\right) \leqslant K$$

   Y la otra inclusión la vemos viendo que todos los elementos que definen $K$ se expresan con operaciones con estos tres, con lo que:

   $$K = \mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}, i\right)$$

   Con vistas al Lema de la Torre, vemos:

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

   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:

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

   Tenemos que el segundo vale 2 por Eisenstein y el primero es menor o igual que 3. En definitiva, tenemos que $\left[\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}\right) : \mathbb{Q}\right] = 6$. Ahora:

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

   Ya que $x^2 + 1$ es irreducible en $\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}\right)$, 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 $\mathrm{Aut}(K)$.

   $F \leqslant K$ es de Galois por ser $K$ cuerpo de descomposición de $f$ con $\mathrm{car}(F) = 0$, por lo que:

   $$|\operatorname{Aut}(K)| = [K : F] = 12$$

   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 $\operatorname{Irr}\left(\sqrt{3}, \mathbb{Q}\right) = x^2 - 3$ en $K$. A saber, son dos determinadas por:

   $$\eta_j(\sqrt{3}) = (-1)^j\sqrt{3} \qquad j \in \{0, 1\}$$

   Análogamente, con la misma Proposición tenemos que cada $\eta_j$ se extienden a 3 homomorfismos $\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}\right) \to K$, ya que las raíces de $x^3 - 2 \in \mathbb{Q}\left(\sqrt{3}\right)[x]$ en $K$ son tres, a saber, $\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}$. Obsérvese que $x^3 - 2 \in \mathbb{Q}\left(\sqrt{3}\right)[x]$ es irreducible porque:

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

   Así, obtengo $\eta_{j,k} : \mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}\right) \to K$, determinados por:

   $$\begin{aligned}\eta_{j,k}\left(\sqrt[3]{2}\right) &= w^k\sqrt{2} \\ \eta_{j,k}\left(\sqrt{3}\right) &= (-1)^j\sqrt{3} \qquad j \in \{0, 1\}, \quad k \in \{0, 1, 2\}\end{aligned}$$

   De la misma manera, extendiendo cada $\eta_{j,k}$ según las raíces de $x^2 + 1$, obtengo que:

   $$\operatorname{Aut}(K) = \{\eta_{j,k,l} : j, l \in \{0, 1\}, k \in \{0, 1, 2\}\}$$

   donde cada uno de ellos está determinado por:

   $$\begin{aligned}\eta_{j,k,l}\left(\sqrt{3}\right) &= (-1)^j\sqrt{3} \\ \eta_{j,k,l}\left(\sqrt[3]{2}\right) &= w^k\sqrt[3]{2} \\ \eta_{j,k.l}(i) &= (-1)^l i\end{aligned}$$

4. Describir los elementos de $\mathrm{Aut}_{\mathbb{Q}\left(i+\sqrt{3}\right)}(K)$ y decidir si es un subgrupo normal de $\mathrm{Aut}(K)$.

   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 $[\mathbb{Q}\left(i + \sqrt{3}\right) : \mathbb{Q}] = 4$, 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:

   $$\mathrm{Aut}_{\mathbb{Q}\left(i+\sqrt{3}\right)}(K) = \{\eta_{0,k,0} : k \in \{0, 1, 2\}\}$$

Que es normal, porque la extensión $\mathbb{Q} \leqslant \mathbb{Q}(i+\sqrt{3})$ es de Galois. Veamos esto último, pues:

$$\mathbb{Q}\left(i+\sqrt{3}\right) = \mathbb{Q}\left(i, \sqrt{3}\right)$$

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 $K = \mathbb{Q}\left(i\sqrt{3}, -i\sqrt{3}, \sqrt[3]{3}, w\sqrt[3]{3}, w^2\sqrt[3]{3}\right)$. Sin embargo, veamos que:

   $$K = \mathbb{Q}\left(i\sqrt{3}, \sqrt[3]{3}\right)$$

   $\subseteq$) 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:

   $$[K:\mathbb{Q}] = \left[\mathbb{Q}\left(i\sqrt{3}, \sqrt[3]{3}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(i\sqrt{3}, \sqrt[3]{3}\right) : \mathbb{Q}\left(\sqrt[3]{3}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{3}\right) : \mathbb{Q}\right]$$

   donde vemos fácilmente que:

   - $\left[\mathbb{Q}\left(\sqrt[3]{3}\right) : \mathbb{Q}\right] = 3$, ya que $\operatorname{Irr}\left(\sqrt[3]{3}, \mathbb{Q}\right) = x^3 - 3$, al ser un polinomio de grado 3 sin raíces en $\mathbb{Z}$ o bien por Eisenstein para $p = 3$.
   - $\left[\mathbb{Q}\left(i\sqrt{3}, \sqrt[3]{3}\right) : \mathbb{Q}\left(\sqrt[3]{3}\right)\right] = 2$, ya que $\operatorname{Irr}\left(i\sqrt{3} : \mathbb{Q}\left(\sqrt[3]{3}\right)\right) = x^2 + 3$, por ser un polinomio de grado 2 sin raíces en $\mathbb{Q}\left(\sqrt[3]{3}\right)$ (sus raíces son complejas).

   Por lo que $[K:\mathbb{Q}] = 6$. Como $\operatorname{car}(\mathbb{Q}) = 0$ y $K$ es cuerpo de descomposición de $f \in \mathbb{Q}[x]$ tenemos que la extensión $\mathbb{Q} \leqslant K$ es de Galois, por lo que:

   $$|\operatorname{Aut}(K)| = 6$$

   Por lo que el grupo de Galois de la extensión será isomorfo a $C_6$ o a $D_3$.

   Calculamos los elementos de $\operatorname{Aut}(K)$, aplicando para ello dos veces la proposición de Extensión. Calculamos en primer lugar las extensiones de la inclusión a $\mathbb{Q}\left(\sqrt[3]{3}\right) \xrightarrow{\eta_j} K$, que están en correspondencia biyectiva con las raíces de:

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

a saber, $\sqrt[3]{3}, w\sqrt[3]{3}, w^2\sqrt[3]{3}$, por lo que las extensiones obtenidas son las determinadas por:

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

Análogamente, para cada $\eta_j$ tenemos 2 extensiones suyas en automorfismos $K \to K$, puesto que estas están a su vez en correspondencia biyectiva con las raíces de:

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

Que son $\pm i\sqrt{3}$, por lo que obtenemos en total 6 automorfismos, que son los determinados por:

$$\begin{aligned}\eta_{j,k}\left(\sqrt[3]{3}\right) &= w^j\sqrt[3]{3} \\ \eta_{j,k}\left(i\sqrt{3}\right) &= (-1)^k i\sqrt{3} \qquad j \in \{0,1,2\}, k \in \{0,1\}\end{aligned}$$

De donde:

$$\operatorname{Aut}(K) = \{\eta_{j,k} : j \in \{0,1,2\}, k \in \{0,1\}\}$$

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 $\eta_{1,0}\left(i\sqrt{3}\right) = i\sqrt{3}$ 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 $\eta_{2,0}\left(i\sqrt{3}\right) = i\sqrt{3}$ 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 $\eta_{1,1}$:

$$\sqrt[3]{3} \longmapsto w\sqrt[3]{3} = \left(\frac{-1}{2} + \frac{i\sqrt{3}}{2}\right)\sqrt[3]{3} \longmapsto \overline{w}w\sqrt[3]{3} = |w|^2\sqrt[3]{3} = \sqrt[3]{3}$$
$$i\sqrt{3} \longmapsto -i\sqrt{3} \longmapsto i\sqrt{3}$$

  Por lo que su orden es 2.

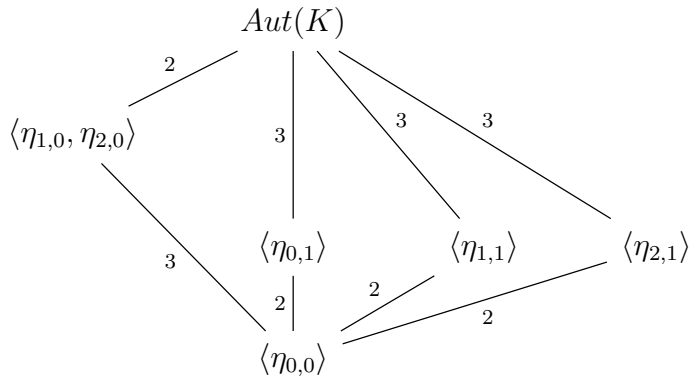
Tenemos por tanto:

| $\eta_{0,0}$ | $\eta_{1,0}$ | $\eta_{2,0}$ | $\eta_{0,1}$ | $\eta_{1,1}$ | $\eta_{2,1}$ |
|---|---|---|---|---|---|
| 1 | 3 | 3 | 2 | 2 | |

Como $C_6$ tiene 2 elementos de orden 6, descartamos automáticamente esta opción, por lo que tiene que ser $|\operatorname{Aut}(K)| \cong D_3$, luego el orden del elemento que falta es 2.

| $\eta_{0,0}$ | $\eta_{1,0}$ | $\eta_{2,0}$ | $\eta_{0,1}$ | $\eta_{1,1}$ | $\eta_{2,1}$ |
|---|---|---|---|---|---|
| 1 | 3 | 3 | 2 | 2 | 2 |

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 correspondiencia biyectiva con los subgrupos no triviales de $\operatorname{Aut}(K)$. En primer lugar observamos que ya conocemos dos subextensiones de $\mathbb{Q} \leqslant K$:

$$\mathbb{Q} \leqslant \mathbb{Q}\left(i\sqrt{3}\right), \qquad \mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt[3]{3}\right)$$

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 $\operatorname{Aut}(K)$ de orden 3 es $\langle \eta_{1,0}, \eta_{2,0}\rangle$, tenemos que este es el subgrupo correspondiente con $\mathbb{Q}\left(i\sqrt{3}\right)$. Buscamos ahora qué subgrupo de $\operatorname{Aut}(K)$ se corresponde con $\mathbb{Q}\left(\sqrt[3]{3}\right)$. 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:

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

extensiones de grado 3, por lo que sus subgrupos correspondientes serán de grado 2. Veamos cuáles de ellos son:

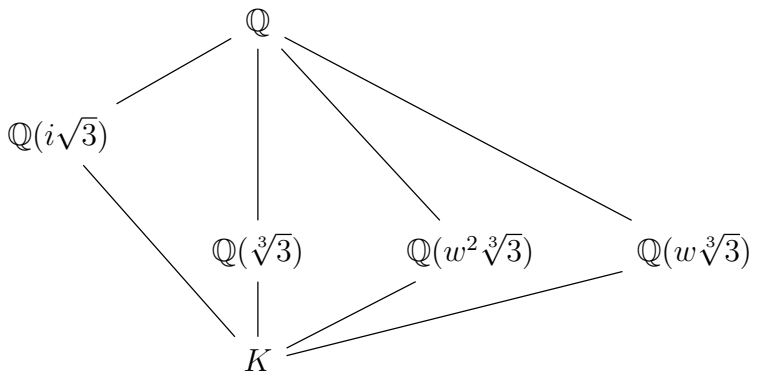
- Para $\mathbb{Q}\left(w^2\sqrt[3]{3}\right)$, veamos que $\eta_{1,1}$ deja fijo a este elemento:

$$w^2\sqrt[3]{3} \longmapsto \overline{w}\overline{w}w\sqrt[3]{3} = \overline{w}\sqrt[3]{3} = w^2\sqrt[3]{3}$$

  Efectivamente.
- Para $\mathbb{Q}\left(w\sqrt[3]{3}\right)$, veamos que $\eta_{2,1}$ defja fijo a dicho elemento:

$$w\sqrt[3]{3} \longmapsto \overline{w}ww\sqrt[3]{3} = w\sqrt[3]{3}$$

En definitiva, los subcuerpos de $K$ son:




2. Demostrar que $\mathbb{Q}\left(\sqrt[3]{3}+i\sqrt{3}\right) = K$.

   Para ello, veamos qué automorfismos $\mathrm{Aut}_{\mathbb{Q}}(K)$ dejan fijo al elemento $\sqrt[3]{3}+i\sqrt{3}$:

$$\begin{aligned}
\sqrt[3]{3}+i\sqrt{3} &\overset{\eta_{1,0}}{\longmapsto} w\sqrt[3]{3}+i\sqrt{3}\\
\sqrt[3]{3}+i\sqrt{3} &\overset{\eta_{2,0}}{\longmapsto} w^2\sqrt[3]{3}+i\sqrt{3}\\
\sqrt[3]{3}+i\sqrt{3} &\overset{\eta_{0,1}}{\longmapsto} \sqrt[3]{3}-i\sqrt{3}\\
\sqrt[3]{3}+i\sqrt{3} &\overset{\eta_{1,1}}{\longmapsto} w\sqrt[3]{3}-i\sqrt{3}\\
\sqrt[3]{3}+i\sqrt{3} &\overset{\eta_{2,1}}{\longmapsto} w^2\sqrt[3]{3}-i\sqrt{3}
\end{aligned}$$

   Como vemos, ningún automorfismo salvo $\eta_{0,0}$ deja fijo al elemento, por lo que:

$$\mathbb{Q}\left(\sqrt[3]{3}+i\sqrt{3}\right) \leqslant K^{\langle\eta_{1,1}\rangle} = K$$

   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[1] y sean $\alpha_1, \ldots, \alpha_n$ sus raíces (repetidas tantas veces como indique su multiplicidad) en algún cuerpo de descomposición $K$ de $f$. Se define el discriminante de $f$ como:

$$\mathrm{Disc}(f) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2 \in K$$

Resulta que $\mathrm{Disc}(f)$ se puede calcular a partir de los coeficientes del polinomio.

*Observación.* Vemos que $f$ es separable $\iff \mathrm{Disc}(f) \neq 0$.

**Notación.** Notaremos usualmente a la raíz del discriminante $\mathrm{Disc}(f)$ por:

$$\Delta(f) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)$$

**Notación.** Dado un conjunto $S = \{\alpha_1, \ldots, \alpha_n\}$, denotaremos normalmente al grupo de permutaciones de dichos elementos por:

$$\mathrm{Sim}(\alpha_1, \ldots, \alpha_n)$$

Observemos que $\mathrm{Sim}(\alpha_1, \ldots, \alpha_n) \cong S_n$.

**Definición 3.2.** Si $f \in F[x]$ es separable y $K$ es su cuerpo de descomposición, diremos que $\mathrm{Aut}_F(K)$ es el grupo de Galois[2] de $f$.

Si $f \in F[x]$ es separable y $K$ es su cuerpo de descomposición, si consideramos $\{\alpha_1, \ldots, \alpha_n\}$ 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:

$$\begin{aligned} \mathrm{Aut}_F(K) &\longrightarrow \mathrm{Sim}(\alpha_1, \ldots, \alpha_n) \\ \sigma &\longmapsto \sigma\big|_{\{\alpha_1, \ldots, \alpha_n\}} \end{aligned}$$

Tenemos que:

[1] Si no, su discriminante se define como cierto elemento de $F$ multiplicado por la cantidad enunciada, pero no será relevante para nosotros.

[2] Observemos que por ser $f$ separable y $K$ cuerpo de descomposición suyo tenemos siempre por el Teorema 2.4 que la extensión $F \leqslant K$ es de Galois.

- La aplicación está bien definida, pues si consideros $\sigma \in \mathrm{Aut}_F(K)$, tendremos siempre que $\sigma^* = \sigma\big|_{\{\alpha_1,\ldots,\alpha_n\}} \in \mathrm{Sim}(\alpha_1,\ldots,\alpha_n)$, pues si $\alpha_i$ es una raíz de $f$ (para $i \in \{1,\ldots,n\}$) tendremos entonces que $\sigma(\alpha_i)$ también es raíz de $f$:

$$f(\sigma(\alpha_i)) = \sum_{i=0}^{n} f_i(\sigma(\alpha_i))^i \overset{(*)}{=} \sigma\left(\sum_{i=0}^{n} f_i\alpha_i^i\right) = \sigma(f(\alpha_i)) = 0$$

  donde en $(*)$ hemos usado que $\sigma \in \mathrm{Aut}_F(K)$ y que $f \in F[x]$.

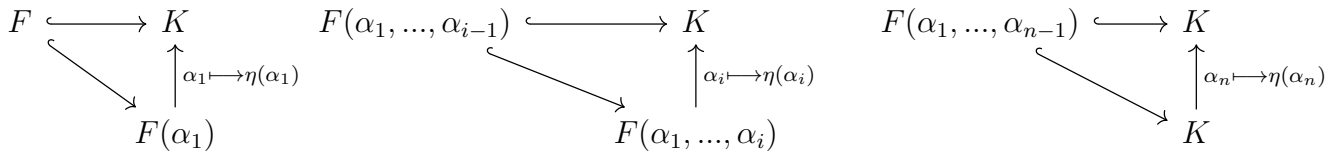
- La aplicación es un homeomorfismo, pues si $\sigma, \tau \in \mathrm{Aut}_F(K)$ tenemos entonces que:

$$(\sigma\tau)\big|_{\{\alpha_1,\ldots,\alpha_n\}} = \sigma\big|_{\{\alpha_1,\ldots,\alpha_n\}}\tau\big|_{\{\alpha_1,\ldots,\alpha_n\}}$$

Además dicho homomorfismo de grupos es siempre inyectivo, pues la Proposición de Extensión nos dice que cada automorfismo del grupo de Galois queda unívocamente 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:

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

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 $\sigma, \tau \in \mathrm{Aut}_F(K)$ coinciden en $\{\alpha_1,\ldots,\alpha_n\}$, tendremos entonces que $\sigma = \tau$, lo que nos prueba la inyectividad del homomorfismo de grupos.

De esta forma, como $\mathrm{Sim}(\alpha_1,\ldots,\alpha_n) \cong S_n$, podemos ver siempre el grupo de Galois de $f$ como subgrupo de $S_n$, aquel que permuta los índices de las raíces de $f$:

$$\alpha_i \overset{\sigma}{\longmapsto} \alpha_{\sigma(i)}$$

**Notación.** En vista de la relación existente entre $\mathrm{Aut}_F(K)$ (el grupo de Galois de cierto polinomio $f \in F[x]$), $\mathrm{Sim}(\alpha_1,\ldots,\alpha_n)$ (el grupo de permutaciones sobre sus raíces) y $S_n$, será habitual identificar $\mathrm{Sim}(\alpha_1,\ldots,\alpha_n)$ con $S_n$, y ver $\mathrm{Aut}_F(K)$ 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 $\mathrm{Aut}_F(K)$.

Una vez tenemos cierta intuición sobre el grupo de Galois $G$ de un polinomio separable, las dos siguientes Proposiciones nos ayudarán a identificar a qué subgrupo de $S_n$ es isomorfo el grupo $G$, sin necesidad de conocer los órdenes de todos los elementos del grupo, como hacíamos en el Capítulo anterior.

*Observación.* Si tomamos $\sigma \in \mathrm{Aut}_F(K)$, una vez visto que $\sigma$ actuando sobre las raíces del polinomio $f$ simplemente las permuta, vemos fácilmente que:

- $\sigma(\mathrm{Disc}(f)) = \mathrm{Disc}(f)$.
- $\sigma(\Delta(f)) = sgn(\sigma)\Delta(f)$.

**Proposición 3.1.** *Sea $f \in F[x]$ separable con grupo de Galois $G = \mathrm{Aut}_F(K)$, entonces* $\mathrm{Disc}(f) \in F$. *Además:*

$$K^{G\cap A_n} = F(\Delta(f))$$

*Por tanto, $\Delta(f) \in F \iff G < A_n$.*

*Demostración.* Para ver que $\mathrm{Disc}(f) \in F$, vimos en el primer punto de la observación superior que:

$$\sigma(\mathrm{Disc}(f)) = \mathrm{Disc}(f) \qquad \forall \sigma \in G$$

Por lo que tenemos que $\mathrm{Disc}(f) \in K^G$, pero como $F \leqslant K$ es de Galois, tenemos que $K^G = F$.

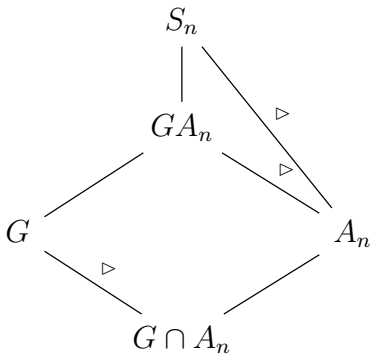
Para ver que $K^{G\cap A_n} = F(\Delta(f))$, en vista del segundo punto de la observación superior:

$$\sigma(\Delta(f)) = sgn(\sigma)\Delta(f) \qquad \forall \sigma \in G$$

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:

$$\left[K^{G\cap A_n} : F\right] = (G : G \cap A_n) \overset{(*)}{\leqslant} (S_n : A_n) = 2$$

donde en $(*)$ hemos usado el Segundo Teorema de Isomorfía para grupos:




Por tanto, solo tenemos dos situaciones posibles ante $F \leqslant F(\Delta(f)) \leqslant K^{G\cap A_n}$:

$$F(\Delta(f)) = F \qquad \text{o} \qquad F(\Delta(f)) = K^{G\cap A_n}$$

- Si $F(\Delta(f)) = F$, tendremos entonces que $\Delta(f) \in F$, así como que:

  $$sgn(\sigma)\Delta(f) = \sigma(\Delta(f)) = \Delta(f)\sigma(1) = \Delta(f) \qquad \forall \sigma \in G$$

  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:

$$sgn(\sigma)\Delta(f) = \sigma(\Delta(f)) \neq \Delta(f) \qquad \forall \sigma \in G$$

  Por lo que $sgn(\sigma) = -1$, de donde $G \not\leqslant A_n$.

□

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 $F$". Así, tenemos que $G < A_n$ si y solo si Disc$(f)$ es un cuadrado en $F$.

**Ejercicio 3.1.1.** Sea $f \in \mathbb{R}[x]$ mónico con $degf = 3$, 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 reaíz compleja $\alpha \in \mathbb{C}$, por lo que $\overline{\alpha} \in \mathbb{C}$ 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 $\overline{\alpha}$ también sería una raíz de $f$, de donde si $\beta \in \mathbb{R}$ es la última raíz de $f$ tendríamos que:

$$\text{Disc}(f) = (\alpha - \overline{\alpha})^2(\alpha - \beta)^2(\overline{\alpha} - \beta)^2$$

  supuesto que $\alpha = a + ib$ para $a, b \in \mathbb{R}$, tenemos entonces que:

  - $\alpha - \overline{\alpha} = 2ib \implies (\alpha - \overline{\alpha})^2 = (2ib)^2 = -4b^2 < 0$
  - Por otra parte:

$$(\alpha - \beta)^2(\overline{\alpha} - \beta)^2 = ((\alpha - \beta)(\overline{\alpha} - \beta))^2$$

    y tenemos que:

$$\begin{aligned}(\alpha - \beta)(\overline{\alpha} - \beta) &= ((a + ib) - \beta)((a - ib) - \beta) = ((a - \beta) + ib)((a - \beta) - ib) \\ &= (a - \beta)^2 + b^2 > 0\end{aligned}$$

  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 $\alpha_1, \ldots, \alpha_n$ 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[3]. Por ejemplo, si $n = 2$ se obtiene:

$$a_0 = \alpha_1 \alpha_2 \qquad a_1 = -(\alpha_1 + \alpha_2)$$

Como $\mathrm{Disc}(f) = (\alpha_1 - \alpha_2)^2$, tenemos que $\mathrm{Disc}(f) = a_1^2 - 4a_0$.
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 $\mathrm{Disc}(f)$ en término de los coeficientes de $f$. Para $n = 3$, la damos para $f = x^3 + px + q$ (cúbica reducida[4]) es:

$$\mathrm{Disc}(f) = -4p^3 - 27q^2$$

Sea $H < S_n$, recordamos que decíamos que "$H$ es transitivo" si dados dos elementos cualesquiera $i, j \in \{1, \ldots, n\}$ somos capaces de encontrar $\sigma \in H$ de forma que $\sigma(i) = j$.

**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 $G = \mathrm{Aut}_F(K)$.

$\Longrightarrow$) Si $f$ es irreducible y $\alpha, \beta \in K$ son raíces de $f$, podemos ($f = \mathrm{Irr}(\alpha, F)$) usar la Proposición de extensión, obteniendo $\sigma : F(\alpha) \to K$ 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.

$\Longleftarrow$) 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 $|G| = [K : F]$. □

[3] Hay una teoría desarrollada sobre esto, siempre se obtienen funciones simétricas en las raíces del polinomio. Ver el Ejercicio 3.1.2

[4] Sin término cuadrático.

**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 $degf = 1$, su grupo de Galois es la identidad, como único elemento de $S_1$.
2. Si $degf = 2$, la Proposición anterior nos dice que $2 = degf$ a de dividir al cardinal del grupo, por lo que su grupo de Galois debe ser isomorfo a $C_2$ (recordemos que $S_2 \cong C_2$).
3. Si $degf = 3$, la Proposición anterior nos dice que bien $G \cong A_3$ o $G \cong S_3$, como los únicos subgrupos transitivos de $S_3$. La Proposición 3.1 nos dice que tenemos el primer caso si $\Delta(f) \in F$ y el segundo si $\Delta(f) \notin F$.
4. Si $degf = 4$, la Proposición anterior nos dice que $G$ es isomorfo a un subgrupo transitivo de $S_4$.

### 3.1.1. Estructura de $S_n$

A partir del ejemplo anterior, conviene repasar ahora la estructura de $S_n$, para $n \leqslant 4$:

- Para $S_1$ tenemos que $S_1 = \{1\}$.
- Para $S_2$ tenemos que $S_2 = \{1, (1\ 2)\}$.

#### Estructura de $S_3$

Tenemos que $|S_3| = 3! = 6$, con:

$$S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

El Teorema de Lagrange nos dice que los subgrupos no triviales de $S_3$ tienen órdenes 2 o 3, por lo que los subgrupos no triviales de $S_3$ son aquellos generados por un único elemento, bien de orden 2 o bien de orden 3. A partir de este razonamiento y observando los elementos de $S_3$ vemos que todos los subgrupos de $S_3$ son los representados en el siguiente diagrama:

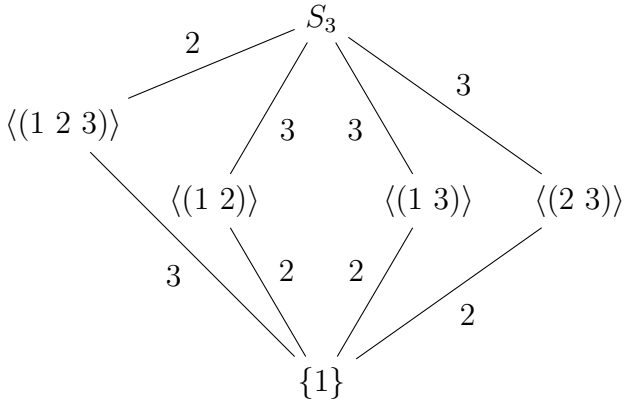



Figura 3.1: Subgrupos de $S_3$.

Donde tenemos que $A_3 = \langle(1\ 2\ 3)\rangle$, vemos que los subgrupos transitivos de $S_3$ son $S_3$ y $A_3$, por lo que estos son los únicos candidatos a ser grupo de Galois de un polinomio separable e irreducible de grado 3.

**Estructura de $S_4$**

Tenemos que $|S_4| = 4! = 24$, con:

$$S_4 = \left\{ \begin{array}{l} 1, (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), \\ (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 3\ 4), (1\ 3\ 2\ 4), (1\ 2\ 4\ 3), \\ (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \end{array} \right\}$$

El Teorema de Lagrange nos dice que los cardinales de los subgrupos de $S_4$ son divisores de $24 = 2^3 \cdot 3$:

$$Div(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}$$

Estudiamos ahora los subgrupos no triviales de $S_4$, estudiando cada divisor no trivial de 24:

**Subgrupos de orden 2.**

Como 2 es primo tenemos que los subgrupos de $S_4$ de orden 2 deben ser cíclicos, luego tenemos un subgrupo de orden 2 por cada elemento de orden 2 de $S_4$, todos ellos cíclicos, y estos son:

$$\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(1\ 4)\rangle, \langle(2\ 3)\rangle, \langle(2\ 4)\rangle, \langle(3\ 4)\rangle, \langle(1\ 2)(3\ 4)\rangle, \langle(1\ 3)(2\ 4)\rangle, \langle(1\ 4)(2\ 3)\rangle$$

Obtenemos así 9 subgrupos de orden 2, 6 de ellos generados por trasposiciones y 3 generados por el producto de dos trasposiciones disjuntas.

Vemos que ninguno de estos subgrupos es transitivo.

**Subgrupos de orden 3.**

Como 3 es primo, volvemos a tener tantos subgrupos de orden 3 de $S_4$ como elementos de orden 3 tiene $S_4$, por lo que estos son:

$$\langle(1\ 2\ 3)\rangle, \langle(1\ 2\ 4)\rangle, \langle(1\ 3\ 4)\rangle, \langle(2\ 3\ 4)\rangle$$

Obtenemos 4 subgrupos de orden 3 (observamos que los $3-$ciclos de $S_4$ que no aparecen como generadores de un subgrupo son inversos de un $3-$ciclo que aparece como generador de un subgrupo, obteniéndose el mismo subgrupo).

Vemos que ninguno es transitivo.

**Subgrupos de orden 4.**

Sabemos que si $H$ es un grupo de orden 4 entonces tiene que ser cíclico o isomorfo a $C_2 \oplus C_2$:

**Subgrupos de orden 4 cíclicos.** Estos tienen que estar generados por un elemento de orden 4, por lo que son:

$$\langle(1\ 2\ 3\ 4)\rangle, \langle(1\ 3\ 2\ 4)\rangle, \langle(1\ 3\ 4\ 2)\rangle$$

Obtenemos 3 subgrupos cíclicos, todos ellos transitivos.

**Subgrupos de orden 4 isomorfos a $C_2 \oplus C_2$.** Sabemos que tienen que ser de la forma $\{1, a, b, ab\}$ con $O(a) = 2 = O(b)$ y $ab = ba$. Los únicos que hay de esta forma en $S_4$ son:

- El grupo de Klein:

$$V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

que es normal y transitivo.

- Los generados por dos trasposiciones disjuntas, obteniendo:

$$\langle (1\ 2), (3\ 4)\rangle = \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$
$$\langle (1\ 3), (2\ 4)\rangle = \{1, (1\ 3), (2\ 4), (1\ 3)(2\ 4)\}$$
$$\langle (1\ 4), (2\ 3)\rangle = \{1, (1\ 4), (2\ 3), (1\ 4)(2\ 3)\}$$

ninguno de ellos es normal o transitivo.

Obtenemos así 7 subgrupos de orden 4, 4 de ellos transitivos.

**Subgrupos de orden 6.**

Si $H$ es un grupo de orden 6 entonces es cíclico o isomorfo a $S_3$, pero como en $S_4$ no hay elementos de orden 6 entonces los únicos subgrupos de $S_4$ que tienen orden 6 son isomorfos a $S_3$. $S_3$ es el grupo de permutaciones de un conjunto de 3 elementos $\{a, b, c\}$, por lo que subgrupos de $S_4$ de esta forma encontramos:

$$Stab(1),\ \text{el subgrupo de permutaciones de } \{2, 3, 4\}$$
$$Stab(2),\ \text{el subgrupo de permutaciones de } \{1, 3, 4\}$$
$$Stab(3),\ \text{el subgrupo de permutaciones de } \{1, 2, 4\}$$
$$Stab(4),\ \text{el subgrupo de permutaciones de } \{1, 2, 3\}$$

Ninguno de ellos es transitivo, puesto que todo elemento $\sigma \in Stab(i)$ verifica que $\sigma(i) = i$, para $i \in \{1, 2, 3, 4\}$.

**Subgrupos de orden 8.**

Como $|S_4| = 2^3 \cdot 3$, los subgrupos de orden $8 = 2^3$ son los $2-$subgrpos de Sylow de $S_4$. Si notamos por $n_2$ al número de $2-$subgrpos de Sylow de $S_4$, el Segundo Teorema de Sylow nos dice que:

$$\left.\begin{array}{c} n_2 \equiv 1 \mod 2 \\ n_2 \mid 3 \end{array}\right\} \iff n_2 \in \{1, 3\}$$

Por lo que hay uno o tres subgrupos de orden 8. Estos serán isomorfos a $C_8, C_4 \oplus C_2, C_2 \oplus C_2 \oplus C_2, Q_8$ o $D_4$. Puede probarse que $S_4$ no tiene subgrupos isomorfos a $C_8$ (no tiene elementos de orden 8), $C_4 \oplus C_2, C_2 \oplus C_2 \oplus C_2$ ni a $Q_8$, por lo que todos son isomorfos a $D_4$. Supuesto que $n_2 = 1$ tendríamos entonces que dicho subgrupo sería normal, pero puede probarse que esto lleva a una contradicción, por lo que $S_4$ tiene 3 subgrupos isomorfos a $D_4$. Uno de ellos es por ejemplo:

$$\langle (1\ 3), (1\ 2\ 3\ 4)\rangle$$

Todos ellos son transitivos.

**Subgrupos de orden 12.**

Sabemos que $A_4$ es un subgrpo de $S_4$ de orden 12, que es normal y transitivo.

Sea $H < S_4$ un subgrupo de orden 12, tenemos entonces que $(S_4 : H) = 2$, por lo que $H \lhd S_4$, y tenemos que $S_4/H \cong C_2$ abeliano, por lo que $H$ debe contener el subgrupo conmutador $[S_4, S_4] = A_4$, es decir, $A_4 < H$ con $|A_4| = 12 = |H|$, por lo que $H = A_4$.

De esta forma, $S_4$ solo tiene un único grupo de orden 12, que es $A_4$.

En resumen:

| Orden | Descripción | Transitivos | Total |
|---|---|---|---|
| 2 | Todos cíclicos, 6 generados por trasposiciones y 3 por dos trasposiciones disjuntas | No | 9 |
| 3 | Todos cíclicos | No | 4 |
| 4 | 3 cíclicos, 4 isomorfos a $C_2 \oplus C_2$ y uno de estos (Klein) normal | Los cíclicos y el normal | 7 |
| 6 | Todos isomorfos a $S_3$ | No | 4 |
| 8 | Todos isomorfos a $D_4$ | Sí | 3 |
| 12 | $A_4$ | Sí | 1 |

Tabla 3.1: Subgrupos de $S_4$.

Tenemos 28 subgrupos no triviales de $S_4$, que junto con $\{1\}$ y $S_4$ hacen un total de 30 subgrupos. Los subgrupos transitivos de $S_4$ son:

- Los tres subgrupos cíclicos de orden 4.
- El grupo de Klein.
- Los tres subgrupos isomorfos a $D_4$ de orden 8.
- $A_4$.
- $S_4$.

Una vez repasadas las estructuras de $S_n$, terminamos esta sección con varios ejemplos y ejercicios:

**Ejemplo.** Estudiando más a fondo el caso de tener $f \in F[x]$ un polinomio separable e irreducible de grado 4, sean $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ las raíces de $f$ en un cuerpo de descomposición $K$ de $f$, tomamos $G = \mathrm{Aut}_F(K)$ y 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 $g \in F[x]$, ya que si $\sigma \in G$ podemos descomponerla como producto de trasposiciones, y cada una de ellas vemos (hágase) que permutan los

elementos $\beta_i$, de donde tenemos que $g^\sigma = g \quad \forall \sigma \in G$, de donde los coeficientes de $g$ están en $K^G = F$. Este polinomio $g$ recibe el nombre resolvente cúbica de $f$, y en general si $f = x^4 + bx^3 + cx^2 + dx + e$, tras algunos cálculos se obtiene que:

$$g = x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2$$

Y además es fácil ver que las raíces de $g$, $\beta_1, \beta_2, \beta_3$ son todas distintas, ya que por ejemplo:

$$\beta_2 - \beta_1 = (\alpha_2 - \alpha_3)(\alpha_4 - \alpha_1)$$

Y como $f$ era separable tenemos que $\beta_2 - \beta_1 \neq 0$, por lo que $g$ seguirá siendo separable. Si calculamos las diferencias $\beta_3 - \beta_1$ y $\beta_3 - \beta_2$ veremos que tenemos que $\mathrm{Disc}(f) = \mathrm{Disc}(g)$.

En definitiva, tenemos que $E = F(\beta_1, \beta_2, \beta_3)$ es cuerpo de descomposición de $g$ (separable), por lo que $F \leqslant E$ es de Galois, lo que nos dice que $N = \mathrm{Aut}_E(K)$ es un subgrupo normal de $G$, así como que:

$$\mathrm{Aut}_F(E) \cong \frac{\mathrm{Aut}_F(K)}{\mathrm{Aut}_E(K)} = \frac{G}{N}$$

donde $\mathrm{Aut}_F(E)$ es el grupo de Galois de $g$.

Para ver quién es $N$, consideramos $S : \mathrm{Sim}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to \mathrm{Sim}(\beta_1, \beta_2, \beta_3)$ la aplicación dada por:

$$S(\sigma)(\alpha_i\alpha_j + \alpha_k\alpha_l) = \alpha_{\sigma(i)}\alpha_{\sigma(j)} + \alpha_{\sigma(k)}\alpha_{\sigma(l)}$$

que es un homomorfimo 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). Para calcular su núcleo, calculamos primero su cardinal: recordamos que:

$$|\mathrm{Sim}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)| = 4! = 24, \qquad |\mathrm{Sim}(\beta_1, \beta_2, \beta_3)| = 3! = 6$$

y como $S$ es sobreyectivo, el Primer Teorema de Isomorfía de grupos nos dice que:

$$\frac{24}{|\ker S|} = 6 \quad \Longrightarrow \quad |V| = 4$$

Si pensamos en los elementos[5] $\sigma \in G < S_4$ de forma que $S(\sigma) = id$, obtenemos que:

$$\ker S \supseteq \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

y como tenemos 4 elementos obtenemos que $\ker S = V$, el grupo de Klein.

Como $F \leqslant E$ es de Galois, tenemos como en la demostración del Teorema 2.7 que $\sigma(E) = E$ para cada $\sigma \in G$, lo que nos permite considerar nuevamente (como en la demostración de dicho Teorema) el epimorfismo $r : G \to \mathrm{Aut}_F(E)$ dado por:

$$r(\sigma) = \sigma\big|_E$$

[5]Aquí hacemos el abuso de pensar que $G < S_4$, ya que $S_4$ contiene un subgrupo isomorfo a $G$.

obtenemos así el diagrama conmutativo:

$$\begin{array}{ccccc} V & \hookrightarrow & Sim(\alpha_1,\alpha_2,\alpha_3,\alpha_4) & \xrightarrow{S} & Sim(\beta_1,\beta_2,\beta_3) \\ & & \uparrow & & \uparrow \\ N & \hookrightarrow & G & \xrightarrow[r]{} & Aut_F(E) \end{array}$$

Donde $V = \ker S$, $N = \ker r$ y las dos fechas verticales se identifican con el monomorfismo de grupos que ve el grupo de Galois de un polinomio dentro del grupo que permuta las raíces del polinomio.

Este diagrama es conmutativo, ya que si tomamos $\sigma \in G$ y lo vemos en $\mathrm{Aut}_F(E)$, tenemos entonces que este permutará (a través de la inyección canónica) las raíces $\beta_i$. Por otra parte, si vemos $\sigma$ sobre $\mathrm{Sim}(\alpha_1, \ldots, \alpha_4)$ a través de su inyección canónica, obtenemos que $\sigma$ sabe actuar sobre $\alpha_1, \ldots, \alpha_4$, permutándolas, y si observamos la definición de los $\beta_i$, por ejemplo, que:

$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$$

Vemos que obtenemos mediante $S$ una forma de permutar los $\beta_i$ mediante $\sigma$, que es la misma que hemos obtenido anteriormente por el otro camino.

De aquí deducimos que (pensando nuevamente que $G < S_n$):

$$N = V \cap G$$

Ya que como el diagrama es conmutativo tenemos que (si denotamos a las dos inclusiones distintas por $\iota$) $S \circ \iota = \iota \circ r$, por lo que los núcleos de ambas aplicaciones han de ser iguales. Si pensamos en calcular el núcleo de $\iota \circ r$, como $\iota$ es inyectiva obtenemos que:

$$\ker(\iota \circ r) = \ker r = N$$

Por lo que el núcleo de $S \circ \iota$ también será $N$, pero el núcleo de $S \circ \iota$ podemos calcularlo, como:

$$\ker(S \circ \iota) = \iota^{-1}(V) \cap G$$

donde usamos que $\iota$ es inyectiva, así como que $V$ es el núcleo de $S$. Si pensamos en identificar $G$ con un subgrupo de $\mathrm{Sim}(\alpha_1, \ldots, \alpha_4)$; obtenemos que $\ker(S \circ \iota) = V \cap G$, y tenemos así que:

$$N = \ker(\iota \circ r) = \ker(S \circ \iota) = V \cap G$$

**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:

$$\overline{f} = x^4 + x + 1 \in \mathbb{Z}_2[x]$$

$\overline{f}$ no tiene raíces y si no fuera irreducible, tendríamos entonces que sería el cuadrado 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 subgrupos transitivos de $S_4$ son:

- Los cíclicos de 4 elementos.
- El grupo de Klein.
- 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 polinomio $f$ su 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 $\mathrm{Disc}(f) = \mathrm{Disc}(g)$. Además, $g$ es una cúbica reducida, y teníamos una fórmula para calcular $\mathrm{Disc}(g)$, obteniendo que:

$$\mathrm{Disc}(f) = \mathrm{Disc}(g) = -4p^3 - 27q^2 = -4(-4)^3 - 27(-1)^2 = 229$$

Y tenemos que $\sqrt{229} \notin \mathbb{Q}$, ya que $x^2 - 229 \in \mathbb{Q}[x]$ 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 $G$ no puede ser el isomorfo a Klein ni $A_4$.

En estas condiciones, teníamos a partir del ejemplo anterior 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:

$$\mathrm{Aut}_E(K) \lhd G$$

Veamos qué aspecto tiene $\mathrm{Aut}_E(K)$, para reducir las opciones sobre $G$, de hecho:

$$\frac{G}{\mathrm{Aut}_E(K)} \cong \mathrm{Aut}_{\mathbb{Q}}(E)$$

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 $|\mathrm{Aut}_{\mathbb{Q}}(E)|$ es múltiplo de $degg = 3$, 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 $\mathrm{Aut}_E(K)$, que ha de ser $V$.

Respecto al tema anterior ganamos que no es necesario calcular de forma explícita cada uno de los automorfismos.

### 3.1.2. Ejercicios

**Ejercicio 3.1.2.** (Identidades de Cardano-Vieta)
Sea $f \in F[x]$ un polinomio mónico de grado $n$ con raíces $\alpha_1, \ldots, \alpha_n$ en un cuerpo de descomposición suyo (no suponemos que $f$ sea separable, así que entre las raíces puede haber repeticiones). Definamos

$$s_k = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \alpha_{i_1} \ldots \alpha_{i_k}$$

para $k \in \{1, \ldots, n\}$ se pide demostrar que:

$$f = x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n$$

**Ejercicio 3.1.3.** Sea $f \in F[x]$ un polinomio separable e irreducible de grado primo $p$. Demostrar que el grupo de Galois de $f$ sobre el cuerpo $F$ contiene un ciclo de orden $p$.
(**Pista:** usar el Teorema de Cauchy de existencia de $p-$subgrupos)

**Ejercicio 3.1.4.** Sea $f \in \mathbb{Q}[x]$ irreducible de grado primo $p$. Demostrar que, si $f$ tiene exactamente dos raíces complejas no reales, entonces el grupo de Galois de $f$ sobre $\mathbb{Q}$ es isomorfo a $S_p$.
(**Pista:** usar el Ejercicio anterior)

**Ejercicio 3.1.5.** Demostrar que el grupo de Galois de $f = x^5 - 4x - 1 \in \mathbb{Q}[x]$ es isomorfo a $S_3$.

**Ejercicio 3.1.6.** Sea $f \in \mathbb{R}[x]$ un polinomio de grado 3. Discutir el número de raíces reales de $f$ en función del signo de su discriminante.

Se hizo ya en el Ejercicio 3.1.1.

## 3.2. Extensiones ciclotómicas

Para $n \geqslant 1$, a lo largo de este capítulo nos interesará 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.* Para ver que $S < K^\times$, sean $\alpha, \beta \in S$, tenemos que:

$$\alpha^n - 1 = 0 = \beta^n - 1 \quad \Longrightarrow \quad \alpha^n = 1 = \beta^n$$

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, ya que $S$ tiene como mucho $n$ elementos. Además, su orden ha de dividir a $n$, pues todos los elementos tienen orden un divisor de $n$, ya que $\alpha^n = 1 \quad \forall \alpha \in S$. □

Además, si $x^n - 1 \in F[x]$ es separable y $K$ contiene un cuerpo de descomposición suyo, entonces $S$ contiene todas las $n$ raíces de $x^n - 1$ y todas estas son distintas, por lo que tenemos que $|S| = n$. Esto motiva a trabajar siempre en esta sección en un cuerpo $F$ en el que $x^n - 1 \in F[x]$ sea separable.

**Definición 3.3.** Si $x^n - 1 \in F[x]$ es separable y $K$ es su cuerpo de descomposición:

- Llamamos raíces $n-$ésimas de la unidad sobre $F$ a las raíces de $x^n - 1$, que se encuentran en $K$.

  Las raíces $n-$ésimas de la unidad forman un subgrupo cíclico de $K^\times$ de orden $n$, a cuyos generadores llamaremos raíces $n-$ésimas primitivas de la unidad.

  Así, un elemento $\alpha \in K$ es raíz $n-$ésima de la unidad sobre $F$ si y solo si tiene orden multiplicativo un divisor de $n$. En el caso de que el orden sea exactamente $n$ tenemos que $\alpha$ es una raíz $n-$ésima primitiva de la unidad sobre $F$.

- Decimos que $K$ es la $n-$ésima extensión ciclotómica de $F$.

  De esta forma, si $\zeta$ es una raíz $n-$ésima primitiva de la unidad sobre $F$, tenemos que $K = F(\zeta)$.

Muchas veces omitiremos el cuerpo $F$ (es decir, no especificaremos "sobre $F$" o "de $F$"), entendiendo que queda claro por el contexto.

Además, siempre que hagamos referencia a "raíces $n-$ésimas de la unidad", supondremos de forma implícita que $x^n - 1 \in F[x]$ es separable.

**Ejemplo.** Si tomamos $F = \mathbb{Q}$ (observamos que $x^n - 1 \in \mathbb{Q}[x]$ es separable), tenemos que las raíces $n-$ésimas de la unidad sobre $\mathbb{Q}$ son las raíces complejas $n-$ésimas de la unidad que ya conocíamos, se trata del grupo cíclico:

$$\left\{ e^{i\frac{2\pi k}{n}} : k \in \{0, 1, \ldots, n-1\} \right\} \cong \mathbb{Z}_n$$

Vemos que $e^{i\frac{2\pi}{n}}$ es una raíz $n-$ésima primitiva de la unidad sobre $\mathbb{Q}$, por lo que $\mathbb{Q}\left(e^{i\frac{2\pi}{n}}\right)$ es la $n-$ésima extensión ciclotómica de $\mathbb{Q}$.

**Ejemplo.** Sea $\zeta$ cualquier raíz $n-$ésima primitiva de la unidad sobre $F$, tenemos que el conjunto de raíces $n-$ésimas de la unidad viene dado por:

$$\left\{ \zeta^k : k \in \mathbb{Z}_n \right\}$$

Y en Álgebra I vimos que $|\mathcal{U}(\mathbb{Z}_n)| = \varphi(n)$, donde $\varphi$ es la función de Euler, por lo que el conjunto de raíces $n-$ésimas primitivas de la unidad sobre $F$ es:

$$\left\{ \zeta^k : k \in \mathcal{U}(\mathbb{Z}_n) \right\}$$

*Observación.* Si $\zeta$ es una raíz $n-$ésima primitiva de la unidad sobre $F$, hemos visto que la $n-$ésima extensión ciclotómica de $F$ es $F(\zeta)$, y vemos ahora que:

$$[F(\zeta) : F] \leqslant n - 1$$

ya que $x^n - 1 \in F[x]$ es un polinomio del que $\zeta$ es raíz, pero es divisible por $x - 1$ (ya que 1 es raíz de $x^n - 1$), por lo que $deg\, \mathrm{Irr}(\zeta, F) \leqslant n - 1$.

**Ejercicio 3.2.1.** Si $\zeta$ es una raíz $n-$ésima primitiva de la unidad sobre $F$ y $\sigma$ es un elemento del grupo de Galois de la $n-$ésima extensión ciclotómica de $F$, entonces $\sigma(\zeta)$ es una raíz $n-$ésima primitiva de la unidad.

Tenemos que $\sigma \in G$, donde $G = \mathrm{Aut}_F(F(\zeta))$. Si tomamos $f = x^n - 1 \in F[x]$, vemos que $G$ es el grupo de Galois de $f$, y en el capítulo anterior vimos que entonces $\sigma$ permuta las raíces de $f$, por lo que $\sigma(\zeta)$ es una raíz $n-$ésima de la unidad.

Por reducción al absurdo, supongamos que $\sigma(\zeta)$ no es una raíz $n-$ésima primitiva de la unidad, por lo que tiene que tener un orden multiplicativo menor estricto que $n$, luego existe $1 \leqslant d < n$ de forma que:

$$(\sigma(\zeta))^d = 1$$

Pero como $\sigma$ es un automorfismo tenemos entonces que:

$$\sigma\left(\zeta^d\right) = (\sigma(\zeta))^d = 1 = \sigma(1) \quad \Longrightarrow \quad \zeta^d = 1$$

donde hemos usado la inyectividad de $\sigma$, llegando a contradicción, pues el orden de $\zeta$ es $n$ al ser una raíz $n-$ésima primitiva. La contradicción viene de suponer que $\sigma(\zeta)$ no es una raíz $n-$ésima primitiva de la unidad.

**Proposición 3.4.** *Si $G$ es el grupo de Galois de la $n-$ésima extensión ciclotómica de $F$, entonces $G$ es isomorfo a un subgrupo de $\mathcal{U}(\mathbb{Z}_n)$.*
*Además, $G$ es isomorfo a $\mathcal{U}(\mathbb{Z}_n)$ si y solo si $G$ actúa transitivamente sobre las raíces $n-$ésimas primitivas de la unidad sobre $F$.*

*Demostración.* Sea $\zeta$ una raíz $n-$primitiva de la unidad sobre $F$, tenemos que:

$$G = \mathrm{Aut}_F(F(\zeta))$$

Hemos visto que las raíces $n-$ésimas primitivas de la unidad sobre $F$ son:

$$\{\zeta^k : k \in \mathcal{U}(\mathbb{Z}_n)\}$$

Observamos ahora que si tomamos $\sigma \in G$ tenemos por el Ejercicio anterior que $\sigma(\zeta)$ debe ser una raíz $n-$ésima primitiva de la unidad sobre $F$, por lo que ha de existir $k \in \mathcal{U}(\mathbb{Z}_n)$ de forma que $\sigma(\zeta) = \zeta^k$. Esto nos permite definir una aplicación $G \to \mathcal{U}(\mathbb{Z}_n)$ dada por:

$$\sigma \longmapsto k$$

donde $k$ queda unívocamente determinado por la condición:

$$\sigma(\zeta) = \zeta^k$$

Si $\sigma, \tau \in G$ de forma que $\tau(\zeta) = \zeta^l$, $\sigma(\zeta) = \zeta^k$ con $l, k \in \mathcal{U}(\mathbb{Z}_n)$, tenemos que:

$$\sigma\tau(\zeta) = \sigma(\zeta^l) = \sigma(\zeta)^l = \left(\zeta^k\right)^l = \zeta^{kl}$$

Por lo que la aplicación considerada es un homomorfismo de grupos, que además es inyectivo ya que cada $\sigma$ está determinado por su valor sobre $\zeta$, gracias a la Proposición de extensión. Tenemos pues que $G$ es isomorfo a la imagen de $G$ por dicho

monomorfismo, subgrupo de $\mathcal{U}(\mathbb{Z}_n)$.

Observamos que el homomorfismo enunciado será sobreyectivo si y solo si para cada $k \in \mathcal{U}(\mathbb{Z}_n)$ existe $\sigma \in G$ de forma que $\sigma(\zeta) = \zeta^k$, condición equivalente a que $G$ actúe transitivamente sobre las raíces $n-$ésimas primitivas de la unidad sobre $F$. □

**Definición 3.4.** Sea $F$ un cuerpo, definimos el $n-$ésimo polinomio ciclotómico como:

$$\phi_n = \prod_{k \in \mathcal{U}(\mathbb{Z}_n)} \left(x - \zeta^k\right)$$

donde $\zeta$ es una raíz $n-$ésima primitiva de la unidad sobre $F$. Observamos que $deg\phi_n = |\mathcal{U}(\mathbb{Z}_n)| = \varphi(n)$.

**Proposición 3.5.** *Se tiene que:*

$$x^n - 1 = \prod_{d \in Div(n)} \phi_d$$

*Demostración.* Consideramos como $R_n$ el conjunto de todas las raíces $n-$ésimas de la unidad, con lo que:

$$x^n - 1 = \prod_{\alpha \in R_n} (x - \alpha)$$

Si para cada $m \geqslant 1$ consideramos también $P_m$, el conjunto de las raíces $m-$ésimas primitivas de la unidad, obtenemos una partición de $R_n$:

$$R_n = \biguplus_{d \in Div(n)} P_d$$

$\supseteq$) Si $\alpha \in P_d$ para $d \in Div(n)$ tenemos entonces que el orden multiplicativo de $\alpha$ es exactamente $d$, divisor de $n$, luego $\alpha \in R_n$.

$\subseteq$) Si $\alpha \in R_n$ tenemos que el orden multiplicativo de $\alpha$ es cierto natural $k$, con $k \mid n$ y es claro que $\alpha \in P_k$.

Vemos así que cada $\alpha \in R_n$ está en un cierto $P_d$ con $d \in Div(n)$, por lo que el monomio $(x - \alpha)$ ha de estar en un único (puesto que la unión es disjunta) $\phi_d$, con lo que:

$$x^n - 1 = \prod_{\alpha \in R_n} (x - \alpha) = \prod_{d \in Div(n)} \phi_d$$

□

*Observación.* Si $F \leqslant K$ con $f, g \in F[x]$, $h \in K[x]$ con $f = hg$, entonces $h \in F[x]$.

*Demostración.* Si dividimos $f$ entre $g$ en $F[x]$ obtenemos $q, r \in F[x]$ con $degr < degg$ y $f = qg + r$. Sin embargo, como también tenemos que $q, r \in K[x]$ y el cociente y resto en el anillo de polinomios de un cuerpo son únicos, tiene que ser $r = 0$ y $q = h$, por lo que en particular $h \in F[x]$. □

**Proposición 3.6.** *Cada $\phi_n$ tiene coeficientes en el subcuerpo primo de $F$. Además, si $\mathrm{car}(F) = 0$, tenemos que $\phi_n \in \mathbb{Z}[x]$.*

*Demostración.* Si $\Pi$ es el subcuerpo primo de $F$, por inducción sobre $n$:

- Si $n = 1$, entonces $\phi_1 = x - 1$ y se tiene la Proposición.
- Si $n > 1$, tenemos por la Proposición anterior que:

$$x^n - 1 = \phi_n \cdot \prod_{\substack{d \in Div(n) \\ d<n}} \phi_d$$

  Por hipótesis de inducción, tenemos que cada $\phi_d$ tiene coeficientes en $\Pi$, por lo que el producto de la derecha también los tendrá. Si vemos ahora $\phi_n$ como cociente de $x^n - 1$ entre dicho producto, como estos dos tienen coeficientes en $\Pi$, $\phi_n$ también ha de tener sus coeficientes en $\Pi$, por la observación anterior.

Si $\text{car}(F) = 0$, procedemos nuevamente por inducción sobre $n$, tratando de probar además que cada $\phi_n$ es primitivo:

- Si $n = 1$, $\phi_1 = x - 1$, se tiene.
- Si $n > 1$, 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, obtenemos que $a\phi_n \in \mathbb{Z}[x]$ con todos sus coeficientes coprimos entre sí, luego $a\phi_n$ es primitivo. Si usamos nuevamente la Proposición anterior, tenemos que:

$$a(x^n - 1) = a\phi_n \prod_{\substack{d \in Div(n) \\ d<n}} \phi_d$$

  Por hipótesis de inducción tenemos que cada $\phi_d$ es primitivo, por lo que por el Lema de Gauss[6] tenemos que $a(x^n - 1)$ es primitivo, por ser igual al producto de la derecha. Luego $a = 1$ (en realidad sería $a \in \{\pm 1\}$, pero en este caso sirve tanto 1 como $-1$), lo que significa que $\phi_n$ tenía en realidad sus coeficientes en $\mathbb{Z}$. Vemos (para seguir la inducción) que $\phi_n$ es primitivo, ya que $\phi_n = a\phi_n$.

□

**Ejemplo.** En característica cero:

- $\phi_1 = x - 1$, ya que 1 es la única raíz de $x - 1$, por lo que es una 1-raíz primitiva de 1.
- $\phi_2 = x + 1$, ya que $\{\pm 1\}$ es el conjunto de raíces de $x^2 - 1$, y $-1$ es la única con orden multiplicativo dos.
- $\phi_3 = x^2 + x + 1$, ya que $\{1, w, w^2\}$ es el conjunto de las raíces cúbicas de la unidad, y tanto $w$ como $w^2$ son generadores, por lo que $\phi_3$ es el cociente tras dividir $x^3 - 1$ entre $x - 1$.
- $\phi_4 = x^2 + 1$, ya que $\{\pm 1, \pm i\}$ es el conjunto de las raíces de $x^4 - 1$ y $i, -i$ son las dos raíces cuárticas primitivas de la unidad.

[6] Visto en Álgebra I, el producto de polinomios primitivo es primitivo.

Para $\phi_6$ usamos la fórmula vista en la Proposición 3.5:

$$x^6 - 1 = \prod_{d \in Div(6)} \phi_d = \phi_1\phi_2\phi_3\phi_6 \quad \Longrightarrow \quad \phi_6 = \frac{x^6-1}{\phi_1\phi_2\phi_3} = x^2 - x + 1$$

Nos ahorramos así tener que calcular las raíces sextas primitivas de la unidad complejas y realizar la multiplicación de los monomios, pero a cambio tenemos que recordar la fórmula y realizar varias divisones de polinomios.

**Ejercicio 3.2.2.** Calcular en característica cero $\phi_8$.

Si aplicamos la fórmula de la Proposición 3.5, tenemos que:

$$\phi_8 = \frac{x^8-1}{\prod_{\substack{d \in Div(8) \\ d<8}} \phi_d} = \frac{x^8-1}{\phi_1\phi_2\phi_4}$$

y sabemos que $\phi_1 = x - 1$, $\phi_2 = x + 1$ y $\phi_4 = x^2 + 1$, por lo que:

$$\phi_1\phi_2\phi_4 = (x-1)(x+1)(x^2+1) = (x^2-1)(x^2+1) = x^4 - 1$$

vemos que:

$$x^8 - 1 = (x^4-1)(x^4+1)$$

por lo que $\phi_8 = x^4 + 1$.

**Teorema 3.7.** *Cada polinomio ciclotómico $\phi_n \in \mathbb{Z}[x]$ es irreducible.*

*Demostración.* Sea $f \in \mathbb{Z}[x]$ un factor irreducible de $\phi_n$, tomamos $\zeta$ cualquier raíz compleja de $f$ en la $n-$ésima extensión ciclotómica. Veamos que si $p$ es un primo que no divide a $n$ entonces $\zeta^p$ es también raíz de $f$. Por reducción al absurdo, si $\zeta^p$ no es raíz de $f$ entonces debe ser raíz de cierto polinomio $g \in \mathbb{Z}[x]$ con:

$$\phi_n = fg \qquad f, g \in \mathbb{Z}[x]$$

Por lo 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 $f \mid h$, y como $f$ además es primitivo, tenemos que $f \mid h$ en $\mathbb{Z}[x]$. Reducimos módulo $p$, obteniendo:

$$\overline{\phi_n} = \overline{f}\,\overline{g}$$

y que:

$$\overline{h} = \overline{g(x^p)} \overset{(*)}{=} \overline{g(x)}^p = \overline{g}^p$$

donde en $(*)$ usamos que como $(a+b)^p = a^p + b^p$ en un cuerpo de característica $p$, entonces si $g = \sum a_i x^i$ tenemos entonces que (usando que $a^p = a$ para $a \in \mathbb{F}_p$):

$$\overline{g(x)}^p = \left(\sum a_i x^i\right)^p = \sum (a_i x^i)^p = \sum a_i^p (x^i)^p = \sum a_i (x^i)^p = \overline{g(x^p)}$$

Como $\overline{f}$ divide a $\overline{h} = \overline{g}^p$, tenemos entonces que $\overline{f}$ y $\overline{g}$ han de tener un factor común en $\mathbb{F}_p[x]$, cierto polinomio $d \in \mathbb{F}_p[x]$, luego $\overline{x^n - 1} = x^n - 1 \in \mathbb{F}_p[x]$ tiene a $d^2$

como factor en el anillo de polinomios de su cuerpo de descomposición, de donde $x^n - 1 \in \mathbb{F}_p[x]$ tiene alguna raíz múltiple. Pero esto no es posible, ya que como $p$ no divide a $n$ tenemos que el polinomio derivado de $x^n - 1$ es $nx^{n-1} \neq 0$, y este no comparte raíces con $x^n - 1$, luego es separable en $\mathbb{F}_p[x]$. Hemos llegado a una contradicción, por lo que por cada primo $p$ que no divide a $n$ tenemos que $\zeta^p$ es raíz de $f$.

Si tomamos ahora $\zeta$ una raíz de $f$, como $f$ dividía a $\phi_n$ vemos que $\zeta$ es una raíz $n-$ésima primitiva de la unidad. Sea $\eta$ cualquier raíz $n-$ésima primitiva de la unidad, existe $k \in \mathbb{Z}_n$ con $\mathrm{mcd}(n,k) = 1$ (ya que $\eta$ es raíz primitiva de la unidad) de forma que $\eta = \zeta^k$, y si descomponemos $k$ como producto de primos:

$$k = p_1 p_2 \dots p_n$$

vemos que ninguno de estos primos puede dividir a $n$, ya que $\mathrm{mcd}(n,k) = 1$. Como $\zeta$ es raíz de $f$ y $p_1$ es un primo que no divide a $n$, tenemos que $\zeta^{p_1}$ es también una raíz de $f$, y aplicando de nuevo que $p_2$ es un primo que no divide a $n$, vemos que $(\zeta^{p_1})^{p_2} = \zeta^{p_1 p_2}$ es una raíz de $f$. En una cantidad finita de pasos obtenemos que $\zeta^{p_1 p_2 \dots p_n} = \zeta^k = \eta$ es una raíz de $f$, por lo que acabamos de ver que cada raíz $n-$ésima primitiva de la unidad es también raíz de $f$, en caso de que $f$ tenga alguna raíz. De aquí vemos que ha de ser $f = \phi_n$, por lo que $\phi_n$ es irreducible, para cada $n \geqslant 1$. □

**Corolario 3.7.1.** *El grupo de Galois de la $n-$ésima extensión ciclotómica sobre $\mathbb{Q}$ es isomorfo a $\mathcal{U}(\mathbb{Z}_n)$, por lo que:*

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$$

*donde $\zeta$ es una raíz $n-$ésima primitiva de la unidad sobre $\mathbb{Q}$.*

*Demostración.* Sea $\zeta$ una raíz $n-$ésima primitiva de la unidad, tenemos que el grupo de Galois de la $n-$ésima extensión ciclotómica sobre $\mathbb{Q}$ es:

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) = \mathrm{Aut}(\mathbb{Q}(\zeta))$$

a partir del Teorema anterior vemos que $\phi_n = \mathrm{Irr}(\zeta, \mathbb{Q})$, por lo que:

$$|\operatorname{Aut}(\mathbb{Q}(\zeta))| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \phi_n = \varphi(n)$$

Y usando la Proposición 3.4 vemos que $\mathrm{Aut}(\mathbb{Q}(\zeta))$ debe ser isomorfo a $\mathcal{U}(\mathbb{Z}_n)$. □

Vemos además por la Proposición 3.4 que el grupo de Galois de la $n-$ésima extensión ciclotómica sobre $\mathbb{Q}$ actúa transitivamente sobre las raíes $n-$ésimas primitivas de la unidad sobre $\mathbb{Q}$, es decir, sobre las raíces de $\phi_n$.

**Ejemplo.** Para $n = 16$, tenemos:

$$\deg \phi_n = \varphi(16) = 8$$

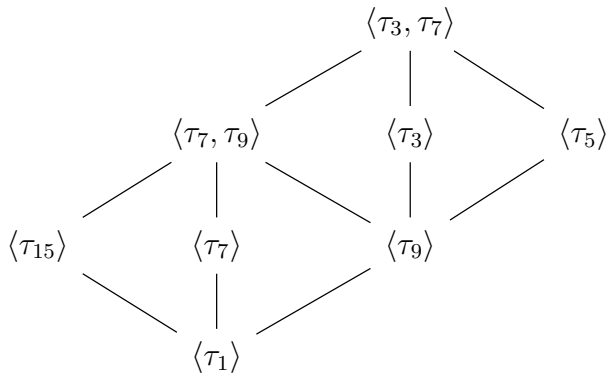
Si $\zeta \in \mathbb{C}$ es una raíz decimosexta primitiva de la unidad tenemos que la decimosexta extensión ciclotómica de $\mathbb{Q}$ es $K = \mathbb{Q}(\zeta)$, con:

$$\mathrm{Aut}(K) \cong \mathcal{U}(\mathbb{Z}_{16})$$

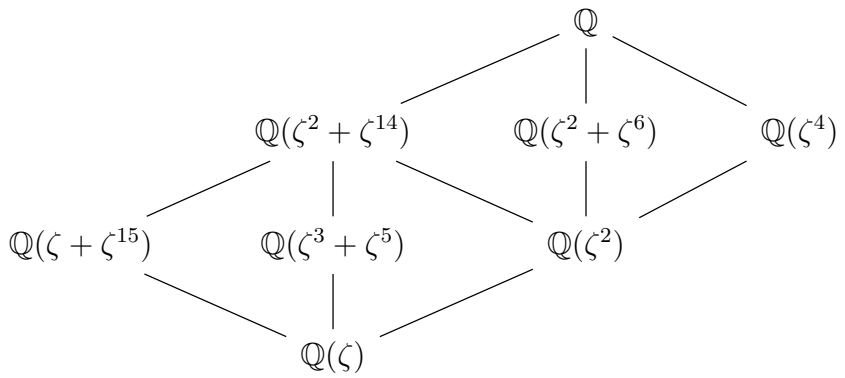
Por el último Corolario vemos que:

$$\mathrm{Aut}(K) = \{\tau_j : j \in \mathcal{U}(\mathbb{Z}_{16})\}$$

donde cada automorfismo viene determinado por $\tau_j(\zeta) = \zeta^j$. Se ve que $\mathrm{Aut}(K) = \langle \tau_3, \tau_7 \rangle$, y se obtiene que el conjunto de subgrupos de $\mathrm{Aut}(K)$ es:




Y por la conexión de Galois obtenemos que los subcuerpos de $\mathbb{Q}(\zeta)$ son:




## 3.3. Construcciones con regla y compás II

Con objetivo de resolver el problema de cuándo es construible un polígono regular mediante regla y compás, complementaremos el Teorema 1.16. Para ello, dado un conjnto $S$ de números complejos en el que $\{0, 1\} \subseteq S$, consideraremos $F = \mathbb{Q}(S \cup \overline{S})$.

**Teorema 3.8.** *Sea $z \in \mathbb{C}$, tenemos que $z$ es constructible a partir de $S$ si, y solo si, existe una extensión de Galois $F \leqslant K$ tal que $z \in K$ y $[K : F] = 2^k$, para $k \geqslant 1$.*

*Demostración.* Por doble implicación:

$\Longrightarrow$) Sé que existe una torre de subcuerpos de $\mathbb{C}$:

$$F = F_0 \leqslant F_1 \leqslant \ldots \leqslant F_s$$

tales que $F_{i+1} = F(\alpha_{\alpha_i+1})$, con $\alpha_{i+1}^2 \in F_i$, para todo $i \in \{0, \ldots, s-1\}$; 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:

$$\mathrm{Aut}_F(E) = \{\sigma_0, \ldots, \sigma_t\}$$

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 $j \in \{0, \ldots, t\}$, por lo que $\alpha_{s+j} \in K$.

Tenemos que:

$$K = E(\alpha_s, \alpha_{s+1}, \ldots, \alpha_{s+t})$$

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 $x^2 - \alpha_j(a_s)$), 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.

$\Longleftarrow$) Tomamos $z \in K$ con $F \leqslant K$ de Galois y $[K : F]$ una potencia de 2. Tenemos por tanto que $\mathrm{Aut}_F(K)$ es un $2-$grupo, luego es resoluble[7]. Podemos por tanto tomar una serie de composición suya, obteniendo:

$$\mathrm{Aut}_F(K) = G_0 \geqslant G_1 \geqslant \ldots \geqslant G_n = \{id\}$$

con factores de composición 2. La conexión de Galois nos transforma esta cadena en una cadena de extensiones de subcuerpos cuadráticas:

$$F = K_0 \leqslant K_1 \leqslant \ldots \leqslant K_n = K \tag{3.1}$$

con $[K_{i+1} : K_i] = 2$, para cada $i \in \{0, \ldots, n-1\}$, por lo que:

$$K_{i+1} = K_i(\beta_i) \qquad \text{con} \qquad \beta_i = \frac{-b_i \pm \sqrt{b_i^2 - 4c_i}}{2}$$

en el caso de que $\mathrm{Irr}(\beta_i, K_i) = x^2 + b_i x + c_i$. 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 $S$.

[7]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 3.2: Qué polígonos regulares son constructibles.

□

Sabemos que el heptágono no es constructible, puesto que $\mathrm{Irr}(\sqrt[7]{algo}, \mathbb{Q})$ 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 sobre $\mathbb{Q}$ es constructible. Por tanto, hemos de ver que $\zeta$ es constructible (como raíz $n-$ésima primitiva de la unidad) si y solo si $\varphi(n)$ es una potencia de 2.

$\Longrightarrow$) Si $\zeta$ es constructible, existe una extensión de Galois $\mathbb{Q} \leqslant K$ de grado 2 que contiene a $\zeta$, luego ha de contener a la $n-$ésima extensión ciclotómica de $\mathbb{Q}$: $\mathbb{Q} \leqslant \mathbb{Q}(\zeta) \leqslant K$, de donde por el Lema de la Torre ha de ser $\varphi(n)$ una potencia de 2.

$\Longleftarrow$) Si $\varphi(n)$ es una potencia de 2, como $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$, tenemos entonces que $\mathbb{Q} \leqslant \mathbb{Q}(\zeta)$ es una extensión de Galois de grado una potencia de 2, por lo que $z$ es constructible.

□

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

Nos interesará ahora el estudio del cuerpo de descomposición y del grupo de Galois de polinomios separables de la forma $x^n - a$.

**Teorema 3.9.** *Si $x^n - a \in F[x]$ es separable y $K$ es su cuerpo de descomposición, entonces $K$ contiene una raíz $n-$ésima primitiva de la unidad $\zeta$ y $K = F(\zeta, r)$ para cualquier raíz $r \in K$ de $x^n - a$.*
*Además, el grupo de Galois de la extensión $F(\zeta) \leqslant K$ es cíclico de orden un divisor de $n$.*

*Demostración.* En el caso $a = 0$, tenemos que $x^n$ es separable si y solo si $n = 1$, 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 $n$ no puede ser múltiplo de $\text{car}(F)$, para que $x^n - a$ sea separable. Sea $R$ el conjunto de las raíces en $K$ de $x^n - a$, tenemos que $|R| = n$, puesto que $x^n - a$ es separable. Si tomamos $r, s \in R$, tenemos que $r^{-1}s \in K$ es una raíz $n-$ésima de la unidad:

$$(r^{-1}s)^n = r^{-n}s^n = a^{-1}a = 1$$

Fijado $r \in R$, entonces el conjunto $\{r^{-1}s : s \in R\}$ contiene $n$ raíces $n-$ésimas de la unidad distintas, por lo que en dicho conjunto las tenemos todas, luego ha de contener al menos una raíz $n-$ésima primitiva de la unidad, llamémosla $\zeta \in K$ .

Para la segunda afirmación, fijado $r \in R$, es claro ahora que:

$$F(\zeta, r) \leqslant K$$

Para la otra inclusión, si $r = r_1, \ldots, r_n$ son las raíces de $x^n - a$ tenemos entonces que $K = F(r_1, \ldots, r_n)$. Hemos visto que:

$$\{\zeta^k : 0 \leqslant k \leqslant n-1\} = \{r^{-1}s : s \in R\} \quad \Longrightarrow \quad \{r\zeta^k : 0 \leqslant k \leqslant n-1\} = R = \{r_1, \ldots, r_n\}$$

Por lo que ahora tenemos que:

$$K = F(r_1, \ldots, r_n) \leqslant F(\zeta, r)$$

Para ver que el grupo de Galois de la extensión $F(\zeta) \leqslant K$ es cíclico, vamos a representar el grupo de manera sencilla. Para ello, tomamos $\sigma \in \text{Aut}_{F(\zeta)}(K)$ y vemos que $\sigma$ toma una raíz de $x^n - a$ y la lleva en otra, siendo el conjunto de todas las raíces:

$$R = \{r, r\zeta, \ldots, r\zeta^{n-1}\}$$

Por lo que tendremos $\sigma(r) = r\zeta^j$ para cierto $j \in \mathbb{Z}_n$. Si tuviéramos que $\sigma(r) = r\zeta^{j'}$ para $j' \in \mathbb{Z}_n$, tendríamos entonces que $\zeta^j = \zeta^{j'}$, pero como $\zeta$ es una raíz $n-$ésima primitiva de la unidad, tenemos que $j = j'$. Esto nos permite definir una aplicación $j : \text{Aut}_{F(\zeta)}(K) \to \mathbb{Z}_n$ de forma que $\sigma \mapsto j$ con $\sigma(r) = r\zeta^j$.
Veamos que $j$ es un homomorfismo de grupos, considerando $\mathbb{Z}_n$ como grupo aditivo, ya que si $\sigma, \tau \in \text{Aut}_{F(\zeta)}(K)$ y consideramos $j(\sigma\tau) \in \mathbb{Z}_n$ dado por la condición:

$$(\sigma\tau)(r) = r\zeta^{j(\sigma\tau)}$$

Tenemos entonces que:

$$r\zeta^{j(\sigma\tau)} = (\sigma\tau)(r) = \sigma(\tau(r)) = \sigma(r\zeta^{j(\tau)}) = \zeta^{j(\tau)}\sigma(r) = \zeta^{j(\tau)}r\zeta^{j(\sigma)} = r\zeta^{j(\sigma)+j(\tau)}$$

de donde $j(\sigma\tau) = j(\sigma) + j(\tau)$, por lo que $j$ es un homomorfismo de grupos. Vemos además que $j$ es inyectivo, pues si $\sigma \in \mathrm{Aut}_{F(\zeta)}(K)$ con $j(\sigma) = 0$ tenemos entonces que $\sigma(r) = r\zeta^0 = r$, por lo que $\sigma = id$.

En definitiva, tenemos que $\mathrm{Aut}_{F(\zeta)}(K)$ es isomorfo a su imagen por $j$, por lo que es isomorfo a un subgrupo de $\mathbb{Z}_n$, que ha de ser cíclico como subgrupo de un grupo cíclico. El Teorema de Lagrange nos dice que el orden debe ser un divisor de $n$. □

**Corolario 3.9.1.** *Sea $x^n - a \in F(\zeta)[x]$, es irreducible si y solo si $[K : F(\zeta)] = n$, donde $K$ es el cuerpo de descomposición de $x^n - a$.*

*Demostración.* Si $r \in K$ es una raíz de $x^n - a$, tenemos que $K = F(\zeta, r)$ a partir del Teorema anterior. Por doble implicación:

$\Longrightarrow$) Si $x^n - a \in F(\zeta)[x]$ es irreducible tenemos entonces que $\mathrm{Irr}(r, F(\zeta)) = x^n - a$, por lo que $[K : F(\zeta)] = n$.

$\Longleftarrow$) Si $[K : F(\zeta)] = n$, vemos que $x^n - a \in F(\zeta)[x]$ es un polinomio mónico de grado $n$ del que $r$ es raíz, por lo que tiene que ser $\mathrm{Irr}(r, F(\zeta)) = x^n - a$, de donde $x^n - a$ es irreducible sobre $F(\zeta)$.

□

**Definición 3.5** (Extensión cíclica)**.** Una extensión $F \leqslant K$ se dice cíclica si es de Galois y su grupo de Galois $\mathrm{Aut}_F(K)$ es cíclico.

**Ejemplo.** Como ejemplos de extensiones cíclicas que ya conocemos:

- Toda extensión de cuerpos finitos es cíclica, ya que si $F \leqslant K$ es una extensión con $K$ finito entonces $F \leqslant K$ es de Galois y existen $p$ primo y $n \geqslant 1$ de forma que:
$$\mathbb{F}_p \leqslant F \leqslant K = \mathbb{F}_{p^n}$$
habíamos visto ya que $\mathrm{Aut}(K)$ es cíclico de orden $n$, por lo que $\mathrm{Aut}_F(K)$ será también un grupo cíclico, como subgrupo de un grupo cíclico.
- Si $F$ contiene una raíz $n-$ésima primitiva de la unidad y $x^n - a \in F[x]$ es separable, si tomamos $K$ su cuerpo de descomposición tenemos que $F \leqslant K$ es cíclica; ya que $F \leqslant K$ es de Galois al ser un cuerpo de descomposición de un polinomio separable y en el Teorema anterior hemos visto que el grupo de Galois de la extensión $F = F(\zeta) \leqslant K$ es cíclico.

Nuestro siguiente objetivo es ver cómo las extensiones cíclicas son, bajo ciertas hipótesis, cuerpos de descomposición de polinomios de la forma $x^n - a$. Para ello, primero será necesario ver un Lema con un resultado muy sorprendente:

**Lema 3.10** (de independencia de Dedekind)**.** *Sean $\sigma_1, \ldots, \sigma_n : F \to E$ homomorfismos de cuerpos distintos, tenemos entonces que $\sigma_1, \ldots, \sigma_n$ son linealmente independientes. Es decir, si $\lambda_1, \ldots, \lambda_n \in E$ verifican que:*

$$\lambda_1\sigma_1(x) + \ldots + \lambda_n\sigma_n(x) = 0 \quad \forall x \in F \qquad \Longrightarrow \qquad \lambda_1 = \ldots = \lambda_n = 0$$

*Demostración.* Para $n = 1$ es cierto. Supuesto que $n > 1$, razonamos por reducción al absurdo. Para ello, tenemos que existe al menos una lista $\lambda_1, \ldots, \lambda_n \in E$ de elementos no todos nulos de forma que:

$$\lambda_1\sigma_1(x) + \ldots + \lambda_n\sigma_n(x) = 0 \qquad \forall x \in F \tag{3.2}$$

de entre todas aquellas listas que verifican esta afirmación tomamos aquella con la mínima cantidad de elementos no nulos, $m > 0$. Vemos que $m \geqslant 2$, pues si $m = 1$ llegamos a que la lista no contenía elementos no nulos. Podemos suponer sin pérdida de generalidad que los $m$ elementos no nulos son los $m$ primeros. Como los homomorfismos son todos distintos entre sí, ha de existir $y \in F$ de forma que $\sigma_1(y) - \sigma_m(y) \neq 0$, y por otra parte tenemos que:

$$\lambda_1\sigma_1(yx) + \ldots + \lambda_n\sigma_n(yx) = 0 \qquad \forall x \in F$$

Restándole a esta última igualdad la igualdad (3.2) multiplicada por $\sigma_m(y)$, obtenemos que:

$$\lambda_1(\sigma_1(y) - \sigma_m(y))\sigma_1(x) + \ldots + \lambda_{m-1}(\sigma_{m-1}(y) - \sigma_m(y))\sigma_{m-1}(x) = 0 \qquad \forall x \in F$$

Por lo que obtenemos una lista de elementos de $E$:

$$\lambda_1(\sigma_1(y) - \sigma_m(y)), \ldots, \lambda_{m-1}(\sigma_{m-1}(y) - \sigma_m(y)), 0, \ldots, 0$$

que verifican la condición (3.2) y con $m-1$ elementos no nulos, hemos llegado a una contradicción, pues la lista $\lambda_1, \ldots, \lambda_n$ verificaba (3.2) y era la que tenía una menor cantidad de elementos no nulos. □

**Teorema 3.11.** *Sea $F \leqslant K$ extensión cíclica tal que $n = [K : F]$ no es múltiplo de $\mathrm{car}(F)$. 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.* Suponemos que $\zeta$ es una raíz $n-$ésima primitiva de la unidad con $\zeta \in F$. Como $F \leqslant K$ es cíclica, el grupo de Galois de la extensión debe ser cíclico de grado $n$, por lo que tendrá un generador $\sigma \in \mathrm{Aut}_F(K)$ de orden $n$. El Lema de independencia de Dedekind para los escalares $1, \zeta, \ldots, \zeta^{n-1}$ nos dice que ha de existir $r \in K$ de forma que:

$$\beta := r + \zeta\sigma(r) + \ldots + \zeta^{n-1}\sigma^{n-1}(r) \neq 0$$

Tendremos entonces que:

$$\begin{aligned}\zeta\sigma(\beta) &= \zeta\sigma(r) + \zeta^2\sigma^2(r) + \ldots + \zeta^{n-1}\sigma^{n-1}(r) + \zeta^n\sigma^n(r) \\ &= \zeta\sigma(r) + \zeta^2\sigma^2(r) + \ldots + \zeta^{n-1}\sigma^{n-1}(r) + r = \beta\end{aligned}$$

Por lo que:

$$\beta^n = \zeta^n\sigma(\beta)^n = \sigma(\beta)^n = \sigma(\beta^n)$$

como $\sigma$ genera todo $\mathrm{Aut}_F(K)$, tenemos que $a := \beta^n \in K^{\langle\sigma\rangle} = K^{\mathrm{Aut}_F(K)} = F$. Como $\zeta$ es una raíz $n-$ésima de la unidad, tenemos que:

$$\beta, \zeta\beta, \ldots, \zeta^{n-1}\beta$$

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 $\beta$ es raíz de $x^n - a$, tenemos que $[F(\beta) : F] \leqslant n$, y para obtener la igualdad observamos que:

$$\sigma^k(\beta) = \zeta^{-k}\beta \qquad \forall k \in \mathbb{Z}_n$$

Por lo que la acción de $\mathrm{Aut}_F(K)$ sobre las raíces de $x^n - a$ es transitiva, por lo que $x^n - a$ es irreducible, luego $\mathrm{Irr}(\beta, F) = x^n - a$, de donde $[F(\beta) : F] = n$. Tenemos en definitiva que $F(\beta) = K$.

La última afirmación es clara, pues si $\alpha$ es raíz de $x^n - a$, entonces $\alpha = \zeta^k\beta$ para $k \in \mathbb{Z}_n$, obteniendo que $K = F(\alpha)$. □

**Proposición 3.12.** *El grupo de Galois de un polinomio separable de la forma $x^n - a \in F[x]$ es resoluble.*

*Demostración.* Sea $K$ el cuerpo de descommposición de $x^n - a$, sabemos que existe $\zeta \in K$ una raíz $n-$ésima primitiva de la unidad, por lo que tenemos la torre de cuerpos:

$$F \leqslant F(\zeta) \leqslant K$$

con $F \leqslant K$ de Galois por ser cuerpo de descommposición de un polinomio separable y $F \leqslant F(\zeta)$ de Galois por ser una extensión ciclotómica. Por ser $F \leqslant F(\zeta)$ de Galois, tenemos que:

$$\mathrm{Aut}_{F(\zeta)}(K) \lhd \mathrm{Aut}_F(K)$$

y que además:

$$\mathrm{Aut}_F(F(\zeta)) \cong \frac{\mathrm{Aut}_F(K)}{\mathrm{Aut}_{F(\zeta)}(K)}$$

Tenemos así la serie normal:

$$\{id_F\} \lhd \mathrm{Aut}_{F(\zeta)}(K) \lhd \mathrm{Aut}_F(K)$$

con el primer factor cíclico, puesto que $\mathrm{Aut}_{F(\zeta)}(K)$ es cíclico y con el segundo abeliano, por ser isomorfo a $\mathrm{Aut}_F(F(\zeta))$, que es abeliano por ser isomorfo a un subgrupo de las unidades de $\mathbb{Z}_n$. □

**Ejemplo.** Si consideramos $x^8 - 3 \in \mathbb{Q}[x]$, si $\zeta$ es una raíz octava primitiva de la unidad y consideramos $K$ el cuerpo de descomposición de $x^8 - 3 \in \mathbb{Q}(\zeta)[x]$, tenemos que el grupo de Galois de la extensión $\mathbb{Q}(\zeta) \leqslant K$ es cíclico. Sabemos además por el Teorema 3.9 que $K = \mathbb{Q}\left(\sqrt[8]{3}, \zeta\right)$. Podemos calcular $\zeta$ 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 $\mathbb{Q} \leqslant \mathbb{Q}(\zeta)$ es de grado 4. Si consideramos ahora $\zeta + \overline{\zeta} \in \mathbb{Q}(\zeta)$:

$$\zeta + \overline{\zeta} = 2\mathrm{Re}(\zeta) = \sqrt{2} \in \mathbb{Q}(\zeta)$$

De donde $\mathbb{Q}\left(\sqrt{2}\right) \leqslant \mathbb{Q}(\zeta)$, por lo que $\mathbb{Q}\left(i,\sqrt{2}\right) = \mathbb{Q}(\zeta)$, al tener claramente $\mathbb{Q}\left(i,\sqrt{2}\right) \leqslant \mathbb{Q}(\zeta)$ y $\left[\mathbb{Q}\left(i,\sqrt{2}\right):\mathbb{Q}\right] = 4$.

Calculamos el grado de la extensión $[K:\mathbb{Q}]$, para saber el cardinal de $\mathrm{Aut}_F(K)$. Por el Lema de la Torre:

$$[K:\mathbb{Q}] = \left[\mathbb{Q}\left(\sqrt[8]{3},\sqrt{2},i\right):\mathbb{Q}\left(\sqrt[8]{3},\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2},\sqrt[8]{3}\right):\mathbb{Q}\left(\sqrt[8]{3}\right)\right]\left[\mathbb{Q}\left(\sqrt[8]{3}\right):\mathbb{Q}\right]$$

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 $\sqrt{2} \notin \mathbb{Q}\left(\sqrt[8]{3}\right)$.
Consideramos:

$$\mathbb{Q} \overset{2}{\leqslant} \mathbb{Q}\left(\sqrt{3}\right) \overset{\leqslant 2}{\leqslant} \mathbb{Q}\left(\sqrt[4]{3}\right) \overset{\leqslant 2}{\leqslant} \mathbb{Q}\left(\sqrt[8]{3}\right)$$

Y como $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt[8]{3}\right)$ es de grado 8, tienen que ser todas estas de grado 2. Veamos:

- $\sqrt{2} \notin \mathbb{Q}\left(\sqrt{3}\right)$, 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.
- $\sqrt{2} \notin \mathbb{Q}\left(\sqrt[4]{3}\right)$, usando que una $\mathbb{Q}\left(\sqrt{3}\right)$ −base es $\left\{1, \sqrt[4]{3}\right\}$, si $\sqrt{2} \in \mathbb{Q}\left(\sqrt[4]{3}\right)$ tendríamos entonces que $\exists a, b \in \mathbb{Q}\left(\sqrt{3}\right)$ de manera que:

  $$\sqrt{2} = a + b\sqrt[4]{3}$$

  Elevando al cuadrado:

  $$2 = a^2 + 2ab\sqrt[4]{3} + b^2\sqrt{3} \Longrightarrow \begin{cases} 2 = a^2 + b^2\sqrt{3} \\ 0 = 2ab \end{cases}$$

  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 $\mathbb{Q}\left(\sqrt{3}\right)$, por lo que igualdando coordenadas:

    $$0 = x^2 + 3y^2 \Longrightarrow x = 0 = y$$

    Luego $b = 0 \Longrightarrow 2 = 0$ <u>contradicción</u>, que viene de suponer que teníamos $\sqrt{2} \in \mathbb{Q}\left(\sqrt[4]{3}\right)$.

- Intentamos ver ahora que $\sqrt{2} \notin \mathbb{Q}\left(\sqrt[8]{3}\right)$. Por reducción al absurdo, si $\sqrt{2} \in \mathbb{Q}\left(\sqrt[8]{3}\right)$, tenemos que $\left\{1, \sqrt[8]{3}\right\}$ es una $\mathbb{Q}\left(\sqrt[4]{3}\right)$ −base, por lo que existirían $c, d \in \mathbb{Q}\left(\sqrt[4]{3}\right)$ 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 $d$:

$$d = z + t\sqrt[4]{3} \qquad z, t \in \mathbb{Q}\left(\sqrt{3}\right)$$

De donde elevando al cuadrado:

$$2 = (z^2 + 2zt\sqrt[4]{3} + t^2\sqrt{3})\sqrt[4]{3}$$

Igualando coordenadas:

$$0 = z^2 + t^2\sqrt{3} \Longrightarrow z = 0 = t$$

lo que nos lleva a una contradicción.

En definitiva, $[K : \mathbb{Q}] = 32$, de donde el grupo ciclico es de orden 8.

**Ejercicio 3.4.1.** Supongamos que el polinomio $x^n - a \in F[x]$ es separable, con $a \neq 0$, y sea $K$ su cuerpo de descomposición. Denotemos por $\zeta \in K$ una raíz primitiva $n-$ésima de la unidad, y $\sqrt[n]{a} \in K$ una raíz de $f$. Dado $\sigma \in \mathrm{Aut}_F(K)$, denotemos por $j(\sigma), k(\sigma) \in \mathbb{Z}_n$ determinados por las condiciones $\sigma(\sqrt[n]{a}) = \zeta^{j(\sigma)}\sqrt[n]{a}$, $\sigma(\zeta) = \zeta^{k(\sigma)}$. Demostrar que la aplicación

$$\mathrm{Aut}_F(K) \to GL_2(\mathbb{Z}_n), \qquad \sigma \longmapsto \begin{pmatrix} 1 & 0 \\ j(\sigma) & k(\sigma) \end{pmatrix}$$

es un homomorfismo inyectivo de grupos. Deducir que $|\mathrm{Aut}_F(K)|$ es un divisor de $n\varphi(n)$. En el caso $F = \mathbb{Q}$, deducir que $|\mathrm{Aut}_F(K)| = n\varphi(n)$ si, y solo si, $x^n - a \in \mathbb{Q}(\zeta)[x]$ es irreducible.

**Ejercicio 3.4.2.** Sea $K = \mathbb{Q}\left(\sqrt[4]{5}, i\right)$.

1. Rzonar que $K$ es una extensión de Galois de $\mathbb{Q}$ y calcular el cardinal de su grupo de Galois.
2. Describir los elementos del grupo $\mathrm{Aut}(K)$.
3. Calcular todos los subcuerpos de $K$ que tienen grado 4 sobre $\mathbb{Q}$.
4. Calcular todos los subcuerpos de $K$.

## 3.5. Ecuaciones resolubles por radicales

A lo largo de esta sección trabajaremos solo con cuerpos de característica 0, aunque es posible desarrollar la teoría para cuerpos de cualquier característica, pero añadiendo muchas hipótesis extra. Preferimos simplificar los enunciados. Así mismo, las definiciones que haremos en este apartado dependen mucho del autor.

La siguiente definición generaliza el concepto de extensión por raíces cuadradas:

**Definición 3.6.** Una extensión de cuerpos $F \leqslant E$ es una extensión por radicales si existe una torre de cuerpos

$$F = E_0 \leqslant E_1 \leqslant \ldots \leqslant E_t = E$$

tal que $E_j = E_{j-1}(\alpha_j)$, con $\alpha_j^{n_j} \in E_{j-1}$, para $j \in \{1, \ldots, t\}$.

**Definición 3.7.** 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 $f$.

**Definición 3.8.** Una extensión $F \leqslant K$ es radical si $K$ es cuerpo de descomposición de un polinomio separable $x^n - a \in F[x]$.

Bajo estas condiciones, toda extensión radical es cíclica, y toda cíclica da una radical. Como estamos en $\text{car}(F) = 0$, la hipótesis de que $x^n - a$ sea separable se traduce en que $a \neq 0$.

**Definición 3.9.** Diremos que una extensión $F \leqslant K$ es radical iterada si $F \leqslant K$ es de Galois y hay una torre de cuerpos

$$F = K_0 \leqslant K_1 \leqslant \ldots \leqslant K_t = K$$

de forma que cada $K_{i-1} \leqslant K_i$ es radical, para $i \in \{1, \ldots, t\}$.

**Proposición 3.13.** *Si $F \leqslant E$ es de Galois y $E \leqslant E(\alpha)$ para $\alpha$ raíz de $x^n - a \in E[x]$ con $a \neq 0$, entonces existe una extensión radical iterada $E \leqslant K$ con $E(\alpha) \leqslant K$ y $F \leqslant K$ de Galois.*

*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 $f \in F[x]$. Como $F \leqslant E$ es de Galois, $E$ es cuerpo de descomposición de cierto polinomio separable $g \in F[x]$. Sea $K$ el cuerpo de descomposición de $fg \in F[x]$, como estamos en característica cero, $F \leqslant K$ es de Galois. Además, vemos que:

- Como $\alpha$ es raíz de $x^n - a$ y este es un factor de $f$ para $\sigma = id$, tenemos que $\alpha \in K$.
- Como $K$ es cuerpo de descomposición de $fg$ y $E$ es cuerpo de descomposición de $g$, tiene que ser $E \leqslant K$.

de aquí deducimos que $E(\alpha) \leqslant K$. Nos falta ver que $E \leqslant K$ es radical iterada, vemos que $E \leqslant K$ es de Galois por ser $F \leqslant K$ de Galois.

Como $x^n - a$ es un factor de $f$, $K$ ha de contener un cuerpo de descomposición de $x^n - a$, por lo que por el Torema 3.9 podemos encontrar $\zeta \in K$ una raíz $n-$ésima primitiva de la unidad. Si enumeramos los elementos de $\text{Aut}_F(E)$:

$$\text{Aut}_F(E) = \{\sigma_1, \ldots, \sigma_s\}$$

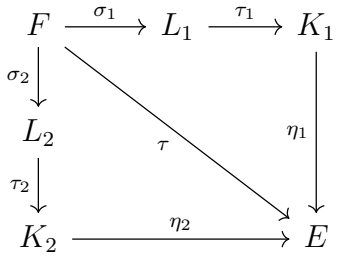
con $\sigma_1 = id_E$. Tomando $K_{-1} = E$ y $K_0 = E(\zeta)$, para cada $i \in \{1, \ldots, s\}$ tomamos $K_i = K_{i-1}(\alpha_i)$, con $\alpha_i$ raíz de $x^n - \sigma_i(a)$.

De esta forma, cada $K_{i-1} \leqslant K_i$ es radical, para $i \in \{0, \ldots, s\}$. □

En cierto momento, usaremos la sigiuente observación:

*Observación.* Sea $F$ un cuerpo, dados $\sigma_1 : F \to L_1$, $\sigma_2 : F \to L_2$ dos homomorfismos de cuerpos tales que las extensiones $\sigma_i(F) \leqslant L_i$ son finitas para $i \in \{1, 2\}$. Para cada $i \in \{1, 2\}$ vamos a construir un polinomio $f_i \in F[x]$ tal que exite un homomorfismo de cuerpos $\tau_i : L_i \to K_i$ de manera que $\tau_i\sigma_i : F \to K_i$ es cuerpo de descomposición de $f_i$. Para ello, como $\sigma_i(F) \leqslant L_i$ es finita, tenemos que $L_i = \sigma_i(F)(\alpha_1, ..., \alpha_t)$ para $\alpha_1, \ldots, \alpha_t$ algebraicos sobre $\sigma_i(F)$. Tomamos $g_j = \mathrm{Irr}(\alpha_j, \sigma_i(F))$ para $j \in \{1, \ldots, t\}$, y definimos $f_i \in F[x]$ de forma que $f_i^{\sigma_i} = g_1 \ldots g_t$.

Consideraremos también un cuerpo de descomposición $\tau : F \to E$ de $f_1 f_2$. La Tercera Proposición de extensión nos permite encontrar homomorfismos $\eta_i : F \to K_i$ en $Ex(\tau, \sigma_i, \tau_i)$, para $i \in \{1, 2\}$. Obtenemos así el diagrama conmutativo:




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:

$$F \cong \tau(F) \leqslant \eta_i\tau_i(L_i) \leqslant E \qquad \forall i \in \{1, 2\}$$

**Proposición 3.14.** *Sea $F \leqslant E$ una extensión por radicales, entonces existe una extensión radical iterada $F \leqslant K$ tal que $E \leqslant K$.*

*Demostración.* Suponemos pues que tenemos una torre:

$$F = E_0 \leqslant E_1 \leqslant \ldots \leqslant E_t = E$$

tal que $E_j = E_{j-1}(\alpha_j)$ con $\alpha_j$ raíz de $x^{n_j} - a_j \in E_{j-1}[x]$, para cada $j \in \{1, \ldots, t\}$. Razonamos por inducción sobre $t \geqslant 0$:

- Para $t = 0$, tomamos $F = E = K$.
- Para $t > 0$, por hipótesis de inducción tenemos que existe una extensión radical iterada

  $$F = K_0 \leqslant K_1 \leqslant \ldots \leqslant K_r$$

  tal que $E_{t-1} \leqslant K_r$. Tomamos una $F-$extensión común de $K_r$ y $E_t$ (como hemos hecho en la observación anterior), dentro de la cual estará $K_r(\alpha_t)$, pues $\alpha_t \in E_t$. Como tenemos $E_{t-1} \leqslant K_r$, será $E_{t-1}(\alpha_t) = E_t \leqslant K_r(\alpha_t)$.

Tenemos que $F \leqslant K_r$ es de Galois por ser $F \leqslant K_r$ radical iterada, así como que $K \leqslant K(\alpha_t)$ con $\alpha_t$ raíz de $x^{n_t} - a_t \in E_{t-1}[x]$ (y $E_{t-1} \leqslant K_r$), por lo que podemos aplicar la Proposición anterior, obteniendo una extensión radical iterada $K_r \leqslant K$ tal que $K_r(\alpha_t) \leqslant K$ y $F \leqslant K$ de Galois.

Por tanto, tenemos una torre de cuerpos

$$K_r \leqslant K_{r+1} \leqslant \ldots \leqslant K_s = K$$

con $K_{i-1} \leqslant K_i$ radical para cada $i \in \{r+1, \ldots, s\}$, de donde:

$$F = K_0 \leqslant K_1 \leqslant \ldots \leqslant K_r \leqslant K_{r+1} \leqslant \ldots \leqslant K_s = K$$

con cada $K_{k-1} \leqslant K_k$ radical para cada $k \in \{1, \ldots, s\}$ y $F \leqslant K$ de Galois. De aquí tenemos que $F \leqslant K$ es radical iterada y que $E \leqslant K$, puesto que $E = E_t \leqslant K_r(\alpha_t) \leqslant K$.

□

**Lema 3.15.** *Toda extensión radical iterada tiene grupo de Galois resoluble.*

*Demostración.* Veamos primero que si $F \leqslant K$ es radical entonces $\mathrm{Aut}_F(K)$ es resoluble. Si $F \leqslant K$ es radical entonces $K$ es cuerpo de descomposición de $x^n - a \in F[x]$ separable, por lo que contiene por el Teorema 3.9 una raíz $n-$ésima primitiva de la unidad $\zeta \in K$. Tenemos por tanto:

$$F \leqslant F(\zeta) \leqslant K$$

Con $F(\zeta) \leqslant K$ de Galois por ser $F \leqslant K$ de Galois (ya que $F \leqslant K$ es radical) y tenemos además que $F \leqslant F(\zeta)$ de Galois por ser la $n-$ésima extensión ciclotómica de $F$ (que siempre son de Galois). Usando ahora la conexión de Galois y el Teorema 2.7, tenemos entonces que:

$$\{id_K\} \lhd \mathrm{Aut}_{F(\zeta)}(K) \lhd \mathrm{Aut}_F(K)$$

y además:

$$\frac{\mathrm{Aut}_F(K)}{\mathrm{Aut}_{F(\zeta)}(K)} \cong \mathrm{Aut}_F(F(\zeta))$$

Como $\mathrm{Aut}_F(F(\zeta))$ es el grupo de Galois de una extensión ciclotómica, tiene que ser abeliano (ya que es isomorfo a un subgrupo de $\mathcal{U}(\mathbb{Z}_n)$, y este grupo es abeliano), por lo que el factor $\mathrm{Aut}_{F(\zeta)}(K) \lhd \mathrm{Aut}_F(K)$ da un cociente abeliano. Ahora, tenemos que $\mathrm{Aut}_{F(\zeta)}(K)$ es cíclico, luego el factor $\{id_K\} \lhd \mathrm{Aut}_{F(\zeta)}(K)$ también es abeliano. En definitiva, tenemos que $\mathrm{Aut}_F(K)$ es resoluble, ya que admite una serie normal con factores abelianos.

Si ahora $F \leqslant K$ es una extensión radical iterada:

$$F = K_0 \leqslant K_1 \leqslant \ldots \leqslant K_t = K$$

tendremos entonces que $F \leqslant K$ es de Galois por definición, así como que cada extensión intermedia es de Galois, por ser cuerpo de descomposición de un polinomio separable. Usando al igual que antes la conexión de Galois y el Torema 2.7, obtenemos una serie normal de grupos:

$$\mathrm{Aut}_F(K) = \mathrm{Aut}_{K_0}(K) \rhd \mathrm{Aut}_{K_1}(K) \rhd \ldots \rhd \mathrm{Aut}_{K_{t-1}}(K) \rhd \{id_K\}$$

con factores:

$$\frac{\mathrm{Aut}_{K_{i-1}}(K)}{\mathrm{Aut}_{K_i}(K)} \cong \mathrm{Aut}_{K_{i-1}}(K_i) \qquad \forall i \in \{1, \ldots, t-1\}$$

y estos factores son resolubles, ya que la extensión $K_{i-1} \leqslant K_i$ es radical, y hemos visto ya que estas extensiones tienen grupo de Galois resoluble. En definitiva, obtenemos que $\mathrm{Aut}_F(K)$ es resoluble, ya que:

**Opción 1, argumento recursivo.** Vemos que:

- Como $K_{t-1} \leqslant K_t$ es radical, tenemos que $\mathrm{Aut}_{K_{t-1}}(K)$ es resoluble.
- Supuesto que $\mathrm{Aut}_{K_{t-s}}(K)$ es resoluble para $s \in \{1, \ldots, t-1\}$, tenemos que $\mathrm{Aut}_{K_{t-s}}(K) \lhd \mathrm{Aut}_{K_{t-(s+1)}}(K)$ con:

$$\mathrm{Aut}_{K_{t-s}}(K), \qquad \frac{\mathrm{Aut}_{K_{t-(s+1)}}(K)}{\mathrm{Aut}_{K_{t-s}}(K)}$$

  resolubles, por lo que $\mathrm{Aut}_{K_{t-(s+1)}}(K)$ es resoluble.

En definitiva, obtenemos que $\mathrm{Aut}_{K_0}(K) = \mathrm{Aut}_F(K)$ es resoluble.

**Opción 2, refinando la serie.** Como cada factor es resoluble, podemos encontrar entre cada dos eslabones de la cadena una serie normal con factores abelianos, y si repetimos este proceso en cada eslabón, obtenemos al final una serie normal con factores abelianos, por lo que $\mathrm{Aut}_F(K)$ es resoluble.

□

**Ejercicio 3.5.1.** Sea $f \in F[x]$ y $L$ cuerpo de descomposición de $f \in F[x]$. Demostrar que para cualquier extensión $F \leqslant E$, si $K$ es un cuerpo de descomposición de $f$ sobre $E$, entonces $\mathrm{Aut}_E(K)$ es isomorfo a un subgrupo de $\mathrm{Aut}_F(L)$.

Es claro que $L \leqslant K$. Como $L = F(\alpha_1, \ldots, \alpha_n)$ siendo $\alpha_1, \ldots, \alpha_n$ las raíces de $f$, tendremos también que $K = E(\alpha_1, \ldots, \alpha_n)$. Si tomamos $\sigma \in \mathrm{Aut}_E(K)$, vemos que tenemos un automorfismo $\sigma : K \to K$ que permuta las raíces de $f$ y que es $E-$lineal. Como $F \leqslant E$ es claro que también es $F-$lineal, y como $L \leqslant K$ podemos restringir $\sigma$ a $L$, obteniendo $\sigma\big|_L : L \to K$. Como $L = F(\alpha_1, \ldots, \alpha_n)$ y $\sigma\big|_L$ deja fijos los elementos de $F$ y permuta las raíces de $f$, vemos que $Im\sigma\big|_L \leqslant L$. Si consideramos la aplicación $\mathrm{Aut}_E(K) \to \mathrm{Aut}_F(L)$ que restringe cada $\sigma$ a $L$ obtenemos lo buscado.

**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 $f$:

$\Longrightarrow$) Tenemos una torre $F \leqslant L \leqslant E$ tal que $F \leqslant E$ es una extensión por radicales. Por las Proposiciones anteriores, se ha visto que existe una extensión radical iterada $F \leqslant K$ tal que $E \leqslant K$, por lo que $F \leqslant K$ es de Galois, y como $F \leqslant L$ también es de Galois (es cuerpo de descomposición en característica cero), aplicando el Torema 2.7 tenemos que $\mathrm{Aut}_L(K) \lhd \mathrm{Aut}_F(K)$. Sabemos además que:

$$\mathrm{Aut}_F(L) \cong \frac{\mathrm{Aut}_F(K)}{\mathrm{Aut}_L(K)}$$

Y en el Lema anterior vimos que $\mathrm{Aut}_F(K)$ es resoluble, por lo que $\mathrm{Aut}_F(L)$ es resoluble, que es el grupo de Galois de $f$.

$\Longleftarrow$) Supuesto que $\mathrm{Aut}_F(L)$ 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 $\mathrm{Aut}_{F(\zeta)}(K)$ es isomorfo a un subgrupo de $\mathrm{Aut}_F(L)$. Como $\mathrm{Aut}_F(L)$ es resoluble, tendremos que $\mathrm{Aut}_{F(\zeta)}(K)$ es resoluble y sabemos que $|\mathrm{Aut}_{F(\zeta)}(K)|$ divide a $n$ (por el Teorema de Lagrange). Como $\mathrm{Aut}_{F(\zeta)}(K)$ es resoluble, podemos encontrar una serie de composición con factores primos:

$$\mathrm{Aut}_{F(\zeta)}(K) = G_0 \rhd G_1 \rhd \ldots \rhd G_{t-1} \rhd G_t = \{id_K\}$$

con $G_{i-1}/G_i$ de cardinal $p_i$ primo que divide a $|\mathrm{Aut}_{F(\zeta)}(K)|$, luego también a $n$. Si aplicamos la conexión de Galois a la serie de composición, obtenemos:

$$F(\zeta) = K^{G_0} \leqslant K^{G_1} \leqslant \ldots \leqslant K^{G_{i-1}} \leqslant K^{G_t} = K$$

Para cada $i \in \{1, \ldots, t\}$ tenemos por el Teorema 2.7 que el grupo de Galois de $K^{G_{i-1}} \leqslant K^{G_i}$ es isomorfo a $G_{i-1}/G_i$, luego es cíclico de orden $p_i$. Además, tenemos que $\zeta^{n/p_i} \in F(\zeta)$ es una raíz $p_i-$ésima de la unidad, que estará contenida también en $K^{G_{i-1}}$ por ser $F(\zeta) = K^{G_0}$. Bajo estas condiciones podemos aplicar el Teorema 3.11 a la extensión $K^{G_{i-1}} \leqslant K^{G_i}$, obteniendo que entonces $K^{G_i}$ es cuerpo de descomposición de un polinomio de la forma $x^{p_i} - a_i \in K^{G_{i-1}}[x]$, por lo que $K^{G_{i-1}} \leqslant K^{G_i}$ es radical.

Como claramente $F \leqslant F(\zeta)$ es radical, obtenemos finalmente una cadena de extensiones radicales:

$$F \leqslant F(\zeta) = K^{G_0} \leqslant K^{G_1} \leqslant \ldots \leqslant K^{G_{t-1}} \leqslant K^{G_t} = K$$

Es decir, $F \leqslant K$ es una extensión por radicales, con $L \leqslant K = L(\zeta)$, por lo que $f$ es resoluble por radicales.

□

**Consecuencias**

1. Si $deg f \leqslant 4$, entones $f$ es resoluble por radicales.

   Esto es porque el grupo de Galois de $f$ está dentro de $S_n$ con $n \leqslant 4$ y estos grupos son resolubles.

2. Si $degf \geqslant 5$, 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 $F$ es un cuerpo, podemos considerar el anillos de polinomios con coeficientes en $F$ y con $n$ indeterminadas, $F[x_1, \ldots, x_n]$.

- 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, y en una cantidad finita de pasos llegamos a que $F[x_1, \ldots, x_n]$ también es un DFU, y en particular un dominio de integridad.

Si aplicamos la construcción de cuerpo de fracciones a $F[x_1, \ldots, x_n]$, obtenemos $F(x_1, \ldots, x_n)$, el cuerpo de fracciones del dominio de integridad $F[x_1, \ldots, x_n]$:

$$F(x_1, \ldots, x_n) = \left\{ \frac{f}{g} : f, g \in F[x_1, \ldots, x_n], g \neq 0 \right\}$$

Dada una permutación $\sigma \in S_n$ y aplicando $n$ veces la Propiedad Universal del anillo de polinomios, podemos obtener un homomorfismo de anillos $F-$lineal $\overline{\sigma} : F[x_1, \ldots, x_n] \to F[x_1, \ldots, x_n]$ determinado por:

$$\begin{aligned} \overline{\sigma}(\alpha) &= \alpha \quad \forall \alpha \in F \\ \overline{\sigma}(x_i) &= x_{\sigma(i)} \quad \forall i \in \{1, \ldots, n\} \end{aligned}$$

Que claramente es un isomorfismo, pues $\overline{\sigma^{-1}}$ es su homomorfismo inverso. Usando la Propiedad Universal de $F(x_1, \ldots, x_n)$ para obtener un automorfismo de cuerpos $\overline{\sigma} : F(x_1, \ldots, x_n) \to F(x_1, \ldots, x_n)$ dado por:

$$\overline{\sigma}\left( \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} \right) = \frac{f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}{g(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}$$

Tenemos así una aplicación $S_n \to \mathrm{Aut}_F(F(x_1, \ldots, x_n))$ que es un homomorfismo de grupos inyectivo.

**Notación.** Ante estas condiciones, usaremos la siguiente notación a lo largo de esta sección:

- $E = F(x_1, \ldots, x_n)$.
- $G$ es la imagen del monomorfismo de grupos $S_n \to \mathrm{Aut}_F(E)$.

**Definición 3.10.** Al cuerpo $E^G$ lo llamamos cuerpo de las funciones simétricas racionales en $x_1, \ldots, x_n$ con coeficientes en $F$.

Tenemos que $E^G \leqslant E$ es de Galois, por el Lema de Artin.

**Notación.** Para cada $k \in \{1, \ldots, n\}$ escribimos:

$$s_k = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} x_{i_1} \ldots x_{i_k} \in F[x_1, \ldots, x_n]$$

Por ejemplo, si $n = 4$, tenemos entonces que:

$$\begin{aligned} S_1 &= x_1 + x_2 + x_3 + x_4 \\ S_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ S_3 &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\ S_4 &= x_1x_2x_3x_4 \end{aligned}$$

Llamaremos a los polinomios $s_k$ para $1 \leqslant k \leqslant n$ polinomios simétricos elementales.

**Proposición 3.17.** *$E^G = F(s_1, \ldots, s_n)$, es decir, toda función simétrica racional en $x_1, \ldots, x_n$ con coeficientes en $F$ puede expresarse exclusivamente en términos de los polinomios simétricos elementales $s_1, \ldots, s_n$.*

*Demostración.* Consideramos el polinomio:

$$f = (x - x_1) \ldots (x - x_n) \in E[x]$$

Y si tomamos $\overline{\sigma} \in G$ es claro que $f^{\overline{\sigma}} = f$, luego $f \in E^G[x]$. El Ejercicio 3.1.2 nos dice que:

$$f = x^n - s_1x^{n-1} + \ldots + (-1)^n s_n$$

por lo que $s_1, \ldots, s_n \in E^G$, de donde $F(s_1, \ldots, s_n) \leqslant E^G$.

Observemos además que $E$ es cuerpo de descomposición de $f$ sobre $F(s_1, \ldots, s_n)$ y como $f$ es separable vemos que $F(s_1, \ldots, s_n) \leqslant E$ es de Galois.

Además, $G \leqslant \mathrm{Aut}_{F(s_1,\ldots,s_n)}(E)$. Pero si $\tau : F \to E$ es un automorfismo de cuerpos $F(s_1, \ldots, s_n)-$lineal, entonces para cada $i \in \{1, \ldots, n\}$ 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:

$$G = \mathrm{Aut}_{F(s_1,\ldots,s_n)}(E)$$

Y como $F(s_1, \ldots, s_n) \leqslant E$ es de Galois tenemos por la conexión de Galois que:

$$E^G = F(s_1, \ldots, s_n)$$

□

Consideramos ahora:

$$g = x^n - \lambda_1 x^{n-1} + \ldots + (-1)^n \lambda_n \in F(\lambda_1, \ldots, \lambda_n)[x]$$

con $\lambda_1, \ldots, \lambda_n$ indeterminadas sobre $F$. La ecuación $g = 0$ en $x$ se llama ecuación general sobre $F$ de grado $n$.

**Lema 3.18.** *Si tomamos $h \in F[\lambda_1, \ldots, \lambda_n]$ con $h \neq 0$, tenemos entonces que:*

$$h(s_1, \ldots, s_n) \neq 0$$

*Demostración.* Llamamos $s_0 := 1$, y definimos:

$$s_n(x_1, \ldots, x_{n-1}) := 0$$

Estas definiciones dan sentido a la fórmula recursiva:

$$s_k(x_1, \ldots, x_n) = s_k(x_1, \ldots, x_{n-1}) + s_{k-1}(x_1, \ldots, x_{n-1})x_n, \quad k \in \{1, \ldots, n\}$$

Por inducción sobre $n$:

- Para $n = 1$, tenemos que $s_1 = x_1$, y tenemos que $h_1(x_1) \neq 0 \Longrightarrow h_1(x_1) \neq 0$.
- Para $n > 1$, razonamos por inducción al absurdo: supongamos que existe $h \neq 0$ pero $h(s_1, \ldots, s_n) = 0$. Entre todos éstos, tomamos:

  $$0 \neq h = h_0 + h_1\lambda_n + \ldots + h_m\lambda_n^m \quad \text{con} \quad h_i \in F[\lambda_1, \ldots, \lambda_{n-1}]$$

  de grado mínimo $m$ en $\lambda_n$. Tenemos entonces que:

  $$\begin{aligned} 0 &= h(s_1, \ldots, s_n) \\ &= h_0(s_1, \ldots, s_{n-1}) + h_1(s_1, \ldots, s_{n-1})s_n + \ldots + h_m(s-1, \ldots, s_{n-1})s_n^m \end{aligned}$$

  Evaluando en $x_n = 0$, obtenemos que $s_n = 0$, por lo que:

  $$\begin{aligned} 0 &= h_0(s_1(x_1, \ldots, x_{n-1}, 0), \ldots, s_{n-1}(x_1, \ldots, x_{n-1}, 0)) \\ &= h_0(s_1(x_1, \ldots, x_{n-1}), \ldots, s_{n-1}(x_1, \ldots, x_{n-1})) \end{aligned}$$

  La hipótesis de inducción nos dice que $h_0(\lambda_1, \ldots, \lambda_{n-1}) = 0$, y sacando factor común $\lambda_n$ de la definición de $h$:

  $$h = (h_1 + h_2\lambda_n + \ldots + h_m\lambda_n^{m-1})\lambda_n$$

  Evaluando en $(s_1, \ldots, s_{n-1})$ obtengo

  $$0 = (h_1(s_1, \ldots, s_{n-1}) + h_2(s_1, \ldots, s_{n-1})s_n + \ldots + h_m(s_1, \ldots, s_{n-1})s_n^{m-1})s_n$$

  y como $s_n \neq 0$, tenemos que:

  $$0 = h_1(s_1, \ldots, s_{n-1}) + h_2(s_1, \ldots, s_{n-1})s_n + \ldots + h_m(s_1, \ldots, s_{n-1})s_n^{m-1}$$

  de donde obtendríamos que $h_1 + h_2\lambda_n + \ldots + h_m\lambda_n^{m-1}$ se anula a $(s_1, \ldots, s_n)$, con grado menor que $h$, lo que nos lleva a una contradicción.

□

**Proposición 3.19.** *El polinomio:*

$$g = x^n - \lambda_1 x^{n-1} + \ldots + (-1)^n\lambda_n \in F(\lambda_1, \ldots, \lambda_n)[x]$$

*es irreducible, separable y su grupo de Galois es isomorfo a $S_n$.*

*Demostración.* Tomamos $\varepsilon : F[\lambda_1, \ldots, \lambda_n] \to F(s_1, \ldots, s_n)$ el anillo de polinomios determinado por $\varepsilon(\alpha) = \alpha \quad \forall \alpha \in F$ y $\varepsilon(\lambda_i) = s_i \quad i \in \{1, \ldots, n\}$, tenemos que $\ker \varepsilon = \{0\}$ por el Lema anterior. La propiedad universal del cuerpo de fracciones $F(\lambda_1, \ldots, \lambda_n)$ nos da un homomorfismo de cuerpos

$$\overline{\varepsilon} : F(\lambda_1, \ldots, \lambda_n) \to F(s_1, \ldots, s_n)$$

que extiende a $\varepsilon$. Tenemos que $\overline{\varepsilon}$ es $F-$lineal y es un isomorfismo de cuerpos. Cardano-Vieta nos dice que $g^{\overline{\varepsilon}} = f$. Teemos que $E = F(x_1, \ldots, x_n)$ es cuerpo de descomposición de $f$, por lo que al aplicar el isomorfismo $\overline{\varepsilon}$ tenemos que la correstricción:

$$\overline{\varepsilon} : F(\lambda_1, \ldots, \lambda_n) \to E$$

da un cuerpo de descomposición de $g \in F(\lambda_1, \ldots, \lambda_n)[x]$. 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 $1, \ldots, n$) tenemos que el grupo de Galois de $f$ es transitivo, luego $f$ es irreducible. □

**Teorema 3.20** (de Abel-Ruffini)**.** *Si* $\text{car}(F) = 0$ *y* $n \geqslant 5$*, entonces* $g$ *no es resoluble por radicales sobre* $F(\lambda_1, \ldots, \lambda_n)$*.*

*Demostración.* El grupo de Galois de $g$ es isomorfo a $S_n$ con $n \geqslant 5$, que no es resoluble, por lo que $f$ no puede ser resoluble por radicales. □

## 3.7. Resolución de ecuaciones de grado hasta 4

El Gran Teorema de Galois nos dice que las ecuaciones de grado hasta 4 son resolubles por radicales en característica cero. Realmente lo son para todas las características, por lo que en esta sección vamos a dar procedimientos clásicos para la resolución de ecuaciones de grado 2, 3 y 4. Sea pues $F$ un cuerpo cualquiera, afrontaremos resolver la ecuación $f(x) = 0$ donde $f \in F[x]$ es un polinomio mónico de grado $degf \in \{2, 3, 4\}$.

### 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 mediante $F \leqslant K$, tratamos de despejar $x$, escribiendo las igualdades con elementos de $K$:

$$x + \frac{b}{2} = \pm\sqrt{\frac{b^2}{4} - c} = \pm\sqrt{\frac{b^2 - 4c}{4}} = \pm\frac{\sqrt{b^2 - 4c}}{2}$$

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[8] $\text{car}(F) \notin \{2, 3\}$, consideramos el polinomio:

$$g(x) = f\left(x - \frac{b}{3}\right) = x^3 + px + q$$

para ciertos $p, q \in F$, ya que:

$$\begin{aligned} g(x) = f\left(x - \frac{b}{3}\right) &= \left(x - \frac{b}{3}\right)^3 + b\left(x - \frac{b}{3}\right)^2 + c\left(x - \frac{b}{3}\right) + d \\ &= x^3 \cancel{- bx^2} + \frac{b^2}{3^2}x - \frac{b^3}{3^3} + \cancel{bx^2} + \frac{b^3}{3^3} - \frac{2}{3}b^2x + cx - \frac{bc}{3} + d \\ &= x^3 + x\left(\frac{b^2}{3^2} - \frac{2}{3}b^2 + c\right) + \left(d - \frac{bc}{3}\right) \end{aligned}$$

Como podemos ver, $g$ no tiene término cuadrático. El polinomio $g$ que se obtiene de esta forma a partir de un polinomio cualquiera $f$ de grado 3 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[9] $\omega$. Sean $\alpha_1, \alpha_2, \alpha_3 \in K$ las raíces de $g$. Tenemos por las ecuaciones de Cardano-Vieta que:

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

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 $x^2 + x + 1 = 0$):

$$\begin{aligned} \beta + \gamma &= 2\alpha_1 + \alpha_2(\omega + \omega^2) + \alpha_3(\omega + \omega^2) = 2\alpha_1 - \alpha_2 - \alpha_3 \\ &= 2\alpha_1 + \alpha_1 = 3\alpha_1 \end{aligned}$$

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:

$$u = \frac{\beta}{3}, \qquad v = \frac{\gamma}{3}$$

tenemos que:

$$\alpha_1 = u + v$$

[8] Distinta de 3 para el truco siguiente y distinta de 2 para poder aplicar luego la resolución de cuadrácticas.

[9] Aquí también necesitamos que $\text{car}(F) \neq 3$, para que $x^3 - 1$ sea separable.

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:

$$0 = u^3 + v^3 + q \quad \Longrightarrow \quad \begin{cases} u^3 + v^3 = -q \\ u^3 v^3 = \frac{-p^3}{27} \end{cases}$$

Si tomamos:

$$h(z) = (z - u^3)(z - v^3) = z^2 + qz - \frac{p^3}{27}$$

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 cúbica 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 cuadŕatica de la reducida cúbica en $\mathbb{C}$ son $u^3 = 16 + i\sqrt{87}$, $v^3 = 16 - i\sqrt{87}$.
Extraemos las raíces cúbicas, obteniendo:

$$u_k = e^{ik2\pi/3}\sqrt[3]{6 + i\sqrt{87}}, \quad k = 0, 1, 2$$
$$v_k = e^{ik2\pi/3}\sqrt[3]{16 - i\sqrt{87}}, \quad k = 0, 1, 2$$

Hemos de elegir de acuerdo con la condición $3uv = -p = 21$, lo que nos da:

$$u_0 v_0 = u_1 v_2 = u_2 v_1 = 7$$

Por tanto, las raíces de la cúbica reducida son:

$$u_0 + v_0 = \sqrt[3]{16 + i\sqrt{87}} + \sqrt[3]{16 - i\sqrt{87}}$$
$$u_1 + v_2 = e^{i2\pi/3}\sqrt[3]{16 + i\sqrt{87}} + e^{i4\pi/3}\sqrt[3]{16 - i\sqrt{87}}$$
$$u_2 + v_1 = e^{i4\pi/3}\sqrt[3]{16 + i\sqrt{87}} + e^{i2\pi/3}\sqrt[3]{16 - i\sqrt{87}}$$

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 cúbica:

$$g = f\left(x - \frac{b}{4}\right) = x^4 + px^2 + qx + r$$

Llamaremos $\beta_1, \beta_2, \beta_3, \beta_4$ a las raíces de $g$ en una extensión adecuada. Por las relaciones de Cardano-Vieta:

$$\beta_1 + \beta_2 + \beta_3 + \beta_4 = 0$$

Tomamos ahora las expresiones (se han obteniedo 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:

$$\rho_1^2 = (\beta_1 + \beta_2)^2 \quad \Longrightarrow \quad \beta_1 + \beta_2 = \sqrt{\rho_1}$$

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 obtenemoas 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 $\alpha_1, \ldots, \alpha_{p-2} \in \mathbb{R}$; $\alpha, \overline{\alpha} \in \mathbb{C} \setminus \mathbb{R}$ las raíces de $f$ tenemos que el cuerpo de descomposición de $f$ es:

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_{p-2})(\alpha, \overline{\alpha}) \leqslant \mathbb{C}$$

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:

$$\overline{f} = x^5 - x - 1 \in \mathbb{Z}_3[x]$$

que no tiene raíces en $\mathbb{Z}_3$. Los posibles factores de grado 2 son todos aquellos de grado 2 irreducibles:

$$x^2 + 1, \qquad x^2 + 2x + 2 \qquad , x^2 + x + 2$$

con la división euclidiana 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:

$$f(-2) = -25 < 0, \qquad f(-1) = 2 > 0, \qquad f(0) = -1 < 0$$

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 $\sigma \in \mathrm{Aut}_F(K)$, denotamos por $j(\sigma), k(\sigma) \in \mathbb{Z}_n$ a los elementos determinados por

$$\sigma\left(\sqrt[n]{a}\right) = \zeta^{j(\sigma)}\sqrt[n]{a}, \qquad \sigma(\zeta) = \zeta^{k(\sigma)}$$

con $k(\sigma) \in \mathcal{U}(\mathbb{Z}_n)$. Comprobar que la aplicación[10] $\mathrm{Aut}_F(K) \to GL_2(\mathbb{Z}_n)$ dada por:

$$\sigma \longmapsto \begin{pmatrix} 1 & 0 \\ j(\sigma) & k(\sigma) \end{pmatrix}$$

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, $|\mathrm{Aut}_F(K)|$ 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.** *Sean $p$ un primo y $k, n \geqslant 1$, si consideramos una extensión de cuerpos finitos $\mathbb{F}_{p^k} \leqslant \mathbb{F}_{p^{kn}}$, tenemos entonces que $\mathbb{F}_{p^{kn}}$ es cuerpo de descomposición de $x^{p^{kn}} - x \in \mathbb{F}_{p^k}[x]$, así como que $\mathrm{Aut}_{\mathbb{F}_{p^k}}(\mathbb{F}_{p^{kn}})$ es cíclico de orden $n$, y está generado por $\phi$, donde:*

$$\phi(\alpha) = \alpha^{p^k} \qquad \forall \alpha \in \mathbb{F}_{p^{kn}}$$

*Demostración.* Vimos ya que $\mathbb{F}_{p^{kn}}$ era cuerpo de descomposición del polinomio $x^{p^{kn}} - x \in \mathbb{F}_p[x]$, y como $\mathbb{F}_p \leqslant \mathbb{F}_{p^k} \leqslant \mathbb{F}_{p^{kn}}$, tenemos entonces que $\mathbb{F}_{p^{kn}}$ es cuerpo de descomposición de $x^{p^{kn}} - x \in \mathbb{F}_{p^k}[x]$.

Observemos que tenemos la torre de cuerpos finitos:

$$\mathbb{F}_p \leqslant \mathbb{F}_{p^k} \leqslant \mathbb{F}_{p^{kn}}$$

Por lo que las tres extensiones de cuerpos que aparecen son de Galois. Vimos que el automorfismo de Frobenius $\tau : \mathbb{F}_{p^{kn}} \to \mathbb{F}_{p^{kn}}$ nos permitía escribir:

$$\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^{kn}}) = \langle \tau \rangle$$

donde:

$$\tau(\alpha) = \alpha^p \qquad \forall \alpha \in \mathbb{F}_{p^{kn}}$$

[10] 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 conmutativo.

Como $\mathrm{Aut}_{\mathbb{F}_{p^k}}(\mathbb{F}_{p^{kn}})$ es un subgrupo de $G = \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^{kn}})$, este último cíclico de orden $kn$, tenemos que el primero es cíclico. Como $\mathbb{F}_{p^k} \leqslant \mathbb{F}_{p^{kn}}$ es de Galois, el orden de $\mathrm{Aut}_{\mathbb{F}_{p^k}}(\mathbb{F}_{p^{kn}})$ será igual al grado de la extensión $\mathbb{F}_{p^k} \leqslant \mathbb{F}_{p^{kn}}$, que es:

$$[\mathbb{F}_{p^{kn}} : \mathbb{F}_{p^k}] = n$$

En vista de que el orden de $\tau$ es $kn$ y que buscamos un elemento de orden $n$, tomamos $\phi = \tau^k$, que verifica:

$$\phi(\alpha) = \tau^k(\alpha) = \alpha^{p^k} \qquad \forall \alpha \in \mathbb{F}_{p^{kn}}$$

Observemos que $\phi$ es $\mathbb{F}_{p^k}-$lineal, ya que si $\gamma \in \mathbb{F}_{p^k}$, tenemos entonces que el orden multiplicativo de $\gamma$ es divisor de $p^k - 1$, con lo que:

$$\phi(\gamma) = \gamma^{p^k} = \gamma^{p^k - 1} \cdot \gamma = \gamma$$

Así, $\phi$ es un elemento de $\mathrm{Aut}_{\mathbb{F}_{p^k}}(\mathbb{F}_{p^{kn}})$ de orden $n$, por lo que ha de generar todo el grupo. □

**Notación.** En vistas el Teorema anterior, bajo sus mismas hipótesis, llamaremos a $\phi$ automorfismo de Frobenius de la extensión $\mathbb{F}_{p^k} \leqslant \mathbb{F}_{p^{kn}}$.

**Teorema 3.22.** *Si $f \in \mathbb{F}_{p^k}[x]$ es un polinomio irreducible de grado $n$, entonces su cuerpo de descomposición es $\mathbb{F}_{p^{kn}}$. Además, si $\alpha \in \mathbb{F}_{p^{kn}}$ es una raíz de $f$, entonces el resto de sus raíces son*

$$\alpha^{p^k}, \alpha^{p^{2k}}, \ldots, \alpha^{p^{(n-1)k}}$$

*Demostración.* Suponemos que $f$ es mónico. Sabemos que $f$ tiene una raíz en alguna extensión de grado $n$ de $\mathbb{F}_{p^k}$, como por ejemplo en:

$$\mathbb{F}_{p^{kn}} := \frac{\mathbb{F}_{p^k}[x]}{\langle f \rangle}$$

Sea $\alpha$ una raíz de $f$ en $\mathbb{F}_{p^{kn}}$, observemos que la extensión $\mathbb{F}_{p^k} \leqslant \mathbb{F}_{p^{kn}}$ es de Galois, por lo que $f$ tiene todas sus raíces en $\mathbb{F}_{p^{kn}}$ (por ser la extensión normal) y como $f = \mathrm{Irr}(\alpha, \mathbb{F}_{p^k})$ tenemos también que $f$ es separable (por ser la extensión separable). Vemos además que el grupo de Galois de $f$ es $\mathrm{Aut}_{\mathbb{F}_{p^k}}(\mathbb{F}_{p^{kn}})$, generado por $\phi$, el automorfismo de Frobenius de la extensión, por lo que:

$$\alpha^{q^k} = \phi(\alpha)^k \qquad \forall k \in \{1, \ldots n\}$$

son todas raíces de $f$. Además, como tenemos $n$ de ellas, hemos obtenido todas las raíces de $f$. □

**Teorema 3.23.** *Un polinomio irreducible $f \in \mathbb{F}_{p^k}[x]$ de grado $n$ divide al polinomio $x^{p^{km}} - x \in \mathbb{F}_{p^k}[x]$ si, y solo si, $n$ divide a $m$.*
*Como consecuencia, $x^{p^{km}} - x \in \mathbb{F}_{p^k}[x]$ es producto de todos los polinomios irreducibles en $\mathbb{F}_{p^k}[x]$ cuyo grado divide a $m$.*

*Demostración.* Por doble implicación y llamando $g = x^{p^{km}} - x \in \mathbb{F}_{p^k}[x]$:

$\Longrightarrow$) Supongamos que $f$ es irreducible y que divide a $g$. Si tomamos los cuerpos de descomposición de ambos polinomios, $\mathbb{F}_{p^{kn}}$ y $\mathbb{F}_{p^{km}}$, como $f$ divide a $g$, todas las raíces de $f$ lo serán de $g$, por lo que tendremos que $\mathbb{F}_{p^{kn}} \leqslant \mathbb{F}_{p^{km}}$. El Lema de la Torre aplicado a:

$$\mathbb{F}_{p^k} \leqslant \mathbb{F}_{p^{kn}} \leqslant \mathbb{F}_{p^{km}}$$

nos dice que $n$ divide a $m$, ya que:

$$[\mathbb{F}_{p^{kn}} : \mathbb{F}_{p^k}] = n, \qquad [\mathbb{F}_{p^{km}} : \mathbb{F}_{p^k}] = m$$

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.

$\Longleftarrow$) Si $f$ es irreducible y $n \mid m$ tenemos entonces que $(p^{kn} - 1)$ divide a $(p^{km} - 1)$, de donde el polinomio $x^{p^{kn}} - x \in \mathbb{F}_{p^k}[x]$ dividirá al polinomio $x^{p^{km}} - x \in \mathbb{F}_{p^k}[x]$, por lo que $\mathbb{F}_{p^{kn}} \leqslant \mathbb{F}_{p^{km}}$.

Como $\mathbb{F}_{p^{kn}}$ es cuerpo de descomposición de $f$, tenemos que todas sus raíces están en $\mathbb{F}_{p^{km}}$, pero todas estas son a su vez raíces de $x^{p^{km}} - x \in \mathbb{F}_{p^k}[x]$, por lo que $f$ divide a $x^{p^{km}} - x$.

Finalmente, como $x^{p^{km}} - x \in \mathbb{F}_{p^k}[x]$ es separable, será producto de polinomios irreducibles mónicos distintos, que por la caracterización recién vista, obtenemos que todos sus términos son los polinomios mónicos irreducibles en $\mathbb{F}_{p^k}[x]$ cuyo grado divide a $m$. □

**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 anterior, el polinomio factoriza como producto de todos los polinomios mónicos irreducibles de grado un divisor de 4:

- De grado 1 sabemos que solo son 2: $x, x - 1 \in \mathbb{F}_2[x]$.
- De grado 2 sabemos que solo hay uno, $x^2 + x + 1 \in \mathbb{F}_2[x]$.
- De grado 4. Sabemos ya que los polinomios anteriores aparecerán en la factorización de $x^{16}+x$, y entre ellos sumamos ya hasta grado 4, por lo que solo puede haber 3 polinomios irreducibles de grado 4, y todos ellos dividen a $x^{16} + x$.

  Para buscarlos, buscamos los polinomios de grado 4 en $\mathbb{F}_2[x]$ que no tengan raíces (y que por tanto tengan un número impar de monomios) y que no sean el polinomio:

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

  Estos son:

  $$x^4 + x + 1, \qquad x^4 + x^3 + 1, \qquad x^4 + x^3 + x^2 + x + 1$$

Por lo que la factorización será:

$$x^{16} + x = x(x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$$

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:

  $$\mathbb{F}_{16} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$$

  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 $\mathbb{F}_4 \leqslant \mathbb{F}_{16}$ 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 $\alpha$:

$$x^3 + x + 1 = 0, \qquad x^3 + x^2 + 1 = 0, \qquad x^2 + x + 1 = 0$$

**Solución.**
Para ver que $F = \mathbb{F}_2(\alpha)$ basta ver que $f$ es irreducible, por lo que entonces $F \leqslant \mathbb{F}_2(\alpha)$ será de Galois y lo tenemos. Comprobamos que $f$ es irreducible, ya que se tiene $f(0) = f(1) = 1 \neq 0$, y $degf = 3$.
Como $\alpha$ es raíz de $f$ y $\mathbb{F}_2 \leqslant F$ 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:

     $$\mathbb{F}_2 \leqslant \mathbb{F}_4 \leqslant \mathbb{F}_8$$

     Pero no puede ser $\mathbb{F}_{2^2} \leqslant \mathbb{F}_{2^3}$, 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 $\mathbb{F}_4 \leqslant K$ 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 tienes 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:

$$x^3 + x + 1 = 0, \qquad x^3 + x^2 + 1 = 0, \qquad x^2 + x + 1 = 0$$

**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 $\gamma \in \mathbb{F}_4 \backslash \mathbb{F}_2$, 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 $Div(6) = \{1, 2, 3, 6\}$)

$$x^{64} - x = x(x+1)(x^2+x+1)(x^3+x+1)(x^3+x^2+1) \prod \text{polinomios grado 6}$$

Como la suma de los grados tiene que ser 64, el último polinomio (el producto) tiene grado:

$$64 - 10 = 54, \qquad \frac{54}{6} = 9$$

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:

$$K = \mathbb{Q}(i, -i, r, \alpha, \overline{\alpha}) = \mathbb{Q}(i, r, \alpha)$$

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 $|\operatorname{Aut}_{\mathbb{Q}}(K)| = [K : \mathbb{Q}]$. 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 $\operatorname{Irr}(\alpha, \mathbb{Q})$ tiene grado 2, y teníamos que $\alpha$ era raíz de $g$, por lo que $\operatorname{Irr}(\alpha, \mathbb{Q}) \mid g$, pero $g$ es irreducible, lo que lleva a una contradicción.
- Como $\alpha \notin \mathbb{Q}(i)$ tenemos entonces que $\overline{\alpha} \notin \mathbb{Q}(i)$.

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:

$$\operatorname{Disc}(g) = -31$$

Por lo que:

$$\Delta = \sqrt{\mathrm{Disc}(g)} = i\sqrt{31} \notin \mathbb{Q}(i)$$

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 $\mathrm{Aut}_{\mathbb{Q}(i)}(K) \cong S_3$, 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 $\mathrm{Aut}_{\mathbb{Q}}(K)$.

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 $\eta_0, \eta_1, \eta_2$:

$$r \overset{\eta_0}{\longmapsto} r, \qquad r \overset{\eta_1}{\longmapsto} \alpha, \qquad r \overset{\eta_2}{\longmapsto} \overline{\alpha}$$

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:

$$K = \mathbb{Q}\left(w, \sqrt{3}\right), \qquad w \text{ una raíz cúbica primitiva de la unidad}$$

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:

$$|\operatorname{Aut}(K)| = [K : \mathbb{Q}] = 4$$

Calculamos sus elementos, por la Proposición de extensión. Calculamos primero los homomorfismos de cuerpos $\mathbb{Q}\left(\sqrt{3}\right) \to K$, que son $\eta_j$ con $j \in \{0, 1\}$, con:

$$\eta_j\left(\sqrt{3}\right) = (-1)^j\sqrt{3}, \qquad j \in \{0, 1\}$$

Extendemos cada uno de estos homomorfismos, cada uno de ellos se extiende a dos homomorfismos $K \to K$, que son $\eta_{j,k}$, donde:

$$\eta_{j,k}\left(\sqrt{3}\right) = (-1)^j\sqrt{3}, \qquad \eta_{j,k}(w) = w^k, \qquad j \in \{0, 1\}, \quad k \in \{1, 2\}$$

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:

$$K = \mathbb{Q}\left(i\sqrt{3}\right)$$

Con lo que $|\operatorname{Aut}_{\mathbb{Q}}(K)| = [K : \mathbb{Q}] = 2$, isomorfo a $C_2$. Sus elementos son $\eta_j$, donde:

$$\eta_j\left(i\sqrt{3}\right) = (-1)^j i\sqrt{3} \qquad j \in \{0, 1\}$$

**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 $\mathbb{Q} \leqslant K$ es un subgrupo transitivo de $S_3$, luego es $A_3$ o $S_3$.

Calculamos ahora:

$$\operatorname{Disc}(f) = -4(-3)^3 - 27 = 81 = 9^2 \quad \Longrightarrow \quad \Delta = \sqrt{\operatorname{Disc}(f)} = 9 \in \mathbb{Q}$$

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 $\mathbb{Q} \leqslant \mathbb{Q}(\alpha) \leqslant K$, por lo que $\mathbb{Q}(\alpha) = K$, ya que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ por ser $f = \operatorname{Irr}(\alpha, \mathbb{Q})$ con $grd(f) = 3$.

**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 $\mathbb{Q}\left(\sqrt[3]{3} + i\sqrt{3}\right) = K$.

Las raíces de $f$ son:

$$\pm i\sqrt{3}, \quad \sqrt[3]{3}, \quad w\sqrt[3]{3}, \quad w^2\sqrt[3]{3}, \qquad w = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$$

con lo que $K = \mathbb{Q}\left(i\sqrt{3}, \sqrt[3]{3}, w\sqrt[3]{3}, w^2\sqrt[3]{3}\right)$. Como $w \in \mathbb{Q}\left(i\sqrt{3}\right)$, tenemos pues que:

$$K = \mathbb{Q}\left(i\sqrt{3}, \sqrt[3]{3}\right)$$

y usando el Lema de la Torre obtenemos que:

$$[K : \mathbb{Q}] = \left[K : \mathbb{Q}\left(\sqrt[3]{3}\right)\right]\left[\mathbb{Q}\left(\sqrt[3]{3}\right) : \mathbb{Q}\right] = 2 \cdot 3 = 6$$

Donde usamos:

- $\operatorname{Irr}\left(\sqrt[3]{3}, \mathbb{Q}\right) = x^3 - 3$ por Eisenstein.
- $\operatorname{Irr}\left(i\sqrt{3}, \mathbb{Q}\left(\sqrt[3]{3}\right)\right) = x^2 + 3$, ya que sus raíces son complejas.

Aplicamos la proposición de extensión, primero a $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt[3]{3}\right)$ para determinar los homomorfismos de cuerpos $\mathbb{Q}\left(\sqrt[3]{3}\right) \to K$, que están en biyección con las raíces de $\operatorname{Irr}\left(\sqrt[3]{3}, \mathbb{Q}\right) = x^3 - 3$ en $K$. Así, aquellos son $\eta_j : \mathbb{Q}\left(\sqrt[3]{3}\right) \to K$ determinados por:

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

Aplicando de nuevo la proposición citada a la extensión $\mathbb{Q}\left(\sqrt[3]{3}\right) \leqslant K = \mathbb{Q}\left(\sqrt[3]{3}\right)\left(i\sqrt{3}\right)$, puesto que $\operatorname{Irr}\left(i\sqrt{3}, \mathbb{Q}\left(\sqrt[3]{3}\right)\right) = x^2 + 3$, obtenemos los homomorfismos $\eta_{j,k} : K \to K$ determinados por:

$$\eta_{j,k}\left(\sqrt[3]{3}\right) = w^j \sqrt[3]{3}, \qquad \eta_{j,k} = (-1)^k \sqrt{3}, \qquad j \in \{0, 1, 2\}, \quad k \in \{0, 1\}$$

De esta forma:

$$\operatorname{Aut}(K) = \{\eta_{j,k} : j = 0, 1, 2,\ k = 0, 1\}$$

Calculamos los órdenes de los elementos:

| $\eta_{0,0}$ | $\eta_{0,1}$ | $\eta_{1,0}$ | $\eta_{1,1}$ | $\eta_{2,0}$ | $\eta_{2,1}$ |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 2 | 3 | 2 |

Por ejemplo:

$$\eta_{1,1}\left(\eta_{1,1}\left(\sqrt[3]{3}\right)\right) = \eta_{1,1}\left(w\sqrt[3]{3}\right) = \eta_{1,1}(w)\eta_{1,1}\left(\sqrt[3]{3}\right) = \overline{w}w\sqrt[3]{3} = \sqrt[3]{3}$$
$$\eta_{1,1}\left(\eta_{1,1}\left(i\sqrt{3}\right)\right) = \eta_{1,1}\left(-i\sqrt{3}\right) = i\sqrt{3}$$

Y ya sabemos en este punto los subgrupos que tenemos de $\operatorname{Aut}(K)$.

- Usando la conexión de Galois, $K^{\langle \eta_{1,0} \rangle}$ ha de ser una extensión de grado 2 de $\mathbb{Q}$. Como $i\sqrt{3} \in K^{\langle \eta_{1,0} \rangle}$:

  $$\eta_{1,0}\left(i\sqrt{3}\right) = i\sqrt{3}$$

  resulta que $\mathbb{Q}\left(i\sqrt{3}\right) \leqslant K^{\langle \eta_{1,0} \rangle}$ con $\left[\mathbb{Q}\left(i\sqrt{3}\right) : \mathbb{Q}\right] = 2$, por lo que:

  $$\mathbb{Q}\left(i\sqrt{3}\right) = K^{\langle \eta_{1,0} \rangle}$$

- Observemos que $\eta_{0,1}\left(\sqrt[3]{3}\right) = \sqrt[3]{3}$, de donde se deduce que $\mathbb{Q}\left(\sqrt[3]{3}\right) \leqslant K^{\langle \eta_{0,1} \rangle}$ con:

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

  por lo que $\mathbb{Q}\left(\sqrt[3]{3}\right) = K^{\langle \eta_{0,1} \rangle}$.

- Si vemos que:

  $$\eta_{1,1}\left(w\sqrt[3]{3}\right) = \eta_{1,1}(w)\eta_{1,1}\left(\sqrt[3]{3}\right) = \overline{w}w\sqrt[3]{3} = \sqrt[3]{3}$$

  no es fijo, probamos ahora con:

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

  Y concluimos que $\mathbb{Q}\left(w\sqrt[3]{3}\right) = K^{\langle \eta_{2,1} \rangle}$.

- 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 $w^2 = \overline{w}$), 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 $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right) : \mathbb{Q}\right]$.

   Sale 6.

2. Decidir razonadamente si $K = \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}, i\sqrt{3}\right)$ 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 $E = \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}, w\right)$ 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 $\mathrm{Aut}(K)$ definiendo explícitamente todos sus elementos.

   Buscamos primero $[K:\mathbb{Q}]$, que por el Lema de la Torre:

   $$[K:\mathbb{Q}] = \left[K:\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2},\sqrt[3]{2}\right)\right] = 2\cdot 6 = 12$$

   Y aplicamos ahora en reiteradas ocasiones la Proposición de extensión, para hayar todos los elementos de $\mathrm{Aut}(K)$, obteniendo:

   $$\begin{aligned}\eta_{j,k,l}\left(\sqrt{2}\right) &= (-1)^j\sqrt{2}\\ \eta_{j,k.l}\left(\sqrt[3]{2}\right) &= w^k\sqrt[3]{2}\\ \eta_{j,k,l}\left(i\sqrt{3}\right) &= (-1)^l i\sqrt{3}\\ j\in\{0,1\},\quad k\in\{0,1,2\},\quad l\in\{0,1\}&\end{aligned}$$

   con todos estos números en $K$, el polinomio $x^2-2$ es irreducible sobre $\mathbb{Q}$, el polinomio $x^3-2$ es irreducible sobre $\mathbb{Q}\left(\sqrt{2}\right)$ por el apartado 2.

4. Calcular razonadamente el grado del polinomio

   $$f = \mathrm{Irr}\left(\sqrt{2}+\sqrt[3]{2},\mathbb{Q}\right)$$

   Como $deg\,\mathrm{Irr}(\alpha,\mathbb{Q}) = [\mathbb{Q}(\alpha):\mathbb{Q}] = (\mathrm{Aut}_{\mathbb{Q}}(K) : \mathrm{Aut}_{\mathbb{Q}(\alpha)}(K)) = \frac{|\mathrm{Aut}_{\mathbb{Q}}(K)|}{|\mathrm{Aut}_{\mathbb{Q}(\alpha)}(K)|}$. Vemos que:

   $$\mathrm{Aut}_{\mathbb{Q}(\alpha)}(K) \supseteq \{\eta_{0,0,0},\eta_{0,0,1}\}$$

   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:

   $$\eta_{j,k,l}(\alpha) = \eta_{j,k,l}\left(\sqrt{2}\right) + \eta_{j,k,l}\left(\sqrt[3]{2}\right) = (-1)^j\sqrt{2} + w^k\sqrt[3]{2}$$

   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:

   $$\mathrm{Aut}_{\mathbb{Q}(\alpha)}(K) = \{\eta_{0,0,0},\eta_{0,0,1}\}$$

   Por lo que:

   $$deg\,\mathrm{Irr}(\alpha,\mathbb{Q}) = [\mathbb{Q}(\alpha):\mathbb{Q}] = \frac{|\mathrm{Aut}_{\mathbb{Q}}(K)|}{|\mathrm{Aut}_{\mathbb{Q}(\alpha)}(K)|} = \frac{12}{2} = 6$$

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 $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{2}\right)$. Otra forma de verlo es tomando $E$ el cuerpo de descomposición de $f$, $\mathbb{Q} \leqslant K$ es de Galois y si la extensión contiene una raíz las tiene todas, por lo que $\mathbb{Q}(\alpha) \leqslant E \leqslant K$. Como es un cuerpo de descomposición, tendremos que $\mathbb{Q} \leqslant E$ 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 $deg\,\mathrm{Irr}(\alpha, \mathbb{Q}) = 6$, 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 sextra primitiva de la unidad, tenemos por un Teorema que $K = \mathbb{Q}\left(\sqrt[6]{3}, w\right)$. 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:

$$\phi_6 = (x-w)(x-w^5) = (x-w)(x-\overline{w}) = x^2 - 2Rew + 1$$

   tenemos que usar por tanto trigonometría, con $\cos(30) = 1/2$. 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:

$$K = \mathbb{Q}\left(\sqrt[6]{3}, w\right) = \mathbb{Q}\left(\sqrt[6]{3}, i\sqrt{3}\right)$$

   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:

$$\sqrt{3} = \left(\sqrt[6]{3}\right)^3 \in K$$

   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 $G = \mathrm{Aut}_{\mathbb{Q}(i+\sqrt{3})}(K)$.

Del apartado anterior vemos que $K = \mathbb{Q}\left(\sqrt[6]{3}, i\right)$, y aplicando la Proposición de extensión vemos que:

$$\mathrm{Aut}(K) = \{\sigma_{j,k} : j \in \{0, \ldots, 5\}, k \in \{0, 1\}\}$$

donde:

$$\sigma_{j,k}\left(\sqrt[6]{3}\right) = w^j \sqrt[6]{3}, \qquad \sigma_{j,k}(i) = (-1)^k i$$

Tenemos que:

$$|G| = (G : \{\sigma_{0,0}\}) = \left[K : \mathbb{Q}\left(i + \sqrt{3}\right)\right] = \frac{[K : \mathbb{Q}]}{\left[\mathbb{Q}\left(i + \sqrt{3}\right) : \mathbb{Q}\right]}$$

y como:

$$\left[\mathbb{Q}\left(i + \sqrt{3}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(i, \sqrt{3}\right) : \mathbb{Q}\right] = 4$$

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 $\mathbb{Q} \leqslant \mathbb{Q}(i + \sqrt{3})$ 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:

$$\mathbb{F}_{81}^\times = \{1, a, \ldots, a^{79}\}$$

Por lo que:

$$\mathbb{F}_{81} = \{1, a, \ldots, a^{80}\}$$

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 $Div(8) = \{1, 2, 4, 8\}$.

**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 $\mathrm{Irr}(a^2, \mathbb{F}_3)$.

   Tenemos que:

   $$a^2 - a - 1 = 0 \quad \Longrightarrow \quad a^2 = a + 1 \notin \mathbb{F}_3$$

   ya que $\{1, a\}$ es una $\mathbb{F}_3-$base de $F$. Por tanto, $\mathrm{Irr}(a, \mathbb{F}_3)$ tiene que tener grado 2.

3. Calcular $\mathrm{Irr}(a^2, \mathbb{F}_3)$.

   Buscamos en los 3 polinomios mónicos irreducibles de $\mathbb{F}_3[x]$, buscando dónde es $a^2$ raíz, y podemos decartar $x^2 - x - 1$, 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 $\mathrm{Irr}(a^2, \mathbb{F}_3) = x^2 + 1$.