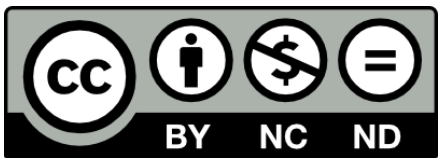
Álgebra III

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

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 e ideal; así como la forma en la que se estudiaba que un polinomio era irreducible.
- En los apuntes de Álgebra II los conceptos de: grupo, subgrupo, homomorfismo de grupos y monoide.

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.

Definición 1.1 (Cuerpo)**.** Un cuerpo es un anillo conmutativo A en el que $A \setminus \{0\}$ es un grupo.

Observemos que estamos suponiendo implícitamente que el anillo $\{0\}$ jamás puede ser un cuerpo.

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 contenido en A.

Demostración. 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 $k = 1$. Como χ y φ son homomorfismos de anillos, estos cumplen

$$\chi(1) = 1 = \varphi(1)$$

Para $k = 0$. De manera análoga, $\chi(0) = 0 = \varphi(0)$.

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 $\chi : \mathbb{Z} \to A$. Este se puede calcular exigiendo $\chi(1) = 1$.

Ahora, 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. 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 $Im\chi \subseteq S$. □

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 se podrá notar por:

$$F \leqslant K$$

Definición 1.4. Sea $F \leqslant K$ una extensión de cuerpos, decimos que una aplicación $\sigma : K \to K$ es $F-$lineal si verifica que:

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

Una forma rápida de ver si un subconjunto de un anillo es un subanillo[1] 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.

$\impliedby$) 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 las intersecciones arbitrarias de cuerpos siguen siendo cuerpos, propiedad que justifica el concepto que vamos a introducir.

Definición 1.5 (Subcuerpo generado por un conjunto)**.** Sea K un cuerpo y $S \subseteq K$, si consideramos:

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

es decir, 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.

[1] Recordemos que un subanillo de un anillo es un subconjunto que contiene al 0, al 1, y que es cerrado para opuestos, para la suma y para el producto.

Definición 1.6 (Subcuerpo primo de un cuerpo)**.** Si dado un cuerpo K pensamos en el subcuerpo generado por el conjunto vacío obtenemos el "subcuerpo primo de K", que viene dado por:

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

donde $\Gamma = \{F \subseteq K : F \leqslant K\}$. Este es 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. Si consideramos el único homomorfismo $\chi : \mathbb{Z} \to K$, tenemos que $Im\chi$ es el menor subanillo de K, por lo que estará contenido en el subcuerpo primo de K (al ser este un subanillo de K), que denotaremos por Π; es decir, $Im\chi \subseteq \Pi$. Aplicando el Primer Teorema de Isomofría sobre χ obtenemos que:

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

Si $p > 0$ tendremos (vimos anteriormente que p debe ser primo):

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

Por lo que $Im\chi$ es un subcuerpo de K, y como Π es el menor subcuerpo de K, tenemos que $\Pi \subseteq Im\chi$, lo que nos da la igualdad $\Pi = Im\chi \cong \mathbb{Z}_p$.

Si $p = 0$ tendremos entonces $\mathbb{Z} \cong Im\chi$, por lo que los cuerpos de fracciones de $\mathbb{Z}$ y de $Im\chi$ (a quien denotaremos por Q) han de ser isomorfos:

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

Como teníamos que $Im\chi \subseteq \Pi$, podemos calcular Q dentro[2] de Π, obteniendo que $Q \subseteq \Pi$, pero como Π es el menor subcuerpo de K, tendremos $\Pi \subseteq Q$, lo que nos da la igualdad $\Pi = Q \cong \mathbb{Q}$. □

Observación. Si $F \leqslant K$ extensión, entonces K es un espacio vectorial sobre F.

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:

[2]Si $A \subseteq B$ como subanillo, entonces el cuerpo de fracciones de A está dentro del cuerpo de fracciones de B, pero si B es un cuerpo, coincide con su cuerpo de fracciones.

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

- Si $[\mathbb{R} : \mathbb{Q}] = n$, entonces tendríamos que $\mathbb{R} \cong \mathbb{Q}^n$ como subespacios vectoriales, por lo que $\mathbb{R}$ no 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, por lo que su característica será un primo p de forma que su cuerpo primo será isomorfo a $\mathbb{Z}_p$. De esta forma, K será 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 $F \leqslant K$ extensión, $S \subseteq K$, 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[3].

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

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

Demostración. Veámoslo:

$\supseteq$) Sean $a, b \in \mathbb{Q}$, tenemos que $a, b, \sqrt{2} \in \mathbb{Q}(\sqrt{2})$, por lo que $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

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

[3]No confundir una extensión finitamente generada con que el conjunto $\{\alpha_1, \ldots, \alpha_t\}$ sea un sistema de generadores de K.

$\alpha = a + b\sqrt{2}$, buscamos calcular un elemento inverso al mismo que sea de la misma forma. Sea:

$$\beta = \frac{a}{a^2 - 2b^2} - \frac{b\sqrt{2}}{a^2 - 2b^2} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

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.

□

Observamos que tenemos $\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2$. Debemos tener en cuenta que aunque este resultado pueda generalizarse a otro más general como que:

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

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

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

Definición 1.9 (Cuerpo de descomposición)**.** Sea K un cuerpo, $f \in K[x]$ y $K \leqslant E$ extensión de cuerpos tal que f se descompone completamente en $E[x]$ como producto de polinomios lineales (es decir, de grado 1) y $E = K(\alpha_1, \ldots, \alpha_t)$ con $\alpha_1, \ldots, \alpha_t \in E$ las raíces de f, entonces diremos que E es un cuerpo de descomposición (o de escisión) de f sobre K.

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

- Si consideramos $x^2 + 1 \in \mathbb{R}[x]$, como $\mathbb{R} \leqslant \mathbb{C}$ y se cumple que $\mathbb{C} = \mathbb{R}(i, -i)$, tenemos que $\mathbb{C}$ es un cuerpo de descomposición de $x^2 + 1$.
- Por ejemplo, si $x^2 + 1 \in \mathbb{Q}[x]$, un cuerpo de descomposición en este caso es $\mathbb{Q}(i)$, ya que $\mathbb{Q} \leqslant \mathbb{Q}(i)$ y $\mathbb{Q}(i) = \mathbb{Q}(i, -i)$.

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

Ejemplo. Si tomamos $x^2 - 2 \in \mathbb{Q}[x]$, entonces un cuerpo de descomposición es $\mathbb{Q}(\sqrt{2})$.

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

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

Demostración. Veámoslo por doble inclusión:

[4]Fundamentado por el Teorema Fundalmental del Álgebra.

$\subseteq$) $F(S \cup T)$ es por definición el menor subucerpo 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 cuerpo 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 cuerpo 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, $F(S)(T) \subseteq F(S \cup T)$.

□

Ejemplo. Si tomamos $f = x^3 - 2 \in \mathbb{Q}[x]$, este polinomios tiene 3 raíces distintas, ya que su polinomio derivado[5] tiene como raíces el cero, que no es raíz de f. Las raíces de f son $\sqrt[3]{2}$ y el resto son dos raíces complejas, que se calculan usando las raíces terciarias de la unidad:

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

Por lo que $\omega^3 = 1$, de donde $\left(\sqrt[3]{2}\omega\right)^3 = 2$. Así que un cuerpo de descomposición de f es $\mathbb{Q}\left(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\right)$, que es igual a $\mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$:

Demostración. Por doble inclusión:

$\subseteq$) Como $\mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$ es un cuerpo que contiene a ω 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 ω, ya que:

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

Por tanto, el menor cuerpo que contiene a ω y $\sqrt[3]{2}$ ha de estar contenido en $\mathbb{Q}\left(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\right)$.

□

Nos preguntamos ahora por un cuerpo de descomposición de $x^2 + x + 1 \in \mathbb{Z}_2[x]$. Todavía no podemos dar respuesta a esta pregunta, por lo que necesitamos una noción más sofisticada de cuerpos de descomposición, a la que llegaremos desarrollando esta teoría.

[5] Recordamos que α es una raíz múltiple de f si, y solo si, α es una raíz de f'.

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 son:

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

Que es un subgrupo cíclico de orden n de $\mathbb{C} \setminus \{0\}$, generado por $e^{\frac{2\pi i}{n}}$. Cada uno de sus generadores se llama raíz $n-$ésima compleja primitiva de la unidad.

Un cuerpo de descomposición de $x^n - 1 \in \mathbb{Q}[x]$ es $\mathbb{Q}(\eta)$, donde η 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 1.10 (Elemento algebraico)**.** Sea $F \leqslant K$ extensión y $\alpha \in K$, diremos que α es algebraico sobre F si $f(\alpha) = 0$ para algún $f \in F[x] \setminus \{0\}$. En caso contrario, diremos que α es trascendente sobre F.

Proposición 1.5. *Sean $F \leqslant K$ extensión, $\alpha \in K$ algebraico sobre F. Existe un único polinomio mónico*[6] *irreducible $f \in F[x]$ tal que $f(\alpha) = 0$. Además, se tiene un isomorfismo de cuerpos $F(\alpha) \cong \dfrac{F[x]}{\langle f \rangle}$, donde $\langle f \rangle$ denota el ideal principal generado por f:*

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

Y además, $\{1, \alpha, \dots, \alpha^{degf-1}\}$ es una $F-$base de $F(\alpha)$. Así, $[F(\alpha) : F] = degf$.

Demostración. Definimos la aplicación "evaluación en α"

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

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 $\ker e_\alpha$ 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:

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

[6] El coeficiente líder es 1.

- Por el Primer Teorema de Isomorfía, e_α induce un isomorfismo de anillos:

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

Donde Ime_α 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 $\langle h \rangle \subseteq \langle f \rangle$. Como h es irreducible, tenemos que $\langle h \rangle$ es un ideal maximal, de donde $\langle h \rangle = \langle f \rangle$. Por tanto, existe $\lambda \in F$ de forma que $h = \lambda f$, pero como ambos son polinomios mónicos, ha de ser $\lambda = 1$, luego $h = f$.

- 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_α es un cuerpo, contenido en K: $Ime_\alpha \leqslant K$.

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 $\alpha \in Ime_\alpha$.

En definitiva, Ime_α 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_α, 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 $\mathcal{B} = \left\{1, \alpha, \ldots, \alpha^{degf-1}\right\}$ 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:

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

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 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 1.11 (Polinomio irreducible)**.** En las condiciones de la Proposición anterior, dicho único polinomio f recibe el nombre "polinomio irreducible (o mínimo) de α 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 α sobre F.

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 α es raíz.

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

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

Ejemplo. Veamos ejemplos de esta última definición:

- $\mathrm{Irr}(i, \mathbb{Q}) = x^2+1 \in \mathbb{Q}[x]$, 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 $\mathbb{Q}(i)$.
- $\mathrm{Irr}(\sqrt{2}, \mathbb{Q}) = x^2-2 \in \mathbb{Q}[x]$, que es irreducible en $\mathbb{Q}[x]$ por Eisenstein para $p=2$, luego $\{1, \sqrt{2}\}$ es una $\mathbb{Q}-$base de $\mathbb{Q}(\sqrt{2})$.
- $\mathrm{Irr}\left(e^{\frac{2\pi i}{3}}, \mathbb{Q}\right)$. 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:

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

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

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

$$x^3 - 1$$

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

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

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

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

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 1.6 (de la Torre)**.** *Si $F \leqslant K \leqslant L$ extensión:*

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

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 sistema de generadores del $F-$subespacio vectorial L, tendremos entonces que este mismo conjunto es un sistema de generadores del $K-$subespacio 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:

$$\begin{aligned}\alpha &= u_1(a_{1,1}v_1 + \ldots + a_{1,m}v_m) + \ldots + u_n(a_{n,1}v_1 + \ldots + a_{n,m}v_m) \\ &= a_{1,1}u_1v_1 + a_{1,2}u_1v_2 + \ldots + a_{1,m}u_1v_m + \ldots + a_{n,m}u_nv_m\end{aligned}$$

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

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

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

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

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

Ejemplo. Queremos calcular $\operatorname{Irr}\left(\sqrt{5} + \sqrt{-2}, \mathbb{Q}\right)$, 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:

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

Ahora, sabemos que el polinomio tiene grado 4, por lo que si encontramos uno de grado 4 del que α 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 α 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 1.7. *Sea $F \leqslant K$, $\alpha \in K$, tenemos que α 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 α 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 1.5 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 α^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:

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

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

□

Definición 1.12 (Extensión algebraica)**.** Una extensión $F \leqslant K$ se dice algebraica si todo elemento $\alpha \in K$ es algebraico sobre F.

Teorema 1.8. *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 α es algebraico sobre F.

$\Longleftarrow$) Suponemos que $K = F(\alpha_1, \ldots, \alpha_n)$ y que α_i es algebraico sobre F para todo $i \in \{1, \ldots, n\}$. Por el lema de la torre y la Proposición 1.5, 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 α_1 es algebraico sobre F, α_2 es algebraico sobre $F(\alpha_1)$, $\ldots$, α_n es algebraico sobre $F(\alpha_1, \ldots, \alpha_{n-1})$, entonces $[F(\alpha_1, \ldots, \alpha_n) : F] < \infty$.

Corolario 1.8.1. *Si $F \leqslant K$ extensión y llamamos:*

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

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

Demostración. Tenemos que ver que Λ 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 α y β 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 α algebraico sobre F, deducimos que la extensión es algebraica, luego $\alpha^{-1} \in \Lambda$.

En definitiva, Λ es un cuerpo contenido en K, luego es un subcuerpo de K y es claro que $F \leqslant K$ es algebraico. □

Definición 1.13 (Clausura algebraica)**.** El conjunto Λ 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 hacer $\mathbb{Q}(\sqrt[n]{2}) \subset \overline{\mathbb{Q}}$ y $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$, 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 $\text{Irr}(\sqrt{2}+i, \mathbb{Q})$.

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 α 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:

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

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 α 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:

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

Ejercicio 1.2.3. Calcular un cuerpo de descomposición de $x^4 + 14 \in \mathbb{Q}[x]$ 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 $\text{Irr}(\alpha, \mathbb{Q})$.

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 α es raíz, con lo que ya sabemos que este es el irreducible.

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

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

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

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

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

Con lo que tomando $f = x^3 - 3x^2 + 3x + 1 \in \mathbb{Q}[x]$ 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:

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

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:

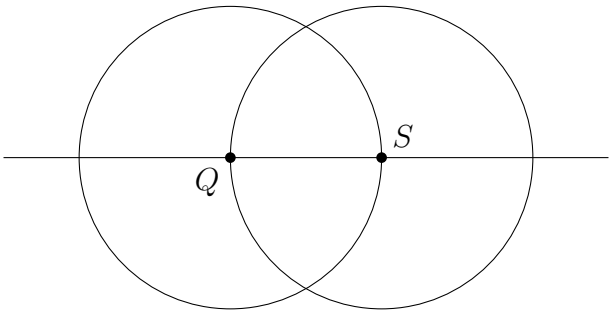


Figura 1.1: Prueba gráfica de que $S \subseteq S^c$.

- 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 Γ, el conjunto cuyos elementos son las rectas y circunferencias que pueden trazarse al considerar dos puntos distintos de S. Definimos además S^c, el conjunto de puntos obtenidos al intersecar cualesquiera dos elementos de Γ. 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 1.14. 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.

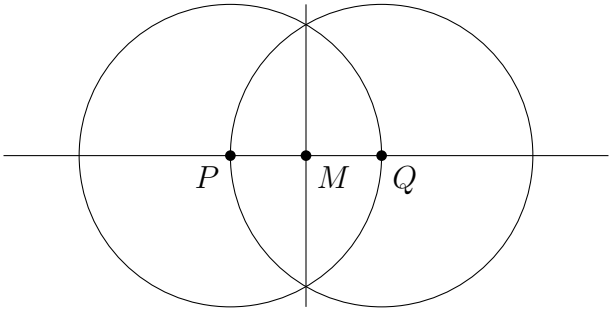


Figura 1.2: Construcción de la mediatriz.

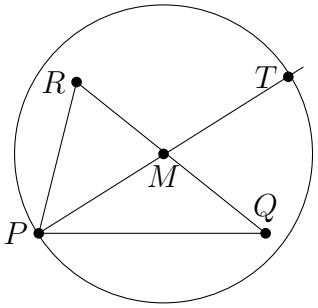


Figura 1.3: Completar el cuarto punto de un paralelogramo.

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 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 1.9. *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

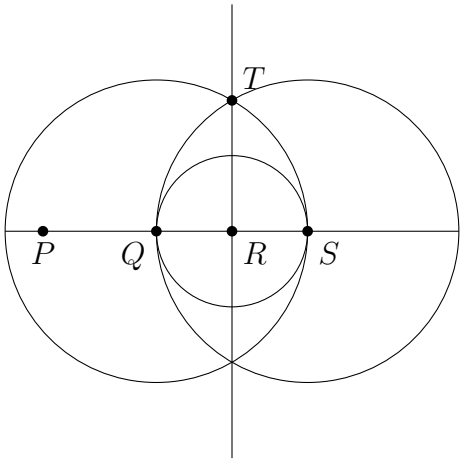


Figura 1.4: Trazar recta perpendicular por R.

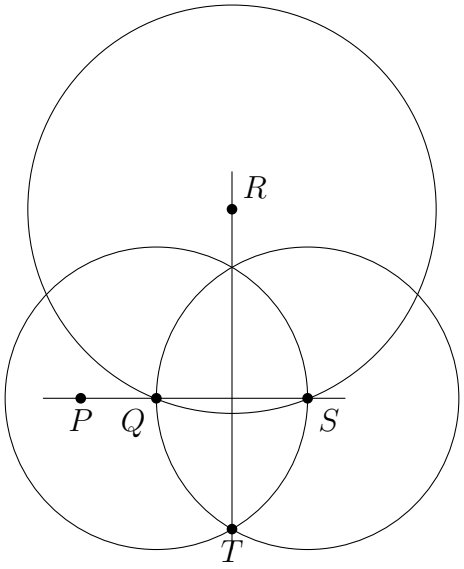


Figura 1.5: Trazar recta parpendicular por R.

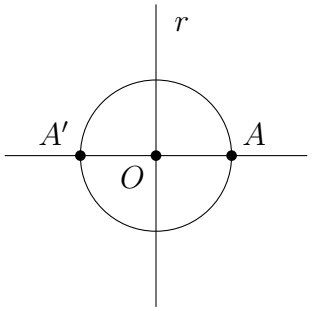
un segundo punto de corte entre las dos circunferencias, T, que unimos con R y obtenemos la situación pedida. El procedimiento se ilustra en la Figura 1.5.

□

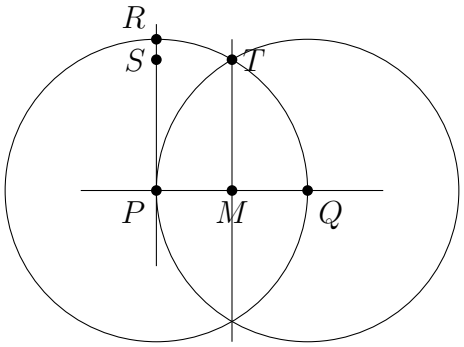
A partir del lema anterior, ya no será necesario recurrir a dichas construcciones cada vez que tengamos dos puntos P y Q que determinan una recta y queramos construir una recta perpendicular a ella que pase por un tercer punto R.

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

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



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



Trazar las dos circunferencias que definen los puntos P y Q, con lo que trazamos la 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 $0, 1 \in S$.

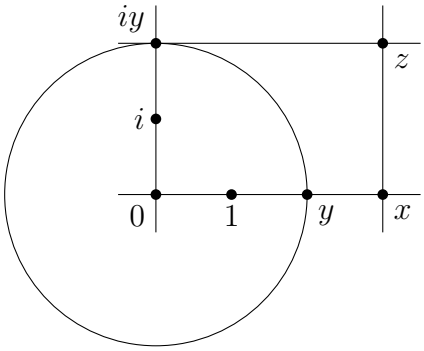


Figura 1.6: Obtención de x, y a partir de z.

Lema 1.10. *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 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 1.11. *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 1.10 que la suma de dos números complejos constructibles es constructible. Análogamente, si demostramos que el producto de

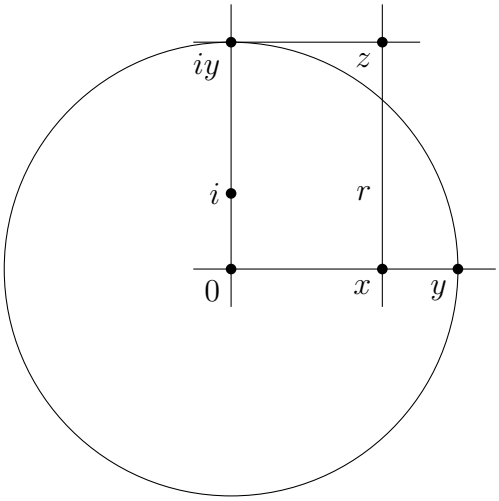


Figura 1.7: Obtención de z a partir de x e y.

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 $r' - r$.

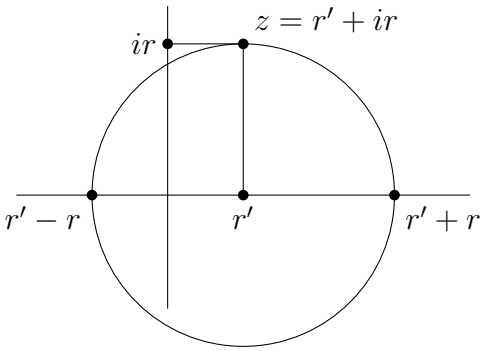
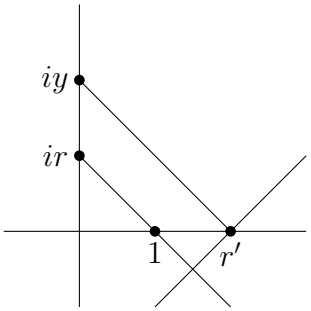


Figura 1.8: Obtención de $r' + r$ y $r' - r$ a partir de r y r'.

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.

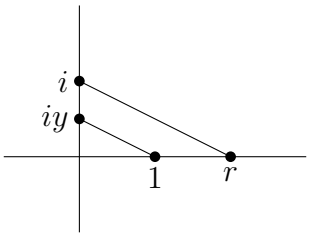
Trazaremos la recta que une el punto 1 con ir y trazaremos la recta paralela a esta última que pasa por el punto r' (podemos hacerlo ya que podemos trazar la recta perpendicular a $1(ir)$ que pasa por r' y a su vez la recta perpendicular a esta última que también pasa por r'), obteniendo el punto iy 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.



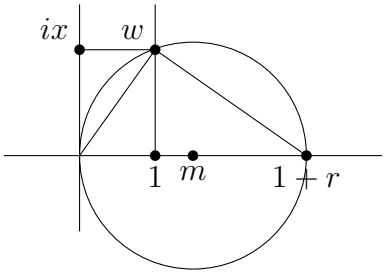
Ambos triángulos semejantes, luego:

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

□

Lema 1.12. *Si $z \in C(S)$, entonces $\sqrt{z} \in C(S)$.*

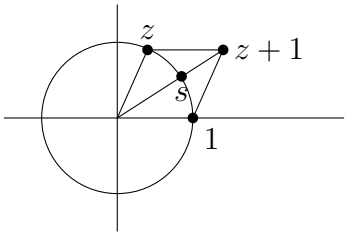
Demostración. Escribiendo z en forma polar, reducimos el problema al caso $|z| = 1$. Si tomamos $r > 0$ con $r \in C(S) \cap \mathbb{R}$, veamos entonces que $\sqrt{r} \in C(S) \cap \mathbb{R}$. Para ello, consideramos el punto $1 + r$ (anteriormente probamos que era constructible), trazamos el punto 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 $e^{i\theta} \in C(S) \cap \mathbb{R}$, entonces $e^{i\frac{\theta}{2}} \in C(S) \cap \mathbb{R}$. 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 1.13. *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 demsotrar 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 1.15. 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 $u_{i+1}^2 \in F(u_1, \ldots, u_i)$ para $i \in \{1, \ldots, t-1\}$

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

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

Teorema 1.14. *Sean $S \subset \mathbb{C}$, $F = \mathbb{Q}(S \cup \overline{S})$ 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:

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

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

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

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

$S \subseteq L$. Sea $z \in L$, queremos ver que $\overline{z} \in L$. 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 la conjugación es lineal, y tenemos que $F(\overline{u_1}, \ldots, \overline{u_t}) \in \mathcal{T}$, de donde $\overline{z} \in L$.

Ahora, si tomamos un elemento de L, este estará en algún K, ... □

Corolario 1.14.1. *$C(S)$ 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.*

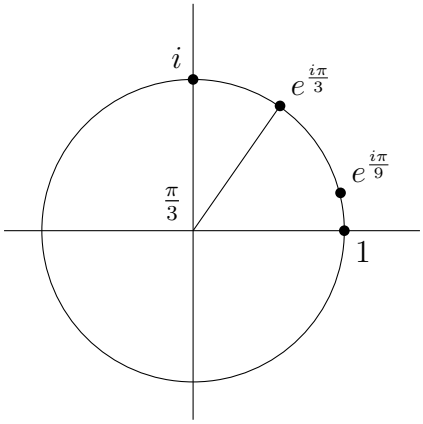
Corolario 1.14.2. *Todo número constructible ($F = \mathbb{Q}$) tiene grado sobre $\mathbb{Q}$ una potencia de 2.*

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

Ejemplo. Supongamos un cuadrado de lado l y una circunferencia de radio 1 centrada en 1. El círculo tiene área π. El área del cuadrado es l^2. Si l es constructible, entonces l^2 es constructible. Si $l^2 = \pi$, entonces π sería constructible, luego sería algebraico, pero esto contradice el Teorema de Lindemann, que dice que π 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 $60^{\underline{0}}$ no se puede trisecar con regla y compás.



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

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:

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

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[7] $2r = \pm 1$. 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 $60^{\underline{o}}$ no se puede trisecar.

[7] Observando los coeficientes de $x^3 - 3x - 1$ y la forma que tienen que tener las raíces racionales.

1.4. Homomorfismos de cuerpos

Lema 1.15. *Sea F un cuerpo y I un ideal suyo, entonces $I = \{0\}$ o $I = F$.*

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

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

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

Lema 1.16. *Sea $\sigma : F \to A$ un homomorfismo de anillos donde F es un cuerpo y A es no trivial, entonces σ 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 $\sigma(1) = 1$), 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 σ un homomorfismo de anillos tenemos que $Im\sigma$ es subanillo de A. □

Definición 1.16 (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 1.17. 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[8]:

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

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 α.

$\supseteq$) 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:

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

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 1.17. *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 $K = F(\alpha)$.

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

Demostración. La demostración se deduce del ejemplo anterior. □

Proposición 1.18. *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^σ.*

Demostración. Suponemos sin pérdida de generalidad que f es mónico. Vamos a ver que existe $F \xrightarrow{\sigma} L$ tal que f^σ 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 1.17, 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^τ en $K[x]$ (sabemos que al menos $s \geqslant 1$, puesto que α es raíz de h^τ):

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

  Con uno de los β_i es α y k sin raíces en K y de grado menor que el de h^τ. 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^ρ 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^σ se descompone como producto de lineales en $L[x]$.

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

Definición 1.18. A un homomorfismo $\sigma : F \to E$ como el de la Proposición anterior se le llama cuerpo de descomposición de f.

Respecto a esta última definición, debemos tener claro que antes hablábamos de 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 hace el papel de la extensión) le llamamos ahora cuerpo de descomopsición, si K cumple unas propiedades relativas a f^σ.

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^σ (usando que $\alpha^2 + \alpha + 1 = 0$):

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

tenemos que σ 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:

- $K = \{0, 1, \alpha, 1 + \alpha\}$.

  Donde vemos que $1 + \alpha$ es distinto del resto porque $\{1, \alpha\}$ es una $\mathbb{F}_2-$base de K. La condición $\alpha^2 + \alpha + 1 = 0$ también nos dice que $\alpha + 1 = \alpha^2$:

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

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 $\mathbb{F}_2(a)$:

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

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 $x + a^2$:

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

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 dos cuerpos son isomorfos entre sí, e isomorfos con todo otro cuerpo que contenga 8 elementos, lo que nos permitirá notarlos a todos por $\mathbb{F}_8$.

Lema 1.19. *Sea $F \xrightarrow{\sigma} K$, $p \in F[x]$ irreducible, si $\alpha \in K$ es raíz de p^σ, 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 1.17 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 $\langle p \rangle \subseteq \ker(\overline{\sigma_\alpha})$, pero como p es irreducible, tenemos que $\langle p \rangle$ es maximal, con lo que $\langle p \rangle = \ker(\overline{\sigma_\alpha})$. 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 1.19. 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 τ si:

$$\eta\sigma = \tau$$

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

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

Proposición 1.20 (Extensión de homomorfismos)**.** *Si tenemos dos homomorfismos de cuerpos:*

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

Si $p \in F[x]$ irreducible y $\alpha \in K$ con $p^\sigma(\alpha) = 0$, si $\mathcal{R} \subseteq E$ es el conjunto de todas las raíces de p^τ y además $K = \sigma(F)(\alpha)$, 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 η de τ de forma que $\eta(\alpha) = \beta$. Usando el Lema 1.19, 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 σ_α como τ_β aplicado sobre constantes son iguales a σ y a τ, 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 α 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 η, η' son $\sigma-$extensiones de τ, 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. □

Obsevemos que en esta última proposición hemos probado además que:

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

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

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

Lema 1.21. *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 1.22. *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 σ 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 σ. 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^τ 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 Π 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 $\sigma = \iota$.

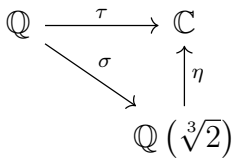
Mostramos a continuación un ejemplo básico de la proposición de extensión.

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 η 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 $\tau : \mathbb{Q} \to \mathbb{C}$, 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 τ hay.



Por lo que el probelma 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:

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

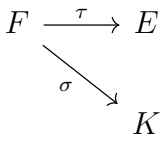
donde η_i está determinado (según la proposición de extensión) por:

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

Como cada uno de los η_j es un homomorfismo definido sobre $\mathbb{Q}\left(\sqrt[3]{2}\right)$ con base $\{1, \sqrt[3]{2}\}$, es suficiente definirlos sobre 1 (todos cumplirán $\eta_j(1) = 1$, por ser homomorfismos) y 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 1.23. *Sean dos homomorfismos de cuerpos:*



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

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

Demostración. La idea es similar a la de la Proposición 1.22, por inducción sobre $n = [K : \sigma(F)]$:

- Para $n = 1$, tenemos que $K = \sigma(F)$, con lo que σ 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^σ, 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^τ hay en E. Sin embargo, como f^τ se factoriza como producto de polinomios de grado 1 en $E[x]$ y p^τ es un factor de f^τ, 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^σ tiene $degf$ raíces distintas, entonces p^σ 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 τ, σ_1 y σ_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 η_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 σ_2-extensiones de η_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 σ_2 extensiones de η_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 ρ 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 1.24 (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 1.23 nos dice que como f^τ 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 η es sobreyectiva, pero como era un homomorfismo de cuerpos, concluimos que η es biyectiva, con lo que η 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 1.18, sabemos que podemos encontrar $\theta : \sigma(F) \to K$ cuerpo de descomposición de f^σ. Trataremos ahora de extender θ 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^θ (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 1.25. *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 1.26 (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 1.25 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 1.20 (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 Π 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 1.27. *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 σ 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 como es $F-$lineal 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 1.28. *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 $\iota : F \to K$ la aplicación inclusión, tenemos por la tercera propiedad 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 1.29. *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 1.25 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 1.28, 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 oren 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 α 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 α 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 α 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 π son trascendentes:

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

Veamos cada caso:

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

  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 $\mathbb{Q}$.
- π^2
- e^2-i
- $i\sqrt{i}+\sqrt{2}$
- $\sqrt{1-\sqrt[3]{2}}$

  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:
  $$(x^2-1)^3 = x^6-3x^4+3x^2-1 = -2$$
  Por lo que si tomamos $f = x^6-3x^4+3x^2+1 \in \mathbb{Q}[x]$, tenemos que $\sqrt{1-\sqrt[3]{2}}$ es raíz de f, con lo que es algebraico sobre $\mathbb{Q}$.
- $\sqrt{\pi}$

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

  Por el Lema de la Torre, tenemos que:

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

  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:

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

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

Ejercicio 1.7.4. Sea $F\leqslant K$ una extensión de cuerpos, $\alpha\in K$ y n natural no nulo. Demostrar que α es algebraico sobre F si, y solo si, α^n es algebraico sobre F.

$\Longrightarrow$) Si α es algebraico sobre F entonces la extensión $F\leqslant F(\alpha)$ es algebraica, y tenemos que $\alpha^n\in F(\alpha)$, por lo que α^n es algebraico sobre F.

$\Longleftarrow$) Si α^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 α 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 α es algebraico sobre F si, y solo si, β es algebraico sobre F:

$\Longrightarrow$) Si α 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 β es algebraico sobre F.

$\Longleftarrow$)

Ejercicio 1.7.6. Calcular $\mathrm{Irr}(\alpha, \mathbb{Q})$ para los siguientes valores de α:

$$3 + \sqrt{2}, \sqrt{3} - \sqrt[4]{3}, \sqrt[3]{2} + \sqrt[3]{4}$$

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 α 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 $\alpha = \sqrt{3} - \sqrt[4]{3}$.

c) Para $\alpha = \sqrt[3]{2} + \sqrt[3]{4}$.

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

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 $\mathrm{Irr}\left(\sqrt[3]{5}, \mathbb{Q}\right) = x^3 - 5$ por Eisenstein para $p = 5$.

- $\left[E : \mathbb{Q}\left(\sqrt[3]{5}\right)\right] = 2$, ya que $\mathrm{Irr}\left(\sqrt{-2}, \mathbb{Q}\right) = x^2 + 2$, 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 primitiv de la unidad.

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

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:

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

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.

Tomamos $x^4+x+1 \in \mathbb{F}_2[x]$, y comprobamos que es irreducible para ello, comporobamos que no tiene raíces y que no puede escribirse como producto de dos polinomios irreducibles de grado 2. Como el único polinomio irreducible de grado 2 en $\mathbb{F}_2[x]$ es $x^2 + x + 1$, basta ver que no es cuadrado del mismo. Como consecuencia:

$$\frac{\mathbb{F}_2[x]}{\langle x^4 + x + 1\rangle}$$

es un cuerpo, que tiene dimensión 4 (el grado de $x^4 + x + 1$) sobre $\mathbb{F}_2$, con lo que el cuerpo "es" $\mathbb{F}_{16}$. Tomamos $b = x + \langle x^4 + x + 1\rangle$ y se tiene.

Para ver ahora todos los homomorfismos de cuerpos, conocido:

$$p = Irr(a, \mathbb{F}_2) = x^2 + x + 1$$

$$\begin{array}{ccc} \mathbb{F}_2 & \xrightarrow{\iota} & \mathbb{F}_2(a) \\ & \searrow^{\iota} & \downarrow \eta \\ & & \mathbb{F}_2(b) \end{array}$$

tenemos que hay tantos homomorfismos entre dichos cuerpos como raíces de p. La Propiedd de Extensión nos dice que los homomorfismos que me piden están parametrizados por las raíces de p en $\mathbb{F}_2(b)$.

Observemos que en este ejercicio (usando el ejercicio siguiente), cada η 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 η 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 $p = \text{car}(\mathbb{F}_q)$.

Ejercicio 1.7.11. Demostrar que los anillos $\frac{\mathbb{Z}[i]}{\langle 3\rangle}$ y $\frac{\mathbb{F}_3[x]}{\langle x^2+x+2\rangle}$ son isomorfos sin necesidad de dar un isomorfismo concreto. ¿Serías capaz de darlo? ¿Y de calcularlos todos?

Tenemos que $\frac{\mathbb{F}_3[x]}{\langle x^2+x+2\rangle}$ es un cuerpo, porque $\mathbb{F}_3[x]$ es un cuerpo y x^2+x+2 es irreducible. Además, tiene dimensión 2 sobre un cuerpo de 3 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 α 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:

   $$\left.\begin{array}{l} 1 = a^2 + 3b^2 \\ 2 = 2ab \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} b = \frac{1}{a} \\ 1 = a^2 + 3\frac{1}{a^2} \end{array}\right\} \Longrightarrow a^2 = a^4 + 3$$

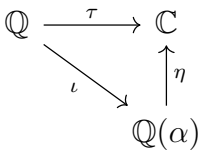
   $$\Longrightarrow a^2 = \frac{1 \pm \sqrt{1-12}}{2} \notin \mathbb{Q} \Longrightarrow a \notin \mathbb{Q}$$

   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 η que cumplen:



   donde τ, ι 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 η_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 η_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 η 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 $\mathrm{Irr}(\alpha, \mathbb{Q}) = x^2 - x - 1$.

2. Extensiones de Galois

2.1. Extensiones de Galois

Del Capítulo anterior recordamos la Proposición 1.27, 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.

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:

$$K^G = \{a \in K : \sigma(a) = a \quad \forall \sigma \in G\}$$

Se verifica que K^G es subcuerpo de K (hágase), con lo que tenemos la extensión $K^G \leqslant K$.

Notación. Para no confundir la notación de "subgrupo" con la de "subcuerpo", siempre que tengamos H un subgrupo de G lo notaremos por $H < G$.

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

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

Demostración. Sea $n = |G|$, suponemos que $G = \{\sigma_1, \ldots, \sigma_n\}$ 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 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 número de componentes no nulas mínimo 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 $v_l = 1$, tras dividir todas las componentes del vector entre la $l-$ésima componente. Si escribimos la igualdad $vA = 0$:

$$\sum_i v_i\sigma_j(\alpha_i) = 0 \qquad \forall j \in \{1, \ldots, n\}$$

Y observamos que para obtener la dependencia lineal de los α_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. Tomamos ahora cualquier $\sigma \in G$ y definimos:

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

Si usamos esto para σ_k:

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

Aplicamos σ_k a la igualdad anterior, con lo que:

$$\sum_i \sigma_k(v_i)\sigma_k(\sigma_j(\alpha_i)) = 0 \qquad \forall j \in \{1, \ldots, n\}$$

Observemos que:

$$G = \{\sigma_1, \ldots, \sigma_n\} = \{\sigma_k\sigma_1, \ldots, \sigma_k\sigma_n\}$$

y lo que hemos hecho ha sido permutar las ecuaciones, variando los coeficientes, con lo que:

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

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 si miramos sus componentes $l'-$ésimas, estas son distintas. Sin embargo, las componentes $l-$ésimas 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:

$$\sum_i v_i \sigma_j(\alpha_i) = 0 \qquad \forall j \in \{1, \dots, n\}$$

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

$$\sum_i v_i \alpha_i = 0, \qquad v_i \in K^G$$

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 es subgrupo de $\mathrm{Aut}(K)$, entonces $G < \mathrm{Aut}_{K^G}(K)$.*
4. *Si $F \leqslant K$, entonces $F \leqslant K^{\mathrm{Aut}_F(K)}$.*

Demostración. Demostramos cada uno de los apartados de forma muy sencilla:

1. Sea $a \in K^G$, si tomamos $\sigma \in H < G$, tendremos que $\sigma(a) = a$, con lo que $a \in K^H$.
2. Sea $\sigma \in \mathrm{Aut}_E(K)$, si tomamos $\lambda \in F \leqslant E, x \in K$ observamos que:

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

   Por lo que $\sigma \in \mathrm{Aut}_F(K)$.
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 $x \in F \leqslant K$ y $\sigma \in \mathrm{Aut}_F(K)$, entonces:

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

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

□

Veamos ahora dónde se da la igualdad en los apartados 2 y 3, que en general no se dan.

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 anterior nos dice que $G \leqslant \mathrm{Aut}_{K^G}(K)$, y la Proposición de Artin nos dice que $[K : K^G] \leqslant |G|$, con lo que en particular la extensión es finita, luego podemos aplicar también la Proposición 1.27 en $(*)$:

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

Por lo que $G = \mathrm{Aut}_{K^G}(K)$. □

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:

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

$$\begin{array}{l} \sqrt[3]{2} \overset{\eta_{1,2}}{\longmapsto} w\sqrt[3]{2} \overset{\eta_{1,2}}{\longmapsto} w^2 w \sqrt[3]{2} = \sqrt[3]{2} \\ \quad w \longmapsto w^2 \longmapsto w \end{array}$$

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 $degf\geqslant 1$, 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:

- f es separable.
- f tiene $degf$ raíces distintas en su cuerpo de descomposición.
- $\mathrm{mcd}(f,f')=1$.

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.

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 1.8 observamos que solo usaba que los α_i eran algebraicos, por lo que podemos concluir que $F \leqslant K$ es finita.

Sea $F' = K^{\mathrm{Aut}_F(K)}$, es claro que $F \leqslant F'$. Además, como $F \leqslant K$ es finita, tendremos que $\mathrm{Aut}_F(K)$ es finito. Por el Teorema 2.3 tenemos que tomando $G = \mathrm{Aut}_F(K)$, se tiene que:

$$\mathrm{Aut}_F(K) = \mathrm{Aut}_{F'}(K)$$

K es cuerpo de descomposición de $f \in F[x]$ y como $F \leqslant F'$, tenemos también que K es cuerpo de descomposición de $f \in F'[x]$. Como f es separable, tenemos que:

$$[K : F] = |\,\mathrm{Aut}_F(K)| = |\,\mathrm{Aut}_{F'}(K)| = [K : F']$$

Con $F \leqslant F'$, por lo que el Lema de la Torre nos dice que $F = F'$

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

iii) $\Longrightarrow$ *iv)* La Proposición de Artin nos dice que $K^G = F \leqslant K$ es finita.

Sean $\alpha \in K$ y $h = \mathrm{Irr}(\alpha, F) \in F[x]$, como G actúa sobre K, podemos considerar la órbita de α (considerando todos sus elementos distintos):

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

y podemos considerar el polinomio:

$$g = \prod_{i=1}^{t}(x - \alpha_i) = \sum_{j=0}^{t} a_j x^j \in K[x]$$

veamos que $a_j \in F$ para todo $j \in \{1, \dots, t\}$, usando que $F = K^G$. Dado $\sigma \in G$:

$$\prod_{i=1}^{t}(x - \sigma(\alpha_i)) = g^\sigma = \sum_{j=0}^{t} \sigma(a_j)x^j$$

y vemos que $g = \prod_{i=1}^{t}(x - \sigma(\alpha_i))$, puesto que al aplicar σ sobre los elementos de la órbita los permuta, con lo que de la igualdad de la derecha deducimos que $\sigma(a_j) = a_j$, para todo $j \in \{1, \dots, t\}$, con lo que $a_j \in F[x]$ para todo $j \in \{1, \dots, t\}$, luego $g \in F[x]$.

Por una parte $g(\alpha) = 0$, puesto que $\alpha \in Orb(\alpha)$. Como $h = \text{Irr}(\alpha, F)$, tenemos que h divide a g.

Por otra parte, cada α_i es raíz de h, ya que $h(\alpha) = 0$ deducimos que si tomamos $\sigma \in G$, entonces:

$$0 = \sigma(0) = \sigma(h(\alpha)) = h(\alpha_i)$$

Como se cumple para todo $\sigma \in G$, tenemos pues que $h(\alpha_i) = 0$ para todo $i \in \{1, \dots, t\}$. Como los elementos α_i son distintos, tenemos que $degh \geqslant t$, pero como g es un polinomio mónico de grado t cuyas raíces son exactamente $Orb(\alpha)$, tenemos que $g = h$. Hemos probado que la extensión es normal y separable.

$iv) \Longrightarrow i)$ Como $F \leqslant K$ es finita, tenemos entonces que existen $\alpha_1, \dots, \alpha_s \in K$ algebraicos de forma que $K = F(\alpha_1, \dots, \alpha_s)$. Podemos por tanto considerar $f_i = \text{Irr}(\alpha_i, F)$, y tomamos como f el producto de los f_i eliminando repeticiones (es decir, multiplicamos todos los f_i distintos). Como la extensión es normal y separable, cada uno de los f_i se descompone como producto de polinomios lineales mónicos distintos. De donde f es un polinomio separable[1], 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 corresponderá con 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 α bajo G que ha aparecido en la demostración, $\{\alpha_1, \dots, \alpha_s\}$ se llaman conjugados de α bajo G.

Se trata de la generalización del concepto "conjugado" de un número complejo.

[1] Notemos que para eso eliminamos antes las repeticiones.

Definición 2.6 (Extensión de Galois)**.** Una extensión $F \leqslant K$ se dice de Galois si es finita, normal y separable.
El grupo $\mathrm{Aut}_F(K)$ recibe el nombre Grupo de Galois de la extensión.

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 puede compartir raíces entre sí por ser irreducibles, 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. □

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.

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

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 inversa 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 sus subextensiones de $F \leqslant K$ correspondientes por la anterior biyección, entonces:
$$(H_2 : H_1) = [E_1 : E_2]$$

Demostración. La primera aplicación está bien definida, puesto que si $H \in \text{Subgr}(G)$, entonces:

$$\{id_K\} < H < G$$

de donde el Lema 2.2 nos dice que:

$$K = K^{\{1\}} \geqslant K^H \geqslant K^G \overset{(*)}{=} F$$

donde en $(*)$ hemos usado el Teorema 2.4. Para la segunda aplicación, si $E \in \text{Subex}(F \leqslant K)$, tenemos que:

$$F \leqslant E \leqslant K$$

de donde el Lema 2.2 nos dice:

$$\{id_K\} = \text{Aut}_K(K) < \text{Aut}_E(K) < \text{Aut}_F(K) = G$$

por lo que $\text{Aut}_E(K) \in \text{Subgr}(G)$.

Para ver ahora que es biyectiva, demostraremos que las dos aplicaciones son inversas la una de la otra:

- Si $H \in \text{Subgr}(G)$, tenemos entonces que:

  $$H \longmapsto K^H \longmapsto \text{Aut}_{K^H}(K) \overset{(*)}{=} H$$

  donde en $(*)$ hemos usado el Teorema 2.3, puesto que $F \leqslant K$ es finita al ser de Galois.

- Si $E \in \text{Subex}(F \leqslant K)$, tenemos que:

  $$E \longmapsto \text{Aut}_E(K) \longmapsto K^{\text{Aut}_E(K)} \overset{(*)}{=} E$$

  donde en $(*)$ usamos el Teorema 2.4.

En consecuencia, la aplicación enunciada es un anti-isomorfismo de conjuntos ordenados.

Para la segunda parte, si $H_1 \subseteq H_2$ son subgrupos de G y $E_2 \leqslant E_1$ son las subextensiones de $F \leqslant K$ correspondientes de dichos subgrupos (es decir, $E_1 = K^{H_1}$, $E_2 = K^{H_2}$), sabemos entonces que:

$$|H_2| = [K : E_2] = [K : E_1][E_1 : E_2] = |H_1|[E_1 : E_2]$$

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 $\tau(\alpha) = \alpha^p$. 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 G de Galois, sean $H \in \mathrm{Subgr}(G)$ y $E \in \mathrm{Subex}(F \leqslant K)$ su correspondencia 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 $\sigma H \sigma^{-1} \in \mathrm{Subgr}(G)$, 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 correspondencia mediante la conexión:*

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

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

Demostración. Si $H \lhd G$, el Lema nos dice que $\sigma(E) = E \quad \forall \sigma \in G$. Definimos $r : G \to \mathrm{Aut}_F(E)$ por $r(\sigma) = \sigma\big|_E$, que:

- Está bien definido.
- r es un homomorfismo de grupos.
- $\ker(r) = \mathrm{Aut}_E(K) = H$.
- r es sobreyectivo, ya que:

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

Donde en $(*)$ usamos el Primer Teorema de Isomorfía de grupos, con lo que la imagen tiene el mismo cardinal que el conjunto de llegada. Además, obtenemos que (por el Primer Torema de Isomorfía de Grupos):

$$\mathrm{Aut}_F(E) \cong \frac{G}{H}$$

Dado $\alpha \in E^{\mathrm{Aut}_F(E)}$, entonces:

$$\alpha = r(\sigma)(\alpha) = \sigma(\alpha) \qquad \forall \sigma \in G$$

de donde $\alpha \in F$, luego $E^{\mathrm{Aut}_F(E)} = F$ y el Teorema (piedra angular) nos dice que $F \leqslant E$ es de Galois. Falta ver que es de Galoois, raices de un polinomio separable, llamamos f al producto de todos los generadores menos algo, aplica σ, que permita las cosas, luego está en E y el Lema dice que es normal. □

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. Calculemos primero las raíces de f. 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 podemos hacerlo con β, 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 $\mathbb{Q}(\alpha)$.

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 2.4 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 $\iota : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha, i\sqrt{2}) = K$ 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 $\left[\mathbb{Q}\left(i\sqrt{2}\right) : K\right] = 4$ que por la conexión de Galois corresponderá con un subgrupo de orden 4. Por lo que:

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

que es normal porque:

- $\mathbb{Q}\left(i\sqrt{2}\right) \leqslant K$ 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, así como todos los subcuerpos de K.

Sabemos ya que $\mathrm{Aut}_{\mathbb{Q}(i\sqrt{2})}(K) = \langle \eta_{1,0}, \eta_{2,0} \rangle$, y para terminar de hallar los subgrupos, nos falta por localizar otro subgrupo isomorfo al de Klein. Como $\alpha = \sqrt{\sqrt{3}+1} \in K$, tenemos que $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{3}) \leqslant K$ de Galois, por lo que tiene que corresponderse con un subgrupo de 4 elementos, que buscaremos cuál es. Probemos con el cíclico, tomamos $\eta_{2,1}$ y:

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

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:

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

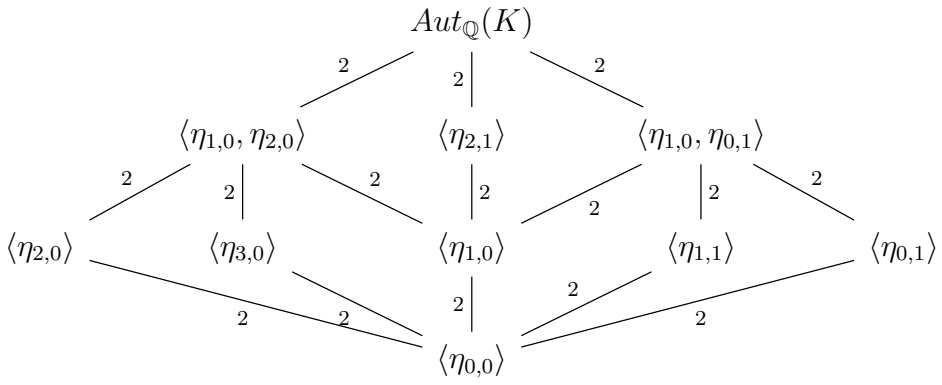
Por lo que $\mathbb{Q} \leqslant \mathbb{Q}(i\sqrt{6})$ de grado 2, tenemos que:

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

También sabemos por la conexión de Galois que:

$$K^{\langle \eta_{2,1} \rangle} = \mathbb{Q}(i\sqrt{6})$$

En resumen, tenemos que:



Y por la conexión de Galois podemos obtener:

- Los tres primeros lo sabíamos ya cuando nos pusimos a buscar el grupo cíclico y los dos isomorfos al de Klein.
- Observeos que $\langle \eta_{1,0} \rangle$ es el mayor subgrupo contenido en la intersección $\langle \eta_{1,0}, \eta_{2,0} \rangle$ y $\langle \eta_{1,0}, \eta_{0,1} \rangle$, por lo que obtenemos $\mathbb{Q}(i\sqrt{2}, \sqrt{3})$.
- Más aún, sabíamos ya que $\mathbb{Q}(\alpha)$ era una extensión de grado 4, por lo que buscamos por qué automorfismo es estable, que es el $\eta_{0,1}$.

  También lo podríamos haber visto porque:

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

  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 α con β 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:

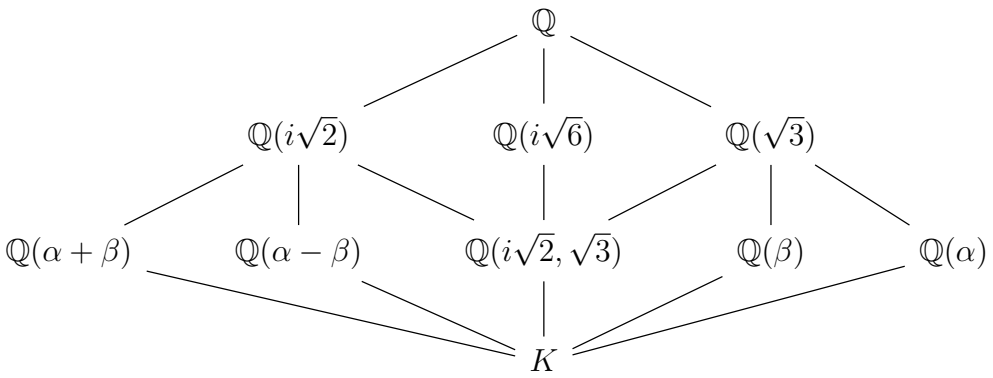


Figura 2.1: Todos los subcuerpos de K.

2.3. El Teorema Fundamental del Álgebra

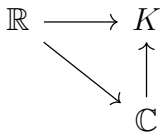
Se tiene que $\mathbb{C}$ es el cuerpo de descomposición de $x^2+1 \in \mathbb{R}[x]$, y $[\mathbb{C}:\mathbb{R}]=2$, por lo que $|\operatorname{Aut}_{\mathbb{R}}(\mathbb{C})|=2$, que son:

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

con σ 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, 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 $|\operatorname{Aut}_{\mathbb{R}}(K)|$ es múltiplo de 2, por lo que $G=\operatorname{Aut}_{\mathbb{R}}(K)$ 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.

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

Sea $\alpha \in K^H$, consideramos $\mathrm{Irr}(\alpha, \mathbb{R})$, que tiene grado impar por el Lema de la Torre, $\mathbb{R} \leqslant K(\alpha) \leqslant K^H$. Si el polinomio es irreducible y de grado impar, sabemos (por PreBolzano) que $deg(\mathrm{Irr}(\alpha, \mathbb{R})) = 1$, de donde $\alpha \in \mathbb{R}$. Por lo que $K^H = \mathbb{R}$, luego $G = H$, de donde G es un $2-$grupo.

Así, $\mathrm{Aut}_{\mathbb{C}}(K)$ es un $2-$grupo (por ser subgrupo de un $2-$grupo). 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 $\beta \in K^N$ y $\mathrm{Irr}(\beta, \mathbb{C})$ tiene 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. Suponiendo que f es mónico:

- Si es de grado 1 está.
- Si no, tiene una raíz, α, por lo que $(x - \alpha)(x - \overline{\alpha}) \ldots$

□

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

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

donde cada uno de ellos está determinado por:

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

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 η_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 $\eta_{1,1}$:

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

  Por lo que su orden es 2.

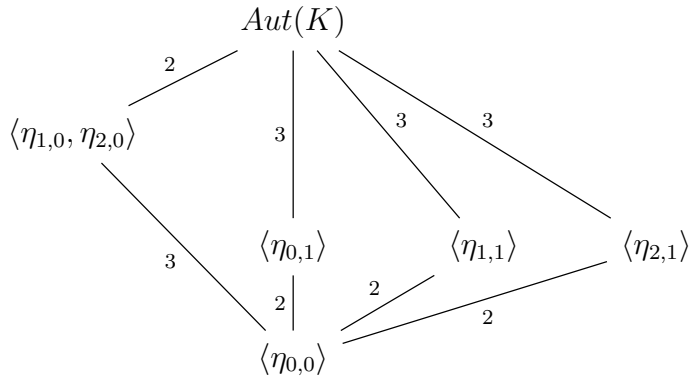
Tenemos por tanto:

$\eta_{0,0}$	$\eta_{1,0}$	$\eta_{2,0}$	$\eta_{0,1}$	$\eta_{1,1}$	$\eta_{2,1}$
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 $\mathrm{Aut}(K)$. 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 $\mathrm{Aut}(K)$ 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 $\mathrm{Aut}(K)$ 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:

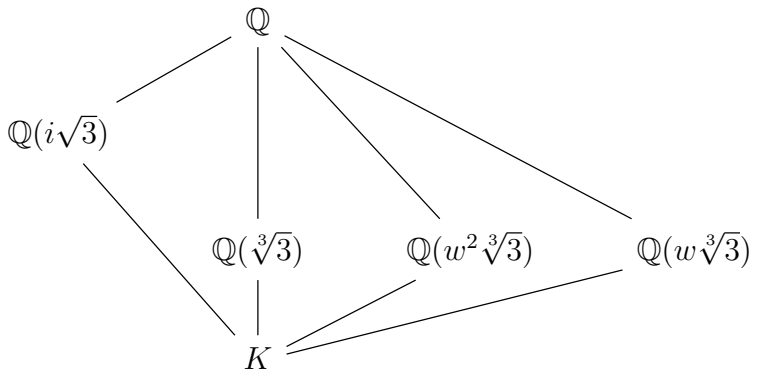
- Para $\mathbb{Q}\left(w^2\sqrt[3]{3}\right)$, veamos que $\eta_{1,1}$ deja fijo a este elemento:

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

  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.

Definición 3.1. Sea $f \in F[x]$ no constante, mónico y sean $\alpha_1, \ldots, \alpha_n$ sus raíces (repetidas tantas veces como indique su multiplicidad) en algún cuerpo K de descomposición de f. El discriminante de f es:

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

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

Observación. 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[1] 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] Observemos que por ser f separable y K cuerpo de descomposición suyo tenemos siempre por el Teorema 2.4 que la exntesión $F \leqslant K$ es de Galois.

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

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

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

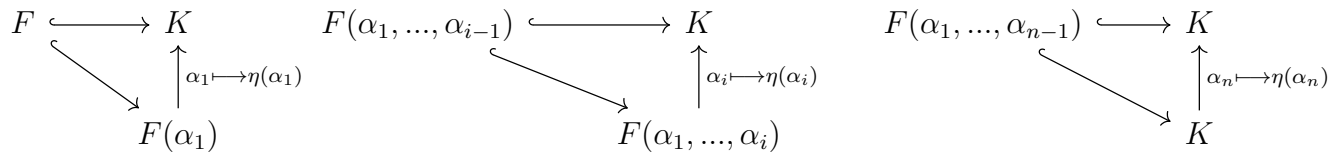
- La aplicación es un homeomorfismo, pues si $\sigma, \tau \in \mathrm{Aut}_F(K)$ tenemos entonces que:

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

Además dicho homomorfismo de grupos es siempre inyectivo, pues la Proposición de Extensión nos dice que cada automorfismo del grupo de Galois queda 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 $\{\alpha_1,\dots,\alpha_n\}$, tendremos entonces que $\sigma = \tau$, lo que nos prueba la inyectividad del homomorfismo de grupos.
De esta forma, como $\mathrm{Sim}(\alpha_1,\dots,\alpha_n) \cong S_n$, podemos ver siempre el grupo de Galois de f como subgrupo de S_n, aquel que permuta los índices de las raíces de f:

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

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

Observación. Si tomamos $\sigma \in \mathrm{Aut}_F(K)$, una vez visto que σ 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, $\Delta(f) \in F \iff G \leqslant A_n$.

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 elementos 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 tnemos dos situaciones posibles:

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

- 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 "$\mathrm{Disc}(f)$ es un cuadrado en F".

Ejercicio 3.1.1. Sea $f \in \mathbb{R}[x]$ con $deg f = 3$, discutir el número de raíces reales de f según el signo de $\mathrm{Disc}(f)$.

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[2]. 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. Por tanto, 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[3]) es:

$$\mathrm{Disc}(f) = -4p^3 - 27q^2$$

Proposición 3.2. *Sea $f \in F[x]$ separable con grupo de Galois G*

$$f \text{ es irreducible} \iff G \text{ actúa transitivamente sobre las raíces de } f$$

En tal caso, $deg f$ divide a $|G|$.

Demostración. Sea K el cuerpo de descomposición de f, tenemos que $G = \mathrm{Aut}_F(K)$.

$\Longrightarrow$) 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 σ se extiende 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. Además, $\sigma(\alpha)$ es raíz de g, para todo $\sigma \in G$, y como G actúa transitivamente sobre las raíces de f; toda raíz de f es de g, con lo que $f = g$, de donde f es irreducible.

Finalmente, para ver que $deg f$ divide a $|G|$, si α es raíz de f, tenemos entonces $[F(\alpha) : F] = deg f$, que divide a $[K : F]$ por el Lema de la Torre, y $|G| = [K : F]$. □

Corolario 3.2.1. *Por tanto, a la hora de buscar el grupo de Galois de un polinomio irreducible, descartaremos automáticamente los subgrupos de S_n no transitivos.*

Ejemplo. Sea $f \in F[x]$ separable e irreducible:

1. Si $deg f = 1$, su grupo de Galois es la identidad, como único elemento de S_1.

[2]Hay una teoría desarrollada sobre esto, siempre se obtienen funciones simétricas en las raíces del polinomio.

[3]Sin término cuadrático.

2. Si $degf = 2$, el cuerpo de Galois de f tiene grado 1 o 2. Si f es irreducible, ha de ser de grado 2, con lo que su grupo de Galois es isomorfo a C_2 (observemos que $S_2 \cong C_2$).

3. Si $degf = 3$, la Proposición anterior nos dice que bien $G \cong A_3$ o $G \cong S_3$. La Proposición 3.1 nos dice que tenemos el primer caso si $\Delta(f) \in F$ y el segundo si $\Delta(f) \notin F$.

4. Si $degf = 4$, la Proposición anterior nos dice que G es isomorfo a un subgrupo transitivo de S_4.

Ejemplo. Sea $f \in F[x]$ polinomio separable e irreducible de grado $degf = 4$, sean $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ las raíces de f en un cuerpo de descomposición K de f, consideramos:

$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$$
$$\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$$
$$\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$$

y definimos:

$$g = (x - \beta_1)(x - \beta_2)(x - \beta_3) \in K[x]$$

Veamos que en realidad $g \in F[x]$. Para ello, como $F \leqslant K$ es de Galois, hemos de ver que el polinomio es fijo por todos los automorfismos del grupo de Galois de f (basta verlo para todas las permutaciones). Concluimos que $g^\sigma = g \quad \forall \sigma \in G$, con lo que g es una resolvente cúbica de f (se verá).
Se puede ver por el algoritmo mencionado anteriormente que si $f = x^4 + bx^3 + cx^2 + dx + e$, entonces:

$$g = x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2$$

Consultamos si sus raíces son distintas:

$$\beta_2 - \beta_1 = (\alpha_2 - \alpha_3)(\alpha_4 - \alpha_1)$$

Por lo que β_2 y β_1 son distintas (análogo para el resto de las parejas), con lo que g es separable, luego $E = F(\beta_1, \beta_2, \beta_3)$ es una extensión de Galois de F, con $F \leqslant E \leqslant K$, de donde el grupo de Galois de g, $N = \mathrm{Aut}_E(K)$ es normal en G. Por lo que:

$$\mathrm{Aut}_F(E) \cong \frac{G}{N}$$

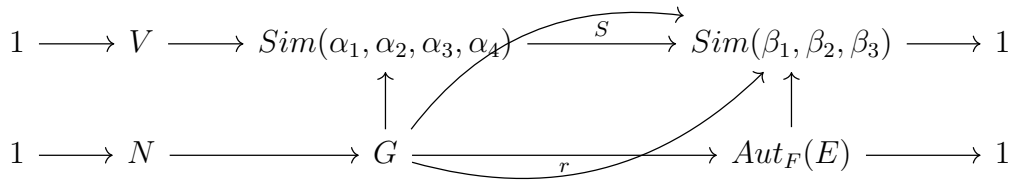
Consideramos $S : \mathrm{Sim}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to \mathrm{Sim}(\beta_1, \beta_2, \beta_3)$ una aplicación de forma que:

$$S(\sigma)(\alpha_i\alpha_j + \alpha_k\alpha_l) = \alpha_{\sigma(i)}\alpha_{\sigma(j)} + \alpha_{\sigma(k)}\alpha_{\sigma(l)}$$

que es un 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). Calculamos su núcleo:

$$\ker S = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Y sabemos que son todas porque como el grupo de la derecha tiene 6 elementos y el de la derecha 24; con lo que $\ker S = V$.



Por lo que:

$$N = V \cap G$$

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 fuera irreducible, tendríamos entonces que es producto del único polinomio irreducible de $\mathbb{Z}_2[x]$ que es $x^2 + x + 1$, pero no lo es, por lo que f es irreducible sobre $\mathbb{Z}[x]$, luego sobre $\mathbb{Q}[x]$ también. Sea G el grupo de Galois de f sobre $\mathbb{Q}$, tenemos que G es un subgrupo transitivo de S_4, así como que $|G|$ es un múltiplo de $degf = 4$. Los transitivos de S_4 son:

- Los cíclicos de 4 elementos.
- Un Klein, de entre los 3 isomorfos a Klein uno es transitivo y dos no.

  Como ejemplo de esto:

  $$V = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), 1\}$$

  es transitivo pero:

  $$\{(1), (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

  es isomorfo a Klein pero no es transitivo (desde 1 no podemos llegar a 3).
- De 8 elementos tenemos los diédricos, que hay varios.
- A_4.

Anteriormente vimos que si $f = x^4 + bx^3 + cx^2 + dx + e$ entonces su resolvente tenía el aspecto:

$$g = x^3 - cx^2 + (bd - 4e)x - b^2 + 4ce - d^2$$

Para nuestro f la resolvente cúbica es:

$$g = x^3 - 4x - 1$$

Si $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ son raíces de f y $\beta_1, \beta_2, \beta_3$ son las de g, teníamos entonces que:

$$\beta_2 - \beta_1 = (\alpha_2 - \alpha_3)(\alpha_4 - \alpha_1)$$

más otras dos relaciones. Usando estas, se demuestra que $\mathrm{Disc}(f) = \mathrm{Disc}(g)$. Además, g es una cúbica reducida, y teníamos una fórmula para calcular $\mathrm{Disc}(g)$, obtniendo que:

$$\mathrm{Disc}(f) = \mathrm{Disc}(g) = 229$$

Y tenemos que $\sqrt{229} \notin \mathbb{Q}$, ya que esto sucede si $x^2 - 229 \in \mathbb{Q}[x]$ es irreducible, porque 229 es primo (se comprueba tratando de dividir entre primos hasta la parte entera de $\sqrt{229}$, que es 15). Como $\sqrt{229} \notin \mathbb{Q}$, tenemos que $G \not\subseteq A_4$, por lo que no puede ser el isomorfo a Klein ni A_4.

En estas condiciones, teníamos una subextensión:

$$\mathbb{Q} \leqslant E = \mathbb{Q}(\beta_1, \beta_2, \beta_3) \leqslant K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$$

Como $\mathbb{Q} \leqslant K$ es de Galois, tenemos que $E \leqslant K$ es de Galois, y la conexión nos dice que:

$$\mathrm{Aut}_E(K) \lhd G$$

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 ± 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.

3.2. 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. 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. Además, su orden ha de dividir a n, pues todos los elementos tienen orden un divisor de n: $\alpha^n = 1 \quad \forall \alpha \in S$. □

El subgrupo cíclico de las raíces será de orden n si K contiene un cuerpo de descomposición de $x^n - 1$ y si $x^n - 1$ es separable, es decir, si n no es múltiplo de $\text{car}(F)$. En este contexto, llamamos a las raíes de $x^n - 1$ raíces $n-$ésimas de la unidad, que es un grupo cíclico de orden n si $x^n - 1$ es separable, por lo que lo supondremos en general. A sus generadores los llamamos raíces $n-$ésimas primitivas de la unidad.

Ejemplo. En característica cero, podemos suponer sin pérdida de generalidad que $F = \mathbb{Q}$, por lo que obtenemos las conocidas raíces $n-$ésimas primitivas de la unidad en $\mathbb{C}$.

En Álgebra I se vió que[4] $|\mathcal{U}(\mathbb{Z}_n)| = \varphi(n)$, sea ζ una raíz $n-$ésima primitiva de la unidad, tenemos que el conjunto de todas las raíces $n-$ésimas de la unidad es:

$$\{\zeta^k : k \in \mathbb{Z}_n\}$$

Y las raíces $n-$ésimas primitivas de la unidad son:

$$\{\zeta^k : k \in \mathcal{U}(\mathbb{Z}_n)\}$$

De esta forma, el cuerpo de descomposición de $x^n - 1 \in F[x]$ es $F(\zeta)$, que recibe el nombre $n-$ésima extensión ciclotómica de F, y como mucho es:

$$[F(\zeta) : F] \leqslant n - 1$$

Puesto que $x^n - 1$ siempre tiene a 1 como raíz.

Proposición 3.4. *Sea $x^n - 1 \in F[x]$ separable, tiene grupo de Galois G isomorfo a un subgrupo de $\mathcal{U}(\mathbb{Z}_n)$. Además, G es isomorfo a $\mathcal{U}(\mathbb{Z}_n)$ si y solo si actúa transitivamente sobre las raíces $n-$ésimas primitivas de la unidad (sobre F).*

Demostración. Sea ζ una raíz primitiva de la unidad, tenemos que:

$$G = \text{Aut}_F(F(\zeta))$$

donde $F(\zeta)$ es la $n-$ésima extensión ciclotómica de F. Habíamos visto que las raíces $n-$ésimas primitivas de la unidad son:

$$\{\zeta^k : k \in \mathcal{U}(\mathbb{Z}_n)\}$$

Sea $\sigma \in G$, tenemos que $\sigma(\zeta) = \zeta^k$ para cierto $k \in \mathcal{U}(\mathbb{Z}_n)$. Podemos definir

$$\begin{array}{rccc} : & G & \longrightarrow & \mathcal{U}(\mathbb{Z}_n) \\ & \sigma & \longmapsto & k \end{array}$$

donde se cumple que:

$$\sigma(\zeta) = \zeta^k$$

Si tomamos $\sigma, \tau \in G$ de forma que $\tau(\zeta) = \zeta^l$ con $l \in \mathcal{U}(\mathbb{Z}_n)$, tenemos que:

$$\sigma\tau(\zeta) = \sigma(\zeta^l) = \sigma(\zeta)^l = (\zeta^k)^l = \eta^{kl}$$

Con lo que la aplicación considerada es un homomorfismo de grupos, que además es inyectivo por su definición. Tenemos pues que G es isomorfo a cierto subgrupo de $\mathcal{U}(\mathbb{Z}_n)$. Esta aplicación será sobreyectiva si para cada exponente tenemos un automorfismo, con lo que G actuará transitivamente sobre estas raíces. □

[4] Donde φ es la función de Euler.

Definición 3.3 (Polinomio ciclotómico)**.** Sea F un cuerpo, definimos el $n-$ésimo polinomio ciclotómico como:

$$\phi_n = \prod_{k \in \mathcal{U}(\mathbb{Z}_n)} \left(x - \zeta^k\right)$$

con ζ una raíz $n-$ésima primitiva de la unidad.

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 de $x^n - 1$ (es decir, el conjunto de todas las raíces $n-$ésimas de la unidad). Si consideramos también P_m, el conjunto de las raíces $m-$ésimas primitivas de la unidad, tenemos una partición de R_n:

$$R_n = \biguplus_{d \in Div(n)} P_d$$

Como:

$$x^n - 1 = \prod_{\alpha \in R_n} (x - \alpha)$$

y cada α está en un cierto P_d, ha de estar en ϕ_d, con lo que:

$$x^n - 1 = \prod_{\alpha \in R_n} (x - \alpha) = \prod_{d \in Div(n)} \phi_d$$

□

Proposición 3.6. *Cada ϕ_n tiene coeficientes en el subcuerpo primo de F y además, si $\mathrm{car}(F) = 0$, tenemos que $\phi_n \in \mathbb{Z}[x]$.*

Demostración. Por inducción sobre n:

- Si $n = 1$, entonces $\phi_1 = x - 1$ y se tiene la Proposición.
- Si $n > 1$, tenemos:

  $$x^n - 1 = \phi_n \cdot \prod_{\substack{d \in Div(n) \\ d < n}} \phi_d$$

  Por hipótesis de inducción, tenemos que el producto de la derecha está en el subcuerpo primo de F. Tenemos además que ϕ_n es cociente de $x^n - 1$ entre el producto de la derecha, con lo que ϕ_n también ha de tener coeficientes en el subcuerpo primo de F.

Si $\mathrm{car}(F) = 0$, sabemos por lo ya probado que $\phi_n \in \mathbb{Q}[x]$. Si expresamos sus coeficientes como fracciones irreducibles y tomamos $a \in \mathbb{Z}$ el mínimo común múltiplo de sus denominadores, tenemos que $a\phi_n \in \mathbb{Z}[x]$, con todos sus coeficientes coprimos entre sí, luego $a\phi_n$ es primitivo. Tenemos pues que:

$$a(x^n - 1) = a\phi_n \prod_{\substack{d \in Div(n) \\ d < n}} \phi_d$$

de nuevo por inducción, suponemos ahora que los polinomios ϕ_d son primitivos (para $n = 1$ es claro que ϕ_1 es primitivo). Por el Lema de Gauss, tenemos que:

$$\prod_{\substack{d \in Div(n) \\ d<n}} \phi_d$$

es primitivo y con coeficientes en $\mathbb{Z}$, si recordamos que $a\phi_n$ es primitivo, de donde todo el producto es primitivo, es decir, $a(x^n - 1)$ es primitivo, luego ha de ser $a = 1$. □

Ejemplo. En característica cero:

$$\phi_1 = x - 1, \qquad \phi_2 = x + 1, \qquad \phi_3 = x^2 + x + 1, \qquad \phi_4 = x^2 + 1$$

Para ϕ_6 usamos la fórmula:

$$\phi_6 = \frac{x^6 - 1}{\phi_1\phi_2\phi_3} = x^2 - x + 1$$

Teorema 3.7. *Cada $\phi_n \in \mathbb{Z}[x]$ es irreducible.*

Demostración. Sea f un factor irreducible de ϕ_n. Tomamos ζ una raíz compleja de f en la $n-$ésima extensión ciclotómica. Probemos que si p es primo y no divide a n, entonces ζ^p es raíz de f. Por reducción al absurdo, tomamos g con:

$$\phi_n = fg \qquad f, g \in \mathbb{Z}[x]$$

Y ha de cumplir $g(\zeta^p) = 0$. Resulta que ζ es raíz de $h = g(x^p) \in \mathbb{Z}[x]$. De esta forma, f y h tienen una raíz común compleja, y la identidad de Bezout nos dice entonces que f y h no son coprimos. Como f es irreducible, ha de ser $f \mid h$. Como f es primitivo, tenemos que $f \mid h$ en $\mathbb{Z}[x]$. Reducimos módulo p:

$$\overline{\phi_n} = \overline{f}\,\overline{g}$$

y tenemos:

$$\overline{h} = \overline{g(x^p)} \overset{(*)}{=} \overline{g(x)}^p = \overline{g}^p$$

donde $(*)$ es porque como $f \mid h$ en $\mathbb{Z}[x]$, tenemos que $\overline{f} \mid \overline{h}$, pero como $\overline{h} = \overline{g}^p$. Como $\mathbb{F}_p[x]$ es DFU, tenemos que $\overline{f}$ y $\overline{g}$ tienen algún factor común no constante. Deducimos que $\overline{x^n - 1}$ tiene una raíz múltiple en su cuerpo de descomposición. Sin embargo, p no divide a n, por lo que:

$$\overline{x^n - 1} = x^n - 1$$

y este polinomio es separable, contradicción; por lo que para cada p primo que no divide a n tenemos que ζ^p es raíz de f. Si tomamos n y lo factorizamos en primos, miramos los primos que no dividen a n, con lo que tomando estos primos nos movemos dentro de las unidades de $\mathbb{Z}_n$, con lo que en alguna cantidad finita de pasos rellenamos todas las unidades de $\mathbb{Z}_n$. Por lo que todas las raíces de ϕ_n son raíces de f. Como f dividía a ϕ_n, $f = \phi_n$. □

Hemos visto ya que el $n-$ésimo polinomio ciclotómico $\phi_n \in \mathbb{Z}[x]$ es irreducible. $\mathbb{Q}(\zeta)$, la $n-$ésima extensión ciclotómica con $\zeta \in \mathbb{C}$ la raíz $n-$ésima primitiva de la unidad. Así, $\mathrm{Irr}(\zeta, \mathbb{Q}) = \phi_n$. Sabemos que $\mathrm{Aut}(\mathbb{Q}(\zeta))$ actúa transitivamente sobre las raíces de ϕ_n.

Esto significa que $|\mathrm{Aut}(\mathbb{Q}(\zeta))| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = deg\phi_n = \varphi(n)$. Además, tenemos que $\mathrm{Aut}(\mathbb{Q}(\zeta)) \cong \mathcal{U}(\mathbb{Z}_n)$.

Ejemplo. Para $n = 16$:

$$\deg \phi_n = \varphi(16) = 8$$

Por lo que tenemos que:

$$\mathrm{Aut}(\mathbb{Q}(\zeta)) \cong \mathcal{U}(\mathbb{Z}_{16})$$

3.3. Construcciones con regla y compás II

A lo largo de la sección, consideraremos siempre que S es un subconjunto de $\mathbb{C}$ con $\{0, 1\} \subseteq S$. Además, consideraremos siempre también $F = \mathbb{Q}(S \cup \overline{S})$.

Teorema 3.8. *Sea $z \in \mathbb{C}$, tenemos que:*

$$z \text{ es constructible a partir de } S \iff z \in K, \text{ donde } F \leqslant K \text{ es de Galois y } [K : F] = 2^k, \text{ para cierto } k \in \mathbb{N}.$$

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 α_{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 α_{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[5]. 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.

□

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 es constructible. Por tanto, hemos de ver que ζ es constructible (como raíz primitiva $n-$ésima de la unidad) si y solo si existe $\mathbb{Q} \leqslant K$ de forma que $[K : \mathbb{Q}]$ es una potencia de 2.

Sabemos que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

[5]Por ser un $p-$grupo.

n	Es constructible
3	Sí
4	Sí
5	Sí
6	Sí
7	No
8	Sí
9	No
10	Sí
11	No
12	No
13	No
14	No
15	Sí
16	Sí
17	Sí

Tabla 3.1: Qué polígonos regulares son constructibles.

$\Longrightarrow$) Si ζ es constructible, existe una extensión de Galois $\mathbb{Q} \leqslant K$ de grado 2 que contiene a ζ, luego ha de contener a $\mathbb{Q}(\zeta)$: $\mathbb{Q}(\zeta) \leqslant K$, de donde por el Lema de la Torre ha de ser $\varphi(n)$ una potencia de 2.

$\Longleftarrow$) Si tomamos $K = \mathbb{Q}(\zeta)$ se tiene.

□

De esta forma:
Si n es primo, tenemos que $\varphi(n) = n - 1$, que es una potencia de 2 si y solo si el primo es de la forma $2^{algo} + 1$. Haciendo la cuenta, tiene que ser:

$$n = 2^{2^m} + 1$$

- $m = 0$, 3
- $m = 1$, 5
- $m = 2$, 17
- $m = 3$, algo
- $m = 4$, 65 mil y pico

Sin embargo, todavía no se ha encontrado un primo más de esta forma, los llamados primos de Fermat

3.4. Extensiones cíclicas

Teorema 3.9. *Sea $x^n - a \in F[x]$ separable siendo K su cuerpo de descomposición. Entonces K contiene una raíz $n-$ésima primitiva de la unidad ζ y $K = F(\zeta, r)$ para cualquier raíz r 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. Si $a = 0$, si x^n es separable ha de ser $n = 1$, con lo que $K = F$ y una raíz $n-$ésima primitiva de la unidad es 1, se trivializa el enunciado. Suponemos por tanto que $a \neq 0$, con lo que n puede ser cualquiera distinto de $\text{car}(F)$. Sea R el conjunto de las raíces en K de $x^n - a$, tenemos que $|R| = n$, puesto que $x^n - a$ es separable. Además, si $r, s \in R$, tenemos que $r^{-1}s \in K$ es una raíz $n-$ésima de la unidad.
Fijado r, entonces el conjunto $\{r^{-1}s : s \in R\}$ contiene n raíces $n-$ésimas de la unidad, por lo que en dicho conjunto las tenemos todas, luego ha de contener al menos una raíz primitiva de la unidad, llamémosla $\zeta \in K$.

Para la segunda afirmación, tenemos que:

$$K = F(\zeta, r)$$

Puesto que ζ genera $\{r^{-1}s : s \in \mathbb{R}\}$ y al multiplicar por s obtenemos r.

Para ver que el grupo de Galois es cíclico, representemos el grupo de manera sencilla. Para ello, tomamos $\sigma \in \text{Aut}_{F(\zeta)}(K)$. Como σ toma una raíz de $x^n - a$, la lleva en otra raíz y el conjunto de todas las raíces es:

$$R = \{r, \zeta r, \ldots, \zeta^{n-1} r\}$$

Por lo que tendremos $\sigma(r) = \zeta^j r$ para cierto $j \in \mathbb{Z}_n$. Si tuviéramos que $\sigma(r) = \zeta^{j'} r$ para $j' \neq j$, como r es una raíz primitiva de la unidad tenemos entonces que $j = j'$, por lo que observamos una dependencia $j \longmapsto \sigma$, que nos da una aplicación $j : \text{Aut}_{F(\zeta)}(K) \to \mathbb{Z}^n$. Podemos ver j como un homomorfismo de grupos, considerando $\mathbb{Z}^n$ como grupo aditivo. Para ello, tomamos $\sigma, \tau \in \text{Aut}_{F(\zeta)}(K)$ y tenemos que $j(\sigma\tau) \in \mathbb{Z}_n$ está determinado por la condición:

$$(\sigma\tau)(r) = \zeta^{j(\sigma\tau)} r$$

Y tenemos que:

$$(\sigma\tau)(r) = \sigma(\tau(r)) = \sigma\left(\zeta^{j(\tau)} r\right) = \zeta^{j(\tau)}\sigma(r) = \zeta^{j(\tau)}\zeta^{j(\sigma)} r = \zeta^{j(\tau)+j(\sigma)} r$$

De donde $j(\sigma\tau) = j(\sigma) + j(\tau)$, por lo que j es un homomorfismo de grupos. Además tenemos que j es inyectivo, pues si $j(\sigma) = 0$, tendríamos por tanto que $\sigma(r) = \zeta^0 r$, de donde $\sigma = id$, por lo que $\ker j = \{id\}$. Tenemos por tanto que $\text{Aut}_{F(\zeta)}(K)$ es isomorfo a un subgrupo de $\mathbb{Z}_n$, por lo que ha de ser cíclico y por el Teorema de Lagrange, de orden menor un divisor de n. □

Corolario 3.9.1. *Sea $x^n - a \in F(\zeta)[x]$, es irreducible si y solo si $[K : F(\zeta)] = n$.*

Demostración. Por doble implicación:

$\Longleftarrow$) En este caso tenemos que j es sobreyectivo, por lo que j es un isomorfimo, de donde todo elemento de $\mathbb{Z}_n$ proviene de un automorfismo, con lo que el conjunto R es transitivo.

$\Longrightarrow$)

□

Definición 3.4 (Extensiones cíclica)**.** Una extensión $F \leqslant K$ se dice cíclica si es de Galois y su grupo de Galois es cíclico.

Observación. Observemos que tanto las extensiones de cuerpos finitos como las extensiones como las del último Teorema son extensiones cíclicas:

Ejemplo.
- Si F contiene una raíz $n-$ésima primitiva de la unidad y $x^n - a \in F[x]$ es separable, entonces para K un cuerpo de descomposición de $x^n - a$ tenemos que $F \leqslant K$ es cíclica.

  Esto se debe a que el ζ del Teorema está ya en F, y tenemos que $\mathrm{Aut}_F(K)$ es subgrupo de un grupo cíclico por el monomorfismo j.

- Toda extensión de cuerpos finitos es cíclica.

Lema 3.10 (de independencia de Dedekind)**.** *Sean $\sigma_1, \ldots, \sigma_n : F \to E$ homomorfismos de cuerpos distintos. Tenemos entonces que $\sigma_1, \ldots, \sigma_n$ son linealmente independientes. Es decir, si $\lambda_1, \ldots, \lambda_n \in E$ es tal 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. Si $n = 1$ es cierto. Suponemos que $n > 1$ y razonamos por reducción al absurdo. Para ello, tomamos de entre todas las posibles elecciones de $\lambda_1, \ldots, \lambda_n$ aquella lista de ellos contengan m elementos no nulos. Reordenando, podemos suponer que:

$$\begin{aligned} \lambda_i &\neq 0 \qquad \forall i \in \{1, \ldots, m\} \\ \lambda_i &= 0 \qquad \forall i > m \end{aligned}$$

Tenemos que $m \geqslant 2$. Como $\sigma_1 \neq \sigma_m$, existe $y \in F$ de forma que $\sigma_1(y) \neq \sigma_m(y)$, de donde:

$$\lambda_1\sigma_1(yx) + \ldots + \lambda_m\sigma_m(yx) = 0$$

Y obtenemos restando la cadena anterior con $n = m$:

$$\lambda_1(\sigma_1(y) - \sigma_m(y))\sigma_1(x) + \ldots + \lambda_{m-1}(\sigma_{m-1}(y) - \sigma_m(y))\sigma_{m-1}(x) = 0 \qquad \forall x \in F$$

Y tenemos que $\sigma_m(y)$ no es cero, pero hemos llegado a una contradicción, pues tenemos $\lambda_1, \ldots, \lambda_{m-1}$ una lista de números menor. □

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 α es una raíz de $x^n - a$ entonces $K = F(\alpha)$.*

Demostración. El grupo de automorfismos debe ser cíclico de grado n, por lo que tendrá un generador $\sigma \in \mathrm{Aut}_F(K)$ de orden n. El Lema de independencia de Dedekind nos dice que ha de existir $r \in K$ de forma que (si $\zeta \in F$ es una raíz $n-$ésima primitiva de la unidad):

$$\beta := r + \zeta\sigma(r) + \ldots + \zeta^{n-1}\sigma^{n-1}(r) \neq 0$$

Tendremos entonces que:

$$\zeta\sigma(\beta) = \beta$$

Por lo que:

$$\beta^n = \zeta^n\sigma(\beta)^n = \sigma(\beta)^n = \sigma(\beta^n)$$

como σ genera todo $\mathrm{Aut}_F(K)$ tenemos que $a := \beta^n \in K^{\mathrm{Aut}_F(K)} = F$. Como $\zeta^n = 1$, tenemos que:

$$\beta, \zeta\beta, \ldots, \zeta^{n-1}\beta$$

son todas raíces distintas de $x^n - a$, y tenemos n, de donde:

$$x^n - a = (x-\beta)(x-\zeta\beta)\ldots(x-\zeta^{n-1}\beta)$$

Y como $\zeta \in F$, tenemos que $F(\beta)$ es cuerpo de descomposición de $x^n - a \in F[x]$. Como el orden de β es menor o igual que n, $[F(\beta) : F] \leqslant n$, y para conseguir la igualdad tenemos que:

$$\sigma^k(\beta) = \zeta^{-k}\beta$$

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, de donde $[F(\beta) : F] = n$. Tenemos en definitiva que $F(\beta) = K$. □

Ejemplo. Si consideramos $x^8 - 3 \in \mathbb{Q}[x]$, si metemos una raíz octava primitiva de la unidad tenemos que su grupo de Galois es cíclico. Sea $K \leqslant \mathbb{C}$ su cuerpo de descomposición, sabemos por el Teorema de ayer que $K = \mathbb{Q}\left(\sqrt[8]{3}, \zeta\right)$, con ζ una raíz octava primitiva de la unidad. Esta podemos calcularla como una raíz cuadrada de i, que es una raíz cuarta de la unidad. Tomamos una de ellas:

$$\zeta = e^{i\frac{\pi}{4}} = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$$

Como el octavo polinomio ciclotómico tiene grado $\varphi(8) = 4$, tenemos que la extensión $\mathbb{Q}(\zeta)$ 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 $\mathbb{Q}\left(i, \sqrt{2}\right) = \mathbb{Q}(\zeta)$.

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 $b = 0 \Longrightarrow 2 = 0$ contradicción, 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.

3.5. Ecuaciones resolubles por radicales

Las definiciones de este apartado dependen mucho del autor.

La siguiente definición generaliza el concepto de extensión por raíces cuadradas:

Definición 3.5. Una extensión de cuerpos $F \leqslant E$ se llamará una extensión por radicales cuando existe una torre de cuerpos

$$F = E_0 \leqslant E_1 \leqslant \ldots \leqslant E_t = E$$

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 3.6. Un polinomio $f \in F[x]$ se dice resoluble por radicales si existe una extensión por radicales $F \leqslant E$ que contiene al cuerpo de descomposición de f.

Supondremos que siempre trabajaremos en $\text{car}(F) = 0$, para simplificar los enunciados siguientes. Es posible hacerlo para $\text{car}(F) \neq 0$, pero entonces los enunciados se complican.

Definición 3.7. Una extensión $F \leqslant K$ es radical si K es cuerpo de descomposición de un polinomio $x^n - a \in F[x]$ y F contiene una raíz $n-$ésima primitiva de la unidad.

Bajo estas condiciones, toda extensión radical es cíclica, y toda cíclica da una radical. Y como estamos en $\text{car}(F) = 0$, no hace falta hipótesis sobre que $x^n - a$ sea separable.

Definición 3.8. Diremos que una extensión $F \leqslant K$ es radical iterada si hay una torre de cuerpos

$$F = K_0 \leqslant K_1 \leqslant \ldots \leqslant K_t = K$$

de forma que cada $K_{i-1} \leqslant K_i$ es radical, para $i \in \{1, \ldots, t\}$.

Proposición 3.12. *Si $F \leqslant E$ es una extensión de Galois, supongamos una extensión $E \leqslant E(\alpha)$ para α raíz de $x^n - a \in E[x]$, $a \neq 0$. Entonces existe una extensión radical iterada $E(\zeta) \leqslant K$ tal que $F \leqslant K$ es de Galois y $E(\alpha) \leqslant K$, para ζ una raíz $n-$ésima primitiva de la unidad.*

Demostración. Consideramos:

$$f = \prod_{\sigma \in \text{Aut}_F(E)} (x^n - \sigma(a)) \in E[x]$$

Como $f^\tau = f \quad \forall \tau \in \text{Aut}_F(E)$, tenemos que en realidad $f \in F[x]$. E es cuerpo de descomposición de $g \in F[x]$. Sea K el cuerpo de descomposición de $fg \in F[x]$. Como $f \in F[x]$, es claro que $E(\alpha) \leqslant K$, al tomar $\sigma = id$.

Como $x^n - a$ es un factor de f, K ha de contener un cuerpo de descomposición de $x^n - a$; por lo que podemos encontrar en K una raíz $n-$ésima primitiva de la unidad, ζ. Si enumeramos los elementos de $\text{Aut}_F(E)$:

$$\text{Aut}_F(E) = \{\sigma_1, \ldots, \sigma_s\}$$

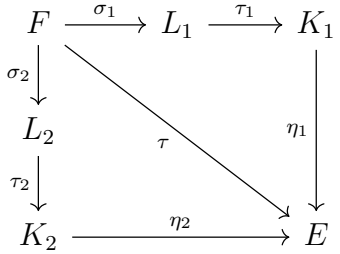
con $\sigma_1 = id_E$. Tomando $K_{-1} = E$ y $K_0 = E(\zeta)$, para cada $i \in \{1, \ldots, s\}$ tomamos $K_i = K_{i-1}(\alpha_i)$, con α_i raíz de $x^n - \sigma_i(a)$.

De esta forma, cada $K_{i-1} \leqslant K_i$ es radical para $i \geqslant 1$. Además, $F \leqslant K$ es claramente de Galois. □

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 $\sigma_i(F) \leqslant L_i$ para $i \in \{1, 2\}$ son finitas. Tomamos los polinomios $f_1, f_2 \in F[x]$ tales que el cuerpo de descomposición de cada $f_i^{\sigma_i}$ venga dado por $\tau_i : L_i \to K_i$, para $i \in \{1, 2\}$. Tenemos $\tau : F \to E$, cuerpo de descomposición de $f_1 f_2$.

La Tercera Proposición de Extensión obtenemos el diagrama de homomorfismos de cuerpos



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:

$$F \cong Im\tau = \tau(F) \leqslant \eta_i \tau_i(L_i) \leqslant E \qquad \forall i \in \{1, 2\}$$

Definición 3.9. Una extensión $F \leqslant K$ se dice radical si K es cuerpo de descomposición de un polinomio separable de la forma $x^n - a \in F[x]$.

Es decir, como $\text{car}(F) = 0$, es equivalente a decir que $a \neq 0$.

Más aún, se dice que es radical iterada si:

$$F = K_0 \leqslant K_1 \leqslant \ldots \leqslant K_t = K$$

con $K_{i-1} \leqslant K_i$ radical, para cada $i \in \{1, \ldots, t\}$ y $F \leqslant K$ de Galois.

Proposición 3.13. *Si $F \leqslant E$ es de Galois y $E \leqslant E(\alpha)$ para α 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.*

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 α_j raíz de $x^{n_j} - a_j \in E_{j-1}[x]$, $j \in \{1, \ldots, t\}$. 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, dentro de la cual esté $K_r(\alpha_t)$. Tenemos que $E_t \leqslant K_r(\alpha_t)$. Por la Proposición anterior aplicada a la extensión $F \leqslant K_r$ de Galois, tenemos que existe una extensión radical iterada $K_r \leqslant K$ tal que $K_r(\alpha_t) \leqslant K$ y $F \leqslant K$ es de Galois.

  Tenemos una torre de cuerpos
$$K_r \leqslant K_{r+1} \leqslant \ldots \leqslant K_s$$
con $K_{i-1} \leqslant K_i$ radical para cada $i \in \{r+1, \ldots, s\}$. Tenemos entonces que:
$$F = K_0 \leqslant K_1 \leqslant \ldots \leqslant K_r \leqslant K_{r+1} \leqslant \ldots \leqslant K_j = K$$
con cada $K_{k-1} \leqslant K_k$ radical para $k \in \{1, \ldots, s\}$ y $F \leqslant K$ de Galois. De aquí tenemos que $F \leqslant K$ es radical iterada y $E \leqslant K$.

□

Lema 3.15. *Toda extensión radical iterada tiene grupo de Galois resoluble.*

Demostración. Veamos 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 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 ($F \leqslant K$ es radical) y $F \leqslant F(\zeta)$ de Galois por ser una extensión ciclotómica (que siempre son de Galois). Usando ahora la conexión de Galois, tenemos entonces que:
$$\{id_K\} \lhd \mathrm{Aut}_{F(\zeta)}(K) \lhd \mathrm{Aut}_F(K)$$
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, 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 de composición con factores simples abelianos.

Si ahora:
$$F = K_0 \leqslant K_1 \leqslant \ldots \leqslant K_t = K$$
es radical iterada, 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 ahora la conexión de Galois, obtenemos una serie de grupos:

$$\mathrm{Aut}_F(K) = \mathrm{Aut}_{K_0}(K) \rhd \mathrm{Aut}_{K_1}(K) \rhd \ldots \rhd \mathrm{Aut}_{K_{t-1}}(K) \rhd \{id_K\}$$

Veamos ahora que:

$$\frac{\mathrm{Aut}_{K_{i-1}}(K)}{\mathrm{Aut}_{K_i}(K)} \cong \mathrm{Aut}_{K_{i-1}}(K_i)$$

con este resoluble, ya que la extensión $K_{i-1} \leqslant K_i$ es de Galois, y hemos visto que estas tienen grupo de Galois resoluble. En definitiva, obtenemos que $\mathrm{Aut}_F(K)$ es resoluble. □

Ejercicio 3.5.1. Sea $f \in F[x]$ y L cuerpo de descomposición de $f \in F[x]$, si $F \leqslant E$ es una extensión, demostrar que para K cuerpo de descomposición de $f \in E[x]$ se tiene que:

$$\mathrm{Aut}_E(K) \text{ es isomorfo a un subgrupo de } \mathrm{Aut}_F(L).$$

Es claro que $L \leqslant K$, como K está generado sobre F por las raíces de f, los generadores que necesitamos obtener para obtener K son los mismos. Si tomamos $\sigma \in \mathrm{Aut}_E(K)$, lleva α_i en α_j y deja fijos a los elementos de L. Estamos llevando un elemento de L en otro de L. Se considera la aplicación restricción.

Teorema 3.16 (Gran Teorema de Galois)**.** *Sea $f \in F[x]$:*

$$f \text{ es resoluble por radicales} \iff \text{el grupo de Galois de } f \text{ es resoluble}$$

Demostración. Sea L el cuerpo de descomposición de f:

$\Longrightarrow$) Tenemos entonces una extensión por radicales E de f que contiene a todas sus raíces, por lo que tenemos la torre $F \leqslant L \leqslant E$. Por las Proposiciones anteriores, se ha visto que existe una extensión radical iterada de F tal que $E \leqslant K$, por lo que $F \leqslant K$ es de Galois, y como $F \leqslant L$ también es de Galois, sabemos por la conexión de Galois que $\mathrm{Aut}_F(K)$ contiene como subgrupo normal al grupo de Galois $\mathrm{Aut}_L(K)$. 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 ζ 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). Usando la conexión de Galois, tenemos una serie de composición de $\mathrm{Aut}_{F(\zeta)}(K)$:

$$\mathrm{Aut}_{F(\zeta)}(K) = G_0 \rhd G_1 \rhd \ldots \rhd G_{t-1} \rhd G_t = \{id_K\}$$

con $\frac{G_{i-1}}{G_i}$ de cardinal p_i primo y esto nos da:

$$F(\zeta) = K^{G_0} \leqslant K^{G_1} \leqslant \ldots \leqslant K^{G_{i-1}} \leqslant K^{G_t} = K$$

con $p_i \mid n \quad \forall i$, ya que el cardinal de cada uno de los factores invariantes dividen al cardinal del grupo del que son factores invariantes, por lo que cada primo divide a n.

Resulta que ζ elevada a una potencia elevada nos da una raíz p_i-ésima de la unidad, por lo que cada K^{G_i} contiene una raíz p_i-ésima primitiva de la unidad. Como los cocientes son cíclicos, cada extensión K^{G_i} es cíclica, por lo que cada K^{G_i} es cuerpo de descomposión de cierto $x^{p_i} - a_i \in K_{i-1}[x]$.

Como K contiene todas las raíces de f y $F(\zeta) \leqslant K$ es radical iterada será una extensión por radicales, con lo que f es resoluble por radicales.

□

Consecuencias

1. Si $degf \leqslant 4$, 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 un cuerpo, consideramos $F[x_1, \ldots, x_n]$ el anillo de polinomios con n indeterminadas.

- recordamos que al alterar el orden de las indeterminadas obtenemos anillos isomorfos
- como F es un cuerpo, $F[x_1]$ es un DFU, por lo que $F[x_1, x_2]$ también, $\ldots$, $F[x_1, \ldots, x_n]$ es un DFU. 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 $\sigma \in S_n$, aplicando n veces la Propiedad Universal del anillo de polinomioa, obtenemos un homomorfismo de anillos $\overline{\sigma} : F[x_1, \ldots, x_n] \to$

$F[x_1, \ldots, xn]$ determinado[6] por:

$$\overline{\sigma}(\alpha) = \alpha \quad \forall \alpha \in F$$
$$\overline{\sigma}(x_i) = x_{\sigma(i)} \quad \forall i \in \{1, \ldots, n\}$$

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 por tanto una aplicación $S_n \to \mathrm{Aut}_F(F(x_1, \ldots, x_n))$ que es un homomorfismo de grupos inyectivo, cuya imagen denotaremos por G.

Definición 3.10. Al cuerpo E^G (donde $E = F(x_1, \ldots, x_n)$) 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.

Ejercicio 3.6.1. Sea $f \in F[x]$ separable, irreducible y de grado primo p, entonces su grupo de Galois contiene un $p-$ciclo.

Si es separable e irreducible, p divide al orden del grupo de Galoios. Como es primo, entonces G ha de contener un elemento de orden p. Descomponemos el elemento como producto de ciclos disjuntos y su orden ha de ser el minimo común múltiplo de todos los órdenes de los ciclos que aparecen en su descomposición. Si estos números tienen como mínimo común múltiplo un número primo, entonces el orden de todos los cicloss es p. En S_p, el primero que aparece ha gastado todos los símbolos, luego ha de ser un $p-$ciclo.

Proposición 3.17. *Para cada $k \in \{1, \ldots, n\}$ escribimos:*

$$S_k = \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} x_{i_1} \ldots x_{i_k} \in F[x_1, \ldots, x_n]$$

Entonces $E^G = F(s_1, \ldots, s_n)$:

Demostración. Recordamos que:

$$E = F(x_1, \ldots, x_n)$$

Y consideramos:

$$f = (x - x_1) \ldots (x - x_n) \in E[x]$$

Y si tomamos $\overline{\sigma} \in G$ es claro que $f^{\overline{\sigma}} = f$, tenemos:

$$f = x^n - s_1 x^{n-1} + \ldots + (-1)^n s_n$$

Y como cada $s_k \in E^G$ tenemos que $F(s_1, \ldots, s_n) \leqslant E^G$. Tenemos que E es cuerpo de descomposición de f sobre $F(s_1, \ldots, s_n)$. Es claro que f es separable por su propia

[6] Por la Propiedad Universal del anillo de polinomios.

definición, con lo que la extensión $F(s_1, \ldots, s_n) \leqslant E$ 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 τ 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:

$$E^G = F(s_1, \ldots, s_n)$$

□

Estos son los polinómios simétricos elementales, porque si les aplicamos una permutación se queda iguales.

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 λ_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 λ_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 ε. Tenemos que $\overline{\varepsilon}$ es $F-$lineal y es un isomorfismo de cuerpos. Cardano-Vietta 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* $\operatorname{car}(F) = 0$ *y* $n \geqslant 5$*, entonces g no es resoluble por radicales.*

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 las ecuaciones de grado hasta 4

Tendremos siempre que F será un cuerpo cualesquiera, y tengamos en cuenta que basta estudiar los polinomios mónicos.

3.7.1. Cuadrática

Tendremos $f = x^2 + bx + c \in F[x]$. Si $\text{car}(F) \neq 2$, podemos escribir:

$$f = \left(x + \frac{b}{2}\right)^2 + c - \frac{b^2}{4}$$

y ahora extendiendo F de forma adecuada: $F \leqslant K$, conseguimos escribir en K despejando x:

$$x + \frac{b}{2} = \pm\sqrt{\frac{b^2}{4} - c} = \pm\sqrt{\frac{b^2 - 4c}{4}} = \pm\frac{\sqrt{b^2 - 4c}}{2}$$

de donde:

$$x = -\frac{b}{2} \pm \frac{\sqrt{b^2 - 4c}}{2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

Por lo que la ecueación 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[7] $\text{car}(F) \notin \{2, 3\}$, podemos escribir:

$$g(x) = f\left(x - \frac{b}{3}\right) = x^3 + px + q$$

para ciertos $p, q \in F$. El polinomio g recibe el nombre cúbica reducida de f. Sea K una extensión de F donde están las raíces de f y una raíz cúbica primitiva de la unidad[8] ω. Sean $\alpha_1, \alpha_2, \alpha_3 \in K$ las raíces de g. Tenemos por las ecuaciones de Cardano-Vietta:

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

tomamos ahora:

$$\beta := \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$$
$$\gamma := \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3$$

Sumando vemos que (ω es raíz de $x^2 + x + 1$):

$$\beta + \gamma = 3\alpha_1 + 0 + 0 = 3\alpha_1$$

[7] Distinta de 3 para el truco siguiente y distinta de 2 para poder aplicar luego la resolución de cuadrácticas.

[8] Aquí también necesitamos que $\text{car}(F) \neq 3$, para que $x^3 - 1$ sea separable.

Multiplicamos ahora β por γ, obteniendo (usando propiedades de ω):

$$\begin{aligned}\beta\gamma &= \alpha_1^2+\alpha_2^2+\alpha_3^2-\alpha_1\alpha_2-\alpha_2\alpha_3-\alpha_1\alpha_3\\ &= \cancelto{0}{(\alpha_1+\alpha_2+\alpha_3)^2} - 3(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_1\alpha_3) = -3p\end{aligned}$$

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:

$$\alpha_1 = u+v$$

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:

$$0 = u^3+v^3+q \quad \Longrightarrow \quad \begin{cases} u^3+v^3 = -q \\ u^3v^3 = \frac{-p^3}{27}\end{cases}$$

Si tomamos:

$$h(z) = (z-u^3)(z-v^3) = z^2+qz-\frac{p^3}{27}$$

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 α_1 es suma de dos valores de forma que estos son raíces cúbicas, puesto que no hemos supuesto nada a α_1 distinto que a α_2 y α_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:

$$\begin{aligned}u_k &= e^{ik2\pi/3}\sqrt[3]{6+i\sqrt{87}}, \quad k=0,1,2\\ v_k &= e^{ik2\pi/3}\sqrt[3]{16-i\sqrt{87}}, \quad k=0,1,2\end{aligned}$$

Hemos de elegir de acuerdo con la condición $3uv = -p = 21$, lo que nos da:

$$u_0v_0 = u_1v_2 = u_2v_1 = 7$$

Por tanto, las raíces de la cúbica reducida son:

$$\begin{aligned} u_0 + v_0 &= \sqrt[3]{16 + i\sqrt{87}} + \sqrt[3]{16 - i\sqrt{87}} \\ u_1 + v_2 &= e^{i2\pi/3}\sqrt[3]{16 + i\sqrt{87}} + e^{i4\pi/3}\sqrt[3]{16 - i\sqrt{87}} \\ u_2 + v_1 &= e^{i4\pi/3}\sqrt[3]{16 + i\sqrt{87}} + e^{i2\pi/3}\sqrt[3]{16 - i\sqrt{87}} \end{aligned}$$

Las raíces para f es sumar 2 a cada una de ellas.

3.7.3. Cuártica

Consideramos ahora $f = x^4 + bx^3 + cx^2 + dx + e \in F[x]$ con $\text{car}(F) \notin \{2, 3\}$.
El primer paso es reducir la ecuación con la resolvente 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-Vietta:

$$\beta_1 + \beta_2 + \beta_3 + \beta_4 = 0$$

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 ρ_1, ρ_2, ρ_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:

$$\beta_1 = \frac{1}{2}(\sqrt{\rho_1} + \sqrt{\rho_2} + \sqrt{\rho_3})$$
$$\beta_2 = \frac{1}{2}(\sqrt{\rho_1} - \sqrt{\rho_2} + \sqrt{\rho_3})$$
$$\beta_3 = \frac{1}{2}(-\sqrt{\rho_1} + \sqrt{\rho_2} - \sqrt{\rho_3})$$
$$\beta_4 = \frac{1}{2}(-\sqrt{\rho_1} - \sqrt{\rho_2} - \sqrt{\rho_3})$$

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[9] $\mathrm{Aut}_F(K) \to GL_2(\mathbb{Z}_n)$ 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 σ 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. *Tomamos (para $q = p^k$) $\mathbb{F}_q \leqslant \mathbb{F}_{q^n}$ una extensión de cuerpos finitos. Entonces $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ es cíclico generado por ϕ, donde:*

$$\phi(\alpha) = \alpha^q \qquad \forall \alpha \in \mathbb{F}_{q^n}$$

Además, $\mathbb{F}_{q^n}$ es cuerpo de descomposición de $x^{qn} - x \in \mathbb{F}_q[x]$.

[9] 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.

Demostración. Con $q = p^k$ con p primo y $k \geqslant 1$, tenemos la extensión:

$$\mathbb{F}_p \leqslant \mathbb{F}_{p^k} \leqslant \mathbb{F}_{p^{kn}}$$

y son las tres extensiones de Galois. El automorfismo de Frobenius τ nos permite describir:

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

donde $\tau : \mathbb{F}_{p^{kn}} \to \mathbb{F}_{p^{kn}}$, donde:

$$\tau(\alpha) = \alpha^p \qquad \forall \alpha \in \mathbb{F}_{p^{kn}}$$

Como $\mathrm{Aut}_{\mathbb{F}_{p^k}}(\mathbb{F}_{p^{kn}})$ es un subgrpo de $G = \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^{kn}})$ este último cíclico tenemos que el primero es cíclico.

Si buscamos ahora su generador, como todas las extensiones son de Galois calcular el orden del grpuo equivale a calcular el grado de la extensión. Si observamos de esta forma que:

$$[\mathbb{F}_{p^{kn}} : \mathbb{F}_{p^k}] = n \quad \Longrightarrow \quad |\mathrm{Aut}_{\mathbb{F}_{p^k}}(\mathbb{F}_{p^{kn}})| = n$$

tenemos entonces en vista de τ y del orden del grupo que un generador suyo es τ^k. Llamamos $\phi = \tau^k$, y calculamos:

$$\phi(\alpha) = (\tau^k)(\alpha) = \alpha^{p^k} = \alpha^q$$

Finalmente, como $\mathbb{F}_p^{kn}$ es cuerpo de descomposición de $x^{p^{kn}} - x = x^{q^n} - x \in \mathbb{F}_p[x]$ tenemos entonces que $\mathbb{F}_{q^n}$ es cuerpo de descomposición de $x^{q^n} - x \in \mathbb{F}_q[x]$. □

Notación. En vistas el Teorema anterior, bajo sus mismas hipótesis, llamaremos a ϕ automorfismo de Frobenius de la extensión $\mathbb{F}_q \leqslant \mathbb{F}_{q^n}$.

Teorema 3.22. *Si $f \in \mathbb{F}_q[x]$ es un polinomio irreducible de grado n, entones su cuerpo de descomposición es $\mathbb{F}_{q^n}$. Además, si $\alpha \in \mathbb{F}_{q^n}$ es una raíz de f, entonces el resto de sus raíces son*

$$\alpha^q, \ldots, \alpha^{q^{n-1}}$$

Demostración. f tiene una raíz en alguna extensión de grado n de $\mathbb{F}_q$, por ejemplo $\frac{\mathbb{F}q[x]}{\langle f \rangle}$. Así, tomamos:

$$\mathbb{F}_{q^n} = \frac{\mathbb{F}_q[x]}{\langle f \rangle}$$

Y como la extensión $\mathbb{F}_q \leqslant \mathbb{F}_{q^n}$ es de Galois, tenemos que f es separable y que todas sus raíces están en $\mathbb{F}_{q^n}$. Si α es una raíz de f en $\mathbb{F}_{q^n}$, entonces:

$$\alpha^{q^k} = \phi(\alpha)^k \qquad \forall k \in \{1, \ldots n\}$$

son raíces de f, gracias al grupo de Galois. Además, como tenemos n, son todas sus raíces. □

Si observamos ahora que cada uno de estos f que montamos es un factor irreducible del polinomio $x^{q^n} - x \in \mathbb{F}_q[x]$.

Teorema 3.23. *Un polinomio irreducible $f \in \mathbb{F}_q[x]$ de grado n divide a $x^{q^m} - x \in \mathbb{F}_q[x]$ si, y solo si, n divide a m.*
Como consecuencia, $x^{q^m} - x \in \mathbb{F}_q[x]$ es producto de todos los polinomios irreducibles en $\mathbb{F}_q[x]$ cuyo grado divide a m.

Demostración. Por doble implicación:

$\Longrightarrow$) Supongamos que f es irreducible y que divide a $x^{q^m} - x \in \mathbb{F}_q[x]$. Tomamos sendos cuerpos de descomposición sobre $\mathbb{F}_q$: $\mathbb{F}_{q^n} \leqslant \mathbb{F}_{q^m}$, de donde $n \mid m$ por el Lema de la Torre.

$\Longleftarrow$) Si f es irreducible y $n \mid m$ tenemos entonces que $\mathbb{F}_{q^n} \leqslant \mathbb{F}_{q^m}$ (tomamos $\mathbb{F}_{q^m}$ y por la conexión de Galois encontramos $\mathbb{F}_{p^n}$, ya que el grupo de Galois es cíclico). Ahora, los elementos de $\mathbb{F}_{q^m}$ son las raíces de $x^{q^m} - x \in \mathbb{F}_q[x]$. n de ellas serán las raíces de f, y como todas las raíces son de $x^{q^m} - x$ tenemos entonces que f divide a este.

La consecuencia viene del Teorema de factorización y por el si y solo si. □

Ejemplo. Factoricemos $x^{16} + x \in \mathbb{F}_2[x]$ como producto de irreducibles.

Vemos que $16 = 2^4$, por lo que según el Teorema, para cada divisor de 4 buscamos divisores de dicho grado:

- De grado 1: $x, x - 1$
- De grado 2: $x^2 + x + 1$.
- De grado 4 sabemos que quedan 3 posibles, que tenemos que buscar sin raíces y distintos de $(x^2 + x + 1)^2 = x^4 + x^2 + 1$.

$$x^4 + x + 1, \qquad x^4 + x^3 + 1, \qquad x^4 + x^3 + x^2 + x + 1$$

Y la factorización es:

$$x^{16} + x = x(x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$$

En esta última factorización vemos que $\mathbb{F}_{16}$ puede presentarse de 3 formas distintas sobre $\mathbb{F}_2$, tomando $\mathbb{F}_{16} = \mathbb{F}_2(a)$ con a raíz de cualquiera de los 3 polinomios de grado 3. 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 α^2, α^4 y α^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 α.

  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 están en $x^{16}+x$.

Para calcular sus raíces, calculemos el orden de α 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 α y α^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 α^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 α, que era raíz de f), por lo que creemos que α^7 (la primera potencia de α 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, α^7 es una raíz de g. Ahora:

- Elevamos α^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 α 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 α^2 son $\mathbb{F}_2-$linealmente independientes, por lo que α^3 es raíz de h y obtenemos todas sus raíces elevando α^3 al cuadrado, obteniendo:

$$\alpha^3, \alpha^6, \alpha^{12} \text{ y } \alpha^9$$

Las que quedan son α^5 y α^{10}, que han de ser raíces de k.

Podríamos haberlo hecho también pensando también en que α^5 tiene orden 3 y α^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 $\mathbb{F}_3^\times$, 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.

3.9. Ejercicios de exámenes finales

Ejercicio 3.9.1. 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 α:

$$x^3 + x + 1 = 0, \qquad x^3 + x^2 + 1 = 0, \qquad x^2 + x + 1 = 0$$

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 α 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 α, α^2 y α^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 α, las raíces de $x^3 + x^2 + 1$ son α^3, α^5 y α^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 $2 \nmid 3$.