Álgebra III

Foto: José Juan Castro

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 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 $s \leqslant k$, 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).

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:

$$F \leqslant K$$

Es fácil ver (hágase) que las intersecciones arbitrarias de cuerpos siguen siendo cuerpos, propiedad que justifica el concepto que vamos a introducir.

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

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

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.

Definición 1.5 (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 1.3. *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 (hágase) en el subcuerpo primo 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[1] 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 $\Pi = Q \cong \mathbb{Q}$. □

[1] 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.

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

Definición 1.6. Si $F \leqslant K$ es una extensión, la dimensión de K sobre F como espacio vectorial recibe el nombre de "grado de la extensión $F \leqslant K$", denotado por:

$$[K : F]$$

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

Ejemplo. Como ejemplos a destacar:

- $\mathbb{R} \leqslant \mathbb{C}$ tiene grado de extensión $[\mathbb{C} : \mathbb{R}] = 2$.
- 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 1.7 (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[2].

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

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

[2]No confundir una extensión finitamente generada con una extensión finita de cuerpos.

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 $\alpha = a + b\sqrt{2}$, 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 puede tener otro más general como que:

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

En general, esta no es la definición del menor subcuerpo generado por cierto conjunto.

Definición 1.8 (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[3] 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 $\mathbb{Q}(\sqrt{2})$.

[3]Fundamentado por el Teorema Fundalmental del Álgebra.

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:

$\subseteq$) $F(S \cup T)$ 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[4] 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 $\mathbb{Q}\left(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\right)$.

□

[4]Recordamos que si α es una raíz múltiple de f, entonces α es una raíz de f'.

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.

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 1.9 (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 1.4. *Sean $F \leqslant K$ extensión, $\alpha \in K$ algebraico sobre F. Existe un único polinomio mónico*[5] *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 $e_\alpha : F[x] \to K$ por:

$$e_\alpha(g) = g(\alpha) \qquad \forall g \in F[x]$$

que es un homomorfismo de anillos (compruébese). 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:

[5] El coeficiente líder es 1.

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

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

- Por el Primer Teorema de Isomorfía, e_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 un cuerpo, luego Ime_α también es un dominio de integridad, 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 tal que $h(\alpha) = 0$, 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 $\frac{F[x]}{\langle f \rangle}$ era un cuerpo, de donde el isomorfismo

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

  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 $\alpha \in F(\alpha)$, de donde $g(\alpha) \in F(\alpha)$, 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 $F(\alpha)$, primero vamos a tratar de buscar una base en $\frac{F[x]}{\langle f\rangle}$ 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 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:

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

Luego $B = \{1+\langle f\rangle, x+\langle f\rangle, \ldots, x^{degf-1}+\langle f\rangle\}$ es un sistema de generadores de $\frac{F[x]}{\langle f\rangle}$, que además es una base por ser sus elementos linealmente independientes. El isomorfismo

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

viene dado por (a partir del Primer Teorema de Isomorfia) la correspondencia $g + \langle f\rangle \mapsto g(\alpha)$. Este es $F-$lineal, por lo que transforma la base B en el conjunto $\mathcal{B}$. Como los isomorfismos lineales transforman bases en bases (visto en Geometría I), tenemos que $\mathcal{B}$ es una $F-$base de $F(\alpha)$.

□

Definición 1.10 (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 $Irr(\alpha, F)$.
Observemos que este cumple $[F(\alpha) : F] = degIrr(\alpha, F)$. 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 $g = hIrr(\alpha, F)$.

Ejemplo. Veamos ejemplos de esta última definición:

- $Irr(i, \mathbb{Q}) = x^2 + 1 \in \mathbb{Q}[x]$, luego $\{1, i\}$ es una $\mathbb{Q}-$base de $\mathbb{Q}(i)$.
- $Irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2 \in \mathbb{Q}[x]$, luego $\{1, \sqrt{2}\}$ es una $\mathbb{Q}-$base de $\mathbb{Q}(\sqrt{2})$.
- $Irr\left(e^{\frac{2\pi i}{3}}, \mathbb{Q}\right)$. 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

Lema 1.5 (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 $L-$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 base de L sobre K y $\{v_1, \ldots, v_m\}$ base de K sobre F, es fácil ver entonces que:

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

es una $F-$base de L.

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:

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

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

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

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

de donde:

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

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

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

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

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

por el lema de la Torre:

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

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

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

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 1.6. *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, tomamos $L=F(\alpha)$ y la Proposición **??** nos da la condición deseada.

$\Longleftarrow$) 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 $F\leqslant F(\alpha)$ es finita. Como el conjunto $\{1,\alpha,\ldots,\alpha^n,\ldots\}$ es un $F-$sistema de generadores de $F(\alpha)$, tenemos entonces que existe $m\in\mathbb{N}$ con $m\geqslant 1$ de forma que α^m depende linealmente sobre F 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:

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

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

□

Definición 1.11 (Extensión algebraica)**.** Una extensión $F \leqslant K$ se dice algebraica si todo $\alpha \in K$ es algebraico sobre F.

Teorema 1.7. *Una extensión $F \leqslant K$ es finita si y solo si es algebraica y finitamente generada.*

Demostración. 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 $\alpha \in K$, entonces $F \leqslant F(\alpha)$ es finita. Tomando $L = F(\alpha)$ y aplicando la Proposición anterior tenemos la implicación.

$\Longleftarrow$) 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 **??**, 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 1.7.1. *Si $F \leqslant K$ extensión y llamamos:*

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

Entonces, Λ es un subcuerpo de K y $F \leqslant \Lambda$ es algebraico.

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 1.12 (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:

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

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

1.2.1. Ejercicios

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

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

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

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:

$$2\alpha\sqrt{2}=\alpha^2+5\Longrightarrow8\alpha^2=\alpha^4+25+10\alpha^2\Longrightarrow\alpha^4+2\alpha^2+25=0$$

Por lo que:

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

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:

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

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

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

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

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

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

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

1.3. Construcciones con regla y compás

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

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

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

En lo que sigue, sea S un conjunto de puntos del plano con al menos dos puntos distintos (ya que bajo los postulados en los que nos basamos con cero o un punto no somos capaces de construir nada más), definimos ahora 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 **??**.

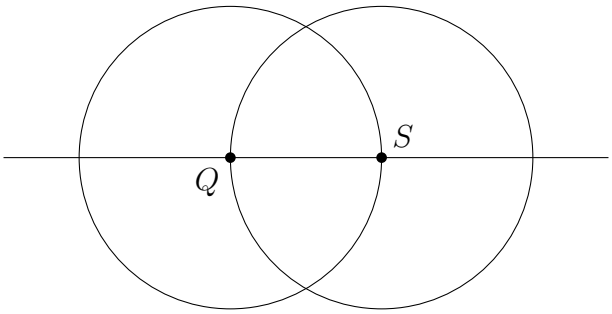


Figura 1.1: Prueba gráfica de que $S \subseteq S^c$.

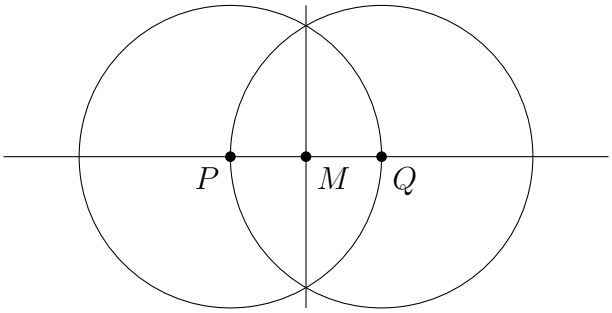


Figura 1.2: Construcción de la mediatriz.

Definición 1.13. Dado un conjunto de puntos del plano S, definimos recursivamente:

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

Llamamos al conjunto:

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

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

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

Para ello, primero necesitamos considerar la construcción de la mediatriz, con la que obtenemos el punto medio entre dos puntos P y Q. Esta viene dada por la Figura **??**. 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 **??**

Lema 1.8. *Sean P, Q, R puntos del plano con P y Q distintos, se puede construir con regla y compás a partir de ellos un punto T tal que las rectas PQ y RT son perpendiculares.*

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

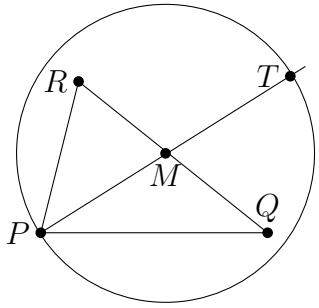


Figura 1.3: Completar el cuarto punto de un paralelogramo.

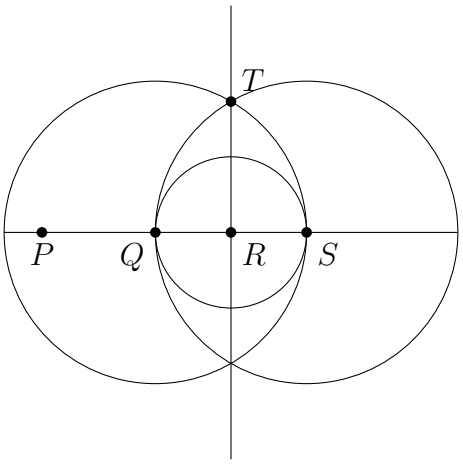


Figura 1.4: Trazar recta perpendicular por R.

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

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

□

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

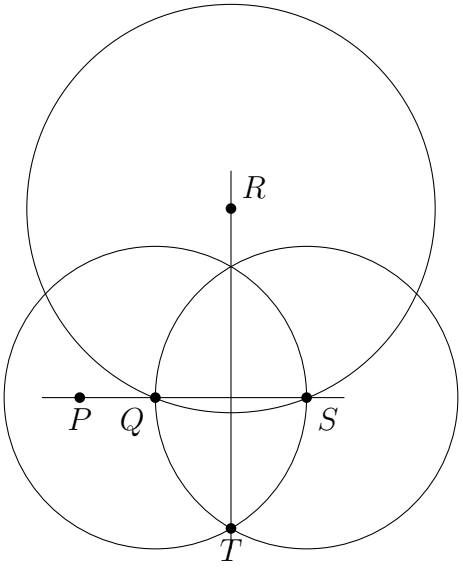
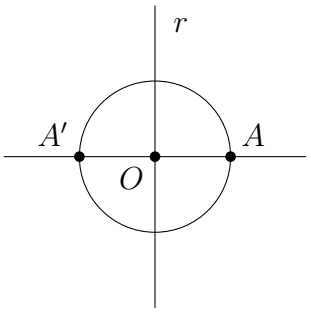
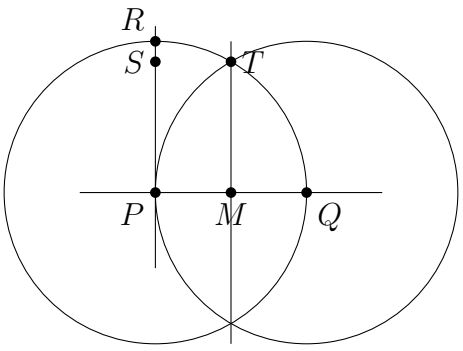


Figura 1.5: Trazar recta parpendicular por R.

de centro O y radio hasta A obtenemos como intersección con la recta perpendicular a r el punto A', simétrico de A respecto de r.



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



Trazar las dos circunferencias que definen los puntos P y Q, con lo que trazamos la mediatriz, la recta que se obtiene uniendo los puntos de intersección de las dos circunferencias. Nombramos a un punto de dicha intersección T. Trazamos la

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

Hemos obtenido lo que consideraríamos un sistema de referencia ortonormal, y podemos renombrar los puntos P, Q y R como $(0,0)$, $(1,0)$ y $(0,1)$, respectivamente. De esta forma, podemos ver el conjunto $C(S)$ de puntos constructibles a partir de S como un subconjunto de $\mathbb{C}$. A partir de ahora, supondremos siempre que S es un conjunto que contiene a los números 0 y 1.

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

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

Lema 1.9. *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 **??**.

$\Longleftarrow$) 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 **??**.

□

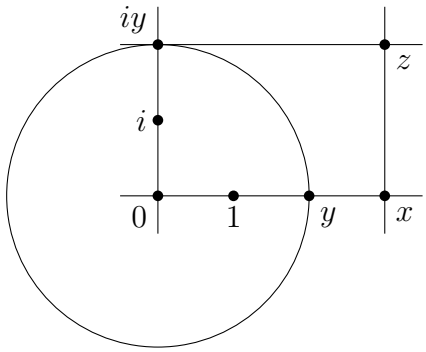


Figura 1.6: Obtención de x, y a partir de z.

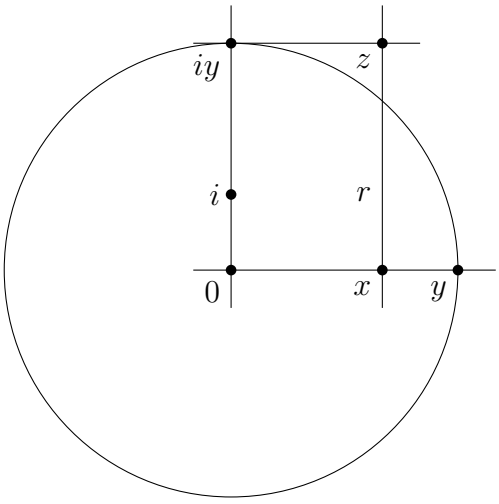


Figura 1.7: Obtención de z a partir de x e y.

Proposición 1.10. *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 **??** que la suma de dos números complejos constructibles es constructible. Análogamente, si demostramos que el producto de dos números reales constructibles es constructible, tendremos que el producto de dos números constructibles es construcible. Para el inverso, si demostramos que todo conjugado de un número construcible es constructible, tendremos probado que los inversos de los números constructibles serán números constructibles, puesto que ya sabemos que el producto de números constructibles es constructible y:

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

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

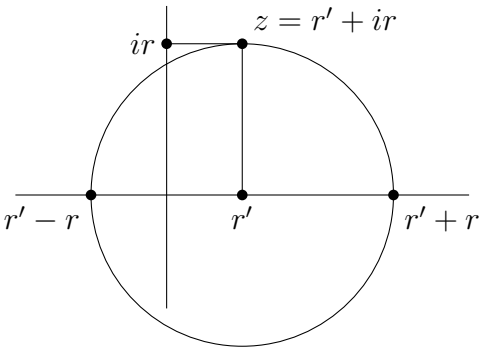
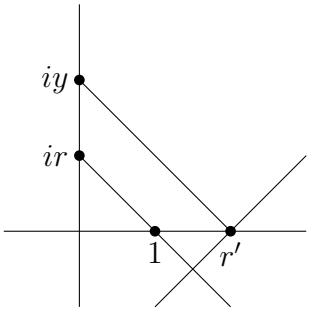


Figura 1.8: Obtención de $r' + r$ y $r' - r$ a partir de r y r'.

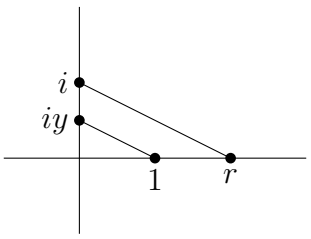
Por lo que $r + r', r - r' \in C(S) \cap \mathbb{R}$.
Bajo las mismas hipótesis, tratamos de probar que $r \cdot r' \in C(S) \cap \mathbb{R}$, supondremos de la misma forma que $r, r' > 0$ y lo que haremos será considerar los puntos r', ir. Trazaremos la recta que une el punto 1 con ir y trazaremos la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



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

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

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



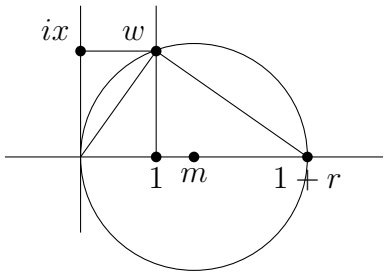
Ambos triángulos semejantes, luego:

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

□

Lema 1.11. *Si $z \in C(S)$, entonces $\sqrt{z} \in C(S)$.*

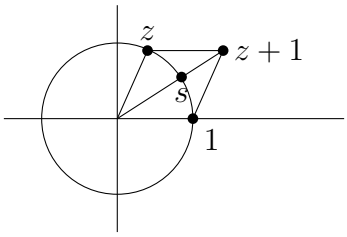
Demostración. Escribiendo z en forma polar, reducimos el problema al caso $|z| = 1$. Si tomamos $r > 0$ con $r \in C(S) \cap \mathbb{R}$, veamos entonces que $\sqrt{r} \in C(S) \cap \mathbb{R}$. Para ello, consideramos el punto $1 + r$ (anteriormente probamos que era constructible), trazamos el punto 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 1.12. *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 **??** 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 1.14. 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 1.13. *Sean $F = \mathbb{Q}(S \cup \overline{S})$ 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 1.13.1. *$C(S)$ 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.*

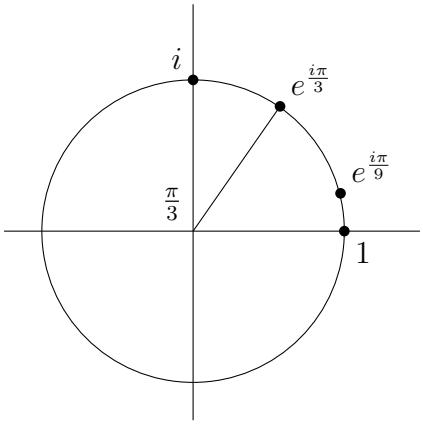
Corolario 1.13.2. *Todo número constructible ($F = \mathbb{Q}$) tiene grado sobre $\mathbb{Q}$ una potencia de 2.*

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^{o} 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:

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

de donde usando la fórmula del ángulo triple:

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

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

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

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

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

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

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

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

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

1.4. Homomorfismos de cuerpos

Lema 1.14. *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:

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

□

Definición 1.15 (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 1.16. Siempre que tengamos $F \xrightarrow{\sigma} K$ y $f \in F[x]$ dada por:

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

Definiremos:

$$f^\sigma = \sum_{i=1}^{n} \sigma(f_i) x^i \in K[x]$$

Se verifica que la correspondencia $f \mapsto f^\sigma$ es un homomorfismo de anillos entre $F[x]$ y $K[x]$.

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

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

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

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

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

que es un homomorfismo de anillos (observemos que es la composición de la proyección al cociente con la inclusión en $F[x]$) entre cuerpos, luego 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:

$$f^\sigma(\alpha) = \sum_{i=1}^{n}(f_i + \langle p\rangle)(x + \langle p\rangle)^i = \sum_{i=1}^{n} f_i x^i + \langle p\rangle = f + \langle p\rangle \overset{(*)}{=} 0 + \langle p\rangle$$

donde en $(*)$ hemos usado que p es un factor de f. Además:

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

$\subset$) Basta ver que K contiene a $\sigma(F)$ y a α.

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

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

Por lo que:

$$g + \langle p\rangle = \sum_{i=1}^{n} g_i x^i + \langle p\rangle = \sum_{i=1}^{n}(g_i + \langle p\rangle)(x + \langle p\rangle)^i \in \sigma(F)(\alpha)$$

Lema 1.15. *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 $\sigma(F)$.

Demostración. La demostración se deduce del ejemplo anterior. □

Proposición 1.16. *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 **??**, con lo que existen $F \xrightarrow{\tau} K$ y $\alpha \in K$ tal que $p^\tau(\alpha) = 0$ y $K = F(\alpha)$. 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 defintiiva, 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 $L[x]$. Tomamos ahora como E el subcuerpo de L generado por las raíces de f^σ y $\sigma(F)$, con lo que E es un cuerpo de descomposición de f^σ.

□

Definición 1.17. A un homomorfismo $\sigma : F \to E$ como el de la Proposición anterior se le llama (haciendo un pequeño abuso de notación) cuerpo de descomposición de f.

Ejemplo. Tomamos $f = x^2 + x + 1 \in \mathbb{F}_2[x]$, donde:

$$\mathbb{F}_2 = \{0, 1\}$$

Como $f(0) = f(1) = 1 \neq 0$, tenemos que f no tiene raíces en $\mathbb{F}_2$. Buscamos 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:

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

Tomaremos:

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

sabemos ya que:

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

Si factorizamos f^σ (usando que $\alpha^2 + \alpha + 1$):

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

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

$$K = \mathbb{F}_2(\alpha), \qquad Irr(\alpha, \mathbb{F}_2) = x^2 + x + 1, \quad \text{ó} \quad \alpha^2 + \alpha + 1 = 0$$

¿Cuántos elementos tiene K?
En vista de que $[K : \mathbb{F}_2] = 2$, tenemos que $|K| = 4$. Para listarlos:

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

  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, tomamos

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

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 $a^3 + a + 1 = 0$, siendo a una raíz de f. Tratamos de factorizar f en $\mathbb{F}_2(a)$:

$$\begin{array}{rcrcrcr|l}
x^3 & + & & + & x & + & 1 & x + a \\
x^3 & + & ax^2 & & & & & \hline
\multicolumn{7}{r|}{x^2 + ax + (a^2 + 1)} \\ \hline
 & & ax^2 & + & x & + & 1 & \\
 & & ax^2 & + & a^2x & & & \\ \hline
 & & & & (a^2 + 1)x & + & 1 & \\
 & & & & (a^2 + 1)x & + & a^3 + a & \\ \hline
 & & & & & & a^3 + a + 1 &
\end{array}$$

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

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

Dividimos ahora entre $x + a^2$:

$$\begin{array}{rcrcrcr|l}
x^2 & + & & + & ax & + & a^2 + 1 & x + a^2 \\
x^2 & + & a^2x & & & & & \hline
\multicolumn{7}{r|}{x + a^4} \\ \hline
a^4x & = & a(a + 1)x & + & a^2 + 1 & & & \\
 & & a^4x & + & a^6 & & & \\ \hline
 & & & & & & a^6 + a^2 + 1 &
\end{array}$$

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 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, 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, con lo que $\mathbb{F}_8 = \mathbb{F}_2(a)$.

Lema 1.17. *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:

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

que es un homomorfismo de anillos, luego 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 $\langle p \rangle = \ker(\overline{\sigma_\alpha})$. 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 1.18. Si tenemos dos homomorfismos de cuerpos:

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

definimos el conjunto de las $\sigma-$extensiones de τ por:

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

Es decir, el conjunto formado por todas las aplicaciones $\eta : K \to E$ que hacen el siguiente diagrama conmutativo:

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

Proposición 1.18 (Extensión)**.** *Si tenemos dos homomorfismos de cuerpos:*

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

Sea $p \in F[x]$ 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, si $K = \sigma(F)(\alpha)$ tenemos entonces que:

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

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 p^η tiene sus coeficientes evaluados por η y está siendo evaluado en $\eta(\alpha)$. Esto prueba que[8] $\eta(\alpha) \in \mathcal{R}$. Veamos ahora que la aplicación enunciada es sobreyectiva[9]. Para ello, sea $\beta \in \mathcal{R}$, buscamos un elemento del dominio cuya imagen vaya a β. Usando el Lema **??**, obtenemos los isomorfismos:

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

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

Si tomamos:

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

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

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

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

$$(\eta \circ \sigma)(a) = (i \circ \tau_\beta \circ \sigma_\alpha^{-1})(\sigma(a)) = (i \circ \tau_\beta)(\sigma_\alpha^{-1}(\sigma(a))) = (i \circ \tau_\beta)(a) = i(\tau_\beta(a)) = a$$

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:

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

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 $K = \sigma(F)(\alpha)$, si tomamos un elemento de K este será de la forma:

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

con lo que:

$$\eta\left(\sum_i \sigma(a_i)\alpha^i\right) = \sum_i \eta(\sigma(a_i))\eta(\alpha)^i = \sum_i \eta'(\sigma(a_i))\eta'(\alpha)^i = \eta'\left(\sum_i \sigma(a_i)\alpha^i\right)$$

para cualquier elemento de K, con lo que $\eta = \eta'$, luego la aplicación es inyectiva. □

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

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

Lema 1.19. *Sean tres homomorfismos esntre cuerpos:*

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

Entonces:

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

Demostración. Por doble inclusión:

$\subseteq$) Si tomamos $\theta \in Ex(\tau, \sigma_2\sigma_1)$, obtenemos:

$$\eta = \theta\sigma_2$$

con lo que tambien está en alguno de la unión de la derecha.

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

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

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

Ahora, la unión es disjunta ya que si tomamos dos η distintos, el resultado de la composición será distinto. □

Proposición 1.20. *Sean:*

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

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 $Ex(\tau, \sigma) = \{\tau\sigma^{-1}\}$

- Supuesto que $n > 1$ y la hipótesis de inducción, existe $\alpha \in K$ de forma que $[\sigma(F)(\alpha) : \sigma(F)] > 1$. El Lema de la Torre nos dice que $[K : \sigma(F)(K)] < n$. Sea $\iota : \sigma(F)(\alpha) \to K$ la inclusión, podemos tomar:

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

con $\sigma' : F \to \sigma(F)(\alpha)$ la restricción en codominio (o correstricción) de σ. 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 tenemos que:

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

con lo que:

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

Tomamos $p \in F[x]$ tal que $Irr(\alpha, \sigma(F)) = p^\sigma$ (notemos que es irreducible). La Proposición de extensión nos dice que:

$$|Ex(\tau, \sigma')| = \text{número de raíces de } p^\tau \text{ en } E \leqslant degp^\tau = [\sigma(F)(\alpha) : \sigma(F)]$$

Con lo que aplicando el Lema de la Torre:

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

lo que completa la inducción.

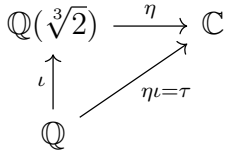
□

Ejercicio 1.4.1. Si $\sigma : P \to K$ es un homomorfismo de cuerpos y P es el subcuerpo primo de K, entonces σ es el homomorfismo inclusión (**Sugerencia:** $\sigma(1) = 1$).

Ejemplo. Ejemplo básido de la proposición de extensión.

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

Tomamos $\eta : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$, si llamamos $\iota : \mathbb{Q} \to \mathbb{Q}(\sqrt[3]{2})$



Lo que quiero calcular es $Ex(\tau, \iota)$. Como si tomamos $\alpha = \sqrt[3]{2}$:

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

Como:

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

donde w es una raíz cúbica primitiva de la unidad. Por lo que tenemos tres homomorfismos de $\mathbb{Q}(\sqrt[3]{2})$ en $\mathbb{C}$. Si consideramos:

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

donde η_i está determinado por:

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

Calculemos:

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

Proposición 1.21. *Sean $\tau : F \to E$, $\sigma : F \to K$ 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 $deg f^\sigma$ raíces distintas, entonces:*

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

Ejercicio 1.4.2. Continuación del ejemplo anterior.
Sea $K = \mathbb{Q}(\sqrt[3]{2}, w)$ con w una raíz cúbica primitiva de la unidad, tenemos:

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

con τ la inclusión de $\mathbb{Q}$ en $\mathbb{C}$, Queremos calcular todos aquellos η_j, para $j \in \{0, 1, 2\}$:

$$\eta_0(\sqrt[3]{2}) = w^0\sqrt[3]{2}$$

Calculamos para cada j todas las σ_2-extensiones:

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

con $\eta_j \in Ex(\tau, \sigma_1)$. Necesitamos calcular el polinomio irreducible de w sobre $\mathbb{Q}(\sqrt[3]{2})$ y calcular sus raíces en $\mathbb{C}$:

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

con raíces w, w^2, tenemos 2 σ_2-extensiones:

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

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

determinadas por

$$\eta_{j,k}(\sqrt[3]{2}) = w^0\sqrt[3]{2}, \qquad \eta_{j,k}(w) = w^k$$

Cuando F es subcuerpo de K, sea σ la inclusión, los elementos de $Ex(\tau, \sigma)$ se llaman extensiones de σ.

Sabíamos que tenían que ser 6 extensiones porque todas las raíces son distintas.

Ejercicio 1.4.3. Sea $F \xrightarrow{\tau} E \xrightarrow{\rho} E$. Sabemos que E es un $\tau(F)-$espacio vectorial, luego:

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

Teorema 1.22 (Unicidad de los cuerpos de descomposición)**.** *Sean $\tau : F \to E$ y $\tau' : F \to E'$ cuerpos de descomposición de $f \in F[x]$. Existe un isomorfismo de cuerpos $\eta : E \to E'$ tal que $\eta\tau = \tau'$.*

Demostración. Por la proposición de hoy, sabemos que existe $\eta : E \to E'$ y $\eta' : E' \to E$ tales que

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

si observamos que:

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

el ejercicio nos dice que $\eta\eta'$ es $F-$lineal. Ahora, como:

$$[E' : \tau'(F)] < \infty$$

tenemos entonces que $\eta\eta' : E \to E$ es inyectiva, con lo que automáticamente obtenemos que $\eta\eta'$ es biyectiva. De aquí concluimos que η es sobreyectiva, pero como era un homomorfismo de cuerpos, concluimos que η es biyectiva, con lo que η es un isomorfismo. □

1.5. Clasificación de los cuerpos finitos

Proposición 1.23. *Sea F un cuerpo finito con[10] $q = p^n$ elementos (para p la característica de F), entonces F es cuerpo de descomposición de $x^q - x \in \mathbb{F}_p[x]$.*

Demostración. Llamamos $f = x^q - x$, tomamos: $F^\times = F \setminus \{0\}$, 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 $qx^{q-1} - 1 = 0$, tenemos entonces que $x^q - x$ tiene exactamente q raíces distintas, que son todos aquellos elementos de F, con lo que F es cuerpo de descomposición de $f \in \mathbb{F}_p[x]$. □

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

Teorema 1.24 (Clasificación de cuerpos finitos)**.** *Para cada primo p y 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 $f = x^q - x \in \mathbb{F}_p[x]$. Sea S el conjunto de las raíces de f en F, veamos que S es un subcuerpo de F, pueso que:

[10] Sabemos que es así por el subcuerpo primo.

- $1 \in S$.
- Si $a, b \in S$, es claro que $ab \in S$, y el Ejercicio **??** nos dice que $a - b \in S$.
- Ahora, si $a \in S \setminus \{0\}$, tenemos entonces que a es raíz de $x^{q-1} - 1$, con lo que a^{-1} también.

Finalmente, como F es un cuerpo de descomposición de f, ha de ser $S = F$. Finalmente, como el polinomio derivado no comparte raíces con f, tenemos que $|S| = q$.

Ahora, si tenemos dos cuerpos del mismo cardinal, la Proposición **??** 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 iguales.

Sea ahora F, tenemos por el Ejercicio **??** 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.

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 1.19 (Grupo de automorfismos de un cuerpo)**.** Sea K un cuerpo, consideremos el conjunto de todos los automorfismos de K:

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

Se verifica que $Aut(K)$ 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, tomamos:

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

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

Si Π es el subcuerpo primo de K, entonces $Aut_\Pi(K) = Aut(K)$.

Proposición 1.25. *Si $F \leqslant K$ es finita, entonces $|Aut_F(K)| \leqslant [K : F]$*

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

$$Aut_F(K) = Ex(\iota, \iota)$$

$\subseteq$) Basta recordar un ejercicio que nos decía $(*)$.

$$Ex(\iota,\iota) = \{\sigma : K \to K : \sigma\iota = \iota\} \overset{(*)}{=} \{\sigma : K \to K : \sigma \text{ es } F-\text{lineal}\}$$

$\supseteq$) Si tomamos $\sigma \in Ex(\iota,\iota)$ como es homomorfismo de cuerpos tenemos que es inyectivo, y como es $F-$lineal, ha de ser necesariamente sobreyectivo, con lo que $\sigma \in Aut_F(K)$

De donde la segunda propiedad de extensión nos dice que:

$$|Aut_F(K)| = |Ex(\iota,\iota)| \leqslant [K:F]$$

□

Proposición 1.26. *Si $F \leqslant K$ es cuerpo de descomposición de $f \in F[x]$, entonces:*

$$|Aut_F(K)| \leqslant [K:F]$$

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

$$|Aut_F(K)| = [K:F]$$

Ejemplo. Según un ejemplo ya visto, tenemos que:

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

con lo que la Proposición nos dice que:

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

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

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

donde:

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

resulta que tenemos un grupo no conmutativo, por lo que es isomorfo a S_3.

Teorema 1.27. *Sea $\mathbb{F}_q$ un cuerpo finito con $q = p^n$, entonces $Aut(\mathbb{F}_q)$ es un grupo cíclico de orden n.*

Demostración. Sabemos por una proposición anterior 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). La proposición que hemos visto antes nos dice que:

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

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 **??** que es un homomorfismo de cuerpos, luego un automorfismo (que recibe el nombre de automorfismo de Frobenius). Veamos que su oren es n: sea $m \in \mathbb{N} \setminus \{0\}$ de forma que:

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

Un ejercicio nos dice que $\mathbb{F}_q^\times$ es cíclico, que usa la descomposición cíclica. Tomamos a como su generador, que será de orden $q-1$, lo que nos dice entonces que:

$$a = \tau^m(a) = a^{p^m}$$

de donde $p^m - 1 \geqslant p^n - 1$, luego $m \geqslant n$, de donde $O(\tau) = n$, con lo que $Aut(\mathbb{F}_q)$ está generado por τ. □

1.7. Ejercicios

2. Extensiones de Galois

Proposición 2.1. *Sea $F \leqslant K$ una extensión finita, entonces $|Aut_F(K)| \leqslant [K : F]$.*

Ejemplo. Sea $Aut(\mathbb{Q}(\sqrt[3]{2}))$, sabemos que:

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

Y afirmamos que es uno solo, ya que:

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

y raíces de $x^3 - 2$ en dicho cuerpo solo hay 1. Sin embargo, anteriormente vimos que:

$$|Aut(\mathbb{Q}(\sqrt[3]{2}))| = 6$$

Por lo que la idea intuitiva es que faltan raíces en el cuerpo.

Definición 2.1. Sea K un cuerpo y $G \leqslant Aut(K)$ subgrupo, definimos el subcuerpo fijo de K bajo (la acción de) G:

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

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

Proposición 2.2 (Artin)**.** *Si G es un subgrupo finito de $Aut(K)$, entonces.*

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

Demostración. Sea $n = |G|$, suponemos $G = \{\sigma_1, \ldots, \sigma_2\}$ y tomamos elementos $\alpha_1, \ldots, \alpha_m \in K$ con $m > n$, basta probar que los elementos α_i son linealmente dependientes. Formamos la matriz:

$$A = (\sigma_j(\alpha_i))_{i,j} \in M_{m \times n}(K)$$

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 aquel con número de componentes no nulas mínimo y tal que alguna

componente, digamos $v_l \in K^G$. De hecho, podemos tomar $v_l = 1$. Si escribimos la igualdad $vA = 0$:

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

Para obtener la dependencia lineal falta ver que realmente los coeficientes v_i están en K^G (por ahora solo sabemos que están en K). Supuesto que algún coeficiente $v_{l'} \neq \sigma_k(v_{l'})$ para alguna pareja de índices l, k, tomamos cualquier $\sigma \in G$, con lo que:

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

Tenemos que:

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

Aplicamos σ_k a la igualdad anterior, con lo que:

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

Observemos que:

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

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

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

Tenemos pues que:

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

Además:

$$v - \sigma_k(v) \neq 0$$

ya que si miramos la componentes $l'-$ésima, estas son distintas. Sin embargo, las componentes $l-$ésimas son iguales. Y tenemos que $v - \sigma_k(v)$ tiene al menos una componente no nula menos que v, contradicción, que viene de suponer que $v_{l'} \neq \sigma_k(v_{l'})$, lo que nos dice que realmente los coeficientes v_i estaban en K^G, tomamos $\sigma_j = id \in G$, con lo que:

$$\sum_i v_i \alpha_i = 0$$

lo que implica que $\alpha_1, \dots, \alpha_m$ eran linealmente dependientes, por lo que:

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

□

Lema 2.3. *Para un cuerpo K, tenemos que:*

1. *Si $H \subseteq G$ son subgrupos de $Aut(K)$, entonces $K^H \geqslant K^G$.*
2. *Si $F \leqslant E$ son subcuerpos de K, entonces $Aut_F(K) \supseteq Aut_E(K)$.*
3. *Si G es subgrupo de $Aut(K)$, entonces $G \subseteq Aut_{K^G}(K)$.*
4. *Si $F \leqslant K$, entonces $F \leqslant F^{Aut_F(K)}$.*

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

Teorema 2.4. *Si G es un subgrupo finito de $Aut(K)$ para un cuerpo K, entonces:*

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

Demostración. El Lema anterior nos dice que $G \leqslant Aut_{K^G}(K)$, y el Lema de Artin nos dice que $[K : K^G] \leqslant |G|$, con lo que en particular la extensión es finita, luego:

$$|G| \leqslant |Aut_{K^G}(K)| \leqslant [K : K^G] \leqslant |G|$$

□

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

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

donde:

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

Los subgrupos propios de $Aut(K)$ (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 de orden 2 sabemos que no es cíclico.

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

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). 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:

$$[K^{\eta_{1,1}} : \mathbb{Q}] = 2$$

buscamos una extensión de grado 2 de $\mathbb{Q}$ que esté dentro de $Aut(K)$. 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 $\eta_{1,1}(w)=w$, por lo que $w\in K^{\langle\eta_{1,1}\rangle}$, lo que implica que $\mathbb{Q}(w)\leqslant K^{\langle\eta_{1,1}\rangle}$. Además, como la extensión es 2 en ambos casos, ha de ser por tanto $\mathbb{Q}(w)=K^{\langle\eta_{1,1}\rangle}$.
Se pide calcular $K^{\langle\eta_{2,2}\rangle}, K^{\langle\eta_{1,2}\rangle}, K^{\langle\eta_{2,2}\rangle}$, para ello buscaremos extensiones de grado 3 en $\mathbb{Q}$, un elemento de grado 3 es $\sqrt[3]{2}$, otro será $w\sqrt[3]{2}$ y otro $w^2\sqrt[3]{2}$.

Ejercicio 1. 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:

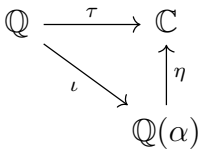
   $$\left.\begin{array}{l}1=a^2+3b^2\\2=2ab\end{array}\right\}\Longrightarrow\left\{\begin{array}{l}b=\frac{1}{a}\\1=a^2+3\frac{1}{a^2}\end{array}\right\}\Longrightarrow a^2=a^4+3$$
   $$\Longrightarrow a^2=\frac{1\pm\sqrt{1-12}}{2}\notin\mathbb{Q}\Longrightarrow a\notin\mathbb{Q}$$

   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 $\alpha, -\alpha, \beta, -\beta$.