

Álgebra III

FACULTAD
DE
CIENCIAS
UNIVERSIDAD DE GRANADA



Los Del DGIIM, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada



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

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

Álgebra III

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán

Granada, 2025

Índice general

1. Extensiones de cuerpos y raíces de polinomios	5
1.1. Extensiones de cuerpos y elementos algebraicos	8
1.1.1. Elementos algebraicos	11
1.2. Extensiones finitas y extensiones algebraicas	15
1.3. Construcciones con regla y compás	20
1.4. Homomorfismos de cuerpos	30

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*

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

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

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

Para $k = 1$. 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 $s \leq k$, vemos que:

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

Acabamos de probar que $\chi = \varphi$, por lo que en caso de existir solo existe un único homomorfismo $\chi : \mathbb{Z} \rightarrow A$. Este se puede calcular exigiendo $\chi(1) = 1$.

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

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

Por lo que $\text{Im}\chi \subseteq S$. □

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

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

En dicho caso, sabemos de Álgebra I que $\ker \chi$ es un ideal en \mathbb{Z} , y como todos los ideales de \mathbb{Z} son principales (por ser \mathbb{Z} un Dominio Euclídeo), sabemos que $\exists n \in \mathbb{N}$ de forma que $\ker \chi = n\mathbb{Z}$. Dicho número n recibe el nombre de “característica de A ” (aunque varios números 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:

$$F \leq K$$

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:

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

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 $\Gamma = \{F \subseteq K : F \leq K\}$. 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 $\chi : \mathbb{Z} \rightarrow K$, tenemos que $\text{Im}\chi$ es el menor subanillo de K , por lo que estará contenido (hágase) en el subcuerpo primo de K , que denotaremos por Π ; es decir, $\text{Im}\chi \subseteq \Pi$. Aplicando el Primer Teorema de Isomofría sobre χ obtenemos que:

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

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

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

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

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

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

Como teníamos que $\text{Im}\chi \subseteq \Pi$, podemos calcular Q dentro¹ 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 $\Pi = Q \cong \mathbb{Q}$. \square

¹Si $A \subseteq B$ 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 $F \leq K$ extensión, entonces K es un espacio vectorial sobre F .

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

$$[K : F]$$

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

Ejemplo. Como ejemplos a destacar:

- $\mathbb{R} \leq \mathbb{C}$ 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 $n \geq 1$.

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:

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

Luego K ha de tener cardinal p^n .

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

1.1. Extensiones de cuerpos y elementos algebraicos

Definición 1.7 (Extensión generada por un subconjunto). Sea $F \leq K$ 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 $S = \{s_1, \dots, s_t\}$, simplificaremos la notación y escribiremos $F(s_1, \dots, s_t)$.
- Si $K = F(\alpha_1, \dots, \alpha_t)$ para ciertos elementos $\alpha_1, \dots, \alpha_t \in K$, diremos entonces que $F \leq K$ es una extensión finitamente generada².

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

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

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

Demostración. Veámoslo:

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

⊆) 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:

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

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

□

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

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

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 $K \leq E$ extensión de cuerpos tal que f se descompone completamente en $E[x]$ como producto de polinomios lineales (es decir, de grado 1) y $E = K(\alpha_1, \dots, \alpha_t)$ con $\alpha_1, \dots, \alpha_t \in E$ 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 $\mathbb{R} \leq \mathbb{C}$ 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 $\mathbb{Q} \leq \mathbb{Q}(i)$ y $\mathbb{Q}(i) = \mathbb{Q}(i, -i)$.

Observación. Si $f \in \mathbb{Q}[x]$ y tomo³ todas sus raíces en \mathbb{C} , digamos $\alpha_1, \dots, \alpha_t$, entonces un cuerpo de descomposición de f es $\mathbb{Q}(\alpha_1, \dots, \alpha_t)$

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

³Fundamentado por el Teorema Fundamental del Álgebra.

Ejercicio 1.1.1. Si tenemos $F \leq K$ 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 subcuerpo de K que contiene a $F \cup S \cup T$, por lo que para ver esta inclusión hemos de ver que $F(S)(T)$ es un 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 polinomio tiene 3 raíces distintas, ya que su polinomio derivado⁴ 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:

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

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

Demostración. Por doble inclusión:

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

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

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

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

□

⁴Recordamos 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 $n \geq 1$ y nos preguntamos sobre un cuerpo de descomposición de dicho polinomio, que tiene n raíces, y:

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

Por lo que no comparte raíces con f' , luego tiene n raíces distintas, todas ellas de multiplicidad 1, que 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 $F \leq K$ 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 $F \leq K$ extensión, $\alpha \in K$ algebraico sobre F . Existe un único polinomio mónico⁵ irreducible $f \in F[x]$ tal que $f(\alpha) = 0$. Además, se tiene un isomorfismo de cuerpos $F(\alpha) \cong \frac{F[x]}{\langle f \rangle}$, donde $\langle f \rangle$ denota el ideal principal generado por f :

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

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

Demostración. Definimos la aplicación $e_\alpha : F[x] \rightarrow K$ por:

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

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:

⁵El 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:

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

Donde $\text{Im}e_\alpha$ será un subanillo de K , que es un dominio de integridad por ser un cuerpo, luego $\text{Im}e_\alpha$ 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

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

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

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 $a \in \text{Im}e_\alpha$, luego $F \leq \text{Im}e_\alpha$.

Si consideramos ahora el polinomio identidad $h = x \in F[x]$, tenemos que: $e_\alpha(h) = h(\alpha) = \alpha$, por lo que $\alpha \in \text{Im}e_\alpha$.

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

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

de donde:

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

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

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

- Para ver que $\mathcal{B} = \{1, \alpha, \dots, \alpha^{\deg f - 1}\}$ es una F -base de $F(\alpha)$, 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 $\deg g \geq \deg f$, entonces podemos encontrar $q, r \in F[x]$ de forma que:

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

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

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

Luego $B = \{1 + \langle f \rangle, x + \langle f \rangle, \dots, x^{\deg f - 1} + \langle f \rangle\}$ 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

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

viene dado por (a partir del Primer Teorema de Isomorfía) 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 $\text{Irr}(\alpha, F)$.

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

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

Observación. Todo otro polinomio $g \in F[x]$ con $g(\alpha) = 0$ satisface que $g = h \text{Irr}(\alpha, F)$.

Ejemplo. Veamos ejemplos de esta última definición:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$x^3 - 1$$

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

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

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

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

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

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

$$x^p - 1$$

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

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

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

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

1.2. Extensiones finitas y extensiones algebraicas

Lema 1.5 (de la torre). Si $F \leq K \leq L$ extensión:

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

Además, $[L : F] = [L : K][K : F]$.

Demostración. Por doble implicación:

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

\impliedby) Sean $\{u_1, \dots, u_n\}$ una base de L sobre K y $\{v_1, \dots, v_m\}$ base de K sobre F , es fácil ver entonces que:

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

es una F -base de L .

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

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

tenemos la fórmula demostrada. \square

Notación. Cuando tenemos extensiones de cuerpos de la forma:

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

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

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

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

Calculemos mediante una torre:

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

Sabemos ya que:

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

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

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

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

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

En definitiva:

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

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

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

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

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

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

de donde:

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

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

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

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

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

por el lema de la Torre:

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

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

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

Ahora, sabemos que el polinomio tiene grado 4, por lo que si encontramos uno de grado 4 del que 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 $F \leq K$, $\alpha \in K$, tenemos que α es algebraico sobre F si y solo si existe una torre de cuerpos $F \leq L \leq K$ tal que $F \leq L$ es finita y $\alpha \in L$.

Demostración. Por doble implicación:

\Rightarrow) Si α es algebraico sobre F , tomamos $L = F(\alpha)$ y la Proposición 1.4 nos da la condición deseada.

\Leftarrow) Sea L un cuerpo en las condiciones del enunciado, tenemos entonces que como $F \leq L$ es finita y $F \leq F(\alpha) \leq L$ entonces $F \leq F(\alpha)$ es finita. Como el conjunto $\{1, \alpha, \dots, \alpha^n, \dots\}$ es un F -sistema de generadores de $F(\alpha)$, tenemos entonces que existe $m \in \mathbb{N}$ con $m \geq 1$ de forma que α^m depende linealmente sobre F de $1, \alpha, \dots, \alpha^{m-1}$, es decir, existen $a_0, \dots, a_{m-1} \in F$ de forma que:

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

Por lo que tomando el polinomio:

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

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

□

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

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

Demostración. Por doble implicación:

\Rightarrow) Tomamos $\{u_1, \dots, u_t\}$ una F -base de K , tenemos entonces que $K = F(u_1, \dots, u_t)$. Además, si $\alpha \in K$, entonces $F \leq F(\alpha)$ es finita. Tomando $L = F(\alpha)$ y aplicando la Proposición anterior tenemos la implicación.

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

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

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

□

Observación. Hemos visto que si $\alpha_1, \dots, \alpha_n \in K$ y α_1 es algebraico sobre F , α_2 es algebraico sobre $F(\alpha_1)$, ..., α_n es algebraico sobre $F(\alpha_1, \dots, \alpha_{n-1})$, entonces $[F(\alpha_1, \dots, \alpha_n) : F] < \infty$.

Corolario 1.7.1. Si $F \leq K$ extensión y llamamos:

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

Entonces, Λ es un subcuerpo de K y $F \leq \Lambda$ 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 $F \leq F(\alpha, \beta)$ 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 $F \leq F(\alpha)$ 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 $F \leq K$ es algebraico. \square

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 $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$, 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:

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

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

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

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

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

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

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

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

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

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

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

En definitiva:

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

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

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

Por lo que tomando:

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

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

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:

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

De donde podemos escribir:

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

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:

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

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} .

Ejercicio 1.2.4. Calcular $Irr(\sqrt{2} + \sqrt[3]{2}, \mathbb{Q})$.

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 intersectar 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:

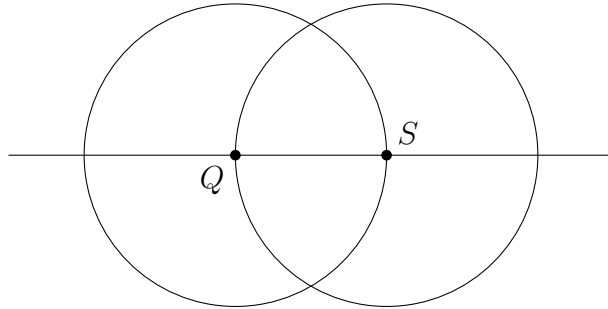


Figura 1.1: Prueba gráfica de que $S \subseteq S^c$.

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

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

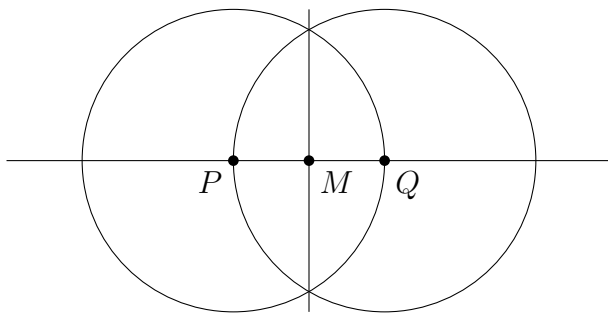
Llamamos al conjunto:

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

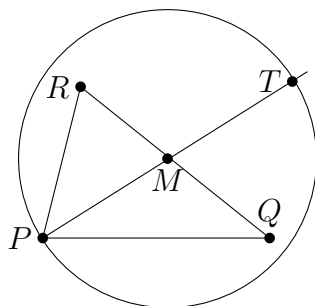
el conjunto de los puntos constructibles (con regla y compás) a partir de S .

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

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



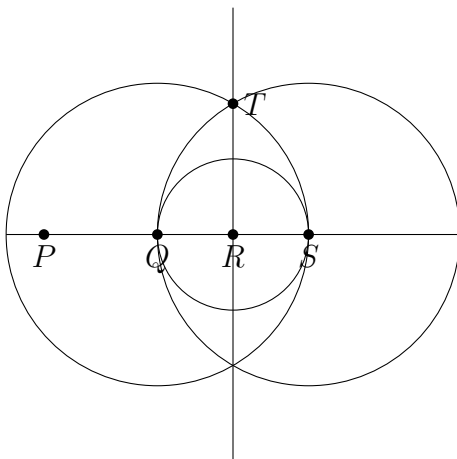
Una vez sabemos como realizar el punto medio de dos puntos dados, supongamos que tenemos 3 puntos: P , Q y R no alineados y que queremos trazar el cuarto punto que completa el paralelogramo. En dicha situación, trazamos las rectas PQ y PR , así como la recta RQ . Trazamos el punto medio M entre los puntos 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.



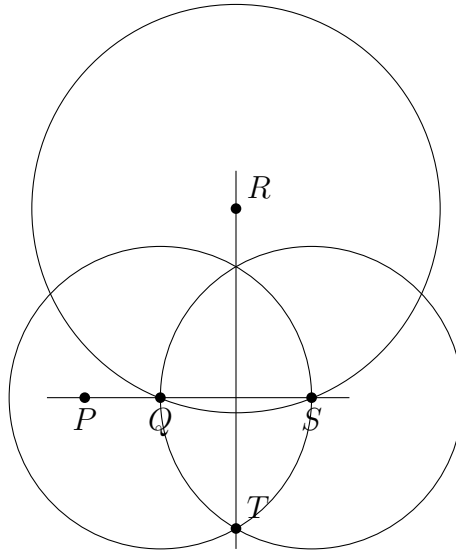
Lema 1.8. Sean P, Q, R puntos del plano con P y Q distintos, se puede construir con regla y compás a partir de ellos un punto T tal que las rectas PQ y RT son perpendiculares.

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

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.



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:

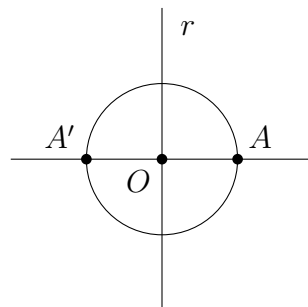


□

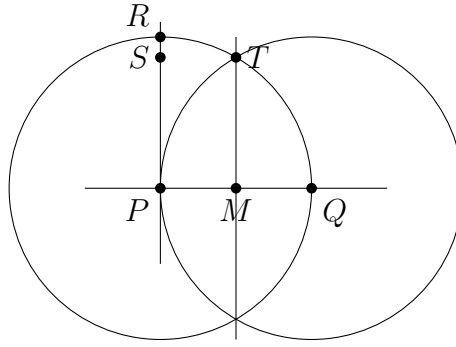
A partir del lema anterior, ya no será necesario recurrir a dichas construcciones cada vez que tengamos dos puntos P y Q que determinan una recta y queramos construir una recta perpendicular a ella que pase por un tercer punto R .

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

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



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



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

Hemos obtenido lo que consideraríamos un sistema de referencia ortonormal, y podemos renombrar a 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 $0, 1 \in S$, es muy fácil ver 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 que $i \in C(S)$.

Lema 1.9. *Dado $z = x + iy \in \mathbb{C}$, tenemos que:*

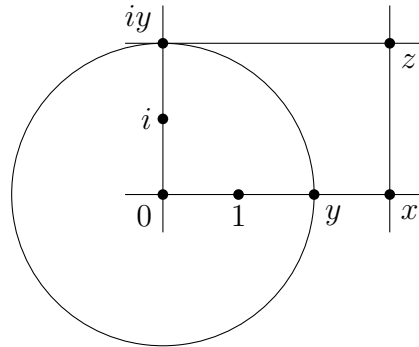
$$z \in C(S) \iff x, y \in C(S)$$

Demostración. Por doble implicación:

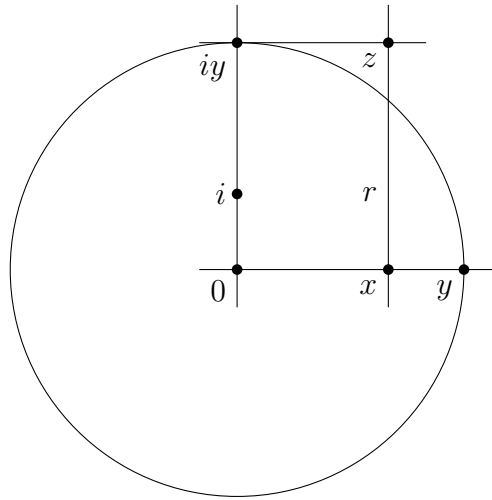
\implies) Supuesto que $z \in C(S)$, vemos que podemos construir x e y de la siguiente forma:

- Si $z \in \mathbb{R}$, tenemos ya construido $x = z$ y sabemos que $y = 0 \in C(S)$.
- Si $\operatorname{Re}(z) = 0$, 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 $0i$ con la circunferencia de centro 0 y radio hasta iy :



\Leftarrow) 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 .



□

Proposición 1.10. *El conjunto $C(S)$ es un subcuerpo de \mathbb{C} . Además, es cerrado por conjugación, es decir:*

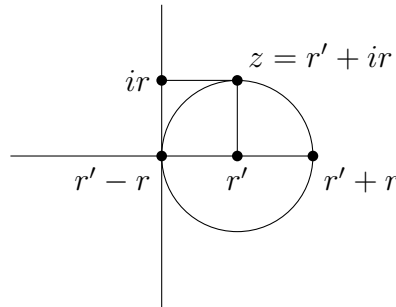
$$z \in C(S) \implies \bar{z} \in C(S)$$

Demostración. Si probamos que la suma de dos números reales constructibles es constructible, obtenemos por el Lema 1.9 que la suma de dos números complejos constructibles es constructible. Análogamente, si demostramos que el producto de dos números reales constructibles es constructible, tendremos que el producto de dos números constructibles es constructible. Para el inverso, si demostramos que

todo conjugado de un número constructible es constructible, tendremos probado que los inversos de los números constructibles serán números constructibles, puesto que:

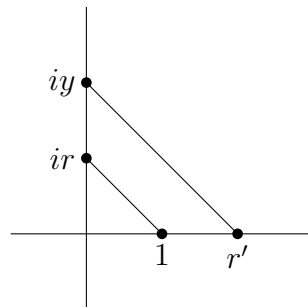
$$z^{-1} = \frac{z\bar{z}}{|z|^2}$$

Por tanto, solo hemos de probar que $C(S) \cap \mathbb{R}$ es un subcuerpo de \mathbb{R} . Sean $r, r' \in C(S) \cap \mathbb{R}$, entonces $r + r', r - r' \in C(S) \cap \mathbb{R}$. Como hemos visto que si un número es constructible entonces el suyo lo es, podemos suponer sin pérdida de generalidad que $r, r' > 0$.



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

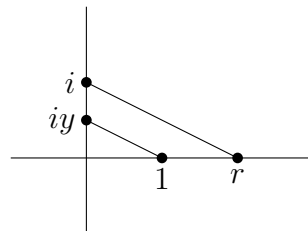
Bajo las mismas hipótesis, tratamos de probar que $r, r' \in C(S) \cap \mathbb{R}$, supondremos de la misma forma que $r, r' > 0$.



Usando que ambos triángulos son semejantes por tener ángulos iguales, tenemos entonces que:

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

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 $r > 0$,



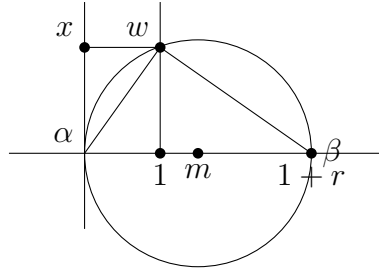
Ambos triángulos semejantes, luego:

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

□

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

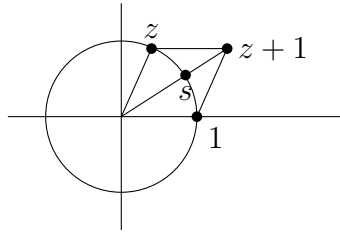
Demostración. Escribiendo z en forma polar, reducimos el problema al caso $|z| = 1$. Si tomamos $r > 0$, con $r \in C(S) \cap \mathbb{R}$, entonces $\sqrt{r} \in C(S) \cap \mathbb{R}$.



Tomando m el punto medio entre $1 + r$ y 0 . Usando que el ángulo del triángulo es recto y que la suma de los ángulos del triángulo es siempre π , tenemos entonces que:

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

Una vez hecha esta distinción, si tomamos un número complejo de módulo 1: $e^{i\theta}$, tenemos que ver que si $e^{i\theta} \in C(S) \cap \mathbb{R}$, entonces $e^{i\frac{\theta}{2}} \in C(S) \cap \mathbb{R}$



□

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 $C(S) \leq C'$. Recordemos que teníamos que:

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

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

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

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

□

Definición 1.14. Sea $F \leq K$ extensión, diremos que K es una torre por raíces cuadradas sobre F si $K = F(u_1, \dots, u_t)$, donde $u_1^2 \in F$ y $u_{i+1}^2 \in F(u_1, \dots, u_i)$ para $i \in \{1, \dots, t-1\}$

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

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

Teorema 1.13. Sean $F = \mathbb{Q}(S \cup \bar{S})$ y \mathcal{T} el conjunto de todas las torres por raíces cuadradas sobre F contenidas en \mathbb{C} , entonces:

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

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

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

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

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

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

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

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

Corolario 1.13.1. $C(S)$ es una extensión algebraica de $F = \mathbb{Q}(S \cup \bar{S})$, de hecho, el grado de cada número en $C(S)$ sobre F es una potencia de 2.

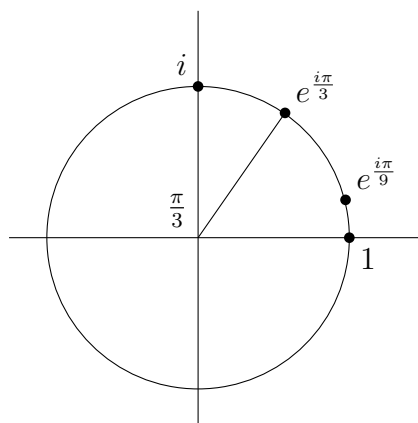
Corolario 1.13.2. Todo número constructible ($F = \mathbb{Q}$) tiene grado sobre \mathbb{Q} una potencia de 2.

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° no se puede trisecar con regla y compás.



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

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

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

de donde usando la fórmula del ángulo triple:

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

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

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

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

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

como es de grado 3, que sea irreducible es equivalente a que tenga alguna 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 donde⁶ $2r = \pm 1$. 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:

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

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

1.4. Homomorfismos de cuerpos

Lema 1.14. Sea $\sigma : F \rightarrow A$ un homomorfismo de anillos donde F es un cuerpo y A es no trivial, entonces σ es inyectivo y, por tanto, $\text{Im}\sigma$ 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 $\text{Im}\sigma \cong F$, basta aplicar el Primer Teorema de Isomorfía:

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

□

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:

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

Como por el Lema anterior todo homomorfismo de cuerpos es inyectivo, tendremos siempre una copia de F dentro de K , que en ocasiones identificaremos con el propio F . Como $\sigma(F) \leq K$ 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:

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

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 $K[x]$.

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

Ejemplo. Sea $f \in F[x]$, f no constante, sea $p \in F[x]$ un factor irreducible de f , consideramos⁷:

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

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

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

que es un homomorfismo de anillos, 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:

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

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

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

⊂) Es obvia por la construcción de K .

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

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

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:

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

Demostración. Observar el ejemplo anterior. □

Proposición 1.16. Sea $f \in F[x]$ con $\deg f = n \geq 1$, entonces existe un homomorfismo de cuerpos $\sigma : F \rightarrow E$ tal que E es un cuerpo de descomposición de f^σ .

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

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

- Si $\deg h = 0$, tomamos $L = F$ y $\tau = id_F$.
- Supuesto que $\deg h > 0$ y la hipótesis de inducción, tomamos p un factor irreducible de f , por lo que podemos aplicar el Lema 1.15, con lo que existe $F \xrightarrow{\tau} K$ tal que p^τ tiene una raíz en $\alpha \in K$ y $K = F(\alpha)$. Observamos que $h^\tau(\alpha) = 0$. El polinomio g que habíamos escogido será de la forma:

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

extraemos ahora los factores lineales a h^τ :

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

Con uno de los β_i es α y k con raíces en K y de grado menor que el de h^τ . Tendremos:

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

Aplicando la hipótesis de inducción, existe un homomorfismo $K \xrightarrow{\rho} L$ tal que $(f^\tau)^\rho$ se descompone como producto de lineales. Si tomamos:

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

tenemos que f^λ 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 el cuerpo de descomposición de f^σ .

□

Definición 1.17. A un homomorfismo $\sigma : F \rightarrow E$ 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:

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

sabemos ya que:

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

Si factorizamos f^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 $\mathbb{F}_2 \leq K$, con lo que:

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

¿Cuántos elementos tiene K ?

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

$$\blacksquare \mathbb{F}_2 = \{1, \alpha, 0, 1 + \alpha\}.$$

Donde vemos que $1 + \alpha$ es distinto del resto porque $\{1, \alpha\}$ es una \mathbb{F}_2 -base de K .

$$\blacksquare \mathbb{F}_2 = \{0, 1, \alpha, \alpha^2\}.$$

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 $a^3 + a + 1 = 0$. f tiene una raíz a . Intentamos factorizar:

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

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 $\mathbb{F}_8 = \mathbb{F}_2(a)$.