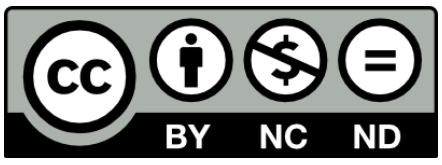
Álgebra III

Los Del DGIIM, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada



Álgebra III

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán

Granada, 2025

Índice general

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

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

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

1. Extensiones de cuerpos y raíces de polinomios

Comenzamos definiendo el objeto de estudio protagonista a lo largo de esta asignatura: los cuerpos, llamados también 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. 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:

$$F \leqslant K$$

1.1. Subcuerpos primos

Es fácil ver 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 1.1.1. 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 sea 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.

1.2. Extensiones de cuerpos y elementos algebraicos

Definición 1.7. 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.

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

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

Demostración. Veámoslo:

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

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

□

Observemos que tenemos $\left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2$.

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[2] todas sus raíces en $\mathbb{C}$, digamos $\alpha_1, \ldots, \alpha_t$, entonces el cuerpo de descomposición de f es $\mathbb{Q}(\alpha_1, \ldots, \alpha_t)$

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

Ejercicio 1.2.1. 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 $F(S \cup T) \subseteq F(S)(T)$.

[2]Fundamentado por el Teorema Fundalmental del Álgebra.

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

□

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

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

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

Demostración. Por doble inclusión:

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

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

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

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

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

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

□

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

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:

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

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

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.

El 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.

1.2.1. Elementos algebraicos

Definición 1.9. 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[4] 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, $\{1, \alpha, \ldots, \alpha^{degf-1}\}$ 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:

- 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 $h = f$.

[4] El coeficiente líder es 1.

- 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. 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 $Irr(\alpha, F)$.

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 $\mathbb{Q}(i)$.
- $Irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2 \in \mathbb{Q}[x]$.
- $Irr\left(e^{\frac{2\pi i}{3}}, \mathbb{Q}\right)$. 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:

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

Ejercicio 1.2.2. Calcular:

$$Irr\left(e^{\frac{2\pi i}{p}}, \mathbb{Q}\right)$$

Para cualquier p primo.

1.3. 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.

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 1.4 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 $\{1, \alpha, \ldots, \alpha^n, \ldots\}$ genera a $F(\alpha)$, 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:

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

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

□

Definición 1.11. 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 $K = F(u_1, \ldots, u_t)$. Además, si $\alpha \in K$, entonces $F \leqslant F(\alpha)$ es finita. Tomando $L = K$ y aplicando la Proposición anterior tenemos la implicación.

$\Longleftarrow$) $K = F(\alpha_1, \ldots, \alpha_n)$ y α_i es algebraico sobre F para todo i. Por el lema de la torre, 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. Veamos primero que Λ es un subanillo de K:

- $1 \in \Lambda$ es claro.
- $\alpha, \beta \in \Lambda$, veamos que $\alpha - \beta, \alpha\beta \in \Lambda$:

  Si $\alpha, \beta \in \Lambda$, sabemos entonces que $F \leqslant F(\alpha, \beta)$ es finita, luego es algebraica, de donde $\alpha - \beta, \alpha\beta \in F(\alpha, \beta)$. En definitiva, $\alpha - \beta, \alpha\beta \in \Lambda$.
- Si $\alpha \neq 0$, entonces $\alpha^{-1} \in F(\alpha)$, de donde $\alpha^{-1} \in \Lambda$.

□

Definición 1.12. El Λ del Corolario anterior recibe el nombre de clausura algebraica de F en K.

Ejemplo. Si tomamos $F = \mathbb{Q}$ y $K = \mathbb{C}$, obtenemos la llamada clausura algebraica (en $\mathbb{C}$) de $\mathbb{Q}$:

$$\overline{\mathbb{Q}}$$

Lo denotaremos de dicha forma, cuyos elementos son los númeos 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 Eissenstein.

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 irreucible por Eisenstein. El segundo sabemos quees menor o igual que 2, pero por ser un número imaginario no puede estar en $\mathbb{Q}\sqrt{5}$, tiene grado 2 y ninguna de sus raíces están en $\mathbb{Q}\left(\sqrt{5}\right)$. 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.

De forma parecida:

- $Irr(\sqrt{2}+i,\mathbb{Q})$. Sí se puede hacer.
- $Irr(\sqrt{2}+\sqrt[3]{2},\mathbb{Q})$. No parece que se pueda hacer de forma parecida, podemos quizás intuir que el grado saldrá 6, razonando pensamos que sale menor o igual que 6. Cambiando la torre sale un número menor o igual que 6 múltiplo de 3 y de 2.

1.4. Construcciones con regla y compás

Reglas: solo se pueden considerar rectas y circunferencias a partir de dos puntos, solo consideramos como puntos intersecciones de dichos elementos. Un punto se dice constructible si es intersección de dos elementos geométricos. Trataremos el plano euclídeo como una idea básica inherente al pensamiento. Trataremos ahora de modelar este comportamiento en lenguaje moderlo.

En lo que sigue, sea S un conjunto de puntos del plano, con al menos dos puntos distintos (un conjunto con un punto no puede construir nada). Definimos ahora Γ, el conjunto cuyos elementos son las rectas trazadas uniendo dos puntos de S, junto

con las circunferencias determinadas por dos puntos de S.

Llamamos S^c al conjunto de los puntos del plano obtenidos por intersección de dos elementos de Γ, a los que llamamos puntos constructibles con regla y compás a partir de S en un paso.

Observación. Se verifica que $S \subseteq S^c$.

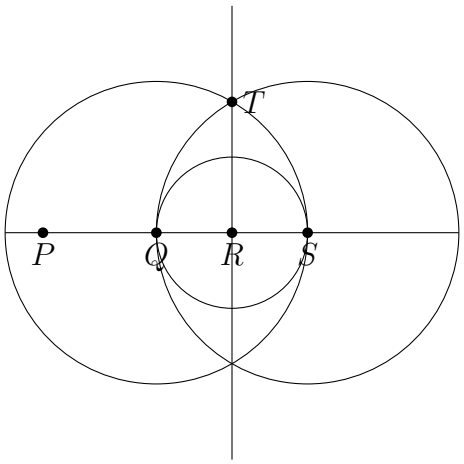
Llamamos $S_0 = S$, $S_{n+1} = S_n^c$ para $n \geqslant 0$. Definimos:

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

Y llamamos a los elementos de $C(S)$ puntos constructibles a partir de S.
La base que nos permite empezar a trazar cosas es el siguiente Lema:

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. **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 no.

□

Sabemos:

- Completar paralelogramos
- Dibujar elementos simétricos.

Otra cosa

Tomamos dos puntos distintos de S, que usando el Lema podemos trazar dos rectas perpendiculares de modo que la distancia de un punto a los otros dos sea la misma, es decir, tenemos un sistema de referencia ortonormal. Pondremos ahora coordenadas a los puntos: $(0,0)$, $(0,1)$ y $(1,0)$, con lo que vemos estos tres puntos dentro de $\mathbb{R}^2$.

Queremos saber a partir de S qué puntos $(x,y) \in \mathbb{R}^2$ son constructibles. Vamos a pensarlo de una forma distinta, viendo $\mathbb{R}^2$ como $\mathbb{C}$, es decir, $C(S) \subseteq \mathbb{C}$.
Llamamos ahora a $C(S)$ conjunto de números constructibles a partir de S.

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

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