Ecuaciones Algebraicas

M. Purificación López López Nieves Rodríguez González

2011-14

Índice general

1. Extensiones de cuerpos	1
1.1. Extensiones de cuerpos	1
1.2. Extensiones algebraicas	5
1.3. Extensión de monomorfismos	12
2. Construcciones con regla y compás	15
2.1. Formulación geométrica	16
2.2. Una aproximación algebraica	17
2.3. Aplicación a algunos problemas clásicos	23
3. Cuerpos de escisión. Clausura algebraica	25
3.1. Teorema de Kronecker	25
3.2. Cuerpo de escisión de un polinomio	27
3.3. Clausura algebraica de un cuerpo	31
4. Extensiones separables. Extensiones normales	37
4.1. Multiplicidad de las raíces de un polinomio	37
4.2. Extensiones separables	39
4.3. Cuerpos finitos	41
4.4. Teorema del elemento primitivo	44
4.5. Extensiones normales	46
5. Teoría de Galois	51
5.1. Extensiones de Galois	51
5.2. Teorema fundamental de la teoría de Galois	56
6. Resolubilidad de ecuaciones por radicales	59
6.1. Grupos resolubles	59
6.2. Raíces de la unidad	65
6.3. El Gran Teorema de Galois	70
7. Aplicaciones	81
7.1. El Teorema Fundamental del Álgebra	81
7.2. Construcción de polígonos regulares	83

Apéndice A.	87
A.1. El anillo de los polinomios	87
A.2. Factorización en $K[x]$	89
A.3. Irreducibilidad en $\mathbb{C}[X]$	90
A.4. Irreducibilidad en $\mathbb{R}[X]$	90
A.5. Irreducibilidad en $\mathbb{Q}[X]$ y en $\mathbb{Z}[X]$	91

Capítulo 1

Extensiones de cuerpos

1.1. Extensiones de cuerpos

Definición 1.1. Un cuerpo F se dice que es una *extensión* de K cuando K es un subcuerpo de F . Escribiremos $F : K$ o $K \subset F$ cuando F es una extensión de K .

Ejemplos 1.2.

$\mathbb{C} : \mathbb{R}$, $\mathbb{C} : \mathbb{Q}$, $\mathbb{R} : \mathbb{Q}$ y $K : K$ si K es un cuerpo, son extensiones de cuerpos.

Si $F : K$ es una extensión, entonces F es un espacio vectorial sobre K con las operaciones:

$$\begin{aligned} F \times F &\rightarrow F & \text{y} & & K \times F &\rightarrow F \\ (b, c) &\mapsto b + c & & & (a, b) &\mapsto ab \end{aligned}$$

donde la suma, $+$, es la del cuerpo F y la multiplicación por escalares (de elementos de K por elementos de F) es la multiplicación en F .

Definición 1.3. La dimensión del K -espacio vectorial F , $\dim_K(F)$, la denotaremos por $[F : K]$ y se llama *grado de la extensión* $F : K$ o *grado de F sobre K* . Diremos que la extensión $F : K$ es *finita* si $[F : K]$ es finito; en otro caso, se dice que es una extensión *infinita*.

Ejemplos 1.4.

1) $[\mathbb{C} : \mathbb{R}] = 2$, ya que cada $\alpha \in \mathbb{C}$ admite una única expresión de la forma $\alpha = a + bi$ con $i^2 = -1$ y $a, b \in \mathbb{R}$, lo que significa que $\{1, i\}$ es una $\mathbb{R}$ -base de $\mathbb{C}$.

2) $[\mathbb{C} : \mathbb{Q}] = [\mathbb{R} : \mathbb{Q}] = \infty$.

Obviamente, $[\mathbb{R} : \mathbb{Q}] \leq [\mathbb{C} : \mathbb{Q}]$. Si $[\mathbb{R} : \mathbb{Q}] = n < \infty$, como $\mathbb{Q}$ -espacio vectorial, $\mathbb{R} \cong \mathbb{Q}^n$; puesto que $\mathbb{Q}$ es numerable, y cualquier producto finito de conjuntos numerables es numerable, $\mathbb{Q}^n$ sería numerable y, por tanto, $\mathbb{R}$ también sería numerable.

3) Si $F : K$ es una extensión, entonces $[F : K] = 1$ si, y solo si, $F = K$. En efecto, K es un K -espacio vectorial de dimensión 1 y, recíprocamente, si $[F : K] = 1$, cualquier elemento no nulo de F , en particular $1 \in F$, es una base de F sobre K , por lo tanto todo $b \in F$ será de la forma $b = a \cdot 1$ con $a \in K$, por lo que $b = a \in K$ y $F = K$.

Definición 1.5. Si $F_{i+1} : F_i$ son extensiones $\forall i : 1, \dots, n-1$, diremos que

$$F_1 \subset F_2 \subset \dots \subset F_n$$

es una *torre de cuerpos* (o *una torre de extensiones*).

Teorema 1.6 (Teorema del grado). *Si $K \subset F \subset E$ es una torre de cuerpos, entonces*

$$[E : K] = [E : F][F : K].$$

Demostración. Supongamos primero que $[E : F] = m < \infty$ y $[F : K] = n < \infty$.

Sean $\{x_i\}_{i:1,\dots,m}$ una base de E sobre F e $\{y_j\}_{j:1,\dots,n}$ una base de F sobre K . Vamos a probar que $\mathcal{B} = \{y_j x_i \mid 1 \leq j \leq n, 1 \leq i \leq m\}$ es una base de E sobre K .

1) $\mathcal{B}$ genera E sobre K :

Sea $z \in E$, como $\{x_i\}_{i:1,\dots,m}$ genera E sobre F , existen $\alpha_1, \dots, \alpha_m \in F$ tales que $z = \sum_{i=1}^m \alpha_i x_i$.

Puesto que $\{y_j\}_{j:1,\dots,n}$ generan F sobre K , y $\alpha_i \in F$, para cada i , $1 \leq i \leq m$, existen $\beta_{1i}, \dots, \beta_{ni} \in K$ tales que $\alpha_i = \sum_{j=1}^n \beta_{ji} y_j$ y, por tanto,

$$z = \sum_{i=1}^m \left(\sum_{j=1}^n \beta_{ji} y_j \right) x_i = \sum_{i=1}^m \sum_{j=1}^n \beta_{ji} y_j x_i \quad \text{con } \beta_{ji} \in K.$$

2) $\mathcal{B}$ es linealmente independiente sobre K :

Supongamos que $0 = \sum_{i=1}^m \sum_{j=1}^n \beta_{ji} y_j x_i$, donde $\beta_{ji} \in K$. Reagrupando en esta suma los términos con el mismo x_i se obtiene que $0 = \sum_{i=1}^m \left(\sum_{j=1}^n \beta_{ji} y_j \right) x_i$ y, ya que los x_i son linealmente independientes sobre F y $\sum_{j=1}^n \beta_{ji} y_j \in F$, se deduce que $\sum_{j=1}^n \beta_{ji} y_j = 0 \forall i : 1, \dots, m$.

De nuevo, como los $\beta_{ji} \in K$ y los y_j son linealmente independientes sobre K , de la última igualdad se concluye que $\beta_{ji} = 0 \forall j : 1, \dots, n, \forall i : 1, \dots, m$.

Así, $\mathcal{B}$ es una base de E sobre K , $E : K$ es finita y $[E : K] = [E : F][F : K]$.

Si $[E : K] = r < \infty$, sea $\mathcal{D} = \{z_1, \dots, z_r\}$ una base de E sobre K . Puesto que $\mathcal{D}$ es un conjunto de generadores de E sobre F , se tiene que $\dim_F(E) = [E : F] \leq r$ y $E : F$ es una extensión finita. Además, F es un K -subespacio de E , así $[F : K] = \dim_K(F) \leq \dim_K(E) = [E : K] = r < \infty$.

Entonces, $[E : K] = \infty$ si, y solo si, $[E : F]$ o $[F : K]$ es ∞ . □

Observaciones 1.7.

1) La anterior demostración es constructiva y muestra que se obtiene una K -base de E multiplicando los elementos de una F -base de E por los de una K -base de F .

2) El Teorema del grado, (1.6), es “análogo” al Teorema de Lagrange para grupos, que establece que si $H \subset L \subset G$ es una torre de grupos entonces $(G : H) = (G : L)(L : H)$. Esto no es algo casual, como se comprobará al estudiar el Teorema fundamental de teoría de Galois.

3) Si $E : K$ es una extensión de grado primo, entonces no existen extensiones intermedias entre E y K . Esto ocurre, por ejemplo, con la extensión $\mathbb{C} : \mathbb{R}$.

Definición 1.8. Sea $F : K$ una extensión de cuerpos y sea A un subconjunto de F .

La intersección de todos los subanillos de F que contienen a A y a K , se denotará por $K[A]$, y se llama *subanillo de F generado por A sobre K* .

La intersección de todos los subcuerpos de F que contienen a A y a K , se denotará por $K(A)$, y se llama *subcuerpo de F generado por A sobre K* .

En particular, cuando $A = \{\alpha_1, \dots, \alpha_n\}$ escribiremos $K[A] = K[\alpha_1, \dots, \alpha_n]$ y $K(A) = K(\alpha_1, \dots, \alpha_n)$.

Observaciones 1.9.

1) $K[A]$ es el “menor” subanillo de F que contiene a A y a K y $K(A)$ es el “menor” subcuerpo de F que contiene a A y a K .

2) $K[A]$ está contenido en $K(A)$ y se tiene la torre de cuerpos $K \subset K(A) \subset F$.

Proposición 1.10. *Si $F : K$ es una extensión y $\alpha \in F$, se verifica que:*

1. $K[\alpha] = \{f(\alpha) \mid f \in K[X]\}$.
2. $K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} = f(\alpha)g(\alpha)^{-1} \text{ con } f, g \in K[X] \text{ y } g(\alpha) \neq 0 \right\}$.

Demostración.

1) Consideramos el “homomorfismo evaluación en α ”

$$\begin{aligned} \varphi_\alpha: K[X] &\rightarrow F \\ f &\mapsto f(\alpha) \end{aligned}$$

es decir, el único homomorfismo de anillos $\varphi_\alpha : K[X] \rightarrow F$ tal que $\varphi_\alpha(X) = \alpha$ y $\varphi_\alpha(a) = a \quad \forall a \in K$.

Puesto que φ_α es un homomorfismo de anillos, $\text{Im } \varphi_\alpha = \{f(\alpha) \mid f \in K[X]\}$ es un subanillo de F y es, claramente, el menor subanillo de F que contiene a K y a α .

2) Sea $E = \left\{ \frac{f(\alpha)}{g(\alpha)} \text{ con } f, g \in K[X] \text{ y } g(\alpha) \neq 0 \right\}$.

i) $E \subset K(\alpha)$:

Todo cuerpo que contiene a K y a α contiene a E .

ii) E es un cuerpo:

Sean $\gamma_1 = \frac{f_1(\alpha)}{g_1(\alpha)}, \gamma_2 = \frac{f_2(\alpha)}{g_2(\alpha)} \in E$, $f_1, g_1, f_2, g_2 \in K[X]$ y $g_1(\alpha), g_2(\alpha) \neq 0$.

Dado que $K[\alpha]$ es subanillo del cuerpo F , es un dominio entero y se tiene que $g_1 g_2(\alpha) = g_1(\alpha) g_2(\alpha) \neq 0$. Así,

$$\gamma_1 - \gamma_2 = \frac{f_1(\alpha)g_2(\alpha) - f_2(\alpha)g_1(\alpha)}{g_1(\alpha)g_2(\alpha)} = \frac{(f_1g_2 - f_2g_1)(\alpha)}{g_1g_2(\alpha)} \in E.$$

Si $\gamma_2 \neq 0$, como $f_2(\alpha) \neq 0$, se tiene que $(g_1 f_2)(\alpha) \neq 0$ y, por tanto,

$$\gamma_1 \gamma_2^{-1} = \frac{f_1(\alpha) g_2(\alpha)}{g_1(\alpha) f_2(\alpha)} = \frac{(f_1 g_2)(\alpha)}{(g_1 f_2)(\alpha)} \in E.$$

iii) Como E es un cuerpo, $K \subset E$ y $\alpha \in E$, se tiene que $K(\alpha) \subset E$.

De i) y iii) se sigue que $K(\alpha) = E$.

Nótese que, $K(\alpha)$ es el cuerpo de fracciones de $K[\alpha]$. □

Análogamente, se demuestra que:

Proposición 1.11. Si $F : K$ es una extensión y $\alpha_1, \dots, \alpha_n \in F$, entonces:

1. $K[\alpha_1, \dots, \alpha_n] = \{f(\alpha_1, \dots, \alpha_n) \mid f \in K[X_1, \dots, X_n]\}$.
2. $K(\alpha_1, \dots, \alpha_n) = \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \mid f, g \in K[X_1, \dots, X_n] \text{ y } g(\alpha_1, \dots, \alpha_n) \neq 0 \right\}$.

Definición 1.12. Si K y F son subcuerpos de un cuerpo E , llamaremos *compuesto de K y F en E* y lo denotaremos por KF , al menor subcuerpo de E que contiene a K y a F , es decir, $KF = K(F) = F(K) = FK$.

Observación 1.13. Si K y F son subcuerpos de un cuerpo E , $K[F] = F[K]$ es el menor subanillo de E que contiene a K y a F . Sus elementos son expresiones de la forma $\sum_i a_i b_i$ con solamente un número finito de sumandos no nulos, donde $a_i \in K$ y $b_i \in F$, ya que el conjunto de tales expresiones es un subanillo de E que contiene a K y a F , y todo subanillo de E que contenga a K y a F debe contener también a dichas expresiones.

Además, $KF = FK = \{\alpha \beta^{-1} \mid \alpha, \beta \in K[F] \text{ con } \beta \neq 0\}$ es el cuerpo de fracciones de $K[F]$.

1.2. Extensiones algebraicas

Definición 1.14. Sea $F : K$ una extensión de cuerpos. Un elemento $\alpha \in F$ se dice que es *algebraico sobre K* si existe un polinomio no nulo $f \in K[X]$ tal que $f(\alpha) = 0$. En caso contrario, es decir, si $f(\alpha) \neq 0$ para todo $f \in K[X]$, $f \neq 0$, se dice α que es *trascendente sobre K* .

Observaciones 1.15.

- 1) Cada $\alpha \in K$ es algebraico sobre K ya que α es cero del polinomio $X - \alpha \in K[X]$.
- 2) Si $K \subset K' \subset F$ es una torre de cuerpos y $\alpha \in F$ es algebraico sobre K , también es algebraico sobre K' .
- 3) Si α es un cero de un polinomio $f \in K[X]$ con coeficiente principal $c \neq 0$, entonces α es un cero de $c^{-1}f \in K[X]$ que es un polinomio mónico.
- 4) Sea $F : K$ una extensión y $\alpha \in F$. Si $\varphi_\alpha : K[X] \rightarrow F$ es el homomorfismo evaluación en α , se verifica que:
 - a) α es algebraico sobre $K \Leftrightarrow \text{Ker } \varphi_\alpha \neq 0$.
 - b) α es trascendente sobre $K \Leftrightarrow \text{Ker } \varphi_\alpha = \{0\}$.
 Nótese que si α es trascendente sobre K , $\text{Im } \varphi_\alpha = K[\alpha] \cong K[X]$.

Definición 1.16. Diremos que $F : K$ es una *extensión algebraica* si todo elemento de F es algebraico sobre K , y que $F : K$ es una *extensión trascendente* cuando existe algún $\alpha \in F$ que es trascendente sobre K .

Ejemplos 1.17.

- 1) La extensión $\mathbb{C} : \mathbb{R}$ es algebraica, pues si $\alpha = a + bi \in \mathbb{C}$ y $\bar{\alpha} = a - bi$ denota su conjugado, entonces

$$f = (X - \alpha)(X - \bar{\alpha}) = X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha} = X^2 - 2aX + a^2 + b^2$$
 es un polinomio no nulo con coeficientes reales y $f(\alpha) = 0$.
- 2) La extensión $\mathbb{R} : \mathbb{Q}$ es trascendente. C. Hermite (1873) y F. von Lindemann (1882) probaron, respectivamente, que los números reales e y π son trascendentes sobre $\mathbb{Q}$.
- 3) $i, \sqrt{7}, \sqrt[3]{5} \in \mathbb{C}$ son algebraicos sobre $\mathbb{Q}$ y, por lo tanto, sobre $\mathbb{R}$. En efecto, i es un cero de $X^2 + 1$, $\sqrt{7}$ lo es de $X^2 - 7$ y $\sqrt[3]{5}$ de $X^3 - 5$, todos ellos polinomios no nulos con coeficientes racionales.
- 4) $\alpha = \sqrt{2} + i \in \mathbb{C}$, que es algebraico sobre $\mathbb{R}$, lo es también sobre $\mathbb{Q}$, pues

$$\alpha - i = \sqrt{2} \Rightarrow 2i\alpha = \alpha^2 - 3 \Rightarrow -4\alpha^2 = (\alpha^2 - 3)^2 \Leftrightarrow \alpha^4 - 2\alpha^2 + 9 = 0,$$
 es decir, α es un cero de $X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$.

Teorema 1.18. *Sea $F : K$ una extensión y $\alpha \in F$ algebraico sobre K .*

1. *Existe un único polinomio mónico e irreducible $f \in K[X]$ tal que $f(\alpha) = 0$, que se llamará el polinomio irreducible o el polinomio mínimo de α sobre K y se denotará $f = \text{Irr}(\alpha, K)$.*

2. $K[\alpha] = K(\alpha)$.

Demostración.

1) Existencia:

Como $K[X]/\text{Ker } \varphi_\alpha \cong \text{Im } \varphi_\alpha = K[\alpha]$ que es un subanillo del cuerpo F , se tiene que $K[\alpha]$ es un dominio entero.

Además, dado que $\text{Ker } \varphi_\alpha \neq 0$, se verifica que $\text{Ker } \varphi_\alpha$ es un ideal primo del dominio de ideales principales $K[X]$ y, en consecuencia, existe $g \in K[X]$ irreducible tal que $\text{Ker } \varphi_\alpha = \langle g \rangle$.

Ahora, si c es el coeficiente principal de g , el polinomio mónico $f = c^{-1}g$ y el polinomio g son asociados y, por ello, f es irreducible y $\text{Ker } \varphi_\alpha = \langle f \rangle$.

Unicidad:

Si $h \in K[X]$ es mónico, irreducible y $h(\alpha) = 0$, entonces $h \in \text{Ker } \varphi_\alpha = \langle f \rangle$, lo que significa que $h = f \cdot q$ con $q \in K[X]$. Teniendo en cuenta que h y f son irreducibles, se deduce que $q \in \mathcal{U}(K)$. Puesto que h y f son mónicos, se obtiene que $q = 1$.

2) Ya hemos visto que $\text{Ker } \varphi_\alpha \neq 0$ es un ideal primo de $K[X]$; dado que $K[X]$ es un dominio de ideales principales, $\text{Ker } \varphi_\alpha$ también es un ideal maximal de $K[X]$. Por tanto, $K[\alpha] \cong K[X]/\text{Ker } \varphi_\alpha$ es un cuerpo.

Ya que $K[\alpha] \subset K(\alpha)$, se tiene que $K[\alpha] = K(\alpha)$. □

Observación 1.19. Si $g \in K[X]$, entonces

$$g(\alpha) = 0 \text{ si, y solo si, } \text{Irr}(\alpha, K) \text{ divide a } g \text{ en } K[X].$$

Proposición 1.20. *Sea $F : K$ una extensión y $\alpha \in F$ algebraico sobre K .*

1. *Si $\partial \text{Irr}(\alpha, K) = n$, el conjunto $\{1, \alpha, \dots, \alpha^{n-1}\}$ es una K -base de $K(\alpha)$.*

2. $[K(\alpha) : K] = \partial \text{Irr}(\alpha, K)$.

Demostración.

1) Sea $f = \text{Irr}(\alpha, K)$. Por el teorema anterior sabemos que $K(\alpha) = K[\alpha] = \{g(\alpha) \mid g \in K[X]\}$.

Los elementos $1, \alpha, \dots, \alpha^{n-1}$ son linealmente independientes sobre K :

Supongamos que $b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1} = 0$, con $b_0, b_1, \dots, b_{n-1} \in K$. El polinomio $h = b_0 + b_1X + \dots + b_{n-1}X^{n-1} \in K[X]$ verifica que $h(\alpha) = 0$ y, por la observación 1.19, f divide a h en $K[X]$ y, como $\partial h < \partial f$, esto solo es posible si $h = 0$.

$\{1, \alpha, \dots, \alpha^{n-1}\}$ genera $K(\alpha)$ sobre K :

Sea $g \in K[X]$, por el algoritmo de la división, existen $q, r \in K[X]$ tales que $g = fq + r$ con $\partial r < \partial f = n$. Suponiendo que $r = a_0 + a_1X + \dots + a_tX^t$, con $t \leq n-1$, y teniendo en cuenta que la evaluación en α es un homomorfismo de anillos, se tiene que $g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha) = a_0 + a_1\alpha + \dots + a_t\alpha^t$.

2) Es consecuencia de 1). □

Ejemplos 1.21.

1) $\sqrt{2} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$ pues es cero del polinomio $X^2 - 2 \in \mathbb{Q}[X]$. Por tanto, $\text{Irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2$ (Eisenstein, $p = 2$).

$\{1, \sqrt{2}\}$ es una $\mathbb{Q}$ -base de $\mathbb{Q}(\sqrt{2})$ y cada elemento $\beta \in \mathbb{Q}(\sqrt{2})$ admite una única expresión de la forma $\beta = a + b\sqrt{2}$ con $a, b \in \mathbb{Q}$.

2) $\alpha = \sqrt{1 + \sqrt{3}} \in \mathbb{R}$ es algebraico sobre $\mathbb{Q}$.

Puesto que $(\alpha^2 - 1)^2 = 3$, α es cero de $X^4 - 2X^2 - 2 \in \mathbb{Q}[X]$. Así, $\text{Irr}(\sqrt{1 + \sqrt{3}}, \mathbb{Q}) = X^4 - 2X^2 - 2$ (Eisenstein, $p = 2$).

$\{1, \sqrt{1 + \sqrt{3}}, 1 + \sqrt{3}, (1 + \sqrt{3})\sqrt{1 + \sqrt{3}}\}$ es una $\mathbb{Q}$ -base de $\mathbb{Q}(\sqrt{1 + \sqrt{3}})$.

3) Sea ω la raíz cuarta real positiva de 2. Por el criterio de Eisenstein ($p = 2$) el polinomio $X^4 - 2$ es irreducible en $\mathbb{Q}[X]$ y tiene a ω como cero. Así, ω es algebraico sobre $\mathbb{Q}$, $\text{Irr}(\omega, \mathbb{Q}) = X^4 - 2$ y $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$. Entonces, $\{1, \omega, \omega^2, \omega^3\}$ es una $\mathbb{Q}$ -base de $\mathbb{Q}(\omega)$ y cada elemento β de $\mathbb{Q}(\omega)$ admite una única expresión como $\beta = a + b\omega + c\omega^2 + d\omega^3$ con $a, b, c, d \in \mathbb{Q}$.

¿Cuál es la expresión de $\gamma = 1 + \omega - 2\omega^6 \in \mathbb{Q}(\omega)$ como $\mathbb{Q}$ -combinación lineal de la

citada base?

$$\begin{aligned}\gamma &= 1 + \omega - 2\omega^6 = \varphi_\omega(1 + X - 2X^6) = \\ &= \varphi_\omega[(X^4 - 2)(-2X^2) + (-4X^2 + X + 1)] = \\ &= \varphi_\omega(X^4 - 2)\varphi_\omega(-2X^2) + \varphi_\omega(-4X^2 + X + 1) = -4\omega^2 + \omega + 1.\end{aligned}$$

Una forma alternativa de proceder consiste en utilizar que $\omega^4 = 2$ para reducir los exponentes de las potencias de ω en la expresión original de γ . En efecto, de $\omega^4 = 2$ se deduce que $\omega^6 = 2\omega^2$ y, entonces, $\gamma = 1 + \omega - 2\omega^6 = 1 + \omega - 4\omega^2$.

Proposición 1.22. *Toda extensión finita es algebraica.*

Demostración. Sea $F : K$ una extensión finita y $\alpha \in F$.

Si consideramos la torre de cuerpos $K \subset K(\alpha) \subset F$, por Teorema del grado (1.6), se tiene que $[K(\alpha) : K]$ divide a $[F : K]$ y, en consecuencia, la extensión $K(\alpha) : K$ es finita.

Si $[K(\alpha) : K] = n$, como en $K(\alpha)$ los elementos $1, \alpha, \dots, \alpha^n$ son linealmente dependientes, existen $a_0, a_1, \dots, a_n \in K$, no todos nulos, tales que $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$. En consecuencia, α es algebraico sobre K ya que es cero del polinomio no nulo $f = a_0 + a_1X + \dots + a_nX^n \in K[X]$. $\square$

Corolario 1.23. *Si $F : K$ es una extensión y $\alpha \in F$ es algebraico sobre K , la extensión $K(\alpha) : K$ es algebraica.*

Demostración. La extensión $K(\alpha) : K$ es finita, por la proposición 1.20, y es algebraica, por la proposición 1.22. $\square$

Observación 1.24. Nótese que existen extensiones algebraicas que no son finitas. Veremos un ejemplo a continuación.

Para cada entero n , $\mathbb{Q}(\sqrt[2^n]{2}) : \mathbb{Q}$ es una extensión finita de grado 2^n y, teniendo en cuenta que $\mathbb{Q}(\sqrt[2^n]{2}) \subset \mathbb{Q}(\sqrt[2^{n+1}]{2})$, se sigue que $E := \bigcup_n \mathbb{Q}(\sqrt[2^n]{2})$ es un cuerpo y la extensión $E : \mathbb{Q}$ es algebraica y no finita.

Definición 1.25. Una extensión $F : K$ es *finitamente generada* si existe un número finito de elementos $\alpha_1, \dots, \alpha_n \in F$ tal que $F = K(\alpha_1, \dots, \alpha_n)$.

En particular, si $F = K(\alpha)$ se dirá que $F : K$ es una *extensión simple*.

Nótese que una extensión finitamente generada no siempre es algebraica. Por ejemplo, si K es un cuerpo, el cuerpo de cocientes del anillo de polinomios en una indeterminada,

$$K(X) = \left\{ \frac{f}{g} \mid f, g \in K[X], g \neq 0 \right\}$$

no es una extensión algebraica de K ya que $X \in K(X)$ es trascendente sobre K .

También, $\mathbb{Q}(\pi) : \mathbb{Q}$ es una extensión simple y trascendente.

Proposición 1.26. Sea $F : K$ una extensión de cuerpos.

$F : K$ es finita si, y solo si, $F : K$ es finitamente generada por elementos algebraicos sobre K .

Demostración.

Si $\{\alpha_1, \dots, \alpha_n\}$ es una K -base de F , se tiene que $F = K(\alpha_1, \dots, \alpha_n)$. Además, como $F : K$ es finita, por la proposición 1.22, cada α_i es algebraico sobre K .

Recíprocamente, supongamos que $F = K(\alpha_1, \dots, \alpha_n)$ con α_i algebraico sobre K , para $i = 1, \dots, n$. Consideremos la siguiente torre de cuerpos

$$F_0 = K \subset F_1 = K(\alpha_1) \subset \dots \subset F_n = K(\alpha_1, \dots, \alpha_n) = F.$$

Para cada $i = 1, \dots, n$, sabemos que α_i es algebraico sobre F_{i-1} ; puesto que $F_i = F_{i-1}(\alpha_i)$, aplicando el corolario 1.23, se deduce que $F_i : F_{i-1}$ es una extensión finita. Por el Teorema del grado (1.6), $[F : K] = [F_n : F_{n-1}] \cdots [F_1 : F_0]$ y la extensión $F : K$ es finita. $\square$

Teorema 1.27. Sea $K \subset F \subset E$ una torre de cuerpos.

$E : K$ es algebraica si, y solo si, $E : F$ y $F : K$ son algebraicas.

Demostración.

“ $\Rightarrow$ ” Trivial.

“ $\Leftarrow$ ” Sea $\alpha \in E$. Si $f = \text{Irr}(\alpha, F) = \sum_{i=0}^n a_i X^i \in F[X]$, entonces α es algebraico sobre $K(a_0, \dots, a_n)$ ya que $0 \neq f \in K(a_0, \dots, a_n)[X]$ y $f(\alpha) = 0$ y, por el corolario 1.23, $K(a_0, \dots, a_n)(\alpha) : K(a_0, \dots, a_n)$ es finita.

Además, la extensión $K(a_0, \dots, a_n) : K$ es finita por ser finitamente generada por elementos algebraicos.

Como $K \subset K(a_0, \dots, a_n) \subset K(a_0, \dots, a_n)(\alpha)$, por el Teorema del grado (1.6), la extensión $K(a_0, \dots, a_n)(\alpha) : K$ es finita y, por la proposición 1.22, α es algebraico sobre K . $\square$

Corolario 1.28. Sea $F : K$ una extensión de cuerpos y

$$\overline{K}^F := \{\alpha \in F \mid \alpha \text{ es algebraico sobre } K\}.$$

$\overline{K}^F$ es un subcuerpo de F y la extensión $\overline{K}^F : K$ es algebraica.

Demostración. $\overline{K}^F$ es un subcuerpo de F :

Sean $\alpha, \beta \in \overline{K}^F$, entonces $\alpha - \beta$ y, si $\beta \neq 0$, $\alpha\beta^{-1} \in K(\alpha, \beta) \subset F$. En efecto, por las proposiciones 1.26 y 1.22, $K(\alpha, \beta) : K$ algebraica y, en consecuencia, $\alpha - \beta$ y, si $\beta \neq 0$, $\alpha\beta^{-1} \in F$ son algebraicos sobre K y $\alpha - \beta$ y, si $\beta \neq 0$, $\alpha\beta^{-1} \in \overline{K}^F$.

Es evidente que $K \subset \overline{K}^F \subset F$ y que la extensión $\overline{K}^F : K$ es algebraica. $\square$

Nótese que si $K \subset E \subset F$ y $E : K$ es algebraica debe verificarse que $E \subset \overline{K}^F$, es decir, $\overline{K}^F : K$ es la subextensión algebraica maximal de $F : K$.

A $\overline{K}^F$ se le denominará *clausura algebraica de K en F* .

Ejemplo 1.29.

La clausura algebraica de $\mathbb{Q}$ en $\mathbb{R}$, $\overline{\mathbb{Q}}^{\mathbb{R}}$, es una extensión algebraica de $\mathbb{Q}$ que no es finita.

Por el corolario anterior, $\overline{\mathbb{Q}}^{\mathbb{R}} : \mathbb{Q}$ es algebraica. Veremos ahora que no es finita. En efecto, $\forall n > 0$ el polinomio $X^n - 2 \in \mathbb{Q}[X]$ es irreducible en $\mathbb{Q}[X]$ (Eisenstein, $p = 2$) y tiene a $\alpha = \sqrt[n]{2} \in \mathbb{R}$ como cero. Así,

$$[\overline{\mathbb{Q}}^{\mathbb{R}} : \mathbb{Q}] \geq [\mathbb{Q}(\alpha) : \mathbb{Q}] = \partial(\text{Irr}(\alpha, \mathbb{Q})) = n.$$

1.3. Extensión de monomorfismos

Recordemos que todos los homomorfismos de cuerpos son monomorfismos.

Definición 1.30. Sean $F : K$ y $F' : K'$ extensiones de cuerpos y $\sigma : K \rightarrow K'$ un monomorfismo. Un monomorfismo $\tau : F \rightarrow F'$ se dirá que es una *extensión* de σ (o que *extiende* a σ) si $\tau|_K = \sigma$, es decir, si es conmutativo el siguiente diagrama

$$\begin{array}{ccc} F & \xrightarrow{\tau} & F' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sigma} & K' \end{array}$$

en el que las flechas verticales indican las inclusiones.

Si $K = K'$ y $\sigma = id_K$, se dirá que τ es un *K-monomorfismo*.

Si $K = K'$, $F = F'$, $\sigma = id_K$ y τ es isomorfismo, se dirá que τ es un *K-automorfismo* de F .

Observación 1.31. Sea $\sigma : K \rightarrow K'$ un monomorfismo y $\bar{\sigma} : K[X] \rightarrow K'[X]$ su extensión a los anillos de polinomios. Se verifica:

1. $f \in K[X]$ es mónico $\Leftrightarrow \bar{\sigma}(f) \in K'[X]$ es mónico.

2. $\partial(f) = \partial(\bar{\sigma}(f))$.

3. Si σ es isomorfismo, entonces

$f \in K[X]$ es irreducible en $K[X] \Leftrightarrow \bar{\sigma}(f) \in K'[X]$ es irreducible en $K'[X]$.

Proposición 1.32. Si $F : K$ y $F' : K'$ son extensiones, $\sigma : K \rightarrow K'$ y $\tau : F \rightarrow F'$ son isomorfismos y τ extiende a σ . Se verifica:

1. $F : K$ es finita si, y solo si, $F' : K'$ es finita.

2. Si $f \in K[X]$ y $\alpha \in F$, entonces

α es cero de f si, y solo si, $\tau(\alpha)$ es cero de $\bar{\sigma}(f)$.

3. $\alpha \in F$ es algebraico sobre K y $f = \text{Irr}(\alpha, K)$ si, y solo si, $\tau(\alpha)$ es algebraico sobre K' y $\bar{\sigma}(f) = \text{Irr}(\tau(\alpha), K')$.

Demostración.

1) Dado que τ es un isomorfismo que extiende a σ , $\{\alpha_1, \dots, \alpha_n\} \subset F$ es una K -base de F si, y solo si, $\{\tau(\alpha_1), \dots, \tau(\alpha_n)\} \subset F'$ es una K' -base de F' .

2) Sea $f = \sum_{i=0}^n a_i X^i \in K[X]$. Teniendo en cuenta que τ es isomorfismo y que $\tau|_K = \sigma$, se verifica que:

$$\alpha \in F \text{ es cero de } f \Leftrightarrow 0 = f(\alpha) = \sum_{i=0}^n a_i \alpha^i \Leftrightarrow 0 = \tau(f(\alpha)) = \sum_{i=0}^n \sigma(a_i) \tau(\alpha)^i = \bar{\sigma}(f)(\tau(\alpha)) \Leftrightarrow \tau(\alpha) \text{ es cero de } \bar{\sigma}(f).$$

3) Sea $\alpha \in F$ algebraico sobre K y $f = \text{Irr}(\alpha, K)$.

$\tau(\alpha)$ es algebraico sobre K' ya que es un cero de $\bar{\sigma}(f) \in K'[X]$ (por 2)). Si $g = \text{Irr}(\tau(\alpha), K')$ sabemos que $g \mid \bar{\sigma}(f)$ y, por tanto, $\partial(g) \leq \partial(\bar{\sigma}(f))$.

Análogamente, puesto que τ^{-1} extiende a σ^{-1} , se obtiene que $\partial(f) \leq \partial(\overline{\sigma^{-1}}(g))$ y, por ello, la desigualdad $\partial(\bar{\sigma}(f)) \leq \partial(g)$. De donde se concluye que $\partial(g) = \partial(\bar{\sigma}(f))$.

Como además $\bar{\sigma}(f)$ es mónico y $g \mid \bar{\sigma}(f)$, se tiene que $\bar{\sigma}(f) = g = \text{Irr}(\tau(\alpha), K')$. $\square$

Corolario 1.33. *Si $F : K$ es una extensión y $\tau : F \rightarrow F$ es un K -automorfismo de F , entonces:*

1. $\alpha \in F$ es un cero de $f \in K[X]$ si, y solo si, $\tau(\alpha)$ es un cero de $f \in K[X]$.

2. $\alpha \in F$ es algebraico sobre K si, y solo si, $\tau(\alpha)$ es algebraico sobre K con $\text{Irr}(\alpha, K) = \text{Irr}(\tau(\alpha), K)$.

Teorema 1.34 (Teorema de extensión para extensiones simples). *Sean $F : K$ y $F' : K'$ extensiones y $\sigma : K \rightarrow K'$ un isomorfismo. Sean $\alpha \in F$ algebraico sobre K y $\beta \in F'$ algebraico sobre K' . Son equivalentes:*

1. Existe un único isomorfismo $\gamma : K(\alpha) \rightarrow K'(\beta)$ que extiende σ y tal que $\gamma(\alpha) = \beta$.

2. $\text{Irr}(\beta, K') = \bar{\sigma}(\text{Irr}(\alpha, K))$.

Demostración.

1) $\Rightarrow$ 2) Se sigue de la proposición anterior.

2) $\Rightarrow$ 1) Teniendo en cuenta que $\bar{\sigma}(\text{Irr}(\alpha, K)) = \text{Irr}(\beta, K')$, se deduce que

$$\bar{\sigma}(\text{Ker } \varphi_\alpha) = \langle \bar{\sigma}(\text{Irr}(\alpha, K)) \rangle = \langle \text{Irr}(\beta, K') \rangle = \text{Ker } \varphi_\beta.$$

Por tanto, existe un único isomorfismo

$$\gamma: K[\alpha] = K(\alpha) \longrightarrow K'[\beta] = K'(\beta)$$

haciendo conmutativo el siguiente diagrama

$$\begin{array}{ccccc} \text{Ker } \varphi_\alpha & \hookrightarrow & K[X] & \xrightarrow{\varphi_\alpha} & K(\alpha) \\ & & \downarrow & & \downarrow \bar{\sigma} \\ & & \downarrow \bar{\sigma} & & \downarrow \gamma \\ \text{Ker } \varphi_\beta & \hookrightarrow & K'[X] & \xrightarrow{\varphi_\beta} & K'(\beta) \end{array}$$

en el cual las flechas horizontales de la izquierda son las inclusiones y $\gamma(\varphi_\alpha(X)) = \bar{\sigma}(\varphi_\beta(X))$.

En particular, $\gamma(\alpha) = \gamma(\varphi_\alpha(X)) = \varphi_\beta(\bar{\sigma}(X)) = \varphi_\beta(X) = \beta$ y $\gamma|_K = \bar{\sigma}|_K = \sigma$. $\square$

Capítulo 2

Construcciones con regla y compás

Uno de los problemas matemáticos más conocidos es el de las construcciones con regla y compás. ¿Quién no ha oído hablar, por ejemplo, de la cuadratura del círculo como sinónimo de algo irrealizable? Estos problemas tienen su origen en la matemática clásica griega; en concreto, en los *Elementos* de Euclides, en torno al siglo III a.C., que recopilan todo el saber matemático de la época, se deducen las propiedades geométricas mediante construcciones con regla y compás.

Aunque no están del todo claras las razones que llevaron a los matemáticos griegos a elegir para sus construcciones geométricas la regla y el compás, se cree que siendo conscientes de la necesidad de demostrar de forma rigurosa sus resultados y no disponiendo de la herramienta algebraica apropiada, optasen por utilizar aquellos instrumentos que, además de tener un uso muy sencillo, menos indujeran a error en los razonamientos; una regla no marcada (carente de marcas que permitan medir y trasladar distancias) y un compás.

Si bien la geometría griega alcanzó un gran nivel, algunos de los problemas surgidos, a pesar de la sencillez de su planteamiento, no pudieron ser resueltos ni por ellos ni por sus sucesores durante 2000 años; entre estos, los más famosos son los siguientes:

Cuadratura del círculo: Construir con regla y compás un cuadrado cuya área sea igual a la de un círculo dado.

Duplicación del cubo: Construir con regla y compás el lado de un cubo cuyo volumen sea el doble del de un cubo dado.

Trisección del ángulo: Dado un ángulo α , construir con regla y compás el ángulo $\alpha/3$.

Construcción de polígonos regulares: Construir con regla y compás el polígono regular de un determinado número de lados.

Vamos a ver que, utilizando las propiedades más básicas de la teoría de extensiones, podemos resolver estos problemas, lo que indica el enorme poder de los métodos algebraicos en la resolución de problemas geométricos.

2.1. Formulación geométrica

Sea $\mathcal{P}$ un conjunto de dos o más puntos del plano euclídeo $\mathbb{R}^2$. Para construir, con regla y compás, nuevos puntos a partir de $\mathcal{P}$, se intersecan las rectas y las circunferencias que podemos dibujar con la regla y el compás, donde las únicas *operaciones* permitidas son:

Tipo I (regla). Trazar la recta que pasa por dos puntos de $\mathcal{P}$.

Tipo II (compás). Trazar la circunferencia cuyo centro es un punto de $\mathcal{P}$ y cuyo radio es la distancia entre dos puntos distintos de $\mathcal{P}$.

Definición 2.1. Sea B un punto de $\mathbb{R}^2$.

i) Diremos que B es *constructible en un paso (o en una etapa) a partir de $\mathcal{P}$* si es un punto de intersección de dos rectas, una recta y una circunferencia o dos circunferencias, todas ellas obtenidas a partir de $\mathcal{P}$ usando operaciones de los tipos I y II.

ii) Se dice que B es *constructible (con regla y compás) a partir de $\mathcal{P}$* si existe una sucesión finita de puntos de $\mathbb{R}^2$, $B_1, B_2, \dots, B_n = B$ tales que:

a) B_1 es constructible en un paso a partir de $\mathcal{P}$.

b) Para cada $i : 2, \dots, n$, B_i es constructible en un paso a partir del conjunto $\mathcal{P} \cup \{B_1, \dots, B_{i-1}\}$.

iii) Diremos que B es *constructible (absolutamente)* si es constructible a partir de un conjunto $\mathcal{P}$ de 2 elementos.

Notación 2.2. Si A , B y C son puntos de $\mathbb{R}^2$, denotaremos con AB la recta que pasa por A y B , con $\overline{BC}$ la distancia entre B y C y con $c(A, \overline{BC})$ la circunferencia con centro A y radio $\overline{BC}$.

Ejemplos 2.3.

1) *Punto medio de un segmento:*

Si A y B son dos puntos distintos del plano, podemos construir un punto M sobre la recta AB tal que $\overline{MA} = \overline{MB}$ como sigue:

1) Trazamos las circunferencias $c(A, \overline{AB})$ y $c(B, \overline{AB})$ que se cortan en dos puntos P y Q ;

2) Trazamos la recta PQ que corta a la recta AB en un punto M tal que $\overline{MA} = \overline{MB}$.

2) *Proyección de un punto sobre una recta:*

Sean AB una recta y M un punto que no está en AB . Podemos construir la proyección, H , del punto M sobre la recta AB , a partir de $\{A, B, M\}$, de la siguiente forma:

- 1) Trazamos la circunferencia $c(A, \overline{AM})$;
- 2) Trazamos la circunferencia $c(B, \overline{BM})$ que interseca a la anterior en los puntos M y N ;
- 3) Trazamos la recta MN que interseca a la recta AB en el punto H .

3) Construcción de una referencia ortonormal a partir de dos puntos distintos O y I :

Consideramos como unidad la distancia entre los puntos O y I , es decir, suponemos que O y I están a distancia 1.

- 1) Trazamos la circunferencia $c(O, \overline{OI})$ que interseca a la recta OI en los puntos I y A ;
- 2) Trazamos la circunferencia $c(I, \overline{IA})$;
- 3) Trazamos la circunferencia $c(A, \overline{IA})$ que interseca a la circunferencia $c(I, \overline{IA})$ en los puntos M y N ;
- 4) Trazamos la recta MN que corta a la circunferencia $c(O, \overline{OI})$ en los puntos B y B' .

La referencia ortonormal es $(O; I, B)$.

4) Perpendicular a una recta por un punto:

Se obtiene como en el ejemplo 2) si el punto no está en la recta y como en el 3) si el punto está en la recta.

5) Paralela a una recta por un punto:

Se usa dos veces la construcción de la perpendicular a una recta por un punto.

2.2. Una aproximación algebraica

Nuestro primer paso es interpretar la situación geométrica anterior en el contexto de teoría de cuerpos.

Nota 2.4. Si A, B y C son tres puntos de $\mathbb{R}^2$ y K es el menor subcuerpo de $\mathbb{R}$ que contiene a $\mathbb{Q}$ y a las coordenadas de estos puntos, entonces:

La ecuación de la recta AB que pasa por A y B es de la forma

$$ax + by + c = 0, \text{ con } a, b, c \in K.$$

La ecuación de la circunferencia $c(A, \overline{BC})$ es de la forma

$$x^2 + y^2 + ax + by + c = 0, \text{ con } a, b, c \in K.$$

Si las coordenadas de A , B y C son, respectivamente, (a_1, a_2) , (b_1, b_2) y (c_1, c_2) , sabemos que:

i) la ecuación de la recta AB está dada por

$$\begin{vmatrix} x - a_1 & a_1 - b_1 \\ y - a_2 & a_2 - b_2 \end{vmatrix} = 0 \Leftrightarrow (x - a_1)(a_2 - b_2) - (y - a_2)(a_1 - b_1) = 0,$$

ii) la ecuación de la circunferencia $c(A, \overline{BC})$ es

$$(x - a_1)^2 + (y - a_2)^2 = (c_1 - b_1)^2 + (c_2 - b_2)^2.$$

Estas ecuaciones son de la forma indicada anteriormente.

Proposición 2.5. *Si $B = (x_n, y_n) \in \mathbb{R}^2$ es constructible a partir de $\mathcal{P}$, entonces existe una torre finita de cuerpos*

$$\mathbb{Q} \subset F_0 \subset F_1 \subset \cdots \subset F_m \subset \mathbb{R}$$

tal que $x_n, y_n \in F_m$ y $[F_i : F_{i-1}] \leq 2$ para cada $i : 1, \dots, m$.

Demostración. Por definición, existe una sucesión de puntos $B_i = (x_i, y_i)$ de $\mathbb{R}^2$, con $i : 1, \dots, n$, tales que B_1 es constructible en un paso a partir de $\mathcal{P}$ y, para cada $i : 2, \dots, n$, B_i es constructible en un paso a partir de $\mathcal{C}_{i-1} = \mathcal{P} \cup \{B_1, \dots, B_{i-1}\}$.

A cada paso de la construcción vamos a asociarle un subcuerpo de $\mathbb{R}$ de la siguiente forma:

Sea $K_0 = \mathbb{Q}(\mathcal{P})$ el subcuerpo de $\mathbb{R}$ generado sobre $\mathbb{Q}$ por las coordenadas de todos los puntos de $\mathcal{P}$.

Para cada $i : 1, \dots, n$, sea $K_i = K_{i-1}(x_i, y_i)$, obtenido por adjunción de las coordenadas del punto B_i al cuerpo K_{i-1} .

Así, se obtiene una torre de cuerpos

$$\mathbb{Q} \subset K_0 \subset K_1 \subset \dots \subset K_n \subset \mathbb{R}$$

tal que $(x_i, y_i) \in K_i$, para cada $i : 1, \dots, n$.

Demostremos ahora que $[K_{i-1}(x_i) : K_{i-1}] \leq 2$ y que $[K_{i-1}(y_i) : K_{i-1}] \leq 2$, para cada $i : 1, \dots, n$, viendo que x_i e y_i son ceros de polinomios de grado ≤ 2 con coeficientes en K_{i-1} . Para ello, debemos distinguir tres casos, según que el punto B_i se haya obtenido a partir de $\mathcal{C}_{i-1} = \mathcal{P} \cup \{B_1, \dots, B_{i-1}\}$, intersecando dos rectas, una recta y una circunferencia o dos circunferencias.

Caso a) $B_i = (x_i, y_i) = r \cap r'$ es la intersección de dos rectas que pasan por puntos de $\mathcal{C}_{i-1}$.

Por la nota 2.4, existen $a, b, c, a', b', c' \in K_{i-1}$ de modo que

$$r \equiv ax + by = c \quad \text{y} \quad r' \equiv a'x + b'y = c'$$

con $ab' - a'b \neq 0$, ya que las dos rectas no son paralelas.

Resolviendo el sistema, por Cramer, obtenemos

$$(x_i, y_i) = \left(\frac{\begin{vmatrix} c & b \\ c' & b' \end{vmatrix}}{\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}}, \frac{\begin{vmatrix} a & c \\ a' & c' \end{vmatrix}}{\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}} \right).$$

Es claro que $x_i, y_i \in K_{i-1}$; en este caso, $[K_{i-1}(x_i) : K_{i-1}] = 1$ y $[K_{i-1}(y_i) : K_{i-1}] = 1$, ya que las coordenadas del nuevo punto verifican un polinomio de grado 1 con coeficientes en K_{i-1} .

Caso b) $B_i = (x_i, y_i) \in r \cap cir$ es la intersección de la recta r que pasa por dos puntos de $\mathcal{C}_{i-1}$ y la circunferencia cir cuyo centro $C = (c_1, c_2)$ es un punto de $\mathcal{C}_{i-1}$ y su radio ρ la distancia entre dos puntos de $\mathcal{C}_{i-1}$.

Por la nota 2.4,

$$r \equiv ax + by = c \text{ y } cir \equiv (x - c_1)^2 + (y - c_2)^2 = \rho^2$$

y los coeficientes de estas ecuaciones están en K_{i-1} .

Las coordenadas x_i e y_i del punto B_i deben satisfacer ambas ecuaciones.

Si $b \neq 0$, entonces $y_i = b^{-1}c - b^{-1}ax_i$ y, por tanto,

$$(x_i - c_1)^2 + (b^{-1}c - b^{-1}ax_i - c_2)^2 = \rho^2.$$

En consecuencia, x_i es raíz de un polinomio de grado ≤ 2 con coeficientes en K_{i-1} y $[K_{i-1}(x_i) : K_{i-1}] \leq 2$.

Analogamente, para $a \neq 0$ se obtendría que $[K_{i-1}(y_i) : K_{i-1}] \leq 2$.

Si $b = 0$, necesariamente $a \neq 0$ y entonces $[K_{i-1}(y_i) : K_{i-1}] \leq 2$ y, como $ax_i = c$, se tiene que $[K_{i-1}(x_i) : K_{i-1}] = 1$.

Caso c) $B_i = (x_i, y_i) \in cir \cap cir'$ es la intersección de dos circunferencias cuyos centros $C = (c_1, c_2)$ y $C' = (c'_1, c'_2)$ tienen coordenadas en K_{i-1} y sus radios ρ y ρ' son las distancias entre dos puntos de $\mathcal{C}_{i-1}$; las ecuaciones de estas circunferencias son:

$$(1) \text{ } cir \equiv (x - c_1)^2 + (y - c_2)^2 = \rho^2 \text{ y } (2) \text{ } cir' \equiv (x - c'_1)^2 + (y - c'_2)^2 = \rho'^2$$

con coeficientes en K_{i-1} .

Haciendo (2) - (1) se tiene

$$r \equiv 2(c_1 - c'_1)x + 2(c_2 - c'_2)y = \rho'^2 - \rho^2 + c_1^2 - c'_1{}^2 + c_2^2 - c'_2{}^2$$

que es la ecuación de una recta ya que $c_1 - c'_1$ y $c_2 - c'_2$ no pueden ser ambos 0, pues cir y cir' no pueden ser concéntricas. Además $B_i = (x_i, y_i)$ es solución del sistema dado por las ecuaciones de cir y de r , y el caso se reduce al caso b).

En conclusión, para cada $i \in \{1, \dots, n\}$, hemos visto que $[K_{i-1}(x_i) : K_{i-1}] \leq 2$ y $[K_{i-1}(x_i, y_i) : K_{i-1}(x_i)] \leq 2$; por tanto, $[K_i : K_{i-1}] = 1, 2$ o 4 .

Tomando $F_0 = K_0$ e intercalando $K_{i-1}(x_i)$ entre K_i y K_{i-1} en los pasos de grado 4, se obtiene una torre como la del enunciado. $\square$

En adelante $\mathcal{P}$ será el conjunto más sencillo posible, es decir, $\mathcal{P}$ tiene dos elementos O e I . Elegimos un sistema de referencia cartesiano en donde la recta OI sea el eje x , O el origen y $\overline{OI}$ la unidad de longitud, de modo que $\mathcal{P} = \{O = (0, 0), I = (1, 0)\}$.

Corolario 2.6. *Si $B = (x_n, y_n) \in \mathbb{R}^2$ es constructible, entonces existe una torre finita de cuerpos*

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_m \subset \mathbb{R}$$

tal que $x_n, y_n \in F_m$ y $[F_i : F_{i-1}] \leq 2$, para cada $i : 1, \dots, m$.

Demostración. En este caso, $F_0 = \mathbb{Q}(0, 1) = \mathbb{Q}$. □

Definición 2.7. Un número real r se dice *constructible* si el punto $(r, 0)$ (o equivalentemente $(0, r)$) es constructible.

Nótese que un número real r es constructible si, y solo si, $|r|$ es la distancia entre dos puntos constructibles.

Proposición 2.8. *Un punto $(r, s) \in \mathbb{R}^2$ es constructible si, y solo si, los números reales r y s son constructibles.*

Proposición 2.9. *El conjunto de los números reales constructibles, $\mathcal{C}$, es un subcuerpo de $\mathbb{R}$ que contiene a $\mathbb{Q}$ y es cerrado para raíces cuadradas de números reales constructibles positivos (es decir, si $r \in \mathbb{R}^+ \cap \mathcal{C}$, entonces $\pm\sqrt{r} \in \mathcal{C}$).*

Demostración. Es evidente que $O = (0, 0)$ e $I = (1, 0)$ son puntos constructibles, en consecuencia 0 y $1 \in \mathcal{C}$.

Si $a, b \in \mathcal{C}$, entonces $a \pm b \in \mathcal{C}$:

$c((a, 0), |b|) \equiv (x - a)^2 + y^2 = b^2$ corta a $OI \equiv y = 0$ en $(a \pm b, 0)$, por tanto, $a \pm b \in \mathcal{C}$.

Si $a \in \mathcal{C}$, se verifica que $-a \in \mathcal{C}$:

$(a, 0)$ es constructible y $OI \cap c(O, |a|) = \{(a, 0), (-a, 0)\}$, por tanto $-a \in \mathcal{C}$.

Si $a, b \in \mathcal{C}$, se tiene que $ab \in \mathcal{C}$:

Supongamos primero que $a > 0$ y $b > 0$. Los puntos $I' = (0, 1)$, $A = (a, 0)$ y $B' = (0, b)$ son constructibles. Trazamos la recta paralela a $I'A$ por B' , que corta a $OI \equiv y = 0$ en $R = (ab, 0)$. Por tanto, R es constructible y $ab \in \mathcal{C}$.

Si $a = 0$ o $b = 0$, $ab = 0 \in \mathcal{C}$.

Si $a > 0$ y $b < 0$, como $-b > 0$, se tiene que $a(-b) = -(ab) \in \mathcal{C}$ y, por tanto, $-(-(ab)) = ab \in \mathcal{C}$.

Si $a \neq 0$ y $a \in \mathcal{C}$, entonces $a^{-1} \in \mathcal{C}$:

Sea $a > 0$. Los puntos $I = (1, 0)$, $I' = (0, 1)$ y $A' = (0, a)$ son constructibles. Trazamos la recta paralela a la recta IA' por I' , dada por $ax + y = 1$, que corta a $OI \equiv y = 0$ en $R = (\frac{1}{a}, 0)$. Por tanto, R es constructible y $a^{-1} \in \mathcal{C}$.

Si $a < 0$, ya que $-a > 0$ y $-a \in \mathcal{C}$, acabamos de ver que entonces $\frac{1}{-a} = -\frac{1}{a} \in \mathcal{C}$ y así $\frac{1}{a} \in \mathcal{C}$.

Por tanto, $\mathcal{C}$ es un subcuerpo de $\mathbb{R}$; puesto que todo subcuerpo de $\mathbb{R}$ contiene a $\mathbb{Q}$, se tiene que $\mathcal{C}$ contiene a $\mathbb{Q}$.

Por último veamos que si $a \in \mathbb{R}^+ \cap \mathcal{C}$, se verifica que $\sqrt{a} \in \mathcal{C}$:

Como $a, 1 \in \mathcal{C}$, entonces $a + 1 \in \mathcal{C}$, por tanto $(a + 1, 0)$ es un punto constructible. Construimos el punto medio del segmento de extremos $(0, 0)$ y $(a + 1, 0)$, $M = (\frac{a + 1}{2}, 0)$.

La circunferencia $c(M, \frac{a + 1}{2})$ y la perpendicular por el punto $(1, 0)$ a la recta $OI \equiv y = 0$, cuya ecuación es $x = 1$, se cortan en $(1, \pm\sqrt{a})$ y, por ello, $\pm\sqrt{a} \in \mathcal{C}$. $\square$

Estamos ahora en condiciones de dar una caracterización de los números reales constructibles en términos de extensiones de cuerpos.

Teorema 2.10 (Teorema fundamental sobre constructibilidad). (*Wantzel, 1837*)

Sea $\alpha \in \mathbb{R}$, α es constructible si, y solo si, existe una torre de cuerpos

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_m \subset \mathbb{R}$$

tal que $\alpha \in F_m$ y $[F_{i+1} : F_i] \leq 2$ para todo $i : 0, \dots, m - 1$.

En particular, si α es un número real constructible entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^r$ para algún $r \geq 0$.

Demostración.

“ $\Leftarrow$ ” Probaremos, por inducción en m , que todos los elementos de F_m son constructibles, es decir, que $F_m \subset \mathcal{C}$.

Si $m = 0$, $\alpha \in F_0 = \mathbb{Q}$ y, así, $\alpha \in \mathcal{C}$.

Supongamos, ahora, que $m > 0$ y que $F_{m-1} \subset \mathcal{C}$.

Sea $\alpha \in F_m$, puesto que $[F_m : F_{m-1}] \leq 2$ y que $F_{m-1} \subset F_{m-1}(\alpha) \subset F_m$, se tiene que $[F_{m-1}(\alpha) : F_{m-1}] = \partial \text{Irr}(\alpha, F_{m-1}) \leq 2$.

Si $[F_{m-1}(\alpha) : F_{m-1}] = 1$, es evidente que $\alpha \in F_{m-1}$ y, por la hipótesis de inducción, $\alpha \in \mathcal{C}$.

Si $[F_{m-1}(\alpha) : F_{m-1}] = 2$, se verifica que $\partial \text{Irr}(\alpha, F_{m-1}) = 2$. Supongamos que $\text{Irr}(\alpha, F_{m-1}) = X^2 + aX + b \in F_{m-1}[X]$. En este caso,

$$\alpha = \frac{-a \pm \sqrt{a^2 - 4b}}{2} \in F_m.$$

Como $F_m \subset \mathbb{R}$, se tiene que $a^2 - 4b \geq 0$.

Además, teniendo en cuenta que $a, b \in F_{m-1}$, se obtiene que a y $a^2 - 4b \in F_{m-1}$ y, por la hipótesis de inducción, a y $a^2 - 4b \in \mathcal{C}$, y como $a^2 - 4b \geq 0$, por la proposición 2.9, también $\sqrt{a^2 - 4b} \in \mathcal{C}$. Puesto que $\mathcal{C}$ es un cuerpo que contiene a $\mathbb{Q}$, se sigue que $\alpha \in \mathcal{C}$.

“ $\Rightarrow$ ” Se sigue del corolario 2.6. □

2.3. Aplicación a algunos problemas clásicos

Proposición 2.11 (Duplicación del cubo). *No es posible construir con regla y compás un cubo cuyo volumen sea el doble del volumen de otro cubo dado.*

Demostración. Eligiendo una referencia en la que los extremos de una arista del cubo inicial sean $(0, 0)$ y $(1, 0)$, entonces su volumen será 1 u.c. La posibilidad de construir un cubo de volumen 2, significaría que el lado del cubo, α , sería un número real constructible tal que $\alpha^3 = 2$. Por el teorema 2.10, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^r$, para algún $r \geq 0$, lo que contradice que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \partial \text{Irr}(\alpha, \mathbb{Q}) = \partial(X^3 - 2) = 3$. □

Proposición 2.12 (Cuadratura del círculo). *Es imposible, construir con regla y compás, un cuadrado cuya área sea igual a la de un círculo dado.*

Demostración. Un círculo está determinado por su centro y un punto y podemos elegir una referencia en la que el centro sea $(0, 0)$ y el punto dado $(1, 0)$. En este caso, el área del círculo sería π u.c. Supongamos que es posible construir un cuadrado de área π ; su lado, l , sería un número real constructible tal que $l \cdot l = \pi$ y, por tanto, $\pi = l \cdot l \in \mathcal{C}$; en virtud del teorema 2.10, $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2^r$ para algún $r \geq 0$, y π sería algebraico sobre $\mathbb{Q}$. $\square$

Proposición 2.13 (Trisección de ángulos). *Existen ángulos que no pueden ser trisecados con regla y compás.*

Demostración. Veremos que el ángulo $\frac{\pi}{3} = 60^\circ$ es constructible y no es trisecable, o equivalentemente, que el ángulo $\frac{\pi}{9} = 20^\circ$ no es constructible.

Elegimos un sistema de referencia con $O = (0, 0)$ e $I = (1, 0)$. Trazamos las circunferencias $c(O, \overline{OI} = 1)$ y $c(I, \overline{OI} = 1)$ que se cortan en los puntos $P = (1/2, \sqrt{3}/2)$ y $P' = (1/2, -\sqrt{3}/2)$. Las rectas PO y OI determinan un ángulo $\angle POI = 60^\circ$.

Si el ángulo $\angle 20^\circ$ es constructible, $(\cos 20^\circ, 0)$ es constructible, con lo cual $\cos 20^\circ \in \mathcal{C}$ y también $\alpha = 2 \cos 20^\circ \in \mathcal{C}$. Por el teorema 2.10, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ sería potencia de 2.

Teniendo en cuenta que $\cos 3\theta = 4 \cos^3 \theta - 3 \cos \theta$, para $\theta = 20^\circ$ se tiene que

$$\cos 60^\circ = \frac{1}{2} = 4 \cos^3 20^\circ - 3 \cos 20^\circ \Leftrightarrow 8 \cos^3 20^\circ - 6 \cos 20^\circ - 1 = 0.$$

Así, $\alpha^3 - 3\alpha - 1 = 0$.

El polinomio $X^3 - 3X - 1$ es irreducible en $\mathbb{Q}[X]$ ya que no tiene ceros en $\mathbb{Q}$, por tanto $\text{Irr}(\alpha, \mathbb{Q}) = X^3 - 3X - 1$ y $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, lo que da una contradicción. $\square$

Capítulo 3

Cuerpos de escisión. Clausura algebraica

Sea K un cuerpo y $f \in K[X]$ con $\partial f \geq 1$. Los objetivos de este capítulo son:

1. Encontrar una extensión simple $K(\alpha) : K$ tal que $f(\alpha) = 0$.
2. Encontrar una extensión finita $E : K$ tal que f tenga todos sus ceros en E .

3.1. Teorema de Kronecker

Lema 3.1. *Si $\sigma : K \rightarrow F$ es un monomorfismo de cuerpos, existe una extensión $E : K$ y un isomorfismo $\tau : E \rightarrow F$ que extiende a σ .*

Demostración. Sean S un conjunto cuya cardinalidad es la misma que la de $F \setminus \sigma(K)$ y que es disjunto con K y $f : S \rightarrow F \setminus \sigma(K)$ una aplicación biyectiva.

Si $E := K \cup S$, la aplicación $\tau : E \rightarrow F$ definida por:

$$\tau(a) := \begin{cases} \sigma(a) & \text{si } a \in K \\ f(a) & \text{si } a \in S \end{cases}$$

es biyectiva y su inversa, τ^{-1} , está definida por:

$$\tau^{-1}(b) := \begin{cases} \sigma^{-1}(b) & \text{si } b \in \sigma(K) \\ f^{-1}(b) & \text{si } b \in F \setminus \sigma(K). \end{cases}$$

Es evidente que $\tau|_K = \sigma$.

Esta biyección permite dotar a E de estructura de cuerpo como sigue:

Si $a, b \in E$,

$$a \oplus b := \tau^{-1}[\tau(a) + \tau(b)] \text{ y } a \odot b := \tau^{-1}[\tau(a) \cdot \tau(b)].$$

La restricción de $\oplus$ y $\odot$ a K , coincide con la suma y el producto de K , de modo que K es un subcuerpo de E .

Trivialmente, τ es un homomorfismo de cuerpos y, por ser biyectiva, es un isomorfismo y, ya hemos visto, que extiende a σ . $\square$

Teorema 3.2 (Teorema de Kronecker). *Si K es un cuerpo y $f \in K[X]$ es irreducible, existe una extensión simple $K(\alpha) : K$ con $f(\alpha) = 0$ y además $[K(\alpha) : K] = \partial f$.*

Demostración. Dado que f irreducible en $K[X]$ y que $K[X]$ es un dominio de ideales principales, se tiene que $\langle f \rangle$ es un ideal maximal en $K[X]$ o, equivalentemente, que $F := K[X] / \langle f \rangle$ es un cuerpo.

Consideremos la aplicación

$$\sigma : K \hookrightarrow K[X] \xrightarrow{\pi} K[X] / \langle f \rangle = F$$

$$a \mapsto \sigma(a) = \bar{a} = a + \langle f \rangle$$

que es monomorfismo de cuerpos y así $K \xrightarrow{\sigma} \sigma(K)$ que es un subcuerpo de F .

Sea $\bar{\sigma}$ el isomorfismo entre los anillos de polinomios $K[X]$ y $\sigma(K)[X]$ dado por:

$$\begin{aligned} \bar{\sigma} : K[X] &\longrightarrow \sigma(K)[X] \\ \sum_{i=0}^m b_i X^i &\mapsto \sum_{i=0}^m \bar{b}_i X^i \end{aligned}$$

Si $\gamma := X + \langle f \rangle \in F$ y $f = \sum_{i=0}^n a_i X^i$, entonces

$$\bar{\sigma}(f)(\gamma) = \left(\sum_{i=0}^n \bar{a}_i X^i \right)(\gamma) = \sum_{i=0}^n \bar{a}_i \gamma^i = \sum_{i=0}^n a_i X^i + \langle f \rangle = f + \langle f \rangle = \bar{0}$$

es decir, $\gamma \in F$ es un cero del polinomio $\bar{\sigma}(f) \in \sigma(K)[X]$.

Por el lema 3.1, existe un cuerpo E tal que K es subcuerpo de E y un isomorfismo τ de modo que los siguientes diagramas son conmutativos:

$$\begin{array}{ccc} E & \xrightarrow{\tau} & F \\ \uparrow i & & \uparrow j \\ K & \xrightarrow{\sigma} & \sigma(K) \end{array} \quad \Leftrightarrow \quad \begin{array}{ccc} E & \xleftarrow{\tau^{-1}} & F \\ \uparrow i & & \uparrow j \\ K & \xleftarrow{\sigma^{-1}} & \sigma(K) \end{array}$$

Utilizando la proposición 1.32, se tiene que:

$\gamma \in F$ es un cero de $\bar{\sigma}(f) \in \sigma(K)[X]$ si, y solo si, $\alpha = \tau^{-1}(\gamma) \in E$ es cero de $\bar{\sigma}^{-1}(\bar{\sigma}(f)) = f \in K[X]$.

Además, $[K(\alpha) : K] = \partial \text{Irr}(\alpha, K) = \partial f$, ya que $\text{Irr}(\alpha, K)$ y f son asociados. $\square$

Corolario 3.3. *Si K es un cuerpo y $f \in K[X]$, con $\partial f \geq 1$, existe una extensión $E : K$ en la que f tiene un cero y $[E : K] \leq \partial f$.*

Demostración. Es conocido que $K[X]$ es un dominio de factorización única. Sea g un factor irreducible de f en $K[X]$. Por el Teorema de Kronecker (3.2), existe una extensión $E = K(\alpha) : K$ con $g(\alpha) = 0$ y $[K(\alpha) : K] = \partial(\text{Irr}(\alpha, K)) = \partial(g) \leq \partial(f)$. Además, como g divide a f y $g(\alpha) = 0$, se tiene que $f(\alpha) = 0$. $\square$

3.2. Cuerpo de escisión de un polinomio

Definición 3.4. Sean K un cuerpo, $f \in K[X]$ con $\partial(f) = n \geq 1$ y $E : K$ una extensión.

Diremos que f *escinde en E* si existen $\alpha_1, \dots, \alpha_n \in E$, no necesariamente distintos, tales que

$$f = c(X - \alpha_1) \cdots (X - \alpha_n) (*)$$

en donde, obviamente, c es el coeficiente principal de f .

Se dirá que E es un *cuerpo de escisión de f sobre K* si además se verifica que

$$E = K(\alpha_1, \dots, \alpha_n).$$

Observaciones 3.5.

1) Si E es un cuerpo de escisión para f sobre K y $\alpha_1, \dots, \alpha_n \in E$ son tales que

$$f = c(X - \alpha_1) \cdots (X - \alpha_n)$$

se verifica que:

a) Si F es un cuerpo de intermedio entre K y E , entonces E es también un cuerpo de escisión para f sobre F , pues las condiciones de la definición anterior se cumplen para F en lugar de K , con los mismos $\alpha_1, \dots, \alpha_n \in E$.

b) $\alpha_1, \dots, \alpha_n$ son ceros de f en E y son los únicos ceros que tiene el polinomio f en cualquier extensión de E .

En efecto, si $E' : E$ es una extensión y suponemos que $\beta \in E'$ es un cero de f , aplicando el homomorfismo evaluación en β , $\varphi_\beta: E[X] \rightarrow E'$, resulta que

$$f(\beta) = c(\beta - \alpha_1) \cdots (\beta - \alpha_n) = 0.$$

Como E' es un dominio entero, alguno de los factores $\beta - \alpha_i$ debe ser 0, es decir, $\beta = \alpha_i$ para algún i .

c) La condición $E = K(\alpha_1, \dots, \alpha_n)$ de la definición anterior es equivalente a que no existe ningún cuerpo intermedio, F , entre E y K tal que f escinda en F .

2) Si $f \in K[X]$ es lineal, entonces f escinde en K y K es un cuerpo de escisión para f sobre K :

Si $f = cX + b \in K[X]$ con $c \neq 0$, tomando $\alpha = -bc^{-1} \in K$, se tiene que $f = c(X - \alpha)$ y $K(\alpha) = K$.

Ejemplos 3.6.

1) Sea $f = X^2 + 1 \in \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$.

Dado que $f = (X - i)(X + i)$ en $\mathbb{C}[X]$, se verifica que:

a) $\mathbb{Q}(i, -i) = \mathbb{Q}(i)$ es un cuerpo de escisión para f sobre $\mathbb{Q}$.

b) Un cuerpo de escisión de f sobre $\mathbb{R}$ es $\mathbb{R}(i) = \mathbb{C}$.

c) $\mathbb{C}$ también es un cuerpo de escisión para f sobre $\mathbb{C}$.

2) Si $f = X^2 - 5 \in \mathbb{Q}[X]$, entonces $\mathbb{Q}(\sqrt{5})$ es un cuerpo de escisión de f sobre $\mathbb{Q}$.

La cuestión que nos planteamos ahora es la existencia y unicidad de los cuerpos de escisión.

Teorema 3.7. *Sea K un cuerpo y $f \in K[X]$ con $\partial f = n \geq 1$. Existe una extensión $E : K$ tal que E es un cuerpo de escisión para f sobre K y $[E : K] \leq n!$*

Demostración. La prueba se hará por inducción en n .

Si $n = 1$. Es trivial, ya que podemos tomar $E = K$.

Supongamos ahora que $n > 1$ y que el resultado es cierto para cualquier polinomio de grado menor que n con coeficientes en cualquier cuerpo.

Por el corolario (3.3), existe una extensión $K(\alpha_1) : K$ tal que α_1 es cero de f y $[K(\alpha_1) : K] \leq n$.

Puesto que $\alpha_1 \in K(\alpha_1)$ es cero de f , se verifica que $X - \alpha_1$ divide a f en $K(\alpha_1)[X]$, es decir, existe $h \in K(\alpha_1)[X]$ tal que $f = (X - \alpha_1)h$ y $\partial h = n - 1 < n$.

Por la hipótesis de inducción, existe una extensión $E : K(\alpha_1)$ tal que E es un cuerpo de escisión para h sobre $K(\alpha_1)$ y $[E : K(\alpha_1)] \leq (n - 1)!$

Nótese que si denotamos por c el coeficiente principal de h (que también es el de f) y $h = c(X - \alpha_2) \cdots (X - \alpha_n)$ en $E[X]$, entonces $E = K(\alpha_1)(\alpha_2, \dots, \alpha_n) = K(\alpha_1, \alpha_2, \dots, \alpha_n)$. Teniendo en cuenta que $f = c(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$, es obvio que E es un cuerpo de escisión para f sobre K .

Puesto que $K \subset K(\alpha_1) \subset E$, del Teorema del grado (1.6), se sigue que:

$$[E : K] = [E : K(\alpha_1)] [K(\alpha_1) : K] \leq (n - 1)! n = n! \quad \square$$

Probaremos, ahora, que “todos los cuerpos de escisión para f sobre K son K -isomorfos”. La idea para demostrar este resultado es usar inductivamente el Teorema de extensión para extensiones simples (1.34).

Teorema 3.8 (Teorema de extensión para cuerpos de escisión).

Sea $\sigma: K \rightarrow K'$ un isomorfismo de cuerpos y $f \in K[X]$ con $\partial(f) \geq 1$. Sea E un cuerpo de escisión de f sobre K y sea E' un cuerpo de escisión de $\bar{\sigma}(f) \in K'[X]$ sobre K' . Entonces, existe un isomorfismo $\tau: E \rightarrow E'$ que extiende σ .

Demostración. Haremos la demostración por inducción en $\partial f = \partial(\bar{\sigma}(f)) = n$.

Si $n = 1$. El resultado es evidente considerando $E = K$, $E' = K'$ y $\tau = \sigma$.

Supongamos, ahora, que $\partial f = \partial(\bar{\sigma}(f)) = n > 1$.

Si $\alpha_1, \dots, \alpha_n$ son los ceros de f en E , se tiene que $f = c(X - \alpha_1) \cdots (X - \alpha_n)$ y $E = K(\alpha_1, \dots, \alpha_n)$.

Como α_1 es algebraico sobre K , si $g = \text{Irr}(\alpha_1, K)$, g es un factor mónico e irreducible de f en $K[X]$. Teniendo en cuenta que $\bar{\sigma}$ es un isomorfismo, $\bar{\sigma}(g)$ es un factor mónico e irreducible de $\bar{\sigma}(f)$ en $K'[X]$ y $\bar{\sigma}(g)$ escinde en E' .

Sea $\beta \in E'$ un cero de $\bar{\sigma}(g)$ (y por tanto de $\bar{\sigma}(f)$), entonces $\bar{\sigma}(g) = \text{Irr}(\beta, K')$. Por el Teorema de extensión para extensiones simples (1.34), existe un único isomorfismo

$$\gamma: K(\alpha_1) \rightarrow K'(\beta) \text{ tal que } \gamma|_K = \sigma \text{ y } \gamma(\alpha_1) = \beta.$$

Ahora veremos, usando la hipótesis de inducción, que γ se extiende a un isomorfismo $\tau: E \rightarrow E'$.

Ya que $\alpha_1 \in K(\alpha_1)$ es cero de f , por el Teorema del factor, $f = (X - \alpha_1)f_1$ en $K(\alpha_1)[X]$ y, por tanto, $\bar{\gamma}(f) = (X - \gamma(\alpha_1))\bar{\gamma}(f_1) = (X - \beta)\bar{\gamma}(f_1)$ en $K'(\beta)[X]$.

Como $f_1 = c(X - \alpha_2) \cdots (X - \alpha_n)$, donde $\alpha_2, \dots, \alpha_n \in E$, es claro que $E = K(\alpha_1)(\alpha_2, \dots, \alpha_n)$ es un cuerpo de escisión de f_1 sobre $K(\alpha_1)$ y, análogamente, E' es un cuerpo de escisión de $\bar{\gamma}(f_1)$ sobre $K'(\beta)$.

Además, al ser $\partial f_1 = n - 1 = \partial(\bar{\gamma}(f_1))$, utilizando la hipótesis de inducción, se obtiene un isomorfismo $\tau: E \rightarrow E'$ tal que $\tau|_{K(\alpha_1)} = \gamma$ y, por tanto, $\tau|_K = \gamma|_K = \sigma$. $\square$

Corolario 3.9 (Unicidad del cuerpo de escisión).

Si E y E' son cuerpos de escisión de un polinomio $f \in K[X]$ sobre K , entonces E y E' son K -isomorfos.

Demostración. Basta aplicar el teorema anterior en el caso $K = K'$ y $\sigma = id_K$. $\square$

Corolario 3.10. *Sea E un cuerpo de escisión de un polinomio $f \in K[X]$ sobre K y sean $\alpha, \beta \in E$ tales que $\text{Irr}(\alpha, K) = \text{Irr}(\beta, K)$. Existe un K -automorfismo $\tau: E \rightarrow E$ tal que $\tau(\alpha) = \beta$.*

Demostración. Ya que $\text{Irr}(\alpha, K) = \text{Irr}(\beta, K)$, por el Teorema de extensión para extensiones simples (1.34), existe un K -isomorfismo $\sigma: K(\alpha) \rightarrow K(\beta)$ con $\sigma(\alpha) = \beta$. Puesto que E es cuerpo de escisión de f sobre K , lo es también sobre $K(\alpha)$ y sobre $K(\beta)$ y, por el Teorema de extensión para cuerpos de escisión (3.8), existe un isomorfismo $\tau: E \rightarrow E$ tal que $\tau|_{K(\alpha)} = \sigma$ y, por tanto, $\tau|_K = \sigma|_K = id_K$ y $\tau(\alpha) = \beta$. $\square$

3.3. Clausura algebraica de un cuerpo

En las secciones anteriores, hemos visto que dado un polinomio $f \in K[X]$, con $\partial(f) = n \geq 1$, existe una extensión finita $E: K$ de modo que f escinde en E .

Ahora, vamos a ver que es posible encontrar una extensión algebraica, $E: K$, tal que todos los polinomios de $K[X]$ escinden en E .

Definición 3.11. Diremos que un cuerpo E es *algebraicamente cerrado* si todo polinomio irreducible en $E[X]$ es lineal.

Proposición 3.12. *Si E es un cuerpo, son equivalentes:*

- i) E es algebraicamente cerrado.
- ii) Todo $f \in E[X]$ con $\partial(f) = n \geq 1$ tiene un cero en E .
- iii) Todo $f \in E[X]$ con $\partial(f) = n \geq 1$ se descompone en $E[X]$ como

$$f = c(X - \alpha_1) \cdots (X - \alpha_n),$$

es decir, escinde en E .

Observación 3.13. Si $\tau: E \rightarrow E'$ es un isomorfismo de cuerpos, entonces E es algebraicamente cerrado si, y solamente si, E' lo es también.

En efecto, cada $f' \in E'[X]$ es de la forma $f' = \bar{\tau}(f)$ para un único $f \in E[X]$ del mismo grado que f' , y un elemento $\alpha \in E$ es un cero de f si, y solamente si, $\tau(\alpha) \in E'$

es un cero de f' . Por lo tanto, cada $f \in E[X]$ no constante tiene un cero en E si, y solo si, cada $f' \in E'[X]$ no constante tiene un cero en E' .

Proposición 3.14. *E es algebraicamente cerrado si, y solo si, E no tiene extensiones finitas (respectivamente algebraicas) propias.*

Demostración.

“ $\Rightarrow$ ” Sea $E' : E$ una extensión finita (respectivamente algebraica). Si $\alpha \in E'$, entonces α es algebraico sobre E y, como E es algebraicamente cerrado, $\text{Irr}(\alpha, E) = X - \alpha$ y así $\alpha \in E$.

“ $\Leftarrow$ ” Sea $f \in E[X]$ un polinomio irreducible, por el Teorema de Kronecker (3.2), existe una extensión $E(\alpha) : E$ tal que $f(\alpha) = 0$ y $[E(\alpha) : E] = \partial \text{Irr}(\alpha, E)$. Como $E(\alpha) : E$ es finita (respectivamente algebraica), por hipótesis, se tiene que $E(\alpha) = E$ y entonces $\alpha \in E$. Por tanto, $\text{Irr}(\alpha, E) = X - \alpha$. Dado que $\text{Irr}(\alpha, E)$ y f son asociados, $\partial f = \partial(\text{Irr}(\alpha, E)) = 1$. $\square$

Definición 3.15. Sea $\bar{K} : K$ una extensión. Diremos que $\bar{K}$ es una *clausura algebraica* de K si $\bar{K} : K$ es una extensión algebraica y $\bar{K}$ es algebraicamente cerrado.

Así, nuestro objetivo es equivalente a demostrar la existencia de una clausura algebraica de K .

Proposición 3.16. *Sean K un cuerpo, $F : K$ una extensión algebraica y L un cuerpo algebraicamente cerrado. Si $\sigma : K \rightarrow L$ es un monomorfismo, entonces existe un monomorfismo $\tau : F \rightarrow L$ que extiende a σ . Si, además, $L : \sigma(K)$ es algebraica y F es algebraicamente cerrado, entonces τ es un isomorfismo. En particular, dos clausuras algebraicas de un mismo cuerpo, K , son K -isomorfas.*

Demostración. Sea $\mathfrak{S}$ el conjunto de pares (E, τ) tales que $K \subset E \subset F$ y $\tau : E \rightarrow L$ es un monomorfismo que extiende a σ . Definimos en $\mathfrak{S}$ una relación de orden como sigue:

$$(E_1, \tau_1) \leq (E_2, \tau_2) :\Leftrightarrow E_1 \subset E_2 \text{ y } \tau_2|_{E_1} = \tau_1.$$

Obsérvese que $\mathfrak{S}$ es no vacío, ya que $(K, \sigma) \in \mathfrak{S}$, y que es inductivo. En efecto, si

$$\cdots \leq (E_i, \tau_i) \leq (E_j, \tau_j) \leq \cdots$$

es una cadena de elementos de $\mathfrak{S}$, el conjunto $E' := \cup_i E_i$ es un subcuerpo de F que contiene a K y, si se define $\tau' : E' \rightarrow L$ mediante $\tau'(x) := \tau_i(x)$ cuando $x \in E_i$, se obtiene que τ' es un monomorfismo que extiende a σ y (E', τ') es una cota superior de dicha cadena.

Nótese que τ' está bien definido, ya que si $x \in E_i$ y $x \in E_k$, como necesariamente se tiene $(E_i, \tau_i) \leq (E_k, \tau_k)$ o bien $(E_k, \tau_k) \leq (E_i, \tau_i)$, resulta que $\tau_k(x) = \tau_i(x)$.

Por el Lema de Zorn, existe un elemento maximal, (E, τ) , de $\mathfrak{S}$. Vamos a ver que $E = F$.

En efecto, supongamos que $E \subsetneq F$ y sea $\alpha \in F \setminus E$, que por hipótesis es algebraico sobre K (y por lo tanto sobre E). Si $f = \text{Irr}(\alpha, E)$, ya que L es algebraicamente cerrado, el polinomio $\bar{\tau}(f) \in L[X]$ tendrá un cero $\beta \in L$ y dado que $\bar{\tau}(f)$ es irreducible en $\tau(E)[X]$, ya que $\bar{\tau} : E[X] \rightarrow \tau(E)[X]$ es isomorfismo de anillos, se tiene que $\bar{\tau}(f) = \text{Irr}(\beta, \tau(E))$. Por el Teorema de extensión de extensiones simples (1.34), existe un isomorfismo $\tau_{\alpha, \beta} : E(\alpha) \rightarrow \tau(E)(\beta)$ que extiende a τ , tal que $\tau_{\alpha, \beta}(\alpha) = \beta$. El isomorfismo $\tau_{\alpha, \beta}$ también extiende a σ (ya que extiende a τ) y, llamando j a la inclusión $\tau(E)(\beta) \hookrightarrow L$, se obtiene un monomorfismo $\gamma := j \circ \tau_{\alpha, \beta} : E(\alpha) \rightarrow L$ que extiende a σ y, así, $(E, \tau) \leq (E(\alpha), \gamma)$. Por la maximalidad de (E, τ) se tiene que $E = E(\alpha)$ y resulta que $\alpha \in E$ en contradicción con la elección de α . Por lo tanto, $E = F$.

Si además $L : \sigma(K)$ es algebraica y F es algebraicamente cerrado, se obtiene una torre de cuerpos $\sigma(K) \subset \tau(F) \subset L$ en la cual todas las extensiones son algebraicas y $\tau(F)$ es también algebraicamente cerrado. Entonces, por la proposición 3.14, resulta $\tau(F) = L$ y, por tanto, τ es un isomorfismo.

En particular, si F y L son dos clausuras algebraicas de K y σ es la inclusión de K en L , se obtiene que τ es un K -isomorfismo. $\square$

Con una demostración “similar” a la del Teorema de Kronecker (3.2), pero usando un anillo de polinomios en infinitas variables sobre el cuerpo K , se prueba que:

Teorema 3.17 (Teorema de Steinitz). *Sea K un cuerpo. Entonces:*

1. *Existe una clausura algebraica $\bar{K}$ de K .*

2. Si $\overline{K}$ y $\overline{\overline{K}}$ son clausuras algebraicas de K , existe un isomorfismo $\sigma: \overline{K} \rightarrow \overline{\overline{K}}$ tal que $\sigma|_K = 1_K$, es decir, $\overline{K}$ y $\overline{\overline{K}}$ son K -isomorfas.

Demostración.

1) En primer lugar se construirá una extensión de K en la que todo polinomio de grado ≥ 1 con coeficientes en K tiene un cero.

Sea $S = \{X_f \mid f \in K[X] \text{ con } \partial(f) \geq 1\}$ y sea $K[S]$ el anillo de polinomios sobre S con coeficientes en K . En el anillo $K[S]$ el ideal

$$I := \langle \{f(X_f) \mid X_f \in S\} \rangle$$

es propio. En otro caso, se tendría que

$$\sum_{i=1}^r h_i \cdot f_i(X_{f_i}) = 1, \text{ con } h_i \in K[S].$$

Si en la expresión anterior, que involucra solo a un número finito, t , de variables X_f , se pone $X_i := X_{f_i}$ resulta que

$$\sum_{i=1}^r h_i(X_1, \dots, X_t) \cdot f_i(X_i) = 1 \quad (*).$$

Sea F una extensión finita de K en la que cada polinomio f_i tiene, al menos, un cero α_i (por ejemplo, podría tomarse como F un cuerpo de escisión sobre K del polinomio $g = f_1 \cdots f_r$).

La propiedad universal del anillo de polinomios nos permite obtener un homomorfismo de anillos $\psi: K[X_1, \dots, X_t] \rightarrow F$ tal que $\psi|_K = id_K$, $\psi(X_i) = \alpha_i$ para $i = 1, \dots, r$ y $\psi(X_j) = 0$ para cada $j = r+1, \dots, t$. Así se tendría que

$$\begin{aligned} 1 &= \psi(1) = \psi \left[\sum_{i=1}^r h_i(X_1, \dots, X_t) \cdot f_i(X_i) \right] \\ &= \sum_{i=1}^r h_i(\alpha_1, \dots, \alpha_r, \dots, 0) \cdot f_i(\alpha_i) = 0 \end{aligned}$$

lo que no es posible pues, en cualquier cuerpo, 1 y 0 son elementos diferentes.

Sea M un ideal maximal de $K[S]$ tal que $I \subset M$. Consideramos el cuerpo $K[S]/M$ y el monomorfismo $\sigma: K \rightarrow K[S]/M$ definido como la composición de la inclusión $i: K \hookrightarrow K[S]$ y el epimorfismo canónico $\pi: K[S] \rightarrow K[S]/M$.

Para todo polinomio $f \in K[X]$ de $\partial(f) \geq 1$, el polinomio $\bar{\sigma}(f)$ tiene un cero en $K[S]/M$ que es una extensión de $\sigma(K)$. Utilizando el mismo razonamiento que en el Teorema de Kronecker (3.2), se deduce que existe una extensión F_1 de K en la que todo polinomio $f \in K[X]$ de grado ≥ 1 tiene al menos un cero.

Por inducción, se puede construir una torre de cuerpos

$$K = F_0 \subset F_1 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots$$

tal que todo polinomio de grado ≥ 1 de $F_i[X]$ tiene un cero en F_{i+1} .

Si $E = \bigcup_i F_i$, entonces E es un cuerpo que admite a cada F_i como subcuerpo y si $f \in E[X]$ existe un i tal que $f \in F_i[X]$ (basta tomar el índice i suficientemente alto para que todos los coeficientes de f pertenezcan a F_i), por lo que, si $\partial(f) \geq 1$, el polinomio f tiene al menos un cero en $F_{i+1} \subset E$. Entonces el cuerpo E es algebraicamente cerrado y contiene a K como subcuerpo.

Sea ahora $\bar{K} := K^E$ la extensión algebraica maximal de K en E (ver corolario 1.28). Por construcción, $\bar{K} : K$ es una extensión algebraica y además $\bar{K}$ es algebraicamente cerrado. En efecto, si $f \in \bar{K}[X]$ es de grado ≥ 1 , el polinomio f tiene algún cero $\alpha \in E$ y entonces α es algebraico sobre $\bar{K}$.

En la torre de cuerpos $K \subset \bar{K} \subset \bar{K}(\alpha)$ todas las extensiones son algebraicas y, por tanto, α es algebraico sobre K (ver teorema 1.27), con lo que se tiene $\alpha \in \bar{K}$, por la construcción de $\bar{K}$.

2) Véase la proposición 3.16 □

Ejemplos 3.18.

1) $\mathbb{C}$ es una clausura algebraica de $\mathbb{R}$.

2) $\mathbb{C}$ no es una clausura algebraica de $\mathbb{Q}$, ya que $\mathbb{C} : \mathbb{Q}$ no es algebraica. Si $\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ es algebraico sobre } \mathbb{Q}\}$, entonces $\bar{\mathbb{Q}}$ es una clausura algebraica de $\mathbb{Q}$.

Nótese que si $f \in \mathbb{Q}[X]$, con $\partial(f) = r \geq 1$, teniendo en cuenta que $\mathbb{C}$ es algebraicamente cerrado, existen $\alpha_1, \dots, \alpha_r \in \mathbb{C}$ y $c \in \mathbb{Q}$ tales que

$$f = c(X - \alpha_1) \cdots (X - \alpha_r).$$

Por tanto, $\alpha_1, \dots, \alpha_r \in \mathbb{C}$ son algebraicos sobre $\mathbb{Q}$ y entonces $\alpha_1, \dots, \alpha_r \in \overline{\mathbb{Q}}$, es decir, f escinde en $\overline{\mathbb{Q}}[X]$.

Capítulo 4

Extensiones separables. Extensiones normales

4.1. Multiplicidad de las raíces de un polinomio

Sea $f \in K[X]$ con $\partial f \geq 1$. Si E_1 y E_2 son dos cuerpos de escisión de f sobre K , existen $\alpha_1, \dots, \alpha_r \in E_1$ y $\beta_1, \dots, \beta_t \in E_2$ tales que

$$f = c(X - \alpha_1)^{m_1} \cdots (X - \alpha_r)^{m_r}, \text{ con los } \alpha_i \text{ distintos y los } m_i \geq 1 \text{ y}$$

$$f = c(X - \beta_1)^{n_1} \cdots (X - \beta_t)^{n_t}, \text{ con los } \beta_j \text{ distintos y los } n_j \geq 1.$$

Por el corolario 3.9, sabemos que existe un K -isomorfismo $\sigma : E_1 \rightarrow E_2$. Denotando por $\bar{\sigma} : E_1[X] \rightarrow E_2[X]$ su extensión al anillo de polinomios, se tiene que

$$\begin{aligned} \bar{\sigma}(f) &= c(X - \sigma(\alpha_1))^{m_1} \cdots (X - \sigma(\alpha_r))^{m_r} \\ &= f = c(X - \beta_1)^{n_1} \cdots (X - \beta_t)^{n_t} \text{ en } E_2[X]. \end{aligned}$$

Puesto que $E_2[X]$ es un dominio de factorización única, para cada $i \in \{1, \dots, r\}$ existe $j \in \{1, \dots, t\}$ tal que $X - \sigma(\alpha_i) = X - \beta_j$ y $m_i = n_j$, por lo cual $r = t$, $\{\sigma(\alpha_1), \dots, \sigma(\alpha_r)\} = \{\beta_1, \dots, \beta_r\}$ y, salvo una permutación de índices γ , se verifica que $\beta_{\gamma(i)} = \sigma(\alpha_i)$ y $n_{\gamma(i)} = m_i$, para todo $i = 1, \dots, r$.

Definición 4.1. Sea $f \in K[X]$ con $\partial f \geq 1$ y sea E_f un cuerpo de escisión de f sobre K . Existen elementos distintos $\alpha_1, \dots, \alpha_r \in E_f$ tales que

$$f = c(X - \alpha_1)^{m_1} \cdots (X - \alpha_r)^{m_r}, \text{ con } m_i \geq 1.$$

Diremos que α_i es una raíz de f de *multiplicidad* m_i en E_f . Si $m_i > 1$ diremos que α_i es una *raíz múltiple* de f en E_f , en otro caso se dirá que es una *raíz simple*.

Como consecuencia de lo anterior, aunque las raíces de un polinomio f dependen del cuerpo de escisión en que éstas se consideren, el número de raíces distintas y los exponentes asociados a ellas, a los que hemos llamado multiplicidades, están determinados por f , es decir, no dependen del cuerpo de escisión en que se consideren. En particular, si en un cuerpo de escisión f tiene todas las raíces simples, también son simples todas sus raíces en cualquier otro cuerpo de escisión.

Vamos a estudiar un criterio para determinar cuando una raíz es múltiple y para ello vamos a utilizar el concepto de derivada.

Sea K un cuerpo y sea $a \in K$. Recordemos que para todo entero n se define na como sigue:

$$\begin{aligned} \text{Si } n > 0: \quad na &:= \underbrace{a + \cdots + a}_{n \text{ sumandos}}; \\ \text{si } n < 0: \quad na &:= -((-n)a) = -\underbrace{(a + \cdots + a)}_{-n \text{ sumandos}} \text{ y} \\ \text{si } n = 0: \quad 0a &:= 0. \end{aligned}$$

Definición 4.2. Si $f = \sum_{i=0}^n a_i X^i \in K[X]$, llamaremos *derivada (formal)* del polinomio f al polinomio $f' = \sum_{i=1}^n i a_i X^{i-1} \in K[X]$.

Es una definición puramente algebraica para polinomios con coeficientes en cualquier cuerpo y se corresponde con la fórmula de la derivada de un polinomio con coeficientes reales dada en cálculo.

Es fácil comprobar que:

Lema 4.3. Si $f, g \in K[X]$ y $a \in K$, se verifica:

- a) $(f + g)' = f' + g'$.
- b) $(f \cdot g)' = f' \cdot g + f \cdot g'$.
- c) $(a \cdot f)' = a \cdot f'$.

Proposición 4.4. Sean $f \in K[X]$ con $\partial f \geq 1$, E_f un cuerpo de escisión para f sobre K y $\alpha \in E_f$. Las siguientes condiciones son equivalentes:

1. α es una raíz múltiple de f .
2. $(X - \alpha)^2$ divide a f en $E_f[X]$.
3. $f(\alpha) = 0 = f'(\alpha)$.

Demostración.

2) $\Rightarrow$ 3) $(X - \alpha)^2$ divide a f en $E_f[X]$ si, y solo si, existe $h \in E_f[X]$ tal que $f = (X - \alpha)^2 h$ y, en consecuencia, $f(\alpha) = 0$. Como $f' = (X - \alpha)^2 h' + 2(X - \alpha)h$, se concluye que $f'(\alpha) = 0$.

3) $\Rightarrow$ 2) Puesto que $f(\alpha) = 0$, por el Teorema del factor, $(X - \alpha)$ divide a f en $E_f[X]$, es decir, existe $h \in E_f[X]$ tal que $f = (X - \alpha)h$. Por tanto, $f' = (X - \alpha)h' + h$. Teniendo en cuenta que $f'(\alpha) = 0$, se tiene que $h(\alpha) = 0$, o equivalentemente, que $(X - \alpha)$ divide a h en $E_f[X]$, es decir, existe $g \in E_f[X]$ tal que $h = (X - \alpha)g$. Así, $f = (X - \alpha)h = (X - \alpha)^2 g$, por lo cual $(X - \alpha)^2$ divide a f en $E_f[X]$. $\square$

Nótese que las condiciones anteriores son equivalentes a que el polinomio $\text{Irr}(\alpha, K)$ divide a (f, f') en $K[X]$.

Ejemplo 4.5.

Para cada $n \geq 1$, las raíces de $f = X^n - 1$ en $\mathbb{C}$ son todas simples.

En efecto, teniendo en cuenta que $f' = nX^{n-1}$ y que cada raíz, α , de f es no nula, se tiene que $f'(\alpha) = n\alpha^{n-1} \neq 0$.

Proposición 4.6. Sean $f \in K[X]$ irreducible, E_f un cuerpo de escisión para f sobre K y $\alpha \in E_f$ una raíz de f . Son equivalentes:

1. α es una raíz múltiple de f en E_f .
2. $f' = 0$.

Demostración.

1) $\Rightarrow$ 2) Por la proposición 4.4, $f'(\alpha) = 0$ y así $\text{Irr}(\alpha, K)$ divide a f' . Como $\partial f > \partial f'$, necesariamente $f' = 0$.

2) $\Rightarrow$ 1) Teniendo en cuenta que $f' = 0$ se obtiene que $f'(\alpha) = 0$ y, aplicando la proposición 4.4, se llega al resultado. $\square$

4.2. Extensiones separables

Recordemos que si K es un cuerpo la aplicación

$$\begin{aligned} \varphi: \mathbb{Z} &\rightarrow K \\ n &\mapsto n1_K \end{aligned}$$

es un homomorfismo de anillos. Dado que $\mathbb{Z}/\text{Ker } \varphi \simeq \text{Im } \varphi$ que es un subanillo de K , se tiene que $\mathbb{Z}/\text{Ker } \varphi$ es un dominio entero y, por tanto, $\text{Ker } \varphi$ es un ideal primo de $\mathbb{Z}$. Hay dos posibilidades:

i) Si $\text{Ker } \varphi = \langle 0 \rangle$, se dice que K es de característica cero y se denota por $\text{Car } K = 0$. En este caso, K es infinito porque contiene un subanillo isomorfo a $\mathbb{Z}$.

ii) Si $\text{Ker } \varphi = \langle p \rangle = p\mathbb{Z}$ (p primo), se dice que K es de característica p y se denota por $\text{Car } K = p$.

Si $\text{Car } K = p$, se verifica que p es el menor entero positivo tal que $p1_K = 0$ y el subcuerpo minimal de K , es decir la intersección de todos sus subcuerpos, llamado subcuerpo *primo*, es $\mathbb{F}_p = \{0_K, 1_K, 21_K, \dots, (p-1)1_K\}$. En efecto, factorizando φ se tiene que $\mathbb{Z}/p\mathbb{Z} \simeq \text{Im } \varphi = \mathbb{F}_p \subset K$ y, puesto que $\mathbb{Z}$ es un dominio de ideales principales y p es un primo, $\mathbb{F}_p$ es cuerpo.

Nótese que la aplicación $\sigma: \mathbb{Z}_p \rightarrow \mathbb{F}_p$, definida por $\bar{n} \mapsto n1_K$, es un isomorfismo.

Definición 4.7. Un polinomio $f \in K[X]$ con $\partial f \geq 1$ se dice *separable sobre K* si sus raíces, en un cuerpo de escisión para f sobre K , son todas simples.

Proposición 4.8. Sea $f \in K[X]$ un polinomio irreducible.

1. Si $\text{Car } K = 0$, entonces f es separable sobre K .

2. Si $\text{Car } K = p > 0$, entonces f es separable sobre K salvo que sea de la forma $f = b_0 + b_1X^p + b_2X^{2p} + \dots + b_mX^{mp}$, es decir, $f = g(X^p)$ para algún $g \in K[X]$.

Demostración. Sea $f = a_0 + a_1X + \dots + a_nX^n \in K[X]$, con $\partial f = n \geq 1$. Entonces, $f' = a_1 + 2a_2X + \dots + na_nX^{n-1}$. Por la proposición 4.6, f es separable si, y solo si, $f' \neq 0$.

1) Si $\text{Car } K = 0$, como $na_n = (n1_K)a_n \neq 0$, $\partial f' = n - 1 \geq 0$ y, por tanto, $f' \neq 0$.

2) Supongamos ahora que $\text{Car } K = p$. Entonces, $f' = 0$ si, y solo si, p divide a i para cada i tal que $a_i \neq 0$. Así, los únicos términos no cero en f son de la forma $a_{rp}X^{rp}$ para $r \geq 0$. Escribiendo a_{rp} como b_r se tiene el resultado buscado. $\square$

Definición 4.9. Sea $F: K$ una extensión de cuerpos.

1) Un elemento $\alpha \in F$ se dice *separable sobre K* si es algebraico sobre K y el polinomio $\text{Irr}(\alpha, K)$ es separable sobre K .

2) Se dirá que la extensión $F: K$ es *separable* si cada elemento de F es separable sobre K .

En particular, toda extensión separable es algebraica.

Observación 4.10. Si $K \subset F \subset E$ es una torre de cuerpos y $\alpha \in E$ es separable sobre K , también lo es sobre F . Esto es consecuencia de que $\text{Irr}(\alpha, F)$ divide a $g = \text{Irr}(\alpha, K)$ en $F[X]$ y, por tanto, también en el anillo $F_g[X]$, para cualquier F_g cuerpo de escisión de g sobre F .

Corolario 4.11. *Sea K un cuerpo de característica cero. Toda extensión algebraica, $F : K$, es separable.*

4.3. Cuerpos finitos

Los cuerpos finitos juegan un papel importante en muchas áreas de las matemáticas tales como: teoría de números, teoría de grupos, criptografía, geometría proyectiva, etc.

Para cada primo p , $\mathbb{Z}_p$ es un cuerpo de p elementos. En esta sección veremos que hay otros cuerpos finitos, daremos una clasificación de ellos y probaremos que están determinados salvo isomorfismos por su orden que debe ser una potencia de su característica.

Proposición 4.12. *Si K un cuerpo finito, entonces $|K| = p^n$ para algún primo p y algún entero $n \geq 1$.*

Demostración. Si K es un cuerpo finito, como ya hemos señalado, su característica es un número primo p . Entonces, K es una extensión finita de $\mathbb{F}_p$ y, si suponemos que $[K : \mathbb{F}_p] = n$, K es un $\mathbb{F}_p$ -espacio vectorial de dimensión n y, así, $|K| = p^n$. $\square$

Lema 4.13. *Sea K es un cuerpo de característica p . La aplicación*

$$\begin{aligned} \phi: K &\rightarrow K \\ a &\mapsto a^p \end{aligned}$$

es un monomorfismo y cuando K es finito es un automorfismo, llamado automorfismo de Frobenius de K .

Demostración. Por el Teorema del binomio sabemos que

$$(a + b)^p = \sum_{j=0}^p \binom{p}{j} a^j b^{p-j},$$

donde $\binom{p}{0} = \binom{p}{p} = 1$ y, para cada $j = 1, \dots, p-1$, por el Teorema Fundamental de la Aritmética, se tiene que p divide a $\binom{p}{j} = \frac{p(p-1)\dots(p-j+1)}{j!}$ y, como $\text{Car } K = p$, se verifica que $\binom{p}{j} a^j b^{p-j} = 0$. Por tanto, $(a+b)^p = a^p + b^p$ para todo $a, b \in K$.

Por la conmutatividad de K , $(ab)^p = a^p b^p$. Además, $\phi(1) = 1$.

Si K es finito, este monomorfismo es un automorfismo de K , puesto que una aplicación inyectiva de un conjunto finito en si mismo es biyectiva. $\square$

Nótese que $(a-b)^p = (a+(-b))^p = a^p + (-b)^p = a^p + (-1)^p b^p = a^p - b^p$ ya que si $p = 2$, entonces $(-1)^p = 1 = -1$ y, si p es impar, entonces $(-1)^p = -1$.

A continuación vamos a dar un resultado que clasifica todos los cuerpos finitos.

Teorema 4.14.

1. Sea K un cuerpo finito. Entonces $|K| = p^n$ para algún primo p y algún entero $n \geq 1$. Cada elemento de K es una raíz del polinomio $f = X^{p^n} - X$ y K es un cuerpo de escisión para este polinomio sobre su subcuerpo primo $\mathbb{F}_p$.

2. Sea p un primo y $n \geq 1$ un entero. Existe, salvo isomorfismo, exactamente un cuerpo de p^n elementos.

Demostración.

1) Ya hemos visto que si $\text{Car } K = p$, $\mathbb{F}_p$ es el subcuerpo primo de K y existe un entero $n \geq 1$ tal que $|K| = p^n$.

El grupo multiplicativo K^* tiene orden $p^n - 1$. Para todo $\alpha \in K^*$, por el Teorema de Lagrange, el orden de α , que es el orden del subgrupo, $\langle \alpha \rangle$, generado por α , divide a $p^n - 1$, por tanto $\alpha^{p^n-1} = 1$ y, en consecuencia, $\alpha^{p^n} - \alpha = 0$.

Como también $0^{p^n} - 0 = 0$, concluimos que cada elemento de K es raíz del polinomio $f = X^{p^n} - X$.

Además, por el Teorema del factor, $X - \alpha$ es un factor de f para cada uno de los p^n elementos α de K y, puesto que K es un dominio entero, el polinomio $\prod_{\alpha \in K} (X - \alpha)$ divide a f y, teniendo en cuenta que ambos polinomios tienen el mismo grado y son mónicos, se obtiene que $f = \prod_{\alpha \in K} (X - \alpha)$. Por tanto, f escinde en K y claramente K es un cuerpo de escisión para f sobre $\mathbb{F}_p$.

2) Sean p un primo y $n \geq 1$ un entero. Sea E' un cuerpo de escisión del polinomio $f = X^{p^n} - X$ sobre $\mathbb{Z}_p$. Puesto que el cuerpo es de característica p ,

$$f' = p^n X^{p^n-1} - 1 = -1$$

y, en consecuencia, como f' no tiene raíces, todas las raíces de f en E' son simples.

Sea $K = \{\alpha \in E' \mid \alpha \text{ es raíz de } f\}$. Se tiene que:

- i) K tiene p^n elementos.
- ii) K es un subcuerpo de E' :

Es claro que $0, 1 \in K$.

Si suponemos que $a, b \in K$, aplicando reiteradamente el lema 4.13, se deduce que:

$$(a - b)^{p^n} = a^{p^n} - b^{p^n} = a - b \text{ y, si } b \neq 0, (ab^{-1})^{p^n} = a^{p^n} (b^{p^n})^{-1} = ab^{-1}.$$

Por lo cual, $a - b \in K$ y, si $b \neq 0$, $ab^{-1} \in K$.

Entonces, $E' = \mathbb{Z}_p(\{\alpha \in E' \mid \alpha \text{ es raíz de } f\}) = \mathbb{Z}_p(K)$ y, dado que $\mathbb{Z}_p \subset K$, se tiene que $E' = K$ y es un cuerpo con p^n elementos.

Hemos visto que, si p es un primo y $n \geq 1$ un entero, existe un cuerpo, E' , de orden p^n , el cuerpo de escisión del polinomio $f = X^{p^n} - X$ sobre $\mathbb{Z}_p$. También hemos visto que cualquier cuerpo, E , de orden p^n es el cuerpo de escisión de $X^{p^n} - X$ sobre su cuerpo primo $\mathbb{F}_p$ y, aplicando el teorema 3.8 al isomorfismo $\sigma : \mathbb{Z}_p \rightarrow \mathbb{F}_p$, definido por $\sigma(\bar{n}) = n1_K$, y a los polinomios $X^{p^n} - X \in \mathbb{Z}_p[X]$ y $\bar{\sigma}(X^{p^n} - X) = X^{p^n} - X \in \mathbb{F}_p[X]$, se sigue que tales cuerpos E' y E son isomorfos. $\square$

El siguiente resultado es un teorema conocido de teoría de grupos que se puede demostrar utilizando, por ejemplo, el Teorema de estructura de grupos abelianos finitos o los Teoremas de Sylow. (Véase: Stewart I., Galois theory, Chapman and Hall Mathematics, 1989.)

Teorema 4.15. *Todo subgrupo finito del grupo multiplicativo de un cuerpo es cíclico.*

Proposición 4.16. *Sean E un cuerpo finito con p^n elementos y $\mathbb{F}_p$ su cuerpo primo.*

1. *Existe $\alpha \in E$ separable sobre $\mathbb{F}_p$ tal que $E = \mathbb{F}_p(\alpha)$.*
2. *El grupo G de los $\mathbb{F}_p$ -automorfismos de E es cíclico de orden n .*

Demostración.

1) Por el teorema anterior, sabemos que existe $\alpha \in E$ con $E^* = \langle \alpha \rangle$. Como para cada $u \in E$, $u \neq 0$, existe $k \in \mathbb{N}$ tal que $u = \alpha^k$, se verifica que $E = \mathbb{F}_p(\alpha)$.

$\alpha \in E$ es un cero del polinomio $X^{p^n} - X \in \mathbb{F}_p[X]$ que, como hemos visto, no tiene raíces múltiples. Puesto que $\text{Irr}(\alpha, \mathbb{F}_p)$ divide a $X^{p^n} - X$ en $\mathbb{F}_p[X]$ se deduce que $\text{Irr}(\alpha, \mathbb{F}_p)$ es separable y, así, α es separable sobre $\mathbb{F}_p$.

2) Sea $\alpha \in E$ separable sobre $\mathbb{F}_p$ tal que $E = \mathbb{F}_p(\alpha)$. Si $\sigma \in G$, σ está determinado por su valor en α y $\sigma(\alpha) \in E$ es un cero de $\text{Irr}(\alpha, \mathbb{F}_p)$. Puesto que $\partial(\text{Irr}(\alpha, \mathbb{F}_p)) = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n$ e $\text{Irr}(\alpha, \mathbb{F}_p)$ es separable, el polinomio $\text{Irr}(\alpha, \mathbb{F}_p)$ tiene n ceros distintos en E . Aplicando el corolario 3.10, se sigue que $|G| = n$.

Sea $\phi : E \rightarrow E$ el automorfismo de Frobenius. Probaremos que $G = \langle \phi \rangle$.

Puesto que $\phi(1) = 1$, ϕ deja fijo $\mathbb{F}_p$ y, por tanto, ϕ es un elemento de G . Ahora probaremos que G es cíclico demostrando que ϕ tiene orden n :

$\phi^n = 1$ ya que para todo $u \in E$, $\phi^n(u) = u^{p^n} = u$, puesto que u es un cero del polinomio $X^{p^n} - X \in \mathbb{F}_p[X]$.

Si d es un entero tal que $\phi^d = 1$, entonces los p^n elementos de E son ceros del polinomio $X^{p^d} - X \in \mathbb{F}_p[X]$ y, como el número de ceros de un polinomio con coeficientes en un cuerpo no puede exceder a su grado, se tiene que $p^d \geq p^n$ y así $d \geq n$. $\square$

4.4. Teorema del elemento primitivo

Teorema 4.17. *Toda extensión finita y separable, $F : K$, es simple, es decir, existe $\alpha \in F$ tal que $F = K(\alpha)$. Tal elemento $\alpha \in F$ se llama elemento primitivo de la extensión $F : K$.*

Demostración. En primer lugar, supongamos que K es un cuerpo finito con $\text{Car } K = p$.

Si $F : K$ es finita, es evidente que F también es un cuerpo finito con el mismo cuerpo primo que K y, por la proposición anterior, existe $\alpha \in F$ separable sobre $\mathbb{F}_p$ y, por tanto, sobre K de modo que $F = \mathbb{F}_p(\alpha) = K(\alpha)$.

Supongamos ahora que K es un cuerpo infinito.

Si $F : K$ es finita, existen $\delta_1, \dots, \delta_s \in F$ algebraicos sobre K tales que $F = K(\delta_1, \dots, \delta_s)$. Puesto que

$$K(\delta_1) \subset K(\delta_1, \delta_2) \subset \dots \subset K(\delta_1, \dots, \delta_s) = F$$

bastará hacer la prueba en el caso $s = 2$. Supongamos pues que $F = K(\alpha, \beta)$.

Sean $f = \text{Irr}(\alpha, K)$, $g \in \text{Irr}(\beta, K)$ y $E = E_{fg}$ un cuerpo de escisión para fg sobre K . Puesto f y g son separables sobre K todas sus raíces en E son simples.

Sean $\alpha = \alpha_1, \dots, \alpha_n$ las raíces de f y $\beta = \beta_1, \dots, \beta_m$ las raíces de g , en E .

Como K es un cuerpo infinito, podemos escoger un elemento $c \in K$ tal que

$$c \neq \frac{\alpha - \alpha_i}{\beta_j - \beta} \Leftrightarrow \alpha + c\beta \neq \alpha_i + c\beta_j, \quad \forall i : 1, \dots, n \text{ y } \forall j : 2, \dots, m.$$

Tomamos $\gamma := \alpha + c\beta \in K(\alpha, \beta)$.

Es claro que $K \subset K(\gamma) \subset K(\alpha, \beta)$.

Ahora vamos a probar que $K(\alpha, \beta) \subset K(\gamma)$.

Consideremos el único homomorfismo de anillos

$$\varphi_{\gamma - cX} : K[X] \rightarrow K(\gamma)[X]$$

tal que $\varphi_{\gamma - cX}|_K = 1_K$ y $\varphi_{\gamma - cX}(X) = \gamma - cX$.

El polinomio $h := \varphi_{\gamma - cX}(f) = f(\gamma - cX) \in K(\gamma)[X]$ verifica que:

i) $h(\beta) = f(\gamma - c\beta) = f(\alpha) = 0$.

ii) Para todo $j : 2, \dots, m$, $h(\beta_j) = f(\gamma - c\beta_j) \neq 0$, ya que por la elección de c se tiene que $\gamma - c\beta_j \neq \alpha_i$, para todo $i = 1, \dots, n$.

Así, β es la única raíz en común de g y h en E y, por tanto, el máximo común divisor de g y h en $E[X]$ es $X - \beta$. Como ambos polinomios, g y h , están en $K(\gamma)[X]$, por la unicidad del cociente y el resto, al aplicar el algoritmo de Euclides extendido, se tiene que $X - \beta \in K(\gamma)[X]$, por lo cual $\beta \in K(\gamma)$. También $\alpha = \gamma - c\beta \in K(\gamma)$ y así $K(\gamma) = K(\alpha, \beta)$. $\square$

Corolario 4.18. Si K es un cuerpo con $\text{Car } K = 0$, toda extensión finita, $F : K$, es simple.

4.5. Extensiones normales

Definición 4.19. Una extensión $E : K$ se dice *normal* si:

- i) $E : K$ es algebraica.
- ii) Todo polinomio irreducible $f \in K[X]$ que tiene un cero en E , tiene todos sus ceros en E , es decir, escinde en E .

También se dice que E es *normal sobre* K .

Ejemplos 4.20.

1) Si $\bar{K}$ es una clausura algebraica de K , $\bar{K} : K$ es una extensión normal; en particular, $\mathbb{C} : \mathbb{R}$ es normal.

2) Si $[E : K] = 2$, entonces la extensión $E : K$ es normal.

$E : K$ es algebraica ya que es finita.

Sea f un polinomio irreducible en $K[X]$ que tiene un cero α en E , veamos que f escinde en E .

α es algebraico sobre K y $[K(\alpha) : K] = \partial \text{Irr}(\alpha, K) = \partial f$.

Como $K \subset K(\alpha) \subset E$, se tiene que $[K(\alpha) : K] \leq [E : K] = 2$. Por ello, $\partial f = 1$ o 2 .

Si $\partial f = 1$: f escinde en K .

Si $\partial f = 2$: Por el Teorema del factor, $X - \alpha$ divide a f en $E[X]$, es decir, existe $g \in E[X]$ con $f = (X - \alpha)g$ y, como $\partial f = 2$, se tiene que $\partial g = 1$ y f escinde en E .

3) $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ no es normal.

Ya que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \partial(X^3 - 2) = 3$, se tiene que $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ es algebraica.

Si $f = \text{Irr}(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$, $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ es cero de f . Sin embargo, f no escinde en $\mathbb{Q}(\sqrt[3]{2})$, pues f tiene ceros no reales en $\mathbb{C}$: $\sqrt[3]{2}\varepsilon$ y $\sqrt[3]{2}\varepsilon^2$, con $\varepsilon = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.

Teorema 4.21. Sea $E : K$ una extensión. Son equivalentes:

1. $E : K$ es finita y normal.
2. E es cuerpo de escisión sobre K de algún polinomio $f \in K[X]$.

Demostración.

1) $\Rightarrow$ 2) Dado que $E : K$ es finita, existen $\alpha_1, \dots, \alpha_n \in E$ algebraicos sobre K tales que $E = K(\alpha_1, \dots, \alpha_n)$.

Sea $f_i = \text{Irr}(\alpha_i, K)$ para $i : 1, \dots, n$. Como f_i tiene un cero $\alpha_i \in E$ y $E : K$ es una extensión normal, f_i escinde en E .

Por tanto, $f = f_1 \cdots f_n \in K[X]$ escinde en E y dado que

$$\{\alpha_1, \dots, \alpha_n\} \subset \{\text{ceros de } f \text{ en } E\},$$

$E = K(\alpha_1, \dots, \alpha_n)$ es un cuerpo de escisión para f sobre K .

2) $\Rightarrow$ 1) Supongamos que E es un cuerpo de escisión sobre K del polinomio f y que

$$f = c(X - \beta_1) \cdots (X - \beta_r), \text{ con } c \in K, \beta_i \in E \text{ y } E = K(\beta_1, \dots, \beta_r).$$

La extensión $E : K$ es finita por estar finitamente generada por elementos algebraicos.

Sea g un polinomio irreducible en $K[X]$ con una raíz, α , en E . Debemos comprobar que g escinde en E .

Supongamos que β es cualquier cero de g en $\overline{E}$ y consideremos el siguiente diagrama:

$$\begin{array}{ccc}
 & \overline{E} & \\
 & \nearrow & \nwarrow \\
 E & & E(\beta) \\
 \uparrow & & \uparrow \\
 K(\alpha) & & K(\beta) \\
 & \nwarrow & \nearrow \\
 & K &
 \end{array}$$

Puesto que α y β tienen el mismo polinomio irreducible sobre K , por el teorema 1.34, existe un K -isomorfismo $\tau : K(\alpha) \rightarrow K(\beta)$ y, en consecuencia, $[K(\alpha) : K] = [K(\beta) : K]$.

Ya que E es un cuerpo de escisión para f sobre K , se sigue que $E(\alpha) = E$ es un cuerpo de escisión para f sobre $K(\alpha)$ y $E(\beta)$ es un cuerpo de escisión para f sobre $K(\beta)$. Por el Teorema de extensión para cuerpos de escisión (3.8), existe un isomorfismo $\tau^* : E \rightarrow E(\beta)$ que extiende τ y así, $[E : K(\alpha)] = [E(\beta) : K(\beta)]$.

Utilizando el Teorema del grado (1.6), se obtiene que

$$[E : K] = [E : K(\alpha)][K(\alpha) : K] = [E(\beta) : K(\beta)][K(\beta) : K] = [E(\beta) : K].$$

Como $K \subset E \subset E(\beta)$, se deduce que $[E(\beta) : E] = 1$ y, por tanto, $\beta \in E$. □

Ejemplos 4.22.

1) Consideremos la torre de cuerpos $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$, con $\varepsilon = e^{\frac{2\pi}{3}i}$.

$\mathbb{Q}(\sqrt[3]{2}, \varepsilon) : \mathbb{Q}$ es normal ya que $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ es cuerpo de escisión del polinomio $X^3 - 2$ sobre $\mathbb{Q}$ y, sin embargo, como ya hemos visto, $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ no es normal.

2) Sea la torre de cuerpos $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

$\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ es normal puesto que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Como $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = \frac{[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]} = \frac{4}{2} = 2$, también $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})$ es normal.

Sin embargo, $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$ no es normal ya que $f = X^4 - 2$ es un polinomio irreducible en $\mathbb{Q}[X]$, que tiene un cero $\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$ pero que no escinde en $\mathbb{Q}(\sqrt[4]{2})$.

3) En general, si $E : K$ es una extensión normal y finita y $K \subset F \subset E$, se tiene que $E : F$ es normal y finita.

Proposición 4.23. *Sea $E : K$ una extensión normal y finita y F un cuerpo intermedio.*

Son equivalentes:

1. $F : K$ es normal.
2. $\tau(F) \subset F$ para todo τ K -automorfismos de E .

Demostración.

1) $\Rightarrow$ 2) Sea τ un K -automorfismos de E . Si $\alpha \in F$, como $E : K$ es finita, α es algebraico sobre K . Como el polinomio $\text{Irr}(\alpha, K)$ tiene un cero en F , α , por la proposición 1.32, sabemos que $\tau(\alpha) \in E$ también es cero de $\text{Irr}(\alpha, K)$. Teniendo en cuenta que $F : K$ es normal, se deduce que $\tau(\alpha) \in F$.

2) $\Rightarrow$ 1) Como $E : K$ es normal y finita, por el teorema 4.21, E es cuerpo de escisión de algún $g \in K[X]$.

Sea $f \in K[X]$ un polinomio irreducible que tiene un cero α en F . Sea $\beta \in E$ un cero de f (como $E : K$ es normal todos los ceros de f están en E). Entonces α y β tienen el mismo polinomio irreducible sobre K , por el corolario 3.10, existe un K -isomorfismo $\tau : E \rightarrow E$ tal que $\tau(\alpha) = \beta$ y, como por hipótesis $\tau(F) \subset F$, se tiene que $\tau(\alpha) = \beta \in F$. $\square$

Concluimos esta sección comprobando que si $L : K$ es una extensión finita de cuerpos, existe una menor extensión normal y finita de K que contiene a L .

Teorema 4.24. *Sea $L : K$ una extensión finita de cuerpos. Existe una extensión $F : L$ que verifica:*

1. $F : K$ es una extensión normal y finita.
 2. Si $F' : K$ es una extensión normal y $K \subset L \subset F' \subset F$, entonces $F' = F$.
- El cuerpo F es único salvo isomorfismos y se llama clausura normal de L sobre K .*

Demostración. Por ser $L : K$ una extensión finita existen $\alpha_1, \dots, \alpha_n \in L$ algebraicos sobre K tales que $L = K(\alpha_1, \dots, \alpha_n)$.

Sea $f = \text{Irr}(\alpha_1, K) \cdots \text{Irr}(\alpha_n, K) \in K[X]$. Si F es un cuerpo de escisión para f sobre K , por la proposición 4.21, la extensión $F : K$ es normal y finita.

Teniendo en cuenta que $f(\alpha_i) = 0$, para $i : 1, \dots, n$, se tiene que $\alpha_i \in F$ y en consecuencia $L = K(\alpha_1, \dots, \alpha_n) \subset F$.

Supongamos ahora que $F' : K$ es una extensión normal verificando que $K \subset L \subset F' \subset F$.

Dado que $L = K(\alpha_1, \dots, \alpha_n) \subset F'$, como $\text{Irr}(\alpha_i, K)$ tiene una raíz, α_i , en F' y $F' : K$ es normal, se tiene que $\text{Irr}(\alpha_i, K)$ escinde en F' . Por tanto, f escinde en F' y $F \subset F'$.

Por último, sea E una extensión de L que verifica las hipótesis del teorema.

El polinomio f escinde en E y, por tanto, existe un cuerpo de escisión, E' , para f sobre K tal que $K \subset L \subset E' \subset E$. Por la proposición 4.21, $E' : K$ es una extensión

normal y finita y, aplicando la hipótesis 2), se tiene que $E' = E$. Al ser E un cuerpo de escisión para f sobre K , por el corolario 3.9, se obtiene que E y F son K -isomorfos. $\square$

Capítulo 5

Teoría de Galois

5.1. Extensiones de Galois

En este tema se consideran cuerpos de característica cero y, por tanto, toda extensión finita es separable.

Definición 5.1. Sea E un cuerpo y G un subgrupo del grupo de automorfismos de E , $\text{Aut}(E)$. El conjunto

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

es un subcuerpo de E , que se llama *cuerpo fijo de E por G* .

Definición 5.2. Sea la extensión $E : K$. El grupo de Galois de E sobre K , denotado $\text{Gal}(E/K)$, es el subgrupo de $\text{Aut}(E)$ definido por:

$$\text{Gal}(E/K) := \{\sigma \in \text{Aut}(E) \mid \sigma|_K = \text{id}_K\}.$$

Lema 5.3. Si $E = K(\alpha)$ con α algebraico sobre K y $\sigma \in \text{Gal}(E/K)$, σ está determinado por su valor en α y $\sigma(\alpha) \in E$ es cero del polinomio $\text{Irr}(\alpha, K)$.

Demostración. Si $\partial \text{Irr}(\alpha, K) = n$, como $\{1, \alpha, \dots, \alpha^{n-1}\}$ es una K -base de $E = K(\alpha)$, cada elemento $z \in K(\alpha)$ admite una única expresión como

$$z = a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}, \quad \text{con } a_i \in K$$

y, por tanto,

$$\sigma(z) = a_0 + a_1\sigma(\alpha) + \cdots + a_{n-1}\sigma(\alpha)^{n-1}.$$

Además, por la proposición 1.32, sabemos que $\sigma(\alpha) \in E$ es un cero del polinomio $\overline{id_K}(\text{Irr}(\alpha, K)) = \text{Irr}(\alpha, K)$. $\square$

Proposición 5.4. *Si $E : K$ es una extensión finita, entonces*

$$|\text{Gal}(E/K)| \leq [E : K].$$

Demostración. Como $E : K$ es una extensión finita, por el Teorema del elemento primitivo (4.17), existe $\alpha \in E$ tal que $E = K(\alpha)$. Por el lema anterior,

$$|\text{Gal}(E/K)| = |\text{Gal}(K(\alpha)/K)| \leq \partial \text{Irr}(\alpha, K) = [K(\alpha) : K] = [E : K]. \quad \square$$

Proposición 5.5. *Sea $E : K$ una extensión normal y finita.*

1. Sean $\alpha, \beta \in E$. Se verifica que:

$$\text{Irr}(\alpha, K) = \text{Irr}(\beta, K) \text{ si, y solo si, existe } \sigma \in \text{Gal}(E/K) \text{ tal que } \sigma(\alpha) = \beta.$$

2. $|\text{Gal}(E/K)| = [E : K]$.

Demostración.

1) Se sigue de los corolarios 3.10 y 1.33.

2) Por la proposición anterior, $|\text{Gal}(E/K)| \leq [E : K] = n$.

Por el Teorema del elemento primitivo (4.17), existe un $\alpha \in E$ tal que $E = K(\alpha)$.

Si $f = \text{Irr}(\alpha, K)$, se tiene que:

a) $\partial f = [K(\alpha) : K] = [E : K] = n$.

b) f es separable sobre K , puesto que es irreducible y $\text{Car } K = 0$.

c) f escinde en E ya que es irreducible sobre K , tiene un cero, α , en E y $E : K$ es normal y finita.

Sean $\alpha = \alpha_1, \dots, \alpha_n$ los n ceros de f en E . Para cada $i : 1, \dots, n$, $f = \text{Irr}(\alpha_i, K)$ y, por 1), existe $\sigma_i \in \text{Gal}(E/K)$ tal que $\sigma_i(\alpha) = \alpha_i$. En consecuencia, $|\text{Gal}(E/K)| \geq n$.

Nótese que $\text{Gal}(E/K) = \{\sigma_i \in \text{Aut}(E) \mid \sigma_i(\alpha) = \alpha_i \text{ y } \sigma_i|_K = id_K, \forall i : 1, \dots, n\}$.

$\square$

Ejemplos 5.6.

1) $\text{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}_2$:

Ya que $[\mathbb{C} : \mathbb{R}] = 2$, la extensión $\mathbb{C} : \mathbb{R}$ es normal y finita.

Por la proposición 5.5, $|\text{Gal}(\mathbb{C}/\mathbb{R})| = 2$ y entonces $\text{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}_2$. Como $\mathbb{C} = \mathbb{R}(i)$ e $\text{Irr}(i, \mathbb{R}) = X^2 + 1 = (X + i)(X - i)$, utilizando de nuevo la proposición 5.5, se tiene que $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{\sigma_1, \sigma_2\}$, donde σ_1 es la identidad y σ_2 es la conjugación.

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

Teniendo en cuenta que $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ no es una extensión normal, utilizando las proposiciones 5.4 y 5.5, se deduce que $|\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| < 3$.

Como $\text{Irr}(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$ tiene un único cero en $\mathbb{Q}(\sqrt[3]{2})$, del lema 5.3, se sigue que $|\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$.

Nota 5.7. Recordemos algunos resultados de grupos que serán utilizados en lo que sigue.

Si $E : K$ es una extensión finita y H es un subgrupo de $\text{Gal}(E/K)$, entonces E es un H -conjunto con la acción definida por:

$$\begin{aligned} H \times E &\rightarrow E \\ (\sigma, \alpha) &\mapsto \sigma(\alpha). \end{aligned}$$

Si $\alpha \in E$, se define la órbita y el estabilizador (o subgrupo de isotropía) de α como sigue:

$$\text{Órbita de } \alpha := \{\sigma(\alpha) \mid \sigma \in H\} \equiv H\alpha.$$

$$\text{Estabilizador de } \alpha := \{\sigma \in H \mid \sigma(\alpha) = \alpha\} \equiv H_\alpha.$$

Es conocido que $|H\alpha| = (H : H_\alpha)$ y, por el Teorema de Lagrange, es un divisor de $|H|$.

Lema 5.8. Si $E : K$ es una extensión finita y H es un subgrupo de $\text{Gal}(E/K)$, entonces:

a) $E : E^H$ es una extensión finita.

b) Si $\alpha \in E$ se tiene que $\text{Irr}(\alpha, E^H) = \prod_{\sigma(\alpha) \in H\alpha} (X - \sigma(\alpha))$.

Demostración.

a) Como $K \subset E^H \subset E$ y la extensión $E : K$ es finita, por el Teorema del grado (1.6), se deduce que $E : E^H$ también es finita.

b) Si $\alpha \in E$, por el apartado a), α es algebraico sobre E^H . Si $f = \text{Irr}(\alpha, E^H)$, para todo $\sigma \in H \subset \text{Gal}(E/E^H)$, como $\alpha \in E$ es cero de $f \in E^H[X]$, se tiene que $\sigma(\alpha) \in E$ es cero de $\bar{\sigma}(f) = f$ (ya que $\sigma|_{E^H} = \text{id}_{E^H}$). Por tanto, el polinomio

$$g = \prod_{\sigma(\alpha) \in H\alpha} (X - \sigma(\alpha))$$

divide a f en $E[X]$.

Además, para todo $\gamma \in H$,

$$\bar{\gamma}(g) = \prod_{\sigma(\alpha) \in H\alpha} (X - \gamma\sigma(\alpha)) = g,$$

ya que la última igualdad se obtiene teniendo en cuenta que la aplicación $H \rightarrow H$, definida por $\sigma \mapsto \gamma\sigma$, es biyectiva y, así, $H\alpha = \{\sigma(\alpha) \mid \sigma \in H\} = \{\gamma\sigma(\alpha) \mid \sigma \in H\}$.

Por tanto, $g \in E^H[X]$ y entonces g divide a f en $E^H[X]$. Dado que f es irreducible y f y g son mónicos, se concluye que $f = g$. $\square$

Teorema 5.9. *Si $E : K$ es una extensión finita y H es un subgrupo de $\text{Gal}(E/K)$, entonces*

$$[E : E^H] = |H| \text{ y } H = \text{Gal}(E/E^H).$$

Demostración. Como $E : E^H$ es finita, por el Teorema del elemento primitivo (4.17), existe $\alpha \in E$ tal que $E = E^H(\alpha)$.

Por el lema anterior,

$$[E : E^H] = [E^H(\alpha) : E^H] = \partial \text{Irr}(\alpha, E^H) = |H\alpha| = (H : H_\alpha).$$

Además,

$$\left. \begin{array}{l} H_\alpha := \{\sigma \in H \mid \sigma(\alpha) = \alpha\} \\ H \subset \text{Gal}(E/E^H) \text{ y } E = E^H(\alpha) \end{array} \right\} \Rightarrow H_\alpha = \{\text{id}_E\} \text{ y } (H : H_\alpha) = |H|.$$

Por tanto, $[E : E^H] = |H|$.

Por otra parte,

$$\left. \begin{array}{l} |\text{Gal}(E/E^H)| \leq [E : E^H] = |H| \\ H \subset \text{Gal}(E/E^H) \end{array} \right\} \Rightarrow H = \text{Gal}(E/E^H). \quad \square$$

Definición 5.10. Una extensión $E : K$ se dice de *Galois* si

- i) $E : K$ es algebraica,
- ii) $E^{\text{Gal}(E/K)} = K$.

Teorema 5.11. Sea $E : K$ una extensión finita. Son equivalentes:

1. $E : K$ es de Galois.
2. $E : K$ es normal.
3. $[E : K] = |\text{Gal}(E/K)|$.

Demostración.

1) $\Rightarrow$ 2) Denotando $H = \text{Gal}(E/K)$, como $E : K$ es de Galois, $E^H = K$. Teniendo en cuenta que $E : K$ es finita, por el Teorema del elemento primitivo (4.17), existe $\alpha \in E$ tal que $E = K(\alpha)$ y, por el lema 5.8,

$$f = \text{Irr}(\alpha, E^H) = \prod_{\sigma(\alpha) \in H\alpha} (X - \sigma(\alpha)).$$

Por tanto, f escinde en E , y un cuerpo de escisión para f sobre K es

$$E_f = K(\{\sigma(\alpha) \mid \sigma \in H\}).$$

Puesto que $\alpha \in E_f$ y $K(\alpha) \subset E_f$. Además, $E_f \subset K(\alpha)$ ya que $\sigma(\alpha) \in E$ para todo $\sigma \in H$.

Así, $E_f = E$ y, por la proposición 4.21, $E : K$ es normal.

2) $\Rightarrow$ 3) Por la proposición 5.5, si $E : K$ es normal y finita, se tiene que $[E : K] = |\text{Gal}(E/K)|$.

3) $\Rightarrow$ 1) Como $E : K$ es una extensión finita, también es algebraica.

Veamos que $E^{\text{Gal}(E/K)} = K$:

Sabemos que $K \subset E^{\text{Gal}(E/K)} \subset E$. Por el teorema 5.9 y la hipótesis 3),

$$\left[E : E^{\text{Gal}(E/K)} \right] = |\text{Gal}(E/K)| = [E : K].$$

Como consecuencia del Teorema del grado (1.6), $[E^{\text{Gal}(E/K)} : K] = 1$ o, equivalentemente, $E^{\text{Gal}(E/K)} = K$. $\square$

Corolario 5.12. *Si $K \subset F \subset E$ es una torre de cuerpos y $E : K$ es una extensión de Galois finita, entonces $E : F$ es de Galois finita.*

5.2. Teorema fundamental de la teoría de Galois

Teorema 5.13. *Sean $E : K$ una extensión de Galois finita con grupo de Galois $G = \text{Gal}(E/K)$, $\mathcal{F} = \{F \text{ cuerpo} \mid K \subset F \subset E\}$ y $\mathcal{S} = \{H \mid H \text{ subgrupo de } G\}$.*

Las aplicaciones

$$\begin{array}{ccc} \mathcal{F} & \longrightarrow & \mathcal{S} & & \text{y} & \mathcal{S} & \longrightarrow & \mathcal{F} \\ F & \mapsto & \text{Gal}(E/F) & & H & \mapsto & E^H \end{array}$$

son biyectivas, inversas la una de la otra e invierten las inclusiones.

Demostración. Es obvio que las dos aplicaciones están bien definidas e invierten las inclusiones. Veamos que son inversas:

Para cada $F \in \mathcal{F}$, puesto que $E : F$ es una extensión de Galois, $E^{\text{Gal}(E/F)} = F$ y así,

$$F \mapsto \text{Gal}(E/F) \mapsto E^{\text{Gal}(E/F)} = F.$$

Para cada $H \in \mathcal{S}$, por el teorema 5.9, $\text{Gal}(E/E^H) = H$ y entonces,

$$H \mapsto E^H \mapsto \text{Gal}(E/E^H) = H.$$

$\square$

Nótese que:

$$\begin{array}{ccc}
 E & & \{1\} \\
 \uparrow [E : F] = |H| & & \downarrow \\
 F = E^H & \longleftrightarrow & H = \text{Gal}(E/F) \\
 \uparrow [F : K] = (G : H) & & \downarrow \\
 K & & G
 \end{array}$$

Corolario 5.14. Sean $E : K$ una extensión finita de Galois, $G = \text{Gal}(E/K)$ y H un subgrupo de G . Entonces

$$H \triangleleft G \text{ si, y solo si, } E^H : K \text{ es normal finita.}$$

Además, en este caso,

$$\text{Gal}(E^H/K) \simeq G/H = \text{Gal}(E/K)/\text{Gal}(E/E^H).$$

Demostración.

“ $\Rightarrow$ ” Por la proposición 4.23, es suficiente demostrar que si $\sigma \in G$ se verifica que $\sigma(E^H) \subset E^H$.

Sean $x \in E^H$ y $\tau \in H$, como H es un subgrupo normal de G , existe $\tau_1 \in H$ tal que $\tau = \sigma\tau_1\sigma^{-1}$. Por tanto,

$$\tau\sigma(x) = \sigma\tau_1\sigma^{-1}\sigma(x) = \sigma\tau_1(x) = \sigma(x),$$

ya que $\tau_1 \in \text{Gal}(E/E^H)$ y $x \in E^H$. En consecuencia, $\sigma(x) \in E^H$ y $\sigma(E^H) \subset E^H$.

“ $\Leftarrow$ ” Si $E^H : K$ normal y finita, entonces $E^H : K$ es de Galois.

Consideramos la aplicación

$$\begin{array}{ccc}
 h: & G = \text{Gal}(E/K) & \rightarrow & \text{Gal}(E^H/K) \\
 & \sigma & & \mapsto \sigma|_{E^H}
 \end{array}$$

Por la proposición 4.23, h está bien definida y, trivialmente, es homomorfismo de grupos.

$$\text{Ker } h := \{\sigma \in G = \text{Gal}(E/K) \mid \sigma|_{E^H} = \text{id}_{E^H}\} = \text{Gal}(E/E^H) = H.$$

Por tanto, H es un subgrupo normal de G .

Factorizando h , se tiene que $G/H \simeq \text{Im } h$.

Además,

$$|\text{Im } h| = |G/H| = \frac{|G|}{|H|} = \frac{[E : K]}{[E : E^H]} = [E^H : K] = |\text{Gal}(E^H/K)|$$

donde la última igualdad se sigue de que $E^H : K$ es de Galois finita.

Como $\text{Im } h$ es un subgrupo de $\text{Gal}(E^H/K)$, se tiene que $\text{Im } h = \text{Gal}(E^H/K)$ y, por tanto, $\text{Gal}(E^H/K) \simeq G/H$. $\square$

Utilizando el Teorema fundamental de la teoría de Galois, el corolario anterior se puede enunciar como:

Corolario 5.15. *Sean $E : K$ una extensión finita de Galois, F un cuerpo intermedio entre K y E y $G = \text{Gal}(E/K)$. Entonces:*

$F : K$ es normal si, y solo si, $\text{Gal}(E/F)$ es un subgrupo normal de G .

En este caso,

$$\text{Gal}(F/K) \simeq \text{Gal}(E/K) / \text{Gal}(E/F).$$

Capítulo 6

Resolubilidad de ecuaciones por radicales

6.1. Grupos resolubles

Los grupos resolubles aparecieron en el estudio de la resolubilidad de ecuaciones por radicales y de ahí el nombre (fueron bautizados por Jordan, en 1867). Estos grupos son mucho más generales que los abelianos, pero aún así poseen algunas de sus propiedades “agradables”. Nótese que si G es un grupo,

$$G \text{ es abeliano} \Leftrightarrow \forall a, b \in G, ab = ba \Leftrightarrow \forall a, b \in G, aba^{-1}b^{-1} = e.$$

De modo que el conjunto $\{aba^{-1}b^{-1} \mid a, b \in G\}$ puede verse como la obstrucción para que G sea abeliano.

Definición 6.1. Sea G un grupo y $a, b \in G$, se llama *conmutador de a y b* , y se denota por $[a, b]$, el elemento $aba^{-1}b^{-1} \in G$.

Se llama *subgrupo conmutador* o *subgrupo derivado de G* , y se denota por G' , el grupo

$$G' := \langle \{[a, b] \mid a, b \in G\} \rangle.$$

Observación 6.2. Nótese que:

- 1) G es abeliano $\Leftrightarrow G' = \{e\}$.
- 2) $[a, b]^{-1} = [b, a]$, $\forall a, b \in G$.
- 3) Los elementos de G' son productos finitos de conmutadores.

Proposición 6.3.

1. Si $f: G \rightarrow T$ es un homomorfismo de grupos, entonces $f(G')$ es un subgrupo de T' . Si además f es sobreyectivo, entonces $f(G') = T'$.
2. Si H es un subgrupo de G , entonces H' es un subgrupo de G' .
3. Para cualquier grupo G , G' es un subgrupo normal de G .

Demostración.

1) Ya que $f([a, b]) = f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} = [f(a), f(b)]$, se tiene que $f([a_1, b_1] \cdots [a_r, b_r]) = [f(a_1), f(b_1)] \cdots [f(a_r), f(b_r)]$ y, en consecuencia, $f(G')$ es un subgrupo de T' .

2) Si $i: H \hookrightarrow G$ es el homomorfismo inclusión, por el apartado anterior, $i(H') = H'$ es un subgrupo de G' .

3) Para cada $a \in G$ se verifica que $aG'a^{-1} = G'$. En efecto, como

$$\begin{aligned} \varphi_a: G &\rightarrow G \\ x &\mapsto axa^{-1} \end{aligned}$$

es isomorfismo de grupos, por el apartado 1), se tiene que $\varphi_a(G') = G'$, es decir, $aG'a^{-1} = G'$. $\square$

Proposición 6.4. Si G es un grupo y N es un subgrupo normal de G , entonces

$$G/N \text{ es abeliano si, y solo si, } G' \subset N.$$

En particular, G/G' es abeliano.

Demostración. G/N es abeliano $\Leftrightarrow aNbN = bNaN, \forall a, b \in G \Leftrightarrow ab(ba)^{-1} \in N, \forall a, b \in G \Leftrightarrow [a, b] \in N, \forall a, b \in G \Leftrightarrow G' \subset N.$ $\square$

Definición 6.5. Un grupo G se dice *resoluble* si, para algún $n \geq 0$, existe una cadena finita de subgrupos

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\} \quad (*)$$

tal que, para $i: 0, \dots, n-1$,

- i) G_{i+1} es subgrupo normal de G_i ,

ii) G_i/G_{i+1} es abeliano.

Una cadena (*) que verifica i) se dice que es una *serie normal de G a $\{e\}$* . Los grupos cocientes G_i/G_{i+1} de ii) se llaman *factores de la serie*.

Así, G es resoluble si existe alguna serie normal de G a $\{e\}$ con factores abelianos.

Ejemplos 6.6.

1) Si G es abeliano, entonces

$$G \supset \{e\}$$

es una serie normal de G a $\{e\}$ con factores abelianos y, por tanto, G es resoluble.

2) S_3 es resoluble. Basta considerar la cadena de grupos

$$S_3 \supset \langle (123) \rangle \supset \{e\}.$$

Como $(S_3 : \langle (123) \rangle) = 2$, se tiene que $\langle (123) \rangle \triangleleft S_3$ y $S_3/\langle (123) \rangle$ es abeliano y, además, $\langle (123) \rangle$ es abeliano porque es cíclico.

Proposición 6.7. *Si $G \neq \{e\}$ es un grupo abeliano finito, existe una serie normal de G a $\{e\}$ cuyos factores son cíclicos de orden primo.*

Proposición 6.8. *Un grupo finito $G \neq \{e\}$ es resoluble si, y solo si, tiene una serie normal cuyos factores son cíclicos de orden primo.*

Definición 6.9. Si G es un grupo, se llama *serie derivada de G* a la cadena de subgrupos de G

$$G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \dots$$

donde: $G^{(0)} := G$, $G^{(i+1)} := (G^{(i)})'$, el derivado de $G^{(i)}$, $\forall i \geq 0$.

Proposición 6.10. *Un grupo G es resoluble si, y solo si, existe $t \geq 0$ tal que $G^{(t)} = \{e\}$.*

Demostración.

“ $\Rightarrow$ ” Sea $G = G_0 \supset G_1 \supset \dots \supset G_n = \{e\}$ una serie normal de G a $\{e\}$ con factores abelianos.

Probaremos, por inducción, que $G^{(i)} \subset G_i \quad \forall i \geq 0$.

$$G^{(0)} = G = G_0.$$

Sea $i > 0$ y supongamos que $G^{(i)} \subset G_i$. Entonces, ya que G_i/G_{i+1} es abeliano,

$$G^{(i+1)} := (G^{(i)})' \subset (G_i)' \subset G_{i+1}.$$

“ $\Leftarrow$ ” De la proposición 6.4 se sigue que la serie derivada

$$G^{(0)} \supset G^{(1)} \supset \dots \supset G^{(t)} = \{e\}$$

es una serie normal de G a $\{e\}$ con factores abelianos. $\square$

Lema 6.11. *Sea $f: G \rightarrow T$ un homomorfismo de grupos. Se verifica que:*

- a) $f(G^{(i)}) \subset T^{(i)}, \forall i \geq 0$.
- b) Si f es sobreyectivo, $f(G^{(i)}) = T^{(i)}, \forall i \geq 0$.

Demostración. Se demuestra usando inducción en i . $\square$

Proposición 6.12. *Sea G un grupo resoluble.*

- 1. Si $f: G \rightarrow T$ es un homomorfismo de grupos sobreyectivo, entonces T es resoluble. En particular, todo grupo isomorfo a uno resoluble es resoluble.
- 2. Si H es un subgrupo de G , entonces H es resoluble.

Demostración. Si G es resoluble, existe $t \geq 0$ tal que $G^{(t)} = \{e\}$.

1) Por el lema anterior $f(G^{(t)}) = T^{(t)} = \{e\}$.

2) Si H es un subgrupo de G , la inclusión $i: H \hookrightarrow G$ es un homomorfismo de grupos. Por el lema anterior $H^{(i)} \subset G^{(i)} \forall i \geq 0$, y como $G^{(t)} = \{e\}$, se tiene que $H^{(t)} = \{e\}$ y H es resoluble. $\square$

Teorema 6.13. *Sean G un grupo y H un subgrupo normal de G , entonces*

G es resoluble si, y solo si, H y G/H son resolubles.

Demostración. Es claro que la aplicación

$$\begin{aligned} p: G &\rightarrow G/H \\ a &\mapsto aH \end{aligned}$$

es homomorfismo sobreyectivo de grupos y que $\text{Ker } p = H$.

“ $\Rightarrow$ ” Considerando la inclusión $i: H \hookrightarrow G$ y la proyección $p: G \rightarrow G/H$, de la proposición anterior, se deduce que H y G/H son resolubles.

“ $\Leftarrow$ ” Dado que G/H es resoluble, existe $t \geq 0$ tal que $(G/H)^{(t)} = \{H\}$.

Además, por el lema 6.11, $p(G^{(t)}) = (G/H)^{(t)}$. Por tanto, $p(G^{(t)}) = \{H\}$ y, en consecuencia, $G^{(t)} \subset \text{Ker } p = H$.

Teniendo en cuenta que H es resoluble y la proposición 6.12 se obtiene que $G^{(t)}$ es resoluble, es decir, $\exists r \geq 0$ tal que $(G^{(t)})^{(r)} = \{e\}$.

Es claro que $(G^{(t)})^{(r)} = G^{(t+r)}$ y, por tanto, G es resoluble. $\square$

Ejercicio 6.14. G y H son grupos resolubles si, y solo si, $G \times H$ es un grupo resoluble.

Demostración.

“ $\Rightarrow$ ” La aplicación

$$\begin{aligned} \pi: G \times H &\rightarrow G \\ (g, h) &\mapsto g \end{aligned}$$

es un homomorfismo sobreyectivo tal que $\text{Ker } \pi = \{e\} \times H \triangleleft G \times H$.

Como $(G \times H)/\text{Ker } \pi \simeq G$ y $\{e\} \times H \simeq H$ son grupos resolubles, por el teorema 6.13, se tiene que $G \times H$ es resoluble. $\square$

Ejercicio 6.15. $\forall n \geq 2$, A_n es resoluble si, y solo si, S_n es resoluble

Demostración. Como $(S_n : A_n) = 2$ se verifica que A_n es un subgrupo normal de S_n .

Como S_n/A_n tiene orden 2, es un grupo abeliano, por lo cual S_n/A_n es resoluble. Por el teorema 6.13, A_n es resoluble si, y solo si, S_n es resoluble. $\square$

Proposición 6.16. S_4 y A_4 son grupos resolubles.

Demostración. Por el ejercicio anterior es suficiente probar que A_4 es un grupo resoluble:

Sabemos que si $\sigma \in S_n$, $\sigma \neq 1$ y $\sigma = \sigma_1 \cdots \sigma_r$ es la descomposición de σ en producto de ciclos disjuntos, entonces $|\sigma| = m.c.m. \{|\sigma_1|, \dots, |\sigma_r|\}$.

Ya que los únicos elementos de orden 4 en S_4 son los 4-ciclos y son permutaciones impares, en A_4 no hay elementos de orden 4 .

En S_4 los elementos de orden 2 son los 2-ciclos o la composición de dos 2-ciclos disjuntos. Puesto que una trasposición es una permutación impar, los elementos de orden 2 de A_4 son $(12)(34)$, $(13)(24)$ y $(14)(23)$.

Por otra parte, como $|A_4| = 2^2 \cdot 3$, si V es un 2-Sylow de A_4 , como en A_4 no hay elementos de orden 4, todo elemento de V , distinto del neutro, tiene orden 2; por tanto V tiene 3 elementos de orden 2. Puesto que en A_4 solo existen 3 elementos de orden 2, V es el único 2-Sylow de A_4 y, en consecuencia, $V \triangleleft A_4$.

$$V = \{1, (12)(34), (13)(24), (14)(23)\} \text{ (Grupo de Klein).}$$

Así,

$$A_4 \supset V \supset \{1\}$$

es una serie normal con factores $A_4/V \simeq \mathbb{Z}_3$ y $V/\{1\} \simeq V$ abelianos. $\square$

Teorema 6.17. *Si $n \geq 5$ el grupo S_n no es resoluble.*

Demostración. La prueba se realizará por reducción al absurdo.

Si S_n es resoluble, existiría una cadena de subgrupos de S_n

$$S_n = H_0 \supset H_1 \supset \cdots \supset H_i \supset H_{i+1} \supset \cdots \supset H_m = \{1\}$$

tal que $H_{i+1} \triangleleft H_i$ y H_i/H_{i+1} es abeliano, $\forall i : 0, \dots, m-1$.

Veremos que cada H_i contiene todos los 3-ciclos de S_n lo que es imposible pues $H_m = \{1\}$.

Sea (abc) un 3-ciclo cualquiera de S_n . Teniendo en cuenta que $n \geq 5$, existen $d, e \in \{1, 2, \dots, n\} \setminus \{a, b, c\}$.

Tomamos $\alpha = (bcd)$, $\beta = (bae) \in S_n$. Como H_0/H_1 es abeliano, el conmutador $[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1} = (bcd)(bae)(dcb)(eab) = (abc)$ es un elemento de H_1 .

Supongamos ahora que $i > 1$ y que H_i contiene todos los 3-ciclos. Sea (abc) un 3-ciclo cualquiera de S_n . Procedemos de forma idéntica al caso $i = 1$ teniendo en cuenta

que $\alpha, \beta \in H_i$ por ser 3-ciclos, y resulta que $(abc) = [\alpha, \beta] \in H_{i+1}$ ya que H_i/H_{i+1} es un grupo abeliano. $\square$

6.2. Raíces de la unidad

En lo que sigue de este tema consideraremos cuerpos de característica cero.

Definición 6.18. Sean K un cuerpo, un entero $n \geq 1$ y $\overline{K}$ una clausura algebraica de K .

Llamaremos *raíz n -ésima de la unidad* en $\overline{K}$ a cualquier $\varepsilon \in \overline{K}$ que sea un cero del polinomio $X^n - 1 \in K[X]$.

Denotaremos con $U_n = \{\varepsilon \in \overline{K} \mid \varepsilon^n = 1\}$.

Proposición 6.19. U_n es un grupo cíclico de orden n . Cada generador de U_n se llamará *raíz n -ésima primitiva de 1*.

Demostración. Es obvio que $1 \in U_n$. Si $\alpha, \beta \in U_n$ se tiene que $\alpha\beta \in U_n$ ya que $(\alpha\beta)^n = \alpha^n\beta^n = 1$. Además, si $\alpha \in U_n$ y $\alpha \neq 0$, dado que $(\alpha^{-1})^n = (\alpha^n)^{-1} = 1$, se deduce que $\alpha^{-1} \in U_n$.

U_n es un grupo de orden n ya que el polinomio $X^n - 1$ es separable (su derivada nX^{n-1} no es nula y solamente admite al 0 como raíz). Además, por el teorema 4.15, es cíclico. $\square$

Observación 6.20. El *indicador de Euler* de n , $\varphi(n)$, es el número de generadores del grupo U_n ,

$$\varphi(n) := |\{r \in \mathbb{N} \mid 1 \leq r < n, (r, n) = 1\}| = |\mathcal{U}(\mathbb{Z}_n)|.$$

Si $U_n = \langle \varepsilon \rangle$ con $|\varepsilon| = n > 1$, entonces el conjunto de generadores de U_n es $\{\varepsilon^r \mid 1 \leq r < n, (r, n) = 1\}$.

Proposición 6.21.

1. Si $n, m \in \mathbb{Z}$ y $(m, n) = 1$ se tiene que $\varphi(nm) = \varphi(n)\varphi(m)$.
2. Si p es un número primo y $k \geq 1$ es un entero, se verifica que

$$\varphi(p^k) = (p-1)p^{k-1}.$$

3. Si $p_1, \dots, p_s$ son primos distintos y $\alpha_1, \dots, \alpha_s \geq 1$ son enteros, entonces

$$\varphi(p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = (p_1 - 1) \cdots (p_s - 1) p_1^{\alpha_1 - 1} \cdots p_s^{\alpha_s - 1}.$$

Demostración.

1) El homomorfismo de anillos

$$\begin{aligned} \mathbb{Z} &\rightarrow \mathbb{Z}_n \times \mathbb{Z}_m \\ a &\mapsto a(\bar{1}, \bar{1}) \end{aligned}$$

tiene como núcleo $nm\mathbb{Z}$ ya que $(m, n) = 1$. Como además $|\mathbb{Z}_{nm}| = |\mathbb{Z}_n \times \mathbb{Z}_m|$, se tiene que $\mathbb{Z}_{nm} \simeq \mathbb{Z}_n \times \mathbb{Z}_m$, y entonces

$$|\mathcal{U}(\mathbb{Z}_{nm})| = |\mathcal{U}(\mathbb{Z}_n \times \mathbb{Z}_m)| = |\mathcal{U}(\mathbb{Z}_n)| |\mathcal{U}(\mathbb{Z}_m)|.$$

2) Como los múltiplos de p entre 1 y p^k son $1 \cdot p, 2 \cdot p, \dots, p^{k-1} \cdot p$, teniendo en cuenta que el número de enteros entre 1 y p^k que no son coprimos con p^k coincide con el número de múltiplos de p entre 1 y p^k , se tiene que

$$\varphi(p^k) = p^k - p^{k-1} = (p - 1)p^{k-1}.$$

3) Se prueba usando inducción. □

Proposición 6.22. Sea K un cuerpo y sea $\varepsilon \in \overline{K}$ una raíz n -ésima primitiva de 1. Se verifica que:

1. $K(\varepsilon) : K$ es una extensión de Galois finita.
2. $\text{Gal}(K(\varepsilon)/K)$ es abeliano y, por lo tanto, resoluble.

Demostración.

1) $K(\varepsilon)$ es cuerpo de escisión sobre K del polinomio $X^n - 1 \in K[X]$ ya que $U_n = \langle \varepsilon \rangle$.

2) Para probar que $\text{Gal}(K(\varepsilon)/K)$ es abeliano bastará con demostrar que si $\sigma, \tau \in \text{Gal}(K(\varepsilon)/K)$ entonces $(\sigma \circ \tau)(\varepsilon) = (\tau \circ \sigma)(\varepsilon)$.

Como $\text{Irr}(\varepsilon, K)$ divide a $X^n - 1$, se tiene que $\sigma(\varepsilon)$ y $\tau(\varepsilon)$ son raíces n -ésimas de 1 y, por ello, existen $r, t \in \mathbb{Z}$ con $0 \leq r, t < n$ tales que $\sigma(\varepsilon) = \varepsilon^r$ y $\tau(\varepsilon) = \varepsilon^t$.

Así, $(\sigma \circ \tau)(\varepsilon) = \sigma(\tau(\varepsilon)) = \sigma(\varepsilon^t) = (\sigma(\varepsilon))^t = (\varepsilon^r)^t = \varepsilon^{rt}$ y $(\tau \circ \sigma)(\varepsilon) = \tau(\sigma(\varepsilon)) = \tau(\varepsilon^r) = (\tau(\varepsilon))^r = (\varepsilon^t)^r = \varepsilon^{tr}$. □

Proposición 6.23. Sean K un cuerpo, $\varepsilon \in \overline{K}$ una raíz n -ésima primitiva de 1 y $\alpha \in \overline{K}$ tal que $\alpha^n \in K$. Se tiene que:

1. $K(\varepsilon, \alpha) : K$ y $K(\varepsilon, \alpha) : K(\varepsilon)$ son extensiones de Galois finitas.
2. $\text{Gal}(K(\varepsilon, \alpha) / K(\varepsilon))$ es abeliano y por tanto resoluble.
3. $\text{Gal}(K(\varepsilon, \alpha) / K)$ es resoluble.

Demostración.

1) $K(\varepsilon, \alpha)$ es cuerpo de escisión del polinomio $X^n - \alpha^n$ sobre K y, en consecuencia, $K(\varepsilon, \alpha) : K$ y $K(\varepsilon, \alpha) : K(\varepsilon)$ son extensiones de Galois finitas.

2) Cada $\sigma \in \text{Gal}(K(\varepsilon, \alpha) / K(\varepsilon))$ está determinado por su valor $\sigma(\alpha)$ y sabemos que $\sigma(\alpha)$ es un cero de $X^n - \alpha^n$.

Si $\sigma, \tau \in \text{Gal}(K(\varepsilon, \alpha) / K(\varepsilon))$ existen enteros r, s con $0 \leq r, s < n$ de forma que $\sigma(\alpha) = \alpha\varepsilon^r$ y $\tau(\alpha) = \alpha\varepsilon^s$.

Así, $(\sigma \circ \tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha\varepsilon^s) = \sigma(\alpha)\sigma(\varepsilon^s) = \alpha\varepsilon^r\varepsilon^s = \alpha\varepsilon^{r+s}$ ya que $\sigma(\varepsilon^s) = \varepsilon^s \in K(\varepsilon)$; de modo análogo, $(\tau \circ \sigma)(\alpha) = \alpha\varepsilon^{s+r}$, de donde resulta que $\sigma \circ \tau = \tau \circ \sigma$.

3) $K \subset K(\varepsilon) \subset K(\varepsilon, \alpha)$ y como $K(\varepsilon) : K$ es de Galois, por el corolario 5.14, $H = \text{Gal}(K(\varepsilon, \alpha) / K(\varepsilon)) \triangleleft G = \text{Gal}(K(\varepsilon, \alpha) / K)$ y $\text{Gal}(K(\varepsilon) / K) \simeq G/H$. Como H y G/H son resolubles, utilizando el teorema 6.13, se tiene que G es resoluble. $\square$

Definición 6.24. Sea $\varepsilon \in \mathbb{C}$ una raíz n -ésima primitiva de 1. Llamaremos *polinomio ciclotómico n -ésimo*, y lo denotaremos por $\Phi_n(X)$, al polinomio

$$\Phi_n(X) = \prod_{m < n, (m, n) = 1} (X - \varepsilon^m).$$

Proposición 6.25. Sea $\varepsilon \in \mathbb{C}$ una raíz n -ésima primitiva de 1. Se verifica que:

1. $\Phi_n(X) \in \mathbb{Z}[X]$.
2. $\Phi_n(X) = \text{Irr}(\varepsilon, \mathbb{Q})$ y $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = \partial(\text{Irr}(\varepsilon, \mathbb{Q})) = \varphi(n)$.

Demostración.

1) Sea E un cuerpo de escisión del polinomio $X^n - 1$ sobre $\mathbb{Q}$ y $G = \text{Gal}(E/\mathbb{Q})$. Si $\sigma \in G$ y ε es una raíz n -ésima primitiva de 1, $\sigma(\varepsilon)$ también es una raíz n -ésima primitiva

de 1 ya que es un cero del polinomio $X^n - 1$ y $|\sigma(\varepsilon)| = |\varepsilon| = n$. Por tanto, si $\bar{\sigma}$ es la extensión del isomorfismo σ al anillo de polinomios $E[X]$, entonces $\bar{\sigma}(\Phi_n(X)) = \Phi_n(X)$ y, como $\mathbb{Q} = E^G$, el polinomio $\Phi_n(X) \in \mathbb{Q}[X]$.

Además, como $\Phi_n(X) \in \mathbb{Q}[X]$ es un factor mónico de $X^n - 1 \in \mathbb{Z}[X]$, se tiene que $\Phi_n(X) \in \mathbb{Z}[X]$.

2) Veamos ahora que $\Phi_n(X) \in \mathbb{Z}[X]$ es irreducible en $\mathbb{Z}[X]$.

Si $f \in \mathbb{Z}[X]$ es un factor irreducible y mónico de $\Phi_n(X)$, existe $h \in \mathbb{Z}[X]$ tal que $\Phi_n(X) = f \cdot h$. Si ε una raíz de f , ε es una raíz n -ésima primitiva de 1. Probaremos ahora que si p es primo que no divide a n , se verifica que ε^p , que también es una raíz n -ésima primitiva de 1, es un cero de f .

Si $f(\varepsilon^p) \neq 0$, entonces $h(\varepsilon^p) = 0$ y así, ε es un cero del polinomio $h(X^p) \in \mathbb{Z}[X]$. Por ello, el polinomio $f = \text{Irr}(\varepsilon, \mathbb{Q})$ divide a $h(X^p)$ en $\mathbb{Q}[X]$. Teniendo en cuenta que ambos polinomios tienen coeficientes enteros, se tiene que f divide a $h(X^p)$ en $\mathbb{Z}[X]$ y, como ambos polinomios son mónicos, existe $g \in \mathbb{Z}[X]$ mónico tal que $h(X^p) = f \cdot g$.

Aplicando el homomorfismo de reducción módulo p , como $\overline{a^p} = \bar{a}$ para cualquier entero a , se tiene que

$$\left(\overline{h(X)}\right)^p = \overline{h(X^p)} = \overline{f(X)} \cdot \overline{g(X)},$$

lo que significa que $\bar{f}$ y $\bar{h}$ tienen algún factor común en el dominio de factorización única $\mathbb{Z}_p[X]$ y, por ello, el polinomio $\overline{\Phi_n(X)}$ tendría raíces múltiples, lo cual es imposible ya que $\overline{\Phi_n(X)}$ divide a $X^n - \bar{1}$ y el polinomio $X^n - \bar{1}$ es separable.

Hemos probado que si p es primo que no divide a n y ε es una raíz de f , también lo es ε^p . Dado que cualquier raíz n -ésima primitiva de 1 se puede obtener elevando ε a una sucesión de potencias primas, con primos que no dividen a n , esto implica que todas las raíces n -ésimas primitivas de 1 son raíces de f . Por tanto, $f = \Phi_n(X)$ y, así, $\Phi_n(X)$ es irreducible en $\mathbb{Z}[X]$.

Por la observación 6.20 se tiene que $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = \partial(\text{Irr}(\varepsilon, \mathbb{Q})) = \varphi(n)$. □

Corolario 6.26. *Sea n un entero, $n \geq 1$. Entonces,*

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Demostración. Sabemos que si $\alpha \in U_n$, por el Teorema de Lagrange, $|\alpha|$ divide a $n = |U_n|$. Además, como U_n es cíclico, si d es un divisor de n , existe $\alpha \in U_n$ con $|\alpha| = d$.

Si en la factorización

$$X^n - 1 = \prod_{\alpha \in U_n} (X - \alpha)$$

reagrupamos los factores correspondientes a aquellas $\alpha \in U_n$ que tienen el mismo orden d , entonces

$$\Phi_d(X) = \prod_{|\alpha|=d} (X - \alpha)$$

y se tiene el resultado. □

Ejemplo 6.27.

1) $\Phi_1(X) = X - 1$.

2) $\Phi_2(X) = X + 1$, pues $X^2 - 1 = \Phi_1(X) \Phi_2(X)$.

3) Si p es un primo, $X^p - 1 = \prod_{d|p} \Phi_d(X) = \Phi_1(X) \Phi_p(X)$, y entonces

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

4) Puesto que $X^4 - 1 = \Phi_1(X) \Phi_2(X) \Phi_4(X)$, se deduce que

$$\Phi_4(X) = X^2 + 1.$$

5) Teniendo en cuenta que $X^6 - 1 = \Phi_1(X) \Phi_2(X) \Phi_3(X) \Phi_6(X)$, se tiene que

$$\Phi_6(X) = \frac{X^6 - 1}{\Phi_1(X) \Phi_2(X) \Phi_3(X)} = \frac{X^6 - 1}{(X + 1)(X^3 - 1)} = X^2 - X + 1.$$

6) Análogamente, se obtiene que

$$\Phi_{12}(X) = \frac{X^{12} - 1}{(X^6 - 1) \Phi_4(X)} = \frac{X^6 + 1}{X^2 + 1} = X^4 - X^2 + 1.$$

6.3. El Gran Teorema de Galois

Definición 6.28. Una extensión $F : K$ es *radical* si existe una torre de cuerpos

$$K = K_0 \subset K_1 \subset \cdots \subset K_{i-1} \subset K_i \subset \cdots \subset K_r = F$$

tal que, para cada $i : 1, \dots, r$, $K_i = K_{i-1}(\alpha_i)$ y existe $n_i \geq 1$ con $\alpha_i^{n_i} \in K_{i-1}$.

Una torre de este tipo se llamará una *torre radical*.

Nótese que existe $a_i \in K_{i-1}$ tal que α_i es un raíz n_i -ésima de a_i y a veces usaremos la notación $\alpha_i = \sqrt[n_i]{a_i}$.

Observaciones 6.29. Sea $F : K$ una extensión radical.

1) $F = K(\alpha_1, \dots, \alpha_r)$ y como, para cada $i : 1, \dots, r$, α_i es algebraico sobre K_{i-1} , la extensión $K_i : K_{i-1}$ es finita y, usando el Teorema del grado (1.6), se tiene que $F : K$ es finita.

2) $\{1, \alpha_1, \dots, \alpha_1^{n_1-1}\}$ es un sistema de generadores de $K(\alpha_1)$ como K -espacio vectorial. Así,

$$\alpha_2 = \sqrt[n_2]{a_2} = \sqrt[n_2]{c_0 + c_1 \sqrt[n_1]{a_1} + \cdots + c_{n_1-1} \sqrt[n_1]{a_1^{n_1-1}}} \quad (*)$$

con $a_1 = \alpha_1^{n_1}$, $c_j \in K$ para $j = 0, 1, \dots, n_1 - 1$.

De forma recurrente el elemento $\alpha_3 = \sqrt[n_3]{a_3}$ con $a_3 \in K(\alpha_1)(\alpha_2)$ y, por tanto, α_3 será una expresión del tipo (*) con a_2 en lugar de a_1 , con n_2 en lugar de n_1 , con n_3 en lugar de n_2 , y con los $c_j \in K(\alpha_1)$ que serán a su vez expresiones del tipo $c_j = g_j(\alpha_1)$ con $g_j \in K[X]$. Iterando el proceso, se puede ver como es la expresión de cualquier elemento de $K(\alpha_1, \dots, \alpha_r)$.

Definición 6.30. Sea $f \in K[X]$ y E_f un cuerpo de escisión para f sobre K .

Se dice que f (o la ecuación algebraica $f(X) = 0$) es *resoluble por radicales sobre* K si E_f está contenido en una extensión radical de K .

El grupo $\text{Gal}(E_f/K)$ se llama *grupo de Galois de f sobre K* y se denota por $\text{Gal}_K(f)$.

Observación 6.31. $\text{Gal}_K(f)$ es único salvo isomorfismos.

En efecto, si E_f y E'_f son cuerpos de escisión de $f \in K[X]$ sobre K , por el corolario 3.9, existe un K -isomorfismo $\sigma: E_f \rightarrow E'_f$. La aplicación $\text{Gal}(E_f/K) \rightarrow \text{Gal}(E'_f/K)$ definida por $\tau \mapsto \sigma \circ \tau \circ \sigma^{-1}$ es un isomorfismo de grupos.

Ejemplos 6.32.

1) Toda ecuación con coeficientes reales es resoluble por radicales sobre $\mathbb{R}$ puesto que $\mathbb{R} \subset \mathbb{R}(i) = \mathbb{C}$ es una torre radical.

Esto no significa que sepamos una fórmula para calcular las raíces de la ecuación, simplemente que es posible obtenerlas mediante operaciones racionales (sumas, restas, multiplicaciones y divisiones) y extracción de radicales.

2) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}$ es una extensión radical ya que

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

es una torre radical.

Lema 6.33. Sean K un cuerpo, $f \in K[X]$ y $K' = K(\alpha)$ con $\alpha^n \in K$ para algún entero $n \geq 1$. Entonces,

$\text{Gal}_K(f)$ es resoluble si, y solo si, $\text{Gal}_{K'}(f)$ es resoluble.

Demostración. Sean $g = X^n - \alpha^n \in K[X]$ y E_{fg} un cuerpo de escisión para fg sobre K . E_{fg} contiene un cuerpo de escisión, E_f , para f sobre K y otro, E_g , para g sobre K .

$$\begin{array}{ccccc}
 & & E_{fg} & & \\
 & \nearrow & & \nwarrow & \\
 E_f & & \uparrow & & E_g \\
 & \nwarrow & & \nearrow & \\
 & & K & &
 \end{array}$$

Por los teoremas 4.21 y 5.11 las extensiones $E_{fg} : K$, $E_f : K$ y $E_g : K$ son de Galois finitas y, por el corolario 5.14, sabemos que

$$\text{Gal}(E_{fg}/E_f) \triangleleft \text{Gal}(E_{fg}/K) \text{ y } \text{Gal}(E_f/K) \simeq \text{Gal}(E_{fg}/K) / \text{Gal}(E_{fg}/E_f) \text{ y}$$

$$\text{Gal}(E_{fg}/E_g) \triangleleft \text{Gal}(E_{fg}/K) \text{ y } \text{Gal}(E_g/K) \simeq \text{Gal}(E_{fg}/K) / \text{Gal}(E_{fg}/E_g).$$

Dado que, E_{fg} es cuerpo de escisión de g sobre E_f y E_g es cuerpo de escisión de g sobre K , por la proposición 6.23, se tiene que $\text{Gal}(E_{fg}/E_f)$ y $\text{Gal}(E_g/K)$ son grupos resolubles.

En el teorema 6.13, hemos visto que si H es un subgrupo normal de un grupo G , entonces G es resoluble si, y solo si, H y G/H son resolubles. Por tanto,

$$\text{Gal}(E_f/K) \text{ es resoluble} \Leftrightarrow \text{Gal}(E_{fg}/K) \text{ es resoluble} \Leftrightarrow \text{Gal}(E_{fg}/E_g) \text{ es resoluble}.$$

Análogamente, puesto que

$$\begin{array}{ccccc} & & E_{fg} & & \\ & \nearrow & & \nwarrow & \\ E_f(\alpha) & & \uparrow & & E_g \\ & \nwarrow & & \nearrow & \\ & & K(\alpha) & & \end{array}$$

$E_f(\alpha)$ es un cuerpo de escisión para f sobre $K(\alpha)$, E_g es un cuerpo de escisión para g sobre $K(\alpha)$ y E_{fg} es un cuerpo de escisión para g sobre $E_f(\alpha)$, repitiendo el razonamiento anterior, se tiene que

$$\text{Gal}(E_f(\alpha)/K(\alpha)) \text{ es resoluble} \Leftrightarrow \text{Gal}(E_{fg}/E_g) \text{ es resoluble}.$$

Por tanto,

$$\text{Gal}(E_f/K) \text{ es resoluble} \Leftrightarrow \text{Gal}(E_f(\alpha)/K(\alpha)) \text{ es resoluble},$$

o equivalentemente,

$$\text{Gal}_K(f) \text{ es resoluble} \Leftrightarrow \text{Gal}_{K'}(f) \text{ es resoluble.} \quad \square$$

Teorema 6.34 (El Gran Teorema de Galois). *Sea $f \in K[X]$. Si f es resoluble por radicales sobre K , entonces $\text{Gal}_K(f)$ es un grupo resoluble.*

Demostración.

Sea E_f un cuerpo de escisión para f sobre K . Como f es resoluble por radicales sobre K , existe un torre de cuerpos

$$K = K_0 \subset K_1 \subset \cdots \subset K_{i-1} \subset K_i \subset \cdots \subset K_r$$

tal que para cada $i : 1, \dots, r$, $K_i = K_{i-1}(\alpha_i)$ y existe $n_i \geq 1$ con $\alpha_i^{n_i} \in K_{i-1}$ y $E_f \subset K_r$.

Por el lema anterior sabemos que:

$$\text{Gal}_K(f) \text{ es resoluble} \Leftrightarrow \text{Gal}_{K_1}(f) \text{ es resoluble} \Leftrightarrow \cdots \Leftrightarrow \text{Gal}_{K_r}(f) \text{ es resoluble.}$$

Ahora bien, como $K \subset E_f \subset K_r$, un cuerpo de escisión para f sobre K_r es K_r , así, $\text{Gal}_{K_r}(f) = \{id\}$ que es un grupo resoluble. En conclusión, $\text{Gal}_K(f)$ es resoluble. $\square$

Nuestro próximo objetivo es demostrar el recíproco del teorema anterior.

Veamos, en primer lugar, que cualquier extensión normal y finita de un cuerpo K de característica cero está contenida en una extensión radical de K .

Proposición 6.35. *Si $E : F$ es una extensión normal y finita y $G = \text{Gal}(E/F)$ es un grupo resoluble, existe una torre de cuerpos*

$$F = F_0 \subset F_1 \subset \cdots \subset F_k = E$$

tal que, para $i : 1, \dots, k$, $F_i : F_{i-1}$ es una extensión normal y finita y $\text{Gal}(F_i/F_{i-1})$ es un grupo cíclico de orden primo.

Demostración. Si G es un grupo resoluble, por la proposición 6.8, existe una cadena de grupos

$$G = G_0 \supset G_1 \supset \cdots \supset G_k = \{e\}$$

con cada $G_i \triangleleft G_{i-1}$ y G_{i-1}/G_i cíclico de orden primo.

Por el teorema 5.13, existe una torre de cuerpos

$$F_0 = F = E^G \subset F_1 = E^{G_1} \subset \cdots \subset F_k = E.$$

Como $E : F$ es una extensión normal y finita, también lo son las extensiones $E : F_i$, para $i : 1, \dots, k$. Entonces, por el corolario 5.14, $F_i : F_{i-1}$ es normal y finita si, y solo si, $G_i = \text{Gal}(E/F_i) \triangleleft G_{i-1} = \text{Gal}(E/F_{i-1})$ y, en este caso, $\text{Gal}(F_i/F_{i-1}) \simeq G_{i-1}/G_i$.

Nótese que, como ya hemos señalado, G_{i-1}/G_i es un grupo cíclico de orden primo. □

Probaremos a continuación que cada una de las extensiones normales $F_i : F_{i-1}$, con $\text{Gal}(F_i/F_{i-1})$ cíclico de orden primo p_i , puede ser descrita mediante la adjunción de una raíz p_i -ésima.

Proposición 6.36. *Si $F_i : F_{i-1}$ es una extensión normal de grado primo p_i y $\varepsilon_{p_i} \in F_{i-1}$ es una raíz p_i -ésima primitiva de 1, entonces existe $\beta \in F_{i-1}$ tal que $F_i = F_{i-1}(\sqrt[p_i]{\beta})$.*

Demostración. Dado que $[F_i : F_{i-1}] = p_i$ primo, para cada $\alpha \in F_i \setminus F_{i-1}$ se tiene que $F_i = F_{i-1}(\alpha)$. Por tanto, es suficiente con encontrar algún $\beta \in F_{i-1}$ tal que $\sqrt[p_i]{\beta} \in F_i \setminus F_{i-1}$.

Sea $\alpha \in F_i \setminus F_{i-1}$ y $\text{Gal}(F_i/F_{i-1}) = \langle \sigma \rangle = \{1, \sigma, \dots, \sigma^{p_i-1}\}$. Si definimos

$$\alpha_j := \alpha + \varepsilon_{p_i}^j \sigma(\alpha) + \dots + \varepsilon_{p_i}^{j(p_i-1)} \sigma^{p_i-1}(\alpha), \text{ para } j : 0, \dots, p_i - 1,$$

aplicando el homomorfismo σ se tiene

$$\sigma(\alpha_j) = \sigma(\alpha) + \varepsilon_{p_i}^j \sigma^2(\alpha) + \dots + \varepsilon_{p_i}^{j(p_i-1)} \alpha = \varepsilon_{p_i}^{-j} \alpha_j$$

ya que, como $\varepsilon_{p_i} \in F_{i-1}$, $\sigma(\varepsilon_{p_i}) = \varepsilon_{p_i}$. Entonces

$$\sigma(\alpha_j^{p_i}) = (\varepsilon_{p_i}^{-j} \alpha_j)^{p_i} = \alpha_j^{p_i}$$

de donde se deduce que $\alpha_j^{p_i} \in F_i^{\langle \sigma \rangle} = F_{i-1}$.

Veamos ahora que existe algún α_j que no pertenece a F_{i-1} . En efecto, dado que $\langle \varepsilon_{p_i} \rangle = \langle \varepsilon_{p_i}^j \rangle$, es decir $\{1, \varepsilon_{p_i}, \dots, \varepsilon_{p_i}^{p_i-1}\} = \{1, \varepsilon_{p_i}^j, \dots, \varepsilon_{p_i}^{j(p_i-1)}\}$, para $j : 1, \dots, p_i - 1$, se tiene que

$$X^{p_i} - 1 = (X - 1)(X - \varepsilon_{p_i}^j) \dots (X - \varepsilon_{p_i}^{j(p_i-1)}),$$

de donde se sigue que $1 + \varepsilon_{p_i}^j + \dots + \varepsilon_{p_i}^{j(p_i-1)} = 0$ (coeficiente de X^{p_i-1}).

Así, teniendo en cuenta que $\alpha \notin F_{i-1}$, se verifica que

$$\sum_{j=0}^{p_i-1} \alpha_j = p_i \alpha + 0\sigma(\alpha) + \dots + 0\sigma^{p_i-1}(\alpha) = p_i \alpha \notin F_{i-1}.$$

Por ello, existe algún j para el cual $\alpha_j \notin F_{i-1}$ y tomando $\beta = \alpha_j^{p_i}$ se tiene el resultado. □

Volviendo a una situación como la de la proposición 6.35, vamos a construir una extensión radical de F que contiene a E , a partir de las etapas $F_0, F_1, \dots, F_k = E$ adjuntando las raíces de la unidad que sean necesarias para poder aplicar la proposición 6.36. La clave para conseguirlo está en el siguiente lema.

Lema 6.37. *Si $F_i : F_{i-1}$ es una extensión normal con $[F_i : F_{i-1}] = p_i$ primo y ε_{p_i} es una raíz p_i -ésima primitiva de 1, entonces $F_i(\varepsilon_{p_i}) : F_{i-1}(\varepsilon_{p_i})$ es una extensión normal y $[F_i(\varepsilon_{p_i}) : F_{i-1}(\varepsilon_{p_i})] = p_i$.*

Demostración. Si $F_i : F_{i-1}$ es una extensión normal y finita, F_i es un cuerpo de escisión sobre F_{i-1} de algún polinomio $f \in F_{i-1}[X]$ y $F_i(\varepsilon_{p_i})$ es un cuerpo de escisión sobre F_{i-1} y sobre $F_{i-1}(\varepsilon_{p_i})$ del polinomio $(X^{p_i} - 1)f \in F_{i-1}[X] \subset F_{i-1}(\varepsilon_{p_i})[X]$. Por ello, $F_i(\varepsilon_{p_i}) : F_{i-1}(\varepsilon_{p_i})$ es una extensión normal y finita.

Si $\{\alpha_1, \dots, \alpha_{p_i}\}$ es una F_{i-1} -base de F_i , es claro que genera $F_i(\varepsilon_{p_i})$ como $F_{i-1}(\varepsilon_{p_i})$ -espacio vectorial y así $[F_i(\varepsilon_{p_i}) : F_{i-1}(\varepsilon_{p_i})] \leq p_i$.

Por otra parte, dado que $F_{i-1} \subset F_{i-1}(\varepsilon_{p_i}) \subset F_i(\varepsilon_{p_i})$ y $F_{i-1} \subset F_i \subset F_i(\varepsilon_{p_i})$, aplicando el Teorema del grado (1.6), se obtiene que

$$[F_i(\varepsilon_{p_i}) : F_{i-1}] = [F_i(\varepsilon_{p_i}) : F_{i-1}(\varepsilon_{p_i})] [F_{i-1}(\varepsilon_{p_i}) : F_{i-1}] \text{ y}$$

$$[F_i(\varepsilon_{p_i}) : F_{i-1}] = [F_i(\varepsilon_{p_i}) : F_i] [F_i : F_{i-1}] = [F_i(\varepsilon_{p_i}) : F_i] \cdot p_i.$$

Teniendo en cuenta que $[F_{i-1}(\varepsilon_{p_i}) : F_{i-1}] = \partial \text{Irr}(\varepsilon_{p_i}, F_{i-1}) \leq p_i - 1$, se tiene que p_i divide a $[F_i(\varepsilon_{p_i}) : F_{i-1}(\varepsilon_{p_i})] \leq p_i$ y, por tanto, $[F_i(\varepsilon_{p_i}) : F_{i-1}(\varepsilon_{p_i})] = p_i$. $\square$

Proposición 6.38. *Si $E : F$ es una extensión normal y finita y $\text{Gal}(E/F)$ es un grupo resoluble, entonces E está contenido en una extensión radical de F .*

Demostración. Si $E : F$ es una extensión normal y finita y $G = \text{Gal}(E/F)$ es un grupo resoluble, por la proposición 6.35, existe una torre de cuerpos

$$F = F_0 \subset F_1 \subset \dots \subset F_k = E$$

con $F_i : F_{i-1}$ normal y finita y $\text{Gal}(F_i/F_{i-1})$ cíclico de orden primo, p_i , para $i : 1, \dots, k$.

Si ε_{p_i} es una raíz p_i -ésima primitiva de 1, por el lema 6.37, $F_i(\varepsilon_{p_i}) : F_{i-1}(\varepsilon_{p_i})$ es una extensión normal y finita y $\text{Gal}(F_i(\varepsilon_{p_i})/F_{i-1}(\varepsilon_{p_i}))$ es cíclico de orden primo, p_i , para $i : 1, \dots, k$.

Puesto que $\varepsilon_{p_i} \in F_{i-1}(\varepsilon_{p_i})$, aplicando la proposición 6.36, se verifica que $F_i(\varepsilon_{p_i}) = F_{i-1}(\varepsilon_{p_i}) \left(\sqrt[p_i]{\beta_i} \right)$ para algún $\beta_i \in F_{i-1}(\varepsilon_{p_i})$.

Extendiendo $F = F_0$ por los sucesivos radicales $\varepsilon_{p_1}, \sqrt[p_1]{\beta_1}, \varepsilon_{p_2}, \sqrt[p_2]{\beta_2}, \dots, \varepsilon_{p_k}$ y $\sqrt[p_k]{\beta_k}$ obtenemos una extensión radical de E , como queríamos. $\square$

Teorema 6.39. *Sea $f \in K[X]$. Si $\text{Gal}_K(f)$ es un grupo resoluble, entonces f es resoluble por radicales sobre K .*

Demostración. La extensión $E_f : K$ es normal y finita y, por hipótesis, el grupo $\text{Gal}(E_f/K)$ es resoluble.

Por la proposición 6.38, E_f está contenido en una extensión radical de K . $\square$

Ahora nos proponemos ver que no todas las ecuaciones son resolubles por radicales.

Proposición 6.40. *Si $f \in K[X]$ tiene m ceros diferentes, el grupo $\text{Gal}_K(f)$ es isomorfo a un subgrupo de S_m .*

Demostración. Sean $E_f = K(\alpha_1, \dots, \alpha_m)$ un cuerpo de escisión para f sobre K y $f = c(X - \alpha_1)^{r_1} \dots (X - \alpha_m)^{r_m} \in E_f[X]$.

Si $\sigma \in \text{Gal}_K(f) = \text{Gal}(E_f/K)$, para todo $i : 1, \dots, m$, se tiene que $\sigma(\alpha_i) \in \{\alpha_1, \dots, \alpha_m\}$ y, como σ es biyectiva, $\{\alpha_1, \dots, \alpha_m\} = \{\sigma(\alpha_1), \dots, \sigma(\alpha_m)\}$. Por tanto, la aplicación

$$\begin{aligned} \text{Gal}_K(f) &\rightarrow S_m \\ \sigma &\mapsto \sigma|_{\{\alpha_1, \dots, \alpha_m\}} \end{aligned}$$

es un homomorfismo de grupos inyectivo (si $\sigma, \tau \in \text{Gal}_K(f)$ con $\sigma|_{\{\alpha_1, \dots, \alpha_m\}} = \tau|_{\{\alpha_1, \dots, \alpha_m\}}$, ya que $E_f = K(\alpha_1, \dots, \alpha_m)$, es obvio que $\sigma = \tau$) y así, $\text{Gal}_K(f)$ es isomorfo a un subgrupo de S_m . $\square$

Corolario 6.41. *Si $f \in K[X]$ y $\partial f \leq 4$, f es resoluble por radicales sobre K .*

Demostración. Si r es el número de raíces diferentes de f , entonces $r \leq \partial f \leq 4$ y, por 6.6 y la proposición 6.16, el grupo S_r es resoluble.

Por la proposición anterior, $\text{Gal}_K(f)$ es isomorfo a un subgrupo del grupo S_r y es resoluble, por la proposición 6.12. Utilizando el teorema 6.34, f es resoluble por radicales sobre K . $\square$

A continuación probaremos que hay polinomios de grado ≥ 5 que no son resolubles por radicales.

Lema 6.42. *Sea p un primo. Si G es un subgrupo de S_p que contiene un p -ciclo y una trasposición, entonces $G = S_p$.*

Demostración. Como toda permutación se descompone en producto de trasposiciones bastará comprobar que G contiene todas las trasposiciones de S_p .

Sea $\sigma \in G$ un p -ciclo. Si $\tau = (i_1, i_2) \in G$, existe un entero s , $0 < s < p$, tal que $\sigma^s(i_1) = i_2$ y $\sigma^s \in G$ también es un p -ciclo ya que los únicos elementos de orden p en S_p son los p -ciclos. Así, haciendo un cambio de notación, podemos suponer que $\tau = (1, 2)$ y $\sigma^s = (1, 2, \dots, p) \equiv \gamma$ y se tiene que:

$$\begin{aligned}\gamma(1, 2)\gamma^{-1} &= (2, 3) \in G, \\ \gamma(2, 3)\gamma^{-1} &= (3, 4) \in G, \\ &\dots \\ \gamma(p-2, p-1)\gamma^{-1} &= (p-1, p) \in G.\end{aligned}$$

Como consecuencia,

$$\forall h : 1, \dots, p-2, \quad (h, h+2) = (h, h+1)(h+1, h+2)(h, h+1) \in G.$$

Y como toda trasposición es de la forma (h, k) con $h < k$, repitiendo el proceso, se tiene que $(h, k) \in G$. $\square$

Lema 6.43. *Si $f \in \mathbb{Q}[X]$ es un polinomio irreducible en $\mathbb{Q}[X]$ de grado primo p y con exactamente dos raíces complejas no reales, entonces $\text{Gal}_{\mathbb{Q}}(f) \cong S_p$.*

Demostración. Puesto que $\text{Car } \mathbb{Q} = 0$, el polinomio f es separable y por lo tanto existen p elementos diferentes $\alpha_1, \dots, \alpha_p \in \mathbb{C}$ tales que

$$f = c \prod_{i=1}^p (X - \alpha_i).$$

Sea $E_f = \mathbb{Q}(\alpha_1, \dots, \alpha_p) \subset \mathbb{C}$ un cuerpo de escisión para f sobre $\mathbb{Q}$.

Sabemos que $\text{Gal}_{\mathbb{Q}}(f)$ es isomorfo a un subgrupo H del grupo S_p y así, $|\text{Gal}_{\mathbb{Q}}(f)| = |H|$. Teniendo en cuenta que $E_f : \mathbb{Q}$ es una extensión de Galois finita, $[E_f : \mathbb{Q}] = |\text{Gal}_{\mathbb{Q}}(f)| = |H|$.

Además, puesto que $\mathbb{Q} \subset \mathbb{Q}(\alpha_i) \subset E_f$ y que $\text{Irr}(\alpha_i, \mathbb{Q}) = c^{-1}f$, se tiene que

$$[E_f : \mathbb{Q}] = [E_f : \mathbb{Q}(\alpha_i)] [\mathbb{Q}(\alpha_i) : \mathbb{Q}] = [E_f : \mathbb{Q}(\alpha_i)] \cdot p.$$

En consecuencia, $p \mid |H|$.

Por el Teorema de Cauchy, existe $\sigma \in H$ que es de orden p que, por tanto, es un p -ciclo.

Supongamos ahora que α_1, α_2 son las únicas raíces complejas no reales de f . Dado que $f \in \mathbb{Q}[X] \subset \mathbb{R}[X]$, como α_1 es una raíz de f , se verifica que $\overline{\alpha_1}$ es también raíz de f por lo cual $\alpha_2 = \overline{\alpha_1}$, ya que $\alpha_1 \neq \overline{\alpha_1}$; además, para cada $i : 3, \dots, p$, $\alpha_i = \overline{\alpha_i}$. Por tanto, la conjugación $(-): \mathbb{C} \rightarrow \mathbb{C}$ se restringe a un $\mathbb{Q}$ -automorfismo

$$\tau: E_f \rightarrow E_f.$$

El automorfismo $\tau \in \text{Gal}_{\mathbb{Q}}(f)$ está definido por $\tau(\alpha_1) = \overline{\alpha_1} = \alpha_2$, $\tau(\alpha_2) = \overline{\alpha_2} = \alpha_1$, y $\tau(\alpha_i) = \alpha_i$ para $i = 3, \dots, p$, en consecuencia, la trasposición $\tau|_{\{\alpha_1, \dots, \alpha_m\}} = (\alpha_1, \alpha_2) \in H$. Puesto que H contiene un p -ciclo y una trasposición, por el lema anterior, $H = S_p$. $\square$

Teorema 6.44 (Teorema de Abel). *Para cada $n \geq 5$ existe una ecuación algebraica $f(X) = 0$ con coeficientes racionales y de grado n que no es resoluble por radicales sobre $\mathbb{Q}$.*

Demostración. Bastará con encontrar un polinomio $f \in \mathbb{Q}[X]$ de grado 5 que no sea resoluble por radicales sobre $\mathbb{Q}$, ya que para $n > 5$, el polinomio $g(X) = X^{n-5} \cdot f(X)$ es de grado n , tiene el mismo cuerpo de escisión que f sobre $\mathbb{Q}$ y, por lo tanto, el mismo grupo de Galois.

Sea $f(X) = 2X^5 - 10X + 5 \in \mathbb{Q}[X]$. Por el criterio de Eisenstein ($p = 5$), f es irreducible sobre $\mathbb{Q}$ (separable sobre $\mathbb{Q}$) y tiene exactamente dos raíces complejas no reales.

En efecto, la función continua $f: \mathbb{R} \rightarrow \mathbb{R}$ es creciente en el intervalo $(-\infty, -1)$, tiene un máximo en $x = -1$, es decreciente en el intervalo $(-1, 1)$, tiene un mínimo en $x = 1$,

y es creciente en el intervalo $(1, \infty)$. Además $f(-2) < 0 < f(-1)$, $f(1) < 0 < f(2)$. Por todo ello, como consecuencia del Teorema de Bolzano, la ecuación $f(X) = 0$ tiene tres raíces reales $\alpha_1 \in [-2, -1]$, $\alpha_2 \in [-1, 1]$, $\alpha_3 \in [1, 2]$. Por el Teorema de Rolle se puede afirmar que éstas son las únicas raíces reales de f . Las otras dos son elementos de la clausura algebraica de $\mathbb{Q}$ que está contenida en $\mathbb{C}$.

Entonces el polinomio f satisface las hipótesis del lema anterior y así $\text{Gal}_{\mathbb{Q}}(f) \cong S_5$, que, como ya hemos probado en el teorema 6.17, es un grupo no resoluble. Finalmente, aplicando el teorema 6.34, se tiene el resultado. $\square$

Capítulo 7

Aplicaciones

7.1. El Teorema Fundamental del Álgebra

No existe una demostración puramente algebraica de este teorema, pues aunque $\mathbb{C}$ se construye a partir de $\mathbb{R}$ por una técnica algebraica, $\mathbb{R}$ se construye con el uso de ideas del Análisis, como sucesiones de Cauchy o cortaduras de Dedekind. Usando teoría de Galois y teoría de grupos finitos, daremos una demostración del teorema que solo usa un resultado de Análisis real, que se prueba en cualquier curso elemental de esta materia ya que es una de las aplicaciones clásicas del Teorema de Bolzano.

Lema 7.1. *Si $f \in \mathbb{R}[X]$ tiene grado impar, entonces f tiene algún cero en $\mathbb{R}$.*

Observación 7.2.

Los únicos polinomios irreducibles en $\mathbb{R}[X]$ de grado impar son los lineales.

Esto significa que si $F : \mathbb{R}$ es una extensión con $[F : \mathbb{R}] = q$ y q es impar, entonces $q = 1$ y $F = \mathbb{R}$ ya que, por el Teorema del elemento primitivo (4.17), existe $\alpha \in F$ tal que $F = \mathbb{R}(\alpha)$ y $[\mathbb{R}(\alpha) : \mathbb{R}] = \partial \text{Irr}(\alpha, \mathbb{R}) = q$, por lo cual, q tiene que ser 1.

Lema 7.3. *Todo elemento de $\mathbb{C}$ tiene raíz cuadrada en $\mathbb{C}$.*

Demostración. Sea $\alpha = a + bi \in \mathbb{C}$. Los números reales $a' = \frac{a + \sqrt{a^2 + b^2}}{2}$ y $b' = \frac{-a + \sqrt{a^2 + b^2}}{2}$ son no negativos y, por tanto, existen $c, d \in \mathbb{R}$ tales que $c^2 = a'$ y $d^2 = b'$. Es fácil comprobar que el número complejo $\beta = c + di$ es tal que $\beta^2 = \alpha$. $\square$

Lema 7.4. *$\mathbb{C}$ no admite extensiones de grado 2.*

Demostración. Como toda extensión de grado 2 es simple, es suficiente comprobar que todo polinomio de grado 2 en $\mathbb{C}[X]$ es reducible. En efecto, si $f = aX^2 + bX + c \in \mathbb{C}[X]$, con $a \neq 0$, por el lema anterior $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \in \mathbb{C}$ y

$$f = a \left(X - \frac{-b + \sqrt{b^2 - 4ac}}{2a} \right) \left(X - \frac{-b - \sqrt{b^2 - 4ac}}{2a} \right).$$

Así, f escinde en $\mathbb{C}[X]$ y f no es irreducible sobre $\mathbb{C}$. $\square$

Teorema 7.5. *El cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado.*

Demostración. Utilizando la proposición 3.14, bastará con demostrar que $\mathbb{C}$ no tiene extensiones finitas propias.

Supongamos que $F : \mathbb{C}$ es una extensión finita. Como $[\mathbb{C} : \mathbb{R}] = 2$, la extensión $F : \mathbb{R}$ también es finita. Si E es una clausura normal de F sobre $\mathbb{R}$, se tiene una torre de cuerpos

$$\mathbb{R} \subset \mathbb{C} \subset F \subset E,$$

en donde $E : \mathbb{R}$ es normal y finita.

Si $G = \text{Gal}(E/\mathbb{R})$, puesto que estamos en característica 0, la extensión $E : \mathbb{R}$ es de Galois finita y $|G| = [E : \mathbb{R}]$.

Por el Teorema del grado (1.6), teniendo en cuenta que $[\mathbb{C} : \mathbb{R}] = 2$, se verifica que

$$|G| = [E : \mathbb{R}] = [E : \mathbb{C}][\mathbb{C} : \mathbb{R}] = 2^m q, \text{ con } m \geq 1 \text{ y } q \text{ impar.}$$

Sea ahora H un 2-subgrupo de Sylow de G , es decir, H es un subgrupo de G tal que $|H| = 2^m$. Aplicando el Teorema fundamental de la teoría de Galois (5.13) a la extensión $E : \mathbb{R}$, si E^H es el cuerpo fijo de H , se tiene que

$$[E^H : \mathbb{R}] = \frac{[E : \mathbb{R}]}{[E : E^H]} = \frac{|G|}{|H|} = \frac{2^m q}{2^m} = q \text{ (impar)}.$$

Utilizando la observación 7.2, se deduce que $q = 1$. Así, $E^H = \mathbb{R}$, $|G| = |H| = 2^m$, con $m \geq 1$, es decir, $G = H$ es un 2-grupo.

La extensión $E : \mathbb{C}$ es de Galois finita puesto que $E : \mathbb{R}$ es de Galois finita y $\mathbb{R} \subset \mathbb{C} \subset E$. Si $H_1 = \text{Gal}(E/\mathbb{C})$, entonces

$$|H_1| = |\text{Gal}(E/\mathbb{C})| = [E : \mathbb{C}] = \frac{[E : \mathbb{R}]}{[\mathbb{C} : \mathbb{R}]} = \frac{|G|}{2} = 2^{m-1}.$$

Veamos que $m = 1$ o, equivalentemente, que $H_1 = \{1\}$:

Si $m > 1$, como H_1 es un 2-grupo tendrá un subgrupo H_2 de orden 2^{m-2} .

Aplicando el Teorema fundamental de la teoría de Galois (5.13) a la extensión $E : \mathbb{C}$, si E^{H_2} es el cuerpo fijo de H_2 , se tiene que

$$\mathbb{C} \subset E^{H_2} \subset E \text{ con } [E^{H_2} : \mathbb{C}] = \frac{[E : \mathbb{C}]}{[E : E^{H_2}]} = \frac{|H_1|}{|H_2|} = 2$$

y E^{H_2} sería una extensión de $\mathbb{C}$ de grado 2, en contradicción con el lema 7.4.

Por tanto, ya que $E : \mathbb{C}$ es una extensión de Galois finita, se verifica que

$$[E : \mathbb{C}] = |\text{Gal}(E/\mathbb{C})| = |H_1| = 1,$$

de modo que $E = \mathbb{C}$ y, como $\mathbb{C} \subset F \subset E$, se obtiene que $F = \mathbb{C}$. □

7.2. Construcción de polígonos regulares

El objetivo de esta sección es ver para que valores de “ n ” se puede construir, con regla y compás, un polígono regular de n lados.

Considerando el polígono regular inscrito en la circunferencia de radio unidad, este problema es equivalente a dividir la circunferencia unidad en “ n ” partes iguales, construir el ángulo $\sphericalangle \frac{2\pi}{n}$, construir la raíz n -ésima primitiva de la unidad $\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, construir el punto $\left(\cos \frac{2\pi}{n}, \sin \frac{2\pi}{n} \right)$ o a que $\cos \frac{2\pi}{n}$ sea un número real constructible.

Ya se sabía antes de Gauss que la respuesta es afirmativa para $n = 3, 4, 5, 6$ y 15 . En cambio, el polígono de 9 lados no es constructible ya que el ángulo de $20^\circ = \frac{2\pi}{18}$ no lo es, como ya hemos visto en la proposición 2.13.

Los griegos ya conocían que la construcción era posible si $n = 2^k, 3 \cdot 2^k$ o $5 \cdot 2^k$.

El problema de la constructibilidad del polígono de 7 lados, el primer caso no conocido, fue estudiado por Gauss en 1796. Utilizando, por primera vez, fuertes herramientas algebraicas, Gauss dio una respuesta parcial del problema demostrando que los polígonos de n lados, con n primo de la forma $2^k + 1$, son constructibles, por ejemplo $n = 17$. Más tarde Wantzel, en 1837, completó el resultado caracterizando exactamente los enteros n para los que el n -ágono regular es constructible.

Definición 7.6. Se llaman *primos de Fermat* a los números primos de la forma $2^{2^n} + 1$, con $n \in \mathbb{N}$.

Estos primos se denominan así puesto que Fermat, observando que $2^{2^0} + 1 = 3$, $2^{2^1} + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$ y $2^{2^4} + 1 = 65.537$ son números primos, conjeturó que $2^{2^n} + 1$ es primo $\forall n \geq 0$. Sin embargo, Euler demostró que el quinto número de Fermat $2^{2^5} + 1 = 4.294.967.297 = 641 \cdot 6700417$ no es primo. Actualmente se sabe que $2^{2^n} + 1$ no es primo si $5 \leq n \leq 16$ y no se conoce si existen otros primos de Fermat.

Lema 7.7. Si $p = 2^m + 1$ es un número primo, entonces p es un primo de Fermat, es decir, $m = 2^n$, para algún entero $n \geq 0$.

Demostración. Si m tuviese un divisor impar $q > 1$, tendríamos $m = qr$ y

$$p = 2^{qr} + 1 = (2^r + 1)(2^{r(q-1)} - 2^{r(q-2)} + \dots - 2^r + 1).$$

Teniendo en cuenta que $q > 1$, se tiene que $1 < 2^r + 1 < 2^{qr} + 1 = p$ y así p tendría un divisor propio y no sería primo.

Nótese que hemos utilizado que $X^q + 1 = (X + 1)(X^{q-1} - X^{q-2} + X^{q-3} - \dots - X + 1)$, al ser q impar. $\square$

Teorema 7.8 (Teorema de Gauss-Wantzel). Sea $n > 2$ un número entero. Son equivalentes:

1. El n -ágono regular es constructible.
2. $\varphi(n)$ es una potencia de 2.
3. Existen $m \in \mathbb{N}$ y primos de Fermat distintos $p_1, \dots, p_r$ tales que

$$n = 2^m p_1 \cdots p_r.$$

Demostración. Sean $\theta = \frac{2\pi}{n}$, $\varepsilon = \cos \theta + i \operatorname{sen} \theta$ y $\varepsilon^{-1} = \frac{\bar{\varepsilon}}{\|\varepsilon\|} = \bar{\varepsilon}$.

1) $\Rightarrow$ 2) Como $\varepsilon + \bar{\varepsilon} = 2 \cos \theta$, se verifica que $\cos \theta = \frac{\varepsilon + \varepsilon^{-1}}{2} \in \mathbb{Q}(\varepsilon)$ y, entonces,

$$\mathbb{Q} \subset \mathbb{Q}(\cos \theta) \subset \mathbb{Q}(\varepsilon).$$

Por el Teorema del grado (1.6),

$$\varphi(n) = [\mathbb{Q}(\varepsilon) : \mathbb{Q}] = [\mathbb{Q}(\varepsilon) : \mathbb{Q}(\cos \theta)] [\mathbb{Q}(\cos \theta) : \mathbb{Q}].$$

Por hipótesis $\cos \theta$ es un número real constructible y, por el teorema 2.10, $[\mathbb{Q}(\cos \theta) : \mathbb{Q}]$ es una potencia de 2.

Además,

$$(X - \varepsilon)(X - \bar{\varepsilon}) = X^2 - (2 \cos \theta)X + 1 \in \mathbb{Q}(\cos \theta)[X]$$

y entonces $[\mathbb{Q}(\cos \theta)(\varepsilon) : \mathbb{Q}(\cos \theta)] = 1$ o 2 .

Por todo ello, $\varphi(n)$ es una potencia de 2.

2) $\Rightarrow$ 1) Por las proposiciones 6.22 y 6.25 la extensión $\mathbb{Q}(\varepsilon) : \mathbb{Q}$ es de Galois finita con grupo de Galois, G , abeliano de orden $\varphi(n)$ que, por hipótesis, es una potencia de 2.

Puesto que $\text{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q}(\cos \theta))$ es un subgrupo normal de G , por el corolario 5.14, $\mathbb{Q}(\cos \theta) : \mathbb{Q}$ es una extensión de Galois finita y

$$H = \text{Gal}(\mathbb{Q}(\cos \theta)/\mathbb{Q}) \simeq G / \text{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q}(\cos \theta)),$$

por lo cual H es un grupo abeliano de orden 2^r , para algún $r \geq 0$. Por tanto, existe una cadena de subgrupos de H

$$H = H_0 \supset H_1 \supset \cdots \supset H_r = \{e\}$$

tal que $H_i \triangleleft H_{i-1}$ y $|H_{i-1}/H_i| = 2$, $\forall i : 1, \dots, r$.

Por el Teorema fundamental de la teoría de Galois (5.13) aplicado a la extensión $\mathbb{Q}(\cos \theta) : \mathbb{Q}$, denotando $E = \mathbb{Q}(\cos \theta)$, tenemos una cadena de cuerpos

$$\mathbb{Q} = E^H = E^{H_0} \subset E^{H_1} \subset \cdots \subset E^{H_r} = E = \mathbb{Q}(\cos \theta) \subset \mathbb{R}$$

verificando que, $\forall i : 1, \dots, r$,

$$[E^{H_i} : E^{H_{i-1}}] = \frac{[E : E^{H_{i-1}}]}{[E : E^{H_i}]} = \frac{|H_{i-1}|}{|H_i|} = 2.$$

Aplicando el Teorema fundamental sobre constructibilidad (2.10), se obtiene que $\cos \theta$ es un número real constructible.

2) $\Leftrightarrow$ 3) Si $n = p_1^{r_1} \cdots p_t^{r_t}$ es la factorización de n en números primos, hemos visto que $\varphi(n) = (p_1 - 1) \cdots (p_t - 1) p_1^{r_1-1} \cdots p_t^{r_t-1}$, por tanto, $\varphi(n)$ es potencia de 2 si, y

solo si, para cada $p_j \neq 2$ se verifica que $r_j = 1$ y $p_j - 1$ es potencia de 2 si, y solo si, para cada $p_j \neq 2$ se tiene que $r_j = 1$ y p_j es un primo de Fermat. $\square$

Apéndice A

A.1. El anillo de los polinomios

Sea R un anillo conmutativo. El conjunto de todos *los polinomios con coeficientes en R en la variable o indeterminada X* ,

$$R[X] = \left\{ f = \sum_{i \in \mathbb{N}} a_i X^i \mid a_i \in R \text{ y } a_i = 0, \text{ para casi todo } i \right\},$$

tiene estructura de anillo conmutativo, definiendo la suma y el producto de dos elementos $f = \sum_i a_i X^i$, $g = \sum_i b_i X^i \in R[X]$ como:

$$f + g = \sum_i (a_i + b_i) X^i \text{ y } fg = \sum_i c_i X^i, \text{ con } c_i = \sum_{k+r=i} a_k b_r.$$

La aplicación

$$\begin{aligned} \lambda: R &\rightarrow R[X] \\ a &\mapsto aX^0 \equiv a \end{aligned}$$

es un homomorfismo inyectivo de anillos, que permite identificar R con un subanillo, $\lambda(R)$, de $R[X]$.

Definición A.1. Si $f = \sum_i a_i X^i \in R[X]$ se define el *grado de f* , ∂f , como

$$\partial f := \begin{cases} \text{máx } \{i \in \mathbb{N} \mid a_i \neq 0\} & \text{si } f \neq 0 \\ -\infty & \text{si } f = 0 \end{cases}$$

a_0 se llama *término independiente* de f .

Si $f \neq 0$ y $\partial f = n$, a_n se llama *coeficiente principal* de f , y si $a_n = 1$ se dice que f es *mónico*.

Los polinomios de grado cero se llaman *polinomios constantes*.

Proposición A.2. Sean $f, g \in R[X]$. Se verifica que:

1. $\partial(f \pm g) \leq \max \{\partial f, \partial g\}$.
2. $\partial(fg) \leq \partial f + \partial g$.
3. Si el coeficiente principal de f o el de g son no divisores de cero, entonces

$$\partial(fg) = \partial f + \partial g.$$

Todas estas propiedades se verifican si $f, g, f + g$ o fg son 0 adoptando el convenio siguiente: $-\infty < i, -\infty + (-\infty) = -\infty$ y $-\infty + i = -\infty, \forall i \in \mathbb{N}$.

Es evidente que en un dominio entero siempre se verifica que $\partial(fg) = \partial f + \partial g$.

Corolario A.3.

1. R es un dominio entero si, y solo si, $R[X]$ es un dominio entero.
2. Si R es un dominio entero, $\mathcal{U}(R[X]) = \{a \equiv aX^0 \mid a \in \mathcal{U}(R)\}$.

Demostración. Vamos a demostrar 2). Si $f \in \mathcal{U}(R[X])$ existe $g \in R[X]$ tal que $fg = 1$, y como $0 = \partial 1 = \partial(fg) = \partial f + \partial g$, se tiene que $\partial f = 0$ y $\partial g = 0$. Por tanto, $f = aX^0, a \neq 0, g = bX^0, b \neq 0$ y $ab = 1$ y así, $a \in \mathcal{U}(R)$. $\square$

Proposición A.4 (Propiedad universal del anillo de polinomios).

Si $\varphi: R \rightarrow S$ es un homomorfismo de anillos conmutativos y $\alpha \in S$, existe un único homomorfismo de anillos $\varphi_\alpha: R[X] \rightarrow S$ tal que $\varphi_\alpha(X) = \alpha$ y $\varphi_\alpha(a) = \varphi(a) \forall a \in R$.

$$\text{Si } f = \sum_{i=0}^n a_i X^i \in R[X], \varphi_\alpha(f) = \sum_{i=0}^n \varphi(a_i) \alpha^i.$$

Ejemplos A.5. Sean R y S anillos conmutativos.

1) Si R es un subanillo de S , $\varphi = i: R \hookrightarrow S$ es el homomorfismo inclusión y $\alpha \in S$, por la propiedad universal anterior, la aplicación

$$\begin{aligned} \varphi_\alpha: R[X] &\rightarrow S \\ f = \sum_{i=0}^n a_i X^i &\mapsto \sum_{i=0}^n a_i \alpha^i \equiv f(\alpha) \end{aligned}$$

es un homomorfismo de anillos, que se llama homomorfismo “evaluación en α ”.

Nótese que $(f + g)(\alpha) = f(\alpha) + g(\alpha)$ y $(fg)(\alpha) = f(\alpha)g(\alpha)$.

Si $f(\alpha) = 0$ se dice que α es un *cero* o una *raíz* de f .

2) Si $\varphi: R \rightarrow S$ es un homomorfismo de anillos

$$\begin{array}{ccc} \lambda' \circ \varphi: & R & \rightarrow S & \rightarrow S[X] \\ & a & \mapsto \varphi(a) & \mapsto \varphi(a)X^0 \equiv \varphi(a) \end{array}$$

es un homomorfismo de anillos, y como $X \in S[X]$, por la propiedad universal anterior, existe un único homomorfismo de anillos $\bar{\varphi}: R[X] \rightarrow S[X]$ tal que $\bar{\varphi}(X) = X$ y que hace conmutativo el diagrama siguiente:

$$\begin{array}{ccc} R & \xrightarrow{\lambda} & R[X] \\ \varphi \downarrow & & \downarrow \bar{\varphi} \\ S & \xrightarrow{\lambda'} & S[X] \end{array}$$

Esto significa que, $\bar{\varphi}\left(\sum_{i=0}^n a_i X^i\right) = \sum_{i=0}^n \varphi(a_i) X^i$.

Nótese que:

φ es inyectivo (sobreyectivo) $\Leftrightarrow \bar{\varphi}$ es inyectivo (sobreyectivo).

En particular, si $p \in \mathbb{N}$, $p \geq 2$, el homomorfismo canónico $\pi_p: \mathbb{Z} \rightarrow \mathbb{Z}_p$ induce el homomorfismo de anillos

$$\begin{array}{ccc} \bar{\pi}_p: & \mathbb{Z}[X] & \rightarrow \mathbb{Z}_p[X] \\ & f = \sum_{i=0}^n a_i X^i & \mapsto \bar{f} = \sum_{i=0}^n \bar{a}_i X^i \end{array}$$

llamado *reducción módulo p* .

A.2. Factorización en $K[x]$

En esta sección K es un cuerpo.

Sabemos que:

1) $K[X]$ es un dominio euclídeo y, por tanto, un dominio de ideales principales y de factorización única.

2) $\mathcal{U}(K[X]) = \{a \equiv aX^0 \mid a \in K, a \neq 0\}$.

3) $f \in K[X]$ es *irreducible en $K[X]$* o *sobre K* si verifica:

i) $\partial f \geq 1$ ($f \neq 0$ y $f \notin \mathcal{U}(K[X])$),

ii) Si $f = gh$ en $K[X]$, entonces $\partial g = 0$ o $\partial h = 0$ (es decir, g o h son unidades en $K[X]$).

Nuestro objetivo es determinar los polinomios irreducibles en $K[X]$, en especial en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.

Proposición A.6.

1. Todo polinomio lineal en $K[X]$, $f = aX + b$, $a \neq 0$, tiene un cero en K y es irreducible sobre K .

2. Si $f \in K[X]$ con $\partial f = 2$ o 3 , entonces f es irreducible sobre K si, y solo si, no tiene ceros en K .

Ejemplos A.7.

1) $X^2 + 1 \in \mathbb{R}[X]$ no tiene ceros en $\mathbb{R}$ y, por tanto, es irreducible sobre $\mathbb{R}$.

2) $2X + 2 = 2(X + 1) \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$, no es irreducible sobre $\mathbb{Z}$ pero es irreducible sobre $\mathbb{Q}$.

3) La propiedad 2) de la proposición anterior no es cierta para polinomios de grado mayor que 3, por ejemplo, el polinomio $(X^2 + 1)^2$ no tiene ceros en $\mathbb{Q}$ ni en $\mathbb{R}$, pero es reducible sobre ambos cuerpos.

A.3. Irreducibilidad en $\mathbb{C}[X]$

Teorema A.8 (Teorema fundamental del Álgebra). $\mathbb{C}$ es un cuerpo algebraicamente cerrado.

Nótese que si $f \in \mathbb{C}[X]$, $\partial f = n \geq 1$, entonces $f = f_1 \cdots f_n$ con $f_i = a_i X + b_i = a_i \left(X - \left(-\frac{b_i}{a_i} \right) \right) \in \mathbb{C}[X]$, por tanto existen $c, \alpha_1, \dots, \alpha_n \in \mathbb{C}$ tales que

$$f = c(X - \alpha_1) \cdots (X - \alpha_n).$$

A.4. Irreducibilidad en $\mathbb{R}[X]$

Sea $f = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{R}[X] \subset \mathbb{C}[X]$, con $\partial f = n \geq 1$.

Hemos visto que $f = a_n(X - \alpha_1) \cdots (X - \alpha_n)$, donde $\alpha_1, \dots, \alpha_n$ son ceros de f en $\mathbb{C}$.

Puesto que la conjugación

$$\begin{aligned} -: \mathbb{C} &\rightarrow \mathbb{C} \\ a + bi &\mapsto \overline{a + bi} = a - bi \end{aligned}$$

es un isomorfismo de anillos que deja fijos los reales,

$$\alpha \text{ es cero de } f \Leftrightarrow a_0 + a_1 \alpha + \cdots + a_n \alpha^n = 0 \Leftrightarrow \overline{a_0 + a_1 \alpha + \cdots + a_n \alpha^n} = \bar{0}$$

$$\Leftrightarrow a_0 + a_1\bar{\alpha} + \cdots + a_n\bar{\alpha}^n = 0 \Leftrightarrow f(\bar{\alpha}) = 0 \Leftrightarrow \bar{\alpha} \text{ cero de } f.$$

Por tanto, si $\alpha \in \mathbb{C} \setminus \mathbb{R}$ es cero de f , entonces $\bar{\alpha} \in \mathbb{C} \setminus \mathbb{R}$ también es cero de f y $\alpha \neq \bar{\alpha}$; además $(X - \alpha)(X - \bar{\alpha}) = X^2 - (\alpha + \bar{\alpha})X + \alpha\bar{\alpha} \in \mathbb{R}[X]$.

En consecuencia, existen $\beta_1, \dots, \beta_s \in \mathbb{R}$ y $\gamma_1, \dots, \gamma_r \in \mathbb{C} \setminus \mathbb{R}$ con $s, r \geq 0$ y $s + 2r = n$ tales que en $\mathbb{R}[X]$,

$$f = a_n(X - \beta_1) \cdots (X - \beta_s)(X^2 - (\gamma_1 + \bar{\gamma}_1)X + \gamma_1\bar{\gamma}_1) \cdots (X^2 - (\gamma_r + \bar{\gamma}_r)X + \gamma_r\bar{\gamma}_r).$$

En esta factorización los factores cuadráticos son irreducibles en $\mathbb{R}[X]$ puesto que no tienen ceros reales, ya que de tenerlos habría dos factorizaciones distintas en el dominio de factorización única $\mathbb{C}[X]$.

Proposición A.9. Sea $f \in \mathbb{R}[X]$,

f es irreducible en $\mathbb{R}[X] \Leftrightarrow \partial f = 1$ o $\partial f = 2$ y f no tiene ceros reales.

Observaciones A.10.

1) $f = aX^2 + bX + c \in \mathbb{R}[X]$, con $a \neq 0$, no tiene ceros reales $\Leftrightarrow b^2 - 4ac < 0$.

2) Todo polinomio de grado impar en $\mathbb{R}[X]$ tiene al menos un cero en $\mathbb{R}$.

A.5. Irreducibilidad en $\mathbb{Q}[X]$ y en $\mathbb{Z}[X]$

El estudio de la irreducibilidad en $\mathbb{Q}[X]$ y en $\mathbb{Z}[X]$ es más complicado, de hecho, veremos que existen polinomios irreducibles de todos los grados. Nuestro próximo objetivo es estudiar algunos criterios de irreducibilidad sobre ambos anillos.

Proposición A.11. Sea $f \in \mathbb{Z}[X]$ con $\partial f \geq 1$.

Si $f = gh$ en $\mathbb{Q}[X]$, entonces existen $g^*, h^* \in \mathbb{Z}[X]$ tales que $f = g^*h^*$, $\partial g = \partial g^*$ y $\partial h = \partial h^*$.

Demostración. Existe $a \in \mathbb{Z}^+$ tal que $ag = g_1 \in \mathbb{Z}[X]$ y $\partial g = \partial g_1$ (por ejemplo, tomando como a el producto de los denominadores de los coeficientes de g). Análogamente, existe $b \in \mathbb{Z}^+$ tal que $bh = h_1 \in \mathbb{Z}[X]$ y $\partial h = \partial h_1$. Así, $ab \in \mathbb{Z}^+$ y $abf = g_1h_1$ en $\mathbb{Z}[X]$, con $\partial g = \partial g_1$ y $\partial h = \partial h_1$. Tomamos el menor $n \in \mathbb{Z}^+$ tal que

$$nf = g^*h^* \text{ en } \mathbb{Z}[X], \partial g^* = \partial g \text{ y } \partial h^* = \partial h \quad (1)$$

La proposición quedará demostrada probando que $n = 1$.

Si $n > 1$, existe un primo p que divide a n . Considerando la reducción módulo p ,

$$\begin{aligned} \overline{\pi}_p: \mathbb{Z}[X] &\rightarrow \mathbb{Z}_p[X] \\ f = \sum_{i=0}^n a_i X^i &\mapsto \sum_{i=0}^n \overline{a}_i X^i \end{aligned}$$

se tiene que $0 = \overline{\pi}_p(nf) = \overline{\pi}_p(g^*h^*) = \overline{\pi}_p(g^*)\overline{\pi}_p(h^*)$.

Sin embargo, por la elección de n , p no puede dividir a todos los coeficientes de g^* , ni de h^* (en otro caso, n/p verificaría la condición (1)); por tanto, $\overline{\pi}_p(g^*) \neq 0$ y $\overline{\pi}_p(h^*) \neq 0$ y, como $\mathbb{Z}_p[X]$ es un dominio entero, $\overline{\pi}_p(g^*)\overline{\pi}_p(h^*) \neq 0$ con lo cual se obtiene una contradicción. $\square$

Definición A.12. Sea $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, $f \neq 0$. Diremos que f es *primitivo* si $m.c.d.(a_0, \dots, a_n) = 1$, es decir no existe ningún primo que divida a todos sus coeficientes.

Proposición A.13. Sea $f \in \mathbb{Z}[X]$ con $\partial f \geq 1$.

1. Si f es irreducible en $\mathbb{Z}[X]$, entonces es irreducible en $\mathbb{Q}[X]$.
2. Si f es irreducible en $\mathbb{Q}[X]$ y primitivo, entonces es irreducible en $\mathbb{Z}[X]$.

Demostración.

1) Es consecuencia de la proposición anterior.

2) Si $\partial f \geq 1$, entonces $f \neq 0$ y $f \notin \mathcal{U}(\mathbb{Z}[X])$. Supongamos que $f = gh$, con $g, h \in \mathbb{Z}[X]$. Puesto que f es irreducible en $\mathbb{Q}[X]$, alguno de los polinomios g o h es constante. Supongamos que, por ejemplo, $g = cX^0 \in \mathbb{Z}[X]$, entonces el entero c divide a todos los coeficientes de f y, como f es primitivo, $c \in \mathcal{U}(\mathbb{Z})$, o equivalentemente $g \in \mathcal{U}(\mathbb{Z}[X])$ y, por tanto, f es irreducible en $\mathbb{Z}[X]$. $\square$

Proposición A.14. Sea $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, $f \neq 0$. Si $\alpha = \frac{r}{s} \in \mathbb{Q}$ con $m.c.d.(r, s) = 1$ es un cero de f , entonces $r \mid a_0$ y $s \mid a_n$ en $\mathbb{Z}$.

Corolario A.15. Si $f \in \mathbb{Z}[X]$ es mónico y $\alpha = \frac{r}{s} \in \mathbb{Q}$ con $m.c.d.(r, s) = 1$ es un cero de f , entonces $s \in \{1, -1\}$ y $\alpha \in \mathbb{Z}$.

Proposición A.16 (Criterio de Eisenstein).

Sea $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ con $\partial f = n \geq 1$. Si existe un primo $p \in \mathbb{Z}$ tal que

$$p \mid a_i \quad \forall i : 0, \dots, n-1, \quad p \nmid a_n \quad \text{y} \quad p^2 \nmid a_0,$$

entonces f es irreducible en $\mathbb{Q}[X]$.

Demostración. Si f es reducible en $\mathbb{Q}[X]$, hemos visto en la proposición A.11 que existen $g, h \in \mathbb{Z}[X]$ tales que $f = gh$ con $\partial g = r > 0$ y $\partial h = s > 0$.

Supongamos que $g = \sum_{i=0}^r b_i X^i$ y $h = \sum_{j=0}^s c_j X^j$. Como $\mathbb{Z}$ es un dominio entero, $n = \partial f = \partial g + \partial h = r + s$.

Si consideramos el homomorfismo reducción módulo p

$$\begin{aligned} \bar{\pi}_p: \quad \mathbb{Z}[X] &\quad \rightarrow \quad \mathbb{Z}_p[X] \\ l = \sum_{i=0}^t l_i X^i &\quad \mapsto \quad \bar{l} = \sum_{i=0}^t \bar{l}_i X^i, \end{aligned}$$

en $\mathbb{Z}_p[X]$ tendríamos

$$\bar{f} = \bar{g}\bar{h} \Leftrightarrow \bar{a}_n X^n = \bar{g}\bar{h}$$

con $\partial \bar{g} \leq \partial g$, $\partial \bar{h} \leq \partial h$ y $\partial \bar{f} = \partial f$ ya que $\bar{a}_n \neq \bar{0}$ pues $p \nmid a_n$.

Dado que $\mathbb{Z}_p$ es un dominio entero $\partial \bar{f} = \partial \bar{g} + \partial \bar{h}$ y, en consecuencia, $\partial \bar{g} = \partial g = r$ y $\partial \bar{h} = \partial h = s$.

Teniendo en cuenta que $\mathbb{Z}_p[X]$ es un dominio de factorización única, existen $\bar{u}, \bar{v} \in \mathcal{U}(\mathbb{Z}_p)$ tales que $\bar{g} = \bar{u}X^r$ y $\bar{h} = \bar{v}X^s$. Por tanto, los términos independientes de $\bar{g}$ y $\bar{h}$, $\bar{b}_0$ y $\bar{c}_0$ son $\bar{0}$, lo que significa que $p \mid b_0$ y $p \mid c_0$ y, como consecuencia, $p^2 \mid a_0 = b_0 c_0$, lo que contradice la hipótesis. $\square$

Observación A.17. Es claro, ahora, que existen polinomios irreducibles sobre $\mathbb{Q}$ de cualquier grado, por ejemplo, $X^n - 2$ para cualquier entero $n \geq 1$.

Proposición A.18 (Criterio de Eisenstein al revés (o hacia atrás)).

Sea $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ con $\partial f = n \geq 1$. Si existe un primo $p \in \mathbb{Z}$ tal que

$$p \mid a_i \quad \forall i : 1, \dots, n, \quad p \nmid a_0 \quad \text{y} \quad p^2 \nmid a_n,$$

entonces f es irreducible en $\mathbb{Q}[X]$.

Proposición A.19. Si p es un primo, el polinomio ciclotómico p -ésimo

$$f = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$$

es irreducible en $\mathbb{Q}[X]$ y, como es primitivo, también es irreducible en $\mathbb{Z}[X]$.

Demostración. Si $p = 2$ es obvio.

Supongamos, entonces, que $p > 2$.

Como $(X - 1)f = X^p - 1$, aplicando el homomorfismo evaluación en $X + 1$,

$$\varphi_{X+1}: \mathbb{Z}[X] \rightarrow \mathbb{Z}[X],$$

se tiene que $X\varphi_{X+1}(f) = (X + 1)^p - 1$, de donde se sigue que

$$\begin{aligned} \varphi_{X+1}(f) = f(X + 1) &= \frac{(X + 1)^p - 1}{X} = \frac{\binom{p}{0}X^p + \binom{p}{1}X^{p-1} + \cdots + \binom{p}{p}X^0 - 1}{X} \\ &= \binom{p}{0}X^{p-1} + \binom{p}{1}X^{p-2} + \cdots + \binom{p}{p-1}1 \in \mathbb{Z}[X]. \end{aligned}$$

Teniendo en cuenta que $\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)\cdots(p-i+1)}{i!}$ se obtiene que $p \mid \binom{p}{i} \forall i : 1, \dots, p-1$, $p \nmid \binom{p}{0}$ y $p^2 \nmid \binom{p}{p-1} = p$. Aplicando el criterio de Eisenstein se deduce que $\varphi_{X+1}(f)$ es irreducible en $\mathbb{Q}[X]$.

Veamos que f es irreducible en $\mathbb{Q}[X]$:

En efecto, $\partial f \geq 2$ y si $f = gh$ en $\mathbb{Q}[X]$ con $0 < \partial g, \partial h < \partial f$, entonces $f = g^*h^*$ en $\mathbb{Z}[X]$ con $0 < \partial g^*, \partial h^* < \partial f$, aplicando el homomorfismo φ_{X+1} que conserva el grado, $\varphi_{X+1}(f) = \varphi_{X+1}(g^*)\varphi_{X+1}(h^*)$ sería una factorización no trivial de $\varphi_{X+1}(f)$ en $\mathbb{Q}[X]$ con lo cual se tendría una contradicción. $\square$

Proposición A.20 (Criterio de reducción).

Sea $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ con $\partial f = n \geq 1$. Si existe un primo $p \in \mathbb{Z}$ tal que $p \nmid a_n$ y $\overline{\pi_p}(f) = \overline{f}$ es irreducible en $\mathbb{Z}_p[X]$, entonces f es irreducible en $\mathbb{Q}[X]$.

Demostración. Si f es reducible en $\mathbb{Q}[X]$, hemos visto que existen $g, h \in \mathbb{Z}[X]$ tales que $f = gh$ con $\partial g > 0$ y $\partial h > 0$. Si consideramos el homomorfismo reducción módulo p

$$\begin{aligned} \bar{\pi}_p: \mathbb{Z}[X] &\rightarrow \mathbb{Z}_p[X] \\ l = \sum_{i=0}^t l_i X^i &\mapsto \bar{l} = \sum_{i=0}^t \bar{l}_i X^i, \end{aligned}$$

en $\mathbb{Z}_p[X]$ tendríamos que $\bar{f} = \bar{g}\bar{h}$.

Ya que $p \nmid a_n$, se verifica que $\partial \bar{f} = \partial f = n = \partial g + \partial h$ y, teniendo en cuenta que $\partial \bar{g} \leq \partial g$ y $\partial \bar{h} \leq \partial h$, se deduce que $\partial \bar{g} = \partial g > 0$ y $\partial \bar{h} = \partial h > 0$, de lo que se concluye que $\bar{f}$ es reducible en $\mathbb{Z}_p[X]$ y así se llega a una contradicción. □

Ejemplos A.21.

1) $f = 15X^5 - 9X^3 + 6X - 2$ es irreducible en $\mathbb{Q}[X]$ aplicando el criterio de Eisenstein al revés para $p = 3$.

2) $f = 15X^5 - 8X^3 + 6X - 2$ es irreducible en $\mathbb{Q}[X]$ aplicando el criterio de Eisenstein para $p = 2$.

3) Aplicando el criterio de reducción módulo 3, $f = X^5 - X^4 + 4$ es irreducible en $\mathbb{Q}[X]$ ya que $\bar{f}$ no tiene ceros en $\mathbb{Z}_3$ y no es divisible por ninguno de los polinomios irreducibles mónicos de grado 2 en $\mathbb{Z}_3[X]$ que son $X^2 + X - 1$, $X^2 - X - 1$ y $X^2 + 1$.