# Ecuaciones algebraicas

Ángel del Río Mateos

May 8, 2023

# Contenidos

En estos apuntes supondremos conocidos los contenidos de la asignatura Grupos y Anillos y utilizaremos los apuntes de esta asignatura que están disponibles en los recursos del aula virtual. El acrónimo GyA corresponderá a estos apuntes.

# Introducción

En la escuela aprendimos a resolver ecuaciones lineales

$$aX + b = 0 \tag{0.0.1}$$

y cuadráticas

$$aX^2 + bX + c = 0. \tag{0.0.2}$$

donde $a, b$ y $c$ son números y suponemos que $a \neq 0$. Es bien sabido que la única solución de la ecuación (0.0.1) es $-\frac{b}{a}$ y que la ecuación (0.0.2) tiene a lo sumo dos soluciones que se obtienen al elegir el signo de la raíz cuadrada en la siguiente expresión:

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{0.0.3}$$

En realidad, si $b^2 = 4ac$, entonces la ecuación (0.0.2) tiene una única solución y, si nos restringimos a los números reales, entonces la ecuación no tiene solución si $b^2 - 4ac$ es negativo.

Las ecuaciones (0.0.1) y (0.0.2) aparecen naturalmente en multitud de problemas y sus soluciones son conocidas desde tiempos de los babilonios. Sin embargo, hasta el Renacimiento no se descubrieron fórmulas para resolver las ecuaciones de tercer y cuarto grado, conocidas con el nombre de cúbicas y cuárticas respectivamente. Al parecer Scipione del Ferro (1465?-1526) fue el primero en descubrir una fórmula para resolver ecuaciones de tercer grado. Los descubrimientos de del Ferro no fueron divulgados y fueron redescubiertos más tarde por Nicolo Fontana (1500?-1557), conocido con el nombre de Tartaglia ("El Tartamudo"). El método para resolver la cúbica fue guardado en secreto por Tartaglia hasta que se lo comunicó a Gerolamo Cardano (1501-1576) con la condición de que no lo hiciera público. Sin embargo, Cardano rompió su promesa con Fontana y en 1545 publicó la fórmula de Tartaglia en su libro *Artis Magnae sive de Regulis Algebricis*, más conocido con el nombre de *Ars Magna*. En este libro Cardano no sólo publica la fórmula de Tartaglia, sino también la solución de la cuártica que entretanto había sido descubierta por Ludovico Ferrari (1522-1565).

Vamos a ver como resolver la cúbica

$$aX^3 + bX^2 + cX + d \quad (a \neq 0). \tag{0.0.4}$$

Está claro que poniendo

$$B = \frac{b}{a}, \quad C = \frac{c}{a} \quad \text{y} \quad D = \frac{d}{a}$$

la ecuación anterior toma la forma

$$X^3 + BX^2 + CX + D.$$

Después de la siguiente igualdad

$$X^3 + BX^2 + CX + D = \left(X + \frac{B}{3}\right)^3 + \left(C - \frac{B^2}{3}\right)\left(X + \frac{B}{3}\right) + D + \frac{2B^3}{27} - \frac{BC}{3}$$

podemos poner

$$Y = X + \frac{B}{3}, \quad p = C - \frac{B^2}{3} \quad \text{y} \quad q = D + \frac{2B^3}{27} - \frac{BC}{3}.$$

de forma que la ecuación anterior toma la forma $Y^3 + pY + q = 0$.

Por tanto podemos concentrarnos en las ecuaciones de la siguiente forma:

$$X^3 + pX + q = 0. \tag{0.0.5}$$

Por ejemplo, podemos plantearnos el problema de calcular la longitud de las aristas de un cubo cuyo volumen sea seis unidades mayor que el área total de las caras exteriores. Si $X$ es la longitud de una arista, entonces el volumen es $X^3$ y cada una de las seis caras exteriores tiene una área igual a $X^2$. Por tanto $X$ satisface la ecuación

$$X^3 = 6X^2 + 6 \quad \text{ó} \quad X^3 - 6X^2 - 6 = 0.$$

Poniendo $Y = X - 2$ nos quedamos con la ecuación

$$\begin{aligned} 0 &= (Y+2)^3 - 6(Y+2)^2 - 6 \\ &= Y^3 + 6Y^2 + 12Y + 8 - 6Y^2 - 24Y - 24 - 6 \\ &= Y^3 - 12Y - 22. \end{aligned}$$

Para resolver la ecuación (0.0.5) del Ferro y Tartaglia ponían

$$X = u + v$$

con lo que la ecuación (0.0.5) se convierte en

$$u^3 + 3u^2v + 3uv^2 + v^3 + pu + pv + q = 0$$

o

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0.$$

Como hemos cambiado una variable por otras dos, es natural imponer alguna condición adicional entre las dos variables $u$ y $v$. Por ejemplo, la última ecuación se simplifica bastante si ponemos $3uv + p = 0$, con lo que nos quedamos con el siguiente sistema

$$u^3 + v^3 + q = 0, \quad v = -\frac{p}{3u}$$

de donde se obtiene

$$u^3 - \frac{p^3}{27u^3} + q = 0.$$

Multiplicando por $u^3$ obtenemos

$$u^6 + qu^3 - \left(\frac{p}{3}\right)^3 = 0 \tag{0.0.6}$$

que parece más complicada que la ecuación original de grado 3 ya que tiene grado 6. Sin embargo la ecuación (0.0.6) es una ecuación de grado 2 en $u^3$ de donde deducimos que

$$u^3 = \frac{-q \pm \sqrt{q^2 + 4(p/3)^3}}{2} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \left(\frac{p}{3}\right)^3}.$$

En este momento es muy tentador concluir que

$$u = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \left(\frac{p}{3}\right)^3}}$$

lo que proporciona 6 soluciones de la ecuación (0.0.6) ya que si

$$\omega = \frac{-1+\sqrt{-3}}{2}$$

entonces $\omega^3 = 1$, con lo que si $u_0$ y $u_1$ son raíces cúbicas de $-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\left(\frac{p}{3}\right)^3}$ y $-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\left(\frac{p}{3}\right)^3}$ respectivamente, entonces $u_0, \omega u_0, \omega^2 u_0$ son raíces cúbicas de $-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\left(\frac{p}{3}\right)^3}$ y $u_1, \omega u_1$ y $\omega^2 u_1$ son raíces cúbicas de $-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\left(\frac{p}{3}\right)^3}$. Por tanto, una vez calculado $v = -\frac{p}{3u}$, obtenemos una solución $X = u + v$ para cada uno de los seis valores obtenidos de $u$. Esto no puede ser correcto ya que una ecuación de grado tres tiene a los sumo tres soluciones. A pesar de esto sólo obtendremos tres soluciones. En efecto, obsérvese que

$$\left(-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\left(\frac{p}{3}\right)^3}\right)\left(-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\left(\frac{p}{3}\right)^3}\right) = -\left(\frac{p}{3}\right)^3 = u^3v^3.$$

Por tanto, si $u$ es una raíz cúbica de $-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\left(\frac{p}{3}\right)^3}$, entonces $v = -\frac{p}{3u}$ es una raíz cúbica de $-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\left(\frac{p}{3}\right)^3}$. En conclusión, las seis soluciones de (0.0.6) son $u, \omega u, \omega^2 u, v = -\frac{p}{3u}, \omega v$ y $\omega^2 v$ y, como hemos impuesto que $uv = -\frac{p}{3}$, podemos unir las tres primeras con las tres segundas y obtener las tres soluciones siguientes de la ecuación original (0.0.5):

$$\alpha_1 = u + v, \quad \alpha_2 = \omega u + \omega^2 v, \quad \alpha_3 = \omega^2 u + \omega v.$$

Esto no tiene el aspecto de una fórmula. Teniendo en cuenta la relación obtenida entre los cubos de $u$ y $v$ nos gustaría poner algo así como

$$X = \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\left(\frac{p}{3}\right)^3}}, \tag{0.0.7}$$

lo que efectivamente nos servirá para calcular las tres soluciones de (0.0.5), si tomamos la siguiente precaución: Si $u$ es la primera raíz cúbica y $v$ es la segunda, entonces $uv = -\frac{p}{3}$. Por ejemplo, en la ecuación

$$Y^3 - 12Y - 22 = 0$$

que nos ha aparecido al plantearnos el problema de calcular el lado $X = Y + 2$ de un cubo cuyo volumen sea seis unidades mayor que el área total de los lados exteriores, tenemos $p = -12$ y $q = -22$ con lo que

$$Y = \sqrt[3]{11+\sqrt{121+64}} + \sqrt[3]{11-\sqrt{121+64}} = \sqrt[3]{11+\sqrt{185}} + \sqrt[3]{11-\sqrt{185}}.$$

y por tanto el lado del cubo buscado es

$$X = 2 + \sqrt[3]{11+\sqrt{185}} + \sqrt[3]{11-\sqrt{185}}$$

ya que no debemos considerar soluciones complejas.

La solución de la cuártica encontrada por Ferrari utiliza argumentos similares a los que hemos visto para resolver la cúbica, aunque algo más complicados. Una vez descubiertas fórmulas para las soluciones de las ecuaciones de segundo, tercer y cuarto grado, resultaba natural buscar fórmulas para resolver las ecuaciones polinómicas de grado mayor que cuatro. Doscientos años después de que Cardano publicara las soluciones de la cúbica y la cuártica encontradas por del Ferro, Tartaglia y Ferrari, seguía

sin encontrarse una fórmula para la ecuación de quinto grado a pesar de que primero D'Alembert en 1746 (de forma incompleta) y más tarde Gauss en 1799 habían demostrado el Teorema Fundamental del Álgebra, que afirma que todo polinomio no constante con coeficientes complejos tiene al menos una raíz. El Teorema Fundamental del Álgebra muestra que el problema no es si un polinomio tiene raíces o no, sino si sus raíces son expresables en términos de los coeficientes mediante operaciones algebraicas elementales. ¿Cuáles son estas operaciones algebraicas elementales? Si observamos las expresiones (0.0.3) y (0.0.7) parece natural considerar como operaciones algebraicas elementales las sumas, restas, productos, cocientes y extracciones de raíces $n$-ésimas. Una expresión de las soluciones de una ecuación algebraica de este tipo es conocido como *solución por radicales*. En 1770 Lagrange publicó un trabajo titulado *Réflexión sur la résolution algébrique des equations* en el que estudiaba cómo podrían permutarse las soluciones de una ecuación polinómica. Si $\alpha_1, \alpha_2, \ldots, \alpha_n$ son las soluciones de una ecuación polinómica $P(X) = 0$, donde

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0$$

entonces

$$P(X) = (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n).$$

Desarrollando el producto de la derecha e igualando coeficientes se obtienen unas relaciones entre las soluciones $\alpha_1, \alpha_2, \ldots, \alpha_n$ y los coeficientes del polinomio $P(X)$. Por ejemplo, la primera y última relación son

$$\begin{aligned} a_0 &= (-1)^n\alpha_1\alpha_2\cdots\alpha_n \\ a_{n-1} &= -(\alpha_1 + \alpha_2 + \cdots\alpha_n). \end{aligned}$$

Estas fórmulas ya habían sido observadas por Cardano y Vieta y son conocidas con el nombre de Fórmulas de Cardano-Vieta. Como es natural el orden en que se escriban las raíces no afecta al polinomio, lo cual se refleja en que las expresiones de los coeficientes en términos de los coeficientes del polinomios en las Fórmulas de Cardano-Vieta son simétricas, es decir, el resultado no se ve afectado por permutar el orden en que se escriben los coeficientes. Recordemos que para resolver la ecuación (0.0.5) lo que hemos hecho es empezar resolviendo la ecuación (0.0.6) que se llama *resolvente* de la ecuación (0.0.5). La razón por la que podemos calcular las soluciones de la resolvente es que en realidad se puede considerar como una ecuación de grado 2. Lagrange observó que la solución de Ferrari de la ecuación de cuarto grado consistía en encontrar otra ecuación de grado 3 cuyas soluciones estaban conectadas con las soluciones de la ecuación de cuarto grado original. Es decir, la ecuación de cuarto grado también tiene una resolvente de grado 3. Obsérvese que la relación entre las soluciones $\alpha_1, \alpha_2$ y $\alpha_3$ de la ecuación (0.0.5) y las soluciones $u_1 = u, u_2 = \omega u, u_3 = \omega^2 u, u_4 = v = -\frac{p}{3v}, u_5 = \omega v$ y $u_6 = \omega^2 v$ es

$$\begin{aligned} \alpha_1 &= u + v = u_1 + u_4 \\ \alpha_2 &= \omega u + \omega^2 v = u_2 + u_6 \\ \alpha_3 &= \omega^2 u + \omega v = u_3 + u_5 \end{aligned}$$

Utilizando que $1 + \omega + \omega^2 = 0$ y $\omega^3 = 1$, se pueden obtener las siguientes expresiones para las soluciones de la resolvente (0.0.6) , en términos de las soluciones de la ecuación original (0.0.5):

$$\begin{aligned} u_1 &= \tfrac{1}{3}(\alpha_1 + \omega\alpha_3 + \omega^2\alpha_2) \\ u_2 &= \tfrac{1}{3}(\alpha_2 + \omega\alpha_1 + \omega^2\alpha_3) \\ u_3 &= \tfrac{1}{3}(\alpha_3 + \omega\alpha_2 + \omega^2\alpha_1) \\ u_4 &= \tfrac{1}{3}(\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3) \\ u_5 &= \tfrac{1}{3}(\alpha_3 + \omega\alpha_1 + \omega^2\alpha_2) \\ u_6 &= \tfrac{1}{3}(\alpha_2 + \omega\alpha_3 + \omega^2\alpha_1). \end{aligned} \tag{0.0.8}$$

Lagrange observó que para pasar de una solución de la resolvente a otra bastaba con permutar los papeles representados por las tres raíces $\alpha_1, \alpha_2$ y $\alpha_3$ de la ecuación original que se pretendía resolver.

La observación de Lagrange es notable porque muestra un método general para encontrar ecuaciones resolventes que no depende de la feliz idea de realizar el cambio $X = u + v$.

Consideremos la cuártica

$$X^4 - pX^3 + qX^2 - rX + s = 0 \tag{0.0.9}$$

y sean $\alpha_1, \alpha_2, \alpha_3$ y $\alpha_4$ las soluciones de (0.0.9). Las potencias de $\omega$ utilizadas en las expresiones (0.0.8) son las soluciones de la ecuación $X^3 = 1$, conocidas como raíces terceras de la unidad. Las raíces cuartas de la unidad, o sea las soluciones de la ecuación $X^4 = 1$, son $1, i, i^2 = -1$ e $i^3 = -i$. Consideremos los 24 números

$$u_{i,j,k,l} = \frac{1}{4}(\alpha_i + i\alpha_j + i^2\alpha_k + i^3\alpha_l) \tag{0.0.10}$$

donde $(i, j, k, l)$ es un elemento del conjunto $S_4$ de todas las permutaciones de $1, 2, 3$ y 4. Definimos la resolvente de (0.0.9) como

$$\phi(X) = \prod_{(i,j,k,l)\in S_4} (X - u_{i,j,k,l}).$$

La ecuación $\phi(X) = 0$ parece ser más complicada que la de grado cuatro original porque tiene grado 24, sin embargo una vez que desarrollamos el producto de los $X - u_{i,j,k,l}$ en términos de las desconocidas raíces $\alpha_i$ y utilizamos las Fórmulas de Cardano-Vieta observamos que $\phi(X) = P(X^4)$ para un polinomio de $P$ de grado 6. Además el polinomio $P$ resulta ser el producto de dos polinomios de grado 3. O sea $\phi(X) = P_1(X^4)P_2(X^4)$, donde $P_1$ y $P_2$ son polinomios de grado 3 cuyos coeficientes dependen de los coeficientes $p, q, r, s$. Resolviendo las ecuaciones $P_1(X) = 0$ y $P_2(X)$ obtenemos los valores de los 24 elementos $u_{i,j,k,l}$, con lo que utilizando las fórmulas (0.0.10) obtenemos las cuatro soluciones de la ecuación (0.0.9).

Aunque Lagrange no consiguió ir más allá en el camino de la búsqueda de la solución de la ecuación de quinto grado, marcó el camino a seguir. La resolvente de la ecuación de quinto grado conduce a una ecuación de grado 120 que es una ecuación de grado 24 en $X^5$. Inspirado en los trabajos de Lagrange, en 1799 Ruffini (1765-1822) publicó un trabajo titulado *Teoría generale delle equazioni* que contenía una demostración, poco rigurosa, aunque esencialmente correcta, de que la ecuación general de quinto grado no es resoluble por radicales. Una demostración completa y correcta fue publicada por Abel (1802-1829) en 1826. El resultado de Abel parece cerrar definitivamente el problema de buscar una fórmula para resolver ecuaciones polinómicas. Sin embargo, no es así ya que obviamente hay algunas ecuaciones de quinto grado o superior que si son resolubles por radicales. La más obvia es la ecuación $X^n = a$ cuya soluciones son las raíces $n$-ésimas de $a$, que claramente se pueden expresar por radicales como $X = \sqrt[n]{a}$. El problema que quedaba por resolver es encontrar un método que sirviera para decidir qué ecuaciones son resolubles por radicales y cuales no lo son, y para las primeras, obtener una expresión que describa por radicales las soluciones en términos de los coeficientes. Este es el problema en el que Abel estaba trabajando cuando murió en 1829 con sólo 27 años. La respuesta definitiva al problema fue obtenida por Galois (1811-1832) mostrando la conexión entre la Teoría de Ecuaciones Algebraicas y la Teoría de Grupos, o mejor dicho introduciendo el concepto de grupo y relacionándolo con la resolubilidad por radicales de una ecuación. Los resultados de Galois fueron escritos de forma precipitada la noche del 29 de mayo de 1832, antes de un duelo que le costó la vida a los 21 años y constituyen uno de los diamantes más brillantes de la historia de las matemáticas y la mayor parte del contenido de este curso.

En realidad la forma de exponer la Teoría de Galois es muy diferente a la expuesta por Galois y sigue el camino marcado por Artin (1898-1962) en la que la Teoría de Galois toma la forma de conexión entre la Teoría de Cuerpos y la Teoría de Grupos. Esta método de exposición puede resultar algo abstracto al principio pero proporciona un lenguaje algebraico muy apropiado para exponer la Teoría de Galois. Además permite conectar el problema de estudiar ecuaciones algebraicas con otros problemas clásicos como son los problemas de construcciones con regla y compás, incluyendo los tres problemas de la antigüedad, trisección del ángulo, duplicación del cubo y cuadratura del círculo, y el de la constructibilidad de polígonos regulares. Por otro lado la Teoría de Cuerpos proporciona

los fundamentos teóricos de otros campos de actualidad por sus aplicaciones en Teoría de Códigos y Criptografía, que es el estudio de cuerpos finitos. Sin embargo, estas aplicaciones no se incluirán en el curso por falta de tiempo.

# Capítulo 1

# Polinomios

## 1.1 Polinomios en varias indeterminadas

En esta sección $A$ es un anillo. Denotamos por $A^*$ el grupo de las unidades de $A$. Recordemos que si $X$ es una indeterminada entonces $A[X]$ denota el anillo de polinomios con coeficientes en $A$. Recordemos también la

> **Propiedad Universal del Anillo de Polinomios en una variable**: Para todo homomorfismo de anillos $f : A \to B$ y todo elemento $b \in B$ existe un único homomorfismo de anillos $\overline{f} : A[X] \to B$ que extiende $f$ y tal que $f(X) = b$.

Para cada entero positivo $n$, definimos el *anillo de polinomios en n indeterminadas con coeficientes en A*, denotado por $A[X_1, \ldots, X_n]$, mediante la fórmula recurrente, donde $A[X_1]$ es el anillo en una indeterminada:

$$A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n].$$

Los elementos $X_1, \ldots, X_n$ de $A[X_1, \ldots, X_n]$ se llaman *indeterminadas* y los elementos de $A[X_1, \ldots, X_n]$ se llaman *polinomios en n indeterminadas* con coeficientes en $A$.

A partir del Corolario 3.2, la Proposición 3.13 y el Teorema 3.17 de GyA, se obtienen fácilmente por inducción las siguientes propiedades:

**Proposición 1.1** *Para un anillo $A$ y un entero positivo $n$ se verifican:*

*(1)* $A[X_1, \ldots, X_n]$ *nunca es un cuerpo.*

*(2)* $A[X_1, \ldots, X_n]$ *es un dominio si y solo si lo es $A$.*

*(3) Si $A$ es un dominio, entonces* $A[X_1, \ldots, X_n]^* = A^*$.

*(4)* $A[X_1, \ldots, X_n]$ *es un DFU si y solo si lo es $A$.*

*(5)* $A[X_1, \ldots, X_n]$ *es un DIP si y solo si $n = 1$ y $A$ es un cuerpo.*

Si $a \in A$ e $i = (i_1, \ldots, i_n) \in \mathbb{N}^n$, el elemento $aX_1^{i_1} \cdots X_n^{i_n}$ de $A[X_1, \ldots, X_n]$ se llama *monomio* de *tipo* $i$ y coeficiente $a$.

**Lema 1.2** *Sean $A$ un anillo y $n$ un entero positivo. Entonces todo elemento $p$ de $A[X_1, \ldots, X_n]$ se escribe de forma única como suma de monomios de distinto tipo, casi todos con coeficiente nulo. Es decir, se tiene una única expresión*

$$p = \sum_{i \in \mathbb{N}_0^n} p_i X_1^{i_1} \cdots X_n^{i_n} \tag{1.1}$$

*con $p_i = 0$ para casi todo $i = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$.*

**Demostración.** Aplicamos inducción en $n$, con el caso $n = 1$ obvio por la propia definición de anillo de polinomios en una variable. Cuando $n > 1$, un elemento de $A[X_1, \ldots, X_n]$ es, por definición, de la forma $\sum_{t\in\mathbb{N}_0} p_t X_n^t$ con cada $p_t \in A[X_1, \ldots, X_{n-1}]$ y casi todos los $p_t$ nulos. Por hipótesis de inducción, cada $p_t$ se expresa como

$$p_t = \sum_{(i_1,\ldots,i_{n-1})\in\mathbb{N}_0^{n-1}} (p_t)_{(i_1,\ldots,i_{n-1})} X_1^{i_1} \cdots X_{n-1}^{i_{n-1}},$$

donde cada $(p_t)_{(i_1,\ldots,i_{n-1})}$ está en $A$ y casi todos son nulos. Definiendo $p_i = (p_{i_n})_{(i_1,\ldots,i_{n-1})}$ (para $i = (i_1, \ldots, i_n)$) tenemos la expresión deseada.

Recíprocamente, una expresión como (1.1) puede reescribirse como un polinomio en $X_n$ con coeficientes en $A[X_1, \ldots, X_{n-1}]$ sin más que definir cada coeficiente como $p_t = \sum p_i X_1^{i_1} \cdots X_{n-1}^{i_{n-1}}$, con la suma extendida a todos los $i = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$ con $i_n = t$. Usando esto es sencillo demostrar que estas expresiones son únicas, asumiendo que lo son en $A[X_1, \ldots, X_{n-1}]$. □

Usando la Propiedad Universal del Anillo de Polinomios en una variable se demuestra fácilmente la siguiente generalización por inducción en el número de indeterminadas.

**Proposición 1.3** *Sean $A$ un anillo, $n \geq 1$ un entero y $u : A \to A[X_1, \ldots, X_n]$ la inclusión.*

*(1)* **(PUAP en $n$ indeterminadas)** *Dados un homomorfismo de anillos $f : A \to B$ y $n$ elementos $b_1, \ldots, b_n \in B$ (no necesariamente distintos) existe un único homomorfismo de anillos $\overline{f}$ de $A[X_1, \ldots, X_n]$ a $B$ tal que $\overline{f} \circ u = f$ y $\overline{f}(X_j) = b_j$ para cada $j = 1, \ldots, n$.*

*(2) Si dos homomorfismos de anillos $g, h : A[X_1, \ldots, X_n] \to B$ coinciden sobre $A$ y en $X_j$ para cada $j = 1, \ldots, n$ entonces son iguales.*

*(3) La PUAP en $n$ indeterminadas determina $A[X_1, \ldots, X_n]$ salvo isomorfismos. Supongamos que existen un anillo $P$ con elementos $T_1, \ldots, T_n$ y un homomorfismo de anillos $v : A \to P$ tales que, dados un homomorfismo de anillos $f : A \to B$ y elementos $b_1, \ldots, b_n \in B$, existe un único homomorfismo de anillos $\overline{f} : P \to B$ tal que $\overline{f} \circ v = f$ y $\overline{f}(T_j) = b_j$ para cada $j = 1, \ldots, n$. Entonces existe un isomorfismo $\phi : A[X_1, \ldots, X_n] \to P$ tal que $\phi \circ u = v$ y $\phi(X_j) = T_j$ para cada $j = 1, \ldots, n$.*

Como en el caso de una indeterminada, se tiene:

**Ejemplos 1.4** *Aplicaciones de la PUAP en $n$ indeterminadas.*

(1) Dados anillos $A \subseteq B$ y elementos $b_1, \ldots, b_n \in B$, existe un homomorfismo $S : A[X_1, \ldots, X_n] \to B$ que es la identidad sobre $A$ y tal que $S(X_j) = b_j$ para cada $j = 1, \ldots, n$. Dado $p \in A[X_1, \ldots, X_n]$, escribiremos a menudo $p(b_1, \ldots, b_n)$ en lugar de $S(p)$. Si $p = \sum_{i\in\mathbb{N}^n} p_i X_1^{i_1} \cdots X_n^{i_n}$ es la expresión de $p$ como suma de monomios, entonces

$$S(p) = p(b_1, \ldots, b_n) = \sum_{i\in\mathbb{N}^n} p_i b_1^{i_1} \cdots b_n^{i_n}.$$

La imagen de este homomorfismo es el subanillo de $B$ generado por $A \cup \{b_1, \ldots, b_n\}$ y que denotamos por $A[b_1, \ldots, b_n]$.

Supongamos que $f, g : A[b_1, \ldots, b_n] \to C$ son dos homomorfismos de anillos. Entonces $f = g$ si y solo si $f|A = g|A$ y $f(b_i) = g(b_i)$ para todo $i$. Para demostrar esto basta aplicar la Proposición 1.3 para deducir que $f \circ S = g \circ S$ y concluir que $f = g$, pues $S$ es suprayectiva.

(2) Sea $A$ un anillo y sea $\sigma$ una biyección del conjunto $\mathbb{N}_n = \{1, \ldots, n\}$ en sí mismo con inversa $\tau = \sigma^{-1}$. Si en el ejemplo anterior tomamos $B = A[X_1, \ldots, X_n]$ y $b_j = X_{\sigma(j)}$, obtenemos un homomorfismo $\overline{\sigma} : A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_n]$ que "permuta las indeterminadas". Es claro que $\overline{\sigma}$ es de hecho un automorfismo con inverso $\overline{\tau}$. Usando estos isomorfismos y la definición de los anillos de polinomios en varias indeterminadas, es fácil establecer isomorfismos

$$A[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \simeq A[X_1, \ldots, X_n][Y_1, \ldots, Y_m] \simeq A[Y_1, \ldots, Y_m][X_1, \ldots, X_n],$$

por lo que, en la práctica, no hay que distinguir entre estos anillos.

(3) Todo homomorfismo de anillos $f : A \to B$ induce un homomorfismo $\overline{f} : A[X_1, \ldots, X_n] \to B[X_1, \ldots, X_n]$ que coincide con $f$ sobre $A$ y verifica $\overline{f}(X_j) = X_j$ para cada $j = 1, \ldots, n$. Si $p = \sum_{i \in \mathbb{N}^n} p_i X_1^{i_1} \cdots X_n^{i_n}$ es la expresión de $p$ como suma de monomios, entonces

$$\overline{f}(p) = \sum_{i \in \mathbb{N}^n} f(p_i) X_1^{i_1} \cdots X_n^{i_n}.$$

En el futuro este homomorfismo lo denotaremos por $f$.

Por definición, el *grado de un monomio* $aX_1^{i_1} \cdots X_n^{i_n}$ de $A[X_1, \ldots, X_n]$ es $i_1 + \cdots + i_n$. El grado $\mathrm{gr}(p)$ de un polinomio $p \neq 0$ de $A[X_1, \ldots, X_n]$ se define como el mayor de los grados de los monomios que aparecen con coeficiente no nulo en la expresión de $p$ como suma de monomios de distinto tipo. Es claro que, dados dos polinomios $p$ y $q$, se tiene

$$\mathrm{gr}(p+q) \leq \max\{\mathrm{gr}(p), \mathrm{gr}(q)\} \qquad \text{y} \qquad \mathrm{gr}(pq) \leq \mathrm{gr}(p) + \mathrm{gr}(q).$$

Sin embargo, no es tan fácil como en el caso de una indeterminada ver que, cuando $A$ es un dominio, la segunda desigualdad es de hecho una igualdad. Para esto, y para otras cosas, es interesante considerar el siguiente concepto:

Un polinomio $p \neq 0$ de $A[X_1, \ldots, X_n]$ se dice *homogéneo de grado* $n \geq 0$ si es suma de monomios de grado $n$. Por ejemplo, de los polinomios de $\mathbb{Z}[X, Y, Z]$

$$X^2Y + Y^3 - 3XYZ + 6YZ^2, \quad X^6 + Y^6 + Z^6 + X^3Y^3 + X^3Z^3 + Y^3Z^3, \quad XYZ + X + Y + Z,$$

los dos primeros son homogéneos (de grados 3 y 6, respectivamente) y el último no lo es.

**Proposición 1.5** *Dados un anillo $A$ y un entero $n \geq 1$, todo polinomio de $A[X_1, \ldots, X_n]$ se escribe de modo único como suma de polinomios homogéneos de distintos grados.*

**Demostración.** Si $p = \sum_{i \in \mathbb{N}^n} p_i X_1^{i_1} \cdots X_n^{i_n}$ es la expresión de $p$ como suma de monomios y ponemos $h_j = \sum_{i_1 + \cdots + i_n = j} p_i X_1^{i_1} \cdots X_n^{i_n}$, es claro que $p = h_0 + h_1 + \cdots + h_k$ (donde $k = \mathrm{gr}(p)$) es la expresión buscada. La unicidad es consecuencia inmediata del Lema 1.2.□

**Corolario 1.6** *Si $D$ es un dominio y $n \geq 1$, se tiene* $\mathrm{gr}(pq) = \mathrm{gr}(p) + \mathrm{gr}(q)$ *para cualesquiera $p, q \in D[X_1, \ldots, X_n]$.*

## 1.2 Polinomios simétricos

Sea $A$ un anillo arbitrario y consideremos $n$ indeterminadas $X_1, \ldots, X_n$. En el Ejemplo 2 de 1.4 vimos que para cada permutación $\sigma \in S_n$, existe un único automorfismo $\overline{\sigma}$ de $A[X_1, \ldots, X_n]$, tal que $\overline{\sigma}(a) = a$, para todo $a \in A$ y $\overline{\sigma}(X_n) = X_{\sigma(n)}$. Obsérvese que $\overline{\sigma \circ \tau} = \overline{\sigma} \circ \overline{\tau}$.

Un polinomio $p \in A[X_1, \ldots, X_n]$ se dice que es *simétrico*, en las indeterminadas $X_1, \ldots, X_n$, si $\overline{\sigma}(p) = p$ para todo $\sigma \in S_n$. Por ejemplo, los polinomios en dos indeterminadas $X_1 + X_2$ y $X_1X_2$ son polinomios simétricos. Sin embargo estos polinomios no serían simétricos como polinomios en más de dos variables. Obsérvese que el conjunto de todos los polinomios simétricos de $A[X_1, \ldots, X_n]$ forma un subanillo de $A[X_1, \ldots, X_n]$.

Para cada $p \in A[X_1, \ldots, X_n]$, sea $O_n(p)$ el conjunto de todos los polinomios de la forma $\overline{\sigma}(p)$ para $\sigma$ recorriendo todos los elementos de $S_n$ y sea $\Sigma_n(p) = \sum_{q \in O_n(p)} q$. Obsérvese que si $\sigma \in \Sigma_n$, entonces $\overline{\sigma}$ se restringe a una biyección de $O_n(p)$ en si mismo pues claramente $\overline{\sigma}(O_n(p)) \subseteq O_n(p)$, $O_n(p)$ es finito y $\overline{\sigma}$ es inyectiva. Luego

$$\overline{\sigma}(\Sigma_n(p)) = \sum_{q \in O_n(p)} \overline{\sigma}(q) = \sum_{q \in O_n(p)} q = \Sigma_n(p),$$

es decir $\Sigma_n(p)$ es un polinomio simétrico.

Por ejemplo,

$$\begin{aligned} O_n(X_1) &= \{X_1, X_2, \ldots, X_n\} \\ O_n(X_1X_2) &= \{X_iX_j : 1 \leq i < j \leq n\} \end{aligned}$$

y por tanto

$$\begin{aligned} \Sigma_n(X_1) &= X_1 + X_2 + \cdots + X_n \\ \Sigma_n(X_1X_2) &= \textstyle\sum_{1 \leq i < j \leq n} X_iX_j. \end{aligned}$$

Los polinomios de la forma

$$\begin{aligned} S_1 = \Sigma_n(X_1) &= X_1 + X_2 + \cdots + X_n, \\ S_2 = \Sigma_n(X_1X_2) &= \textstyle\sum_{1 \leq i < j \leq n} X_iX_j, \\ S_3 = \Sigma_n(X_1X_2X_3) &= \textstyle\sum_{1 \leq i < j < k \leq n} X_iX_jX_k, \\ &\vdots \\ S_4 = \Sigma_n(X_1X_2 \cdots X_n) &= X_1X_2 \cdots X_n. \end{aligned}$$

se llaman *polinomios simétricos elementales* en $n$ variables. Obsérvese que $S_i$ para $i \leq n \leq m$ tiene distintos valores según que consideremos $n$ ó $m$ variables. Por ejemplo para dos variables los polinomios simétricos elementales son

$$\begin{aligned} S_1 &= X_1 + X_2, \\ S_2 &= X_1X_2 \end{aligned}$$

y para tres variables son

$$\begin{aligned} S_1 &= X_1 + X_2 + X_3, \\ S_2 &= X_1X_2 + X_1X_3 + X_2X_3, \\ S_3 &= X_1X_2X_3. \end{aligned}$$

La siguiente

**Lema 1.7** *Se verifican las siguientes propiedades para $f \in A[X_1, \ldots, X_n]$ y $\sigma \in S_n$.*

*(1) Si $f$ es homogéneo de grado $n$, entonces $\sigma(f)$ es homogéneo de grado $n$.*

*(2) Un polinomio es simétrico si y solo si sus componentes homogéneas son simétricas.*

**Demostración.** (1) es obvio.

(2) Sea $p = p_0 + p_1 + \ldots + p_m$ un polinomio en $n$ variables $X_1, \ldots, X_n$ con coeficientes en el anillo $A$, donde $p_i$ denota la componente homogénea de grado $i$. Como el conjunto de los polinomios simétricos es un subanillo de $A[X_1, \ldots, X_n]$ está claro que si $p_0, p_1, \ldots, p_n$ son simétricos entonces $p$ también es simétrico.

Recíprocamente, supongamos que $p$ es simétrico y sea $\sigma \in S_n$. Entonces

$$p = \overline{\sigma}(p) = \overline{\sigma}(p_0) + \overline{\sigma}(p_1) + \cdots + \overline{\sigma}(p_m)$$

y cada $\overline{\sigma}(p_i)$ es homogéneo de grado $i$, por (1). Como la descomposición de un polinomio en suma de polinomios homogéneos de distintos grados es única, deducimos que $p_i = \overline{\sigma}(p_i)$ para todo $i$. Por tanto $p_i$ es simétrico para todo $i$. □

Si $a$ denota un elemento de $\mathbb{N}^n$, entonces $a_i$ denotará la $i$-ésima coordenada de $a$, es decir $a = (a_1, \ldots, a_n)$. Si $p \in A[X_1, \ldots, X_n]$ y $a \in \mathbb{N}^n$, entonces vamos a denotar por $p_a$ al coeficiente de $X_1^{a_1} \cdots X_n^{a_n}$ en $p$. De esta forma cada polinomio $p \in A[X_1, \ldots, X_n]$ se expresa como

$$p = \sum_{a \in \mathbb{N}^n} p_a X_1^{a_1} X_2^{a_2} \cdots X_n^{a^n}.$$

Vamos a denotar por $\preccurlyeq$ el orden lexicográfico en el conjunto $\mathbb{N}^n$ de las n-uplas de números enteros no negativos. Es decir, dados dos elementos $a$ y $b$ de $\mathbb{N}^n$, diremos que $a \preccurlyeq b$ si o bien $a = b$ o existe un $i$ tal que $a_0 = b_0, a_1 = b_1, \ldots, a_{i-1} = b_{i-1}$ y $a_i < b_i$. Por ejemplo

$$(1,1,2) \preccurlyeq (1,3,1) \preccurlyeq (2,0,0) \preccurlyeq (2,0,1) \preccurlyeq (2,1,0) \preccurlyeq (3,0,1).$$

Este orden es un orden total en $\mathbb{N}^n$ y por tanto todo subconjunto finito de $\mathbb{N}^n$ tiene un mínimo y un máximo respecto de este orden. Por ejemplo, si

$$X = \{(2,2,1), (3,3,1), (2,0,2), (3,0,2), (2,1,0), (2,1,1), (3,0,0)\}$$

entonces

$$(2,0,2) \preccurlyeq (2,1,0) \preccurlyeq (2,1,1) \preccurlyeq (2,2,1) \preccurlyeq (3,0,0) \preccurlyeq (3,0,2) \preccurlyeq (3,3,1)$$

y por tanto, el mínimo de $X$ es $(2,0,2)$ y su máximo es $(3,0,0)$.

De hecho $\preccurlyeq$ es un buen orden, es decir todo subconjunto no vacío $X \subseteq \mathbb{N}^n$ tiene un mínimo en $\mathbb{N}^n$. En efecto, es fácil ver que el mínimo de $X$ es el elemento $a = (a_1, \ldots, a_n)$ definido de la siguiente forma: $a_1$ es el menor entero no negativo $m$ tal que existe un elemento de $X$ cuya primera coordenada es $m$, $a_2$ es el primer entero no negativo $m$ tal que existe un elemento de $X$ cuyas dos primeras coordenadas son $(a_1, m)$, $a_3$ es el primer entero no negativo $m$ tal que existe un elemento de $X$ cuyas tres primeras coordenadas son $(a_1, a_2, m)$. En general, $a_i$ es el primer entero no negativo $m$ tal que existe un elemento de $X$ cuyas $i$ primeras coordenadas son $(a_1, \ldots, a_{i-1}, m)$.

Si $0 \neq p \in A[X_1, \ldots, X_n]$, entonces vamos a denotar por $\delta(p)$ al mayor elemento $a \in \mathbb{N}^n$, con respecto a $\preccurlyeq$, tal que $p_a \neq 0$. Por ejemplo, $\delta(X_1^2X_2^2 + X_1X_2 + X_1^3 + X_1^3X_2 + X_2^6) = (3,1)$, pues $(0,6) \preccurlyeq (1,1) \preccurlyeq (2,2) \preccurlyeq (3,0) \preccurlyeq (3,1)$. De forma análoga a como se hizo para el grado habitual ponemos que $\delta(0) = -\infty$ y consideramos $-\infty \preccurlyeq a$ para todo $a \in \mathbb{N}^n$.

Obsérvese que $\delta$ satisface propiedades similares a gr. En efecto se verifica el siguiente lema cuya demostración dejamos como ejercicio.

**Lema 1.8** *Si $p, q \in A[X_1, \ldots, X_n]$, entonces*

*(1) $\delta(p+q) \leq \max\{\delta(p), \delta(q)\}$ y $\delta(p+q) < \max\{\delta(p), \delta(q)\}$ si y solo si $\delta(p) = \delta(q)$ y $p_{\delta(p)} + q_{\delta(q)} = 0$.*

*(2) $\delta(pq) \leq \delta(p) + \delta(q)$ y se verifica la igualdad si y solo si se verifica una de las tres siguientes condiciones: (a) $p = 0$, (b) $q = 0$, (c) $p$ y $q$ son diferentes de 0 y $p_{\delta(a)}q_{\delta(b)} \neq 0$.*

*(3) Si $A$ es un dominio, entonces $\delta(pq) = \delta(p)\delta(q)$.*

**Teorema 1.9** *Todo polinomio simétrico en n variables se puede escribir de forma única como un polinomio en los polinomios simétricos elementales. Más precisamente, si $S_1, \ldots, S_n$ son los polinomios simétricos elementales en las variables $X_1, \ldots, X_n$, entonces el homomorfismo de sustitución*

$$\begin{array}{rcl} \varphi : A[X_1, \ldots, X_n] & \to & A[X_1, \ldots, X_n] \\ F & \mapsto & F(S_1, \ldots, S_n) \end{array}$$

*es inyectivo y su imagen es el conjunto de los polinomios simétricos elementales.*

**Demostración.** En primer lugar observemos que $\delta(S_i)$ es el elemento de $\mathbb{N}^n$ que empieza con $i$ unos y acaba con $i$ ceros. Es decir

$$\delta(S_1) = (1, 0, \ldots, 0), \quad \delta(S_2) = (1, 1, 0, \ldots, 0), \quad \ldots, \quad \delta(S_n) = (1, 1, \ldots, 1).$$

Por tanto, utilizando la propiedad (2) del Lema 1.8 se tiene que

$$\delta(S_1^{a_1} \cdots S_n^{a_n}) = (a_1 + a_2 + a_3 + \cdots + a_n, a_2 + a_3 + \cdots + a_n, a_3 + \cdots + a_n, \ldots, a_{n-1} + a_n, a_n).$$

Obsérvese que la aplicación $\psi : \mathbb{Q}^n \to \mathbb{Q}^n$ dada por

$$\psi(a_1, \ldots, a_n) = (a_1 + a_2 + a_3 + \cdots + a_n, a_2 + a_3 + \cdots + a_n, a_3 + \cdots + a_n, \ldots, a_{n-1} + a_n, a_n)$$

es lineal y su matriz asociada en la base canónica es

$$A = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 1 & \cdots & 1 & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

La matriz $A$ es invertible y su inversa es la matriz

$$A^{-1} = \begin{pmatrix} 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & -1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Obsérvese que si $a = (a_1, \ldots, a_n)$ con $a_1 \geq a_2 \cdots \geq a_n \geq 0$ y $b = A^{-1}a = (a_1 - a_2, a_2 - a_3, \ldots, a_{n-1} - a_n, a_n)$, entonces $b_i \geq 0$ para todo $i$. Recíprocamente, si $a = \psi(b)$ con $b_i \geq 0$ para todo $i = 1, \ldots, n$ entonces $a_1 \geq a_2 \geq \ldots a_n \geq 0$. En particular $\psi(\mathbb{N}^n) = \{a \in \mathbb{N}^n : a_1 \geq a_2 \geq \cdots \geq a_n\}$. Por tanto para todo polinomio $P \in K[X_1, X_2, \ldots, X_n]$ tal que $\delta(P) = (a_1, \ldots, a_n)$ con $a_1 \geq a_2 \cdots \geq a_n \geq 0$ se tiene que $\delta(P) = \delta(S_1^{b_1} \cdots S_n^{b_n})$ donde $b = (b_1, \ldots, b_n) = A^{-1}\delta(P)$.

*$\varphi$ es inyectiva.* Sea $0 \neq p \in K[X_1, \ldots, X_n]$ y sea $X$ el conjunto de elementos $a \in \mathbb{N}^n$ tales $p_a \neq 0$. Como la aplicación $\psi$ es inyectiva existe un elemento $a \in X$ tal que $\delta(S_1^{a_1} \cdots S_n^{a_n}) > \delta(S_1^{b_1} \cdots S_n^{b_n})$ para todo $b \in X \setminus \{a\}$. Como

$$\varphi(p) = p_a S_1^{a_1} \cdots S_n^{a_n} + \sum_{b \in X \setminus \{a\}} p_b S_1^{b_1} \cdots S_n^{b_n},$$

aplicando la propiedad (1) del Lema 1.8 se tiene que $\delta(\varphi(p)) = \delta(S_1^{a_1} \cdots S_n^{a_n})$ y, en particular $\varphi(p) \neq 0$. Como $\varphi$ es un homomorfismo, esto demuestra que $\varphi$ es inyectiva.

*La imagen de $\varphi$ es el conjunto de los polinomios simétricos.* Está claro que todo elemento de la imagen de $\varphi$ es un polinomio simétrico. Demostramos la otra inclusión por reducción al absurdo. Supongamos que hay un polinomio simétrico que no está en la imagen y elegimos uno de dichos polinomios $p$ para el que $a = \delta(p)$ sea mínimo con respecto a la relación de orden $\preccurlyeq$. Como $p$ es simétrico, $a_1 \geq a_2 \geq \cdots \geq a_n \geq 0$ y por tanto existe $a \in \mathbb{N}^n$ tal que $\psi(b) = a$. Eso implica que $\delta(S_1^{b_1} \cdots S_n^{b_n}) = a$ y, de la propiedad (1) del Lema 1.8 se deduce que si $q = p - p_a S_1^{b_1} \cdots S_n^{b_n}$, entonces $\delta(q) < \delta(p)$. Por la elección de $p$, se tiene que $q$ está en la imagen de $\varphi$, es decir existe $r \in K[X_1, \ldots, X_n]$ tal que $\varphi(r) = q$. Entonces $p = \varphi(r) + \varphi(p_a X_1^{b_1} \cdots X_n^{b_n}) = \varphi(r + p_a X_1^{b_1} \cdots X_n^{b_n})$, en contra de que $p$ no está en la imagen de $\varphi$. $\square$

La demostración del Teorema 1.9 es constructiva, es decir, proporciona un método efectivo para escribir cada polinomio simétrico como un polinomio en los polinomios simétricos elementales siguiendo el siguiente proceso recursivo.

*Entrada*: Un polinomio simétrico $p$.
$q = p, f = 0$.
Mientras que $q \neq 0$.
$a = \delta(q)$.
$b = \psi^{-1}(a) = (a_1 - a_2, a_2 - a_3, \ldots, a_{n-1} - a_n, a_n)$
$f = f + p_a X_1^{b_1} \cdots X_n^{b_n}$
$q = q - p_a S_1^{b_1} \cdots S_n^{b_n}$
*Salida*: $f$.

**Ejemplo 1.10** Sea $p = X_1^3 + X_2^3 + X_3^3$, un polinomio simétrico en tres variables. Entonces $\delta(p) = (3, 0, 0)$ y por tanto $\psi^{-1}(3, 0, 0) = (3, 0, 0)$. Sea

$$\begin{aligned} q_1 &= p - S_1^3 = X_1^3 + X_2^3 + X_3^3 - (X_1 + X_2 + X_3)^3 \\ &= -3(X_1^2 X_2 + X_1 X_2^2 + X_1^2 X_3 + X_1 X_3^2 + X_2^2 X_3 + X_2 X_3^2) - 6X_1 X_2 X_3. \end{aligned}$$

Entonces $\delta(q_1) = (2, 1, 0)$ y $\psi^{-1}(2, 1, 0) = (1, 1, 0)$, por lo que ponemos

$$\begin{aligned} q_2 &= q_1 + 3S_1 S_2 \\ &= 3(X_1 + X_2 + X_3)(X_1 X_2 + X_1 X_3 + X_2 X_3) \\ &\quad -3(X_1^2 X_2 + X_1 X_2^2 + X_1^2 X_3 + X_1 X_3^2 + X_2^2 X_3 + X_2 X_3^2) - 6X_1 X_2 X_3 \\ &= 3X_1 X_2 X_3 = 3S_3. \end{aligned}$$

Por tanto

$$X_1^3 + X_2^3 + X_3^3 = p = S_1^3 + q_1 = S_1^3 - 3S_1 S_2 + q_2 = S_1^3 - 3S_1 S_2 + 3S_3.$$

La siguiente fórmula, es muy fácil de demostrar y es conocida con el nombre de Fórmula de Cardano-Vieta

$$\begin{aligned} &(T - X_1)(T - X_2) \cdots (T - X_n) = T^n + \textstyle\sum_{i=1}^n (-1)^i S_i T^{n-i} = \\ &T^n - S_1 T^{n-1} + S_2 T^{n-2} - \cdots + (-1)^{n-2} S_{n-2} T^2 + (-1)^{n-1} S_{n-1} T + (-1)^n S_n, \end{aligned} \tag{1.2}$$

donde $S_1, S_2, \ldots, S_n$ son los polinomios simétricos elementales en las variables $X_1, X_2, \ldots, X_n$.

La Fórmula de Cardano-Vieta, junto con el Teorema 1.9 permite obtener el resultado de sustituir las raíces de un polinomio en un polinomio simétrico. Veamos un ejemplo.

**Ejemplo 1.11** Supongamos que queremos calcular la suma de los cubos de las raíces $\alpha_1, \alpha_2$ y $\alpha_3$ del polinomio $T^3 - T + 1$. Aplicando las Fórmulas de Cardano-Vieta obtenemos

$$T^3 - T + 1 = (T - \alpha_1)(T - \alpha_2)(T - \alpha_3) = T^3 - s_1 T^2 + s_2 T - s_3$$

donde $s_i = S_i(\alpha_1, \alpha_2, \alpha_3)$. Es decir,

$$\begin{array}{rcl} s_1 & = & \alpha_1 + \alpha_2 + \alpha_3 = 0 \\ s_2 & = & \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = -1 \\ s_3 & = & \alpha_1\alpha_2\alpha_3 = -1 \end{array}$$

Entonces

$$\alpha_1^3 + \alpha_2^3 + \alpha_3^3 = s_1^3 - 3s_1s_2 + 3s_3 = -3.$$

Podemos utilizar las Fórmulas de Cardano-Vieta en sentido contrario para resolver sistemas de ecuaciones en polinomios simétricos.

**Ejemplo 1.12** Vamos a resolver el siguiente sistema de ecuaciones

$$\begin{array}{rcl} x_1 + x_2 + x_3 & = & 2 \\ x_1^2 + x_2^2 + x_3^2 & = & 4 \\ x_1^3 + x_2^3 + x_3^3 & = & 5 \end{array}$$

Si ponemos $s_1 = S_1(x_1, x_2, x_3) = x_1 + x_2 + x_3$, $s_2 = S_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$ y $s_3 = S_3(x_1x_2x_3)$, entonces de las Fórmulas de Cardano-Vieta se deduce que $x_1, x_2$ y $x_3$ son las raíces del polinomio $T^3 - s_1T^2 + s_2T - s_3$. Sabemos que $s_1 = 2$. Además $4 = x_1^2 + x_2^2 + x_3^2 = s_1^2 - 2s_2 = 4 - 2s_2$, con lo que $s_2 = 0$, y $5 = x_1^3 + x_2^3 + x_3^3 = s_1^3 - 3s_1s_2 + 3s_3 = 8 + 3s_3$ y, por tanto, $s_3 = -1$. Luego $x_1, x_2$ y $x_3$ son las raíces del polinomio $T^3 - 2T^2 + 1$. Claramente una de estas raíces es 1 y tenemos $T^3 - 2T^2 + 1 = (T - 1)(T^2 - T - 1)$. Por tanto $\{x_1, x_2, x_3\} = \left\{1, \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right\}$.

# Problemas

**1.1** Demostrar el Lema 1.8, las Proposiciones 1.1 y 1.3 y la Fórmula de Cardano-Vieta (1.2).

**1.2** Sea $A$ un anillo. Demostrar que si $P \in A[X_1, \ldots, X_n]$ tiene grado 1 y uno de los coeficientes de $P$ distinto del término constante, es una unidad de $A$, entonces $A[X_1, \ldots, X_n]/(P) \simeq A[X_1, \ldots, X_{n-1}]$.

**1.3** Sea $K$ un cuerpo y sea $P \in K[X, Y]$. Supongamos que $P(1, Y)$ es irreducible en $K[Y]$ y, considerado como polinomio en la variable en $Y$ con coeficientes en $K[X]$, $P$ es primitivo y su coeficiente principal no es divisible por $X - 1$. Demostrar que $P(X, Y)$ es irreducible en $K[X, Y]$. Encontrar tres polinomios no irreducibles $P_1, P_2, P_3 \in K[X, Y]$ de forma que cada uno de ellos cumpla dos de las tres hipótesis.

**1.4** Demostrar que si $K$ es un cuerpo y $P, Q \in K[X, Y]$ son coprimos, entonces el conjunto

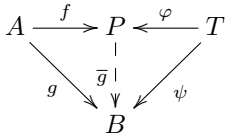
$$V(P) \cap V(Q) = \{(a, b) \in K^2 : P(a, b) = Q(a, b) = 0\}$$

es finito. (Indicación:$K(X)[Y]$ es un DIP donde $K(X)$ es el cuerpo de cocientes de $K[X]$.)

**1.5** Expresar los siguientes polinomios simétricos como polinomios en los polinomios simétricos elementales: $X_1^2 + X_2^2$, $X_1^2 + X_2^2 + X_3^2$, $X_1X_2^3 + X_1^3X_2$, $X_1X_2^2 + X_1^2X_2 + X_1X_3^2 + X_1^2X_3 + X_2X_3^2 + X_2^2X_3$.

**1.6** Haz un programa que dado un polinomio $p$ en $n$ variables $X_1, \ldots, X_n$, decida si se trata de un polinomio simétrico y en tal caso calcule un polinomio $q$ en $n$ variables tal que $q(S_1, S_2, \ldots, S_n) = p$, donde $S_1, S_2, \ldots, S_n$ son los polinomios simétricos elementales en las variables dadas. (Indicación: Observa que no basta dar el polinomio $p$ como entrada del programa, sino que también es necesario dar las variables en los que lo consideramos. Por ejemplo, $X_1 + X_2$ y $X_1X_3 + X_2X_3$ son polinomios simétricos en las variables $X_1$ y $X_2$ pero no lo son en las variables $X_1, X_2, X_3$.

**1.7** Sea $T$ un conjunto no vacío cuyos elementos llamaremos indeterminadas, y sean $A$ y $P$ dos anillos. Decimos que $P$ es una anillo de polinomios en las indeterminadas de $T$ y coeficientes en $A$ si existen un homomorfismo de anillos $f : A \to P$ y una aplicación $\varphi : T \to P$ tal que se cumple la siguiente propiedad que llamaremos *Propiedad Universal del Anillo de Polinomios*: Para todo homomorfismo de anillos $g : A \to B$ y toda aplicación $\psi : T \to B$ existe un único homomorfismo de anillos $\overline{g} : P \to B$ tal que $\overline{g}(f(a)) = g(a)$ para todo $a \in A$ y $\overline{g}(\phi(t)) = \psi(t)$ para todo $t \in$, es decir que hace conmutativo el diagrama




Demostrar:

(1) Si $T = \{T_1, \ldots, T_n\}$ entonces el anillo de polinomios $A[T_1, \ldots, T_n]$ satisface la Propiedad Universal del Anillo de Polinomios para las aplicaciones naturales $A \to A[T_1, \ldots, T_n]$ y $T \to A[T_1, \ldots, T_n]$.

(2) Existe un anillo de polinomios en las indeterminadas de $T$ con coeficientes en $A$.

(3) Todos los anillos de polinomios en las indeterminadas de $T$ con coeficientes en $A$ son isomorfos. Denotaremos $A[T]$ a cualquiera de ellos.

(4) Si $T_1$ es otro conjunto con el mismo cardinal entonces $A[T] \cong A[T_1]$.

# Capítulo 2

# Extensiones de cuerpos

## 2.1 Extensiones de cuerpos

**Definición 2.1** *Sea $K$ un cuerpo. Una* extensión *de $K$ es un cuerpo $L$ que contiene a $K$ como subcuerpo. En tal caso decimos que $L/K$ ó $K \subseteq L$ es una* extensión de cuerpos *o simplemente una extensión.*

Obsérvese que si $L/K$ es una extensión de cuerpos, entonces $L$ tiene una estructura natural de espacio vectorial sobre $K$, en la que la suma de vectores (elementos de $L$) es la suma en $L$ y el producto de escalares (elementos de $K$) por vectores (elementos de $L$) se obtiene multiplicando en $L$. Denotaremos este espacio vectorial como $L_K$ y una *base de la extensión* $L/K$ es simplemente una base de este espacio vectorial. La dimensión de este espacio vectorial se llama *grado* de la extensión $L/K$ y se representa por $[L : K]$. O sea

$$[L : K] = \dim_K(L).$$

Decimos que $L/K$ es una *extensión finita* si $[L : K] < \infty$. Obsérvese que si $L/K$ es una extensión de grado $n$ entonces $L_K \simeq K^n$. Por tanto, $|L| = |K|^n$. Eso implica que si $K$ es finito de orden $q$, entonces $L$ es finito de orden $q^n$ y si $K$ es infinito entonces $L$ tiene el mismo cardinal que $K$.

**Ejemplos 2.2** (1) Si $L/K$ es una extensión de cuerpos, entonces $[L : K] = 1$ si y solo si $K = L$.

(2) $\mathbb{C}/\mathbb{R}$ es una extensión finita de grado 2.

(3) $\mathbb{R}/\mathbb{Q}$ y $\mathbb{C}/\mathbb{Q}$ son extensiones de grado infinito pues $\mathbb{Q}$ es infinito y $\mathbb{R}$ y $\mathbb{C}$ tienen mayor cardinal que $\mathbb{Q}$.

(4) Si $n \in \mathbb{Q}$, entonces $\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} : a, b \in \mathbb{Q}\}$ es una extensión que tiene grado 1 si $n$ es un cuadrado de un número racional y grado 2 en caso contrario pues, en el segundo caso, $\{1, \sqrt{n}\}$ es una base de $\mathbb{Q}(\sqrt{n})/\mathbb{Q}$.

(5) El cuerpo de fracciones $K(X)$ del anillo de polinomios $K[X]$ es una extensión de $K$ de grado infinito.

Una *torre de extensiones de cuerpos* es una sucesión

$$K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n$$

de extensiones de cuerpos. Cada extensión $K_{i+1}/K_i$ se llama *subextensión* de la torre.

Una clase $\mathcal{C}$ de extensiones de cuerpos se dice que es *multiplicativa* si para cada torre $K_1 \subseteq K_2 \subseteq K_3$, la extensión $K_3/K_1$ está en $\mathcal{C}$ si y solo si $K_2/K_1$ y $K_3/K_1$ están en $\mathcal{C}$.

Si $L_1$ y $L_2$ son dos extensiones de $K$, entonces un *homomorfismo* de $L_1/K$ en $L_2/K$ (también llamado $K$-*homomorfismo*) es un homomorfismo de cuerpos $f : L_1 \to L_2$ tal que $f(a) = a$ para todo $a \in K$. Un *endomorfismo de una extensión* $L/K$ es un homomorfismo de $L/K$ en si misma. Un *isomorfismo de extensiones* (o $K$-isomorfismo) es un homomorfismo de extensiones que es isomorfismo de cuerpos y un *automorfismo de extensiones* (o $K$-automorfismo) es un isomorfismo de una extensión de $K$ en si misma. Obsérvese que el conjunto de los automorfismos de una extensión $L/K$ es un grupo que llamaremos *grupo de Galois* de $L/K$, en el que el producto es la composición de aplicaciones, y que denotaremos por $\mathrm{Gal}(L/K)$.

Una *subextensión* de una extensión de cuerpos $L/K$ es un subcuerpo de $L$ que contiene a $K$. Dos extensiones $L_1$ y $L_2$ de un cuerpo $K$ se dice que son *admisibles* si existe un cuerpo $L$ que es extensión de $L_1$ y $L_2$, o lo que es lo mismo, si ambas son subextensiones de una extensión común $L/K$.

Por convenio en todos los cuerpos suponemos que $0 \neq 1$. Eso implica que todos los homomorfismos entre cuerpos son inyectivos. Además los $K$-homomorfismos son homomorfismos de $K$-espacios vectoriales. De esta forma siempre que exista un homomorfismo de cuerpos $f : K \to L$, el cuerpo $L$ contiene un subcuerpo isomorfo a $K$, la imagen $f(K)$ de $f$. Por otro lado $K$ admite una extensión isomorfa a $L$, a saber el conjunto $K \cup (L \setminus f(K))$, en el que se define el producto de la forma obvia. Abusaremos a menudo de la notación y cada vez que tengamos un homomorfismo de cuerpos $f : K \to L$, simplemente consideraremos $K$ como subcuerpo de $L$, identificando los elementos de $K$ y $f(K)$, a través de $f$.

**Proposición 2.3** *(1) Sean $L_1$ y $L_2$ extensiones de $K$. Si existe un homomorfismo de $L_1/K$ en $L_2/K$, entonces $[L_1 : K] \leq [L_2 : K]$.*

*(2) Todo endomorfismo de una extensión finita es un automorfismo.*

*(3) Sea $K \subseteq E \subseteq L$ una torre de cuerpos y sean $B$ una base de $E_K$ y $B'$ una base de $L_E$. Entonces $A = \{bb' : b \in B, b' \in B'\}$ es una base de $L_K$. En particular la clase de extensiones finitas es multiplicativa y si $L/K$ es finita entonces*

*[Propiedad Multiplicativa del Grado]* $[L : K] = [L : E][E : K]$.

*(4) Si $L_1$ y $L_2$ son admisibles y $L$ es un cuerpo que contiene a $L_1$ y $L_2$ como subcuerpos, entonces*

$$L_1L_2 = \left\{ \frac{a_1b_1 + \cdots + a_nb_n}{a'_1b'_1 + \cdots + a'_nb'_n} : a_i, a'_i \in L_1, b_i, b'_i \in L_2, a'_1b'_1 + \cdots + a'_nb'_n \neq 0 \right\}$$

*es el menor subcuerpo de $L$ que contiene a $L_1$ y $L_2$. Este cuerpo se llama* compuesto *de $L_1$ y $L_2$.*

*(5) Sean $L/K$ una extensión de cuerpos y $S$ es un subconjunto de $L$. Entonces el menor subanillo de $L$ que contiene a $K$ y a $S$ está formado por los elementos de la forma $p(s_1, \ldots, s_n)$ con $p \in K[X_1, \ldots, X_n]$ y $s_1, \ldots, s_n$. Además, el menor subcuerpo de $L$ que contiene a $K$ y a $S$ está formado por los elementos de la forma*

$$\frac{p(s_1, s_2, \ldots, s_n)}{q(s_1, s_2, \ldots, s_n)}$$

*donde $n$ es un número natural arbitrario, $p, q \in K[X_1, \ldots, X_n]$, $s_1, \ldots, s_n \in S$ y $q(s_1, s_2, \ldots, s_n) \neq 0$.*

**Demostración.** (1) y (2) son una consecuencia inmediata de que todo $K$-homomorfismo de cuerpos $L_1 \to L_2$ es un homomorfismo inyectivo de espacios vectoriales sobre $K$ y de que todo endomorfismo inyectivo de un espacio vectorial de dimensión finita en si mismo es un isomorfismo.

(3) Si $l \in L$, entonces $l = \sum_{i=1}^{n} e_i b'_i$ para ciertos $e_i \in E$ y $b_i \in B'$. Cada $e_i$ es una combinación lineal $e_i = \sum_{j=1}^{m_i} k_{ij} b_{ij}$, con $k_i \in K$ y $b_i \in B$. Por tanto

$$l = \sum_{i=1} \sum_{j=1}^{m_i} k_{ij} b_{ij} b'_i$$

lo que muestra que $A$ es un conjunto generador de $L_K$.

Supongamos que $\sum_{b \in B, b' \in B'} k_{b,b'} bb' = 0$, con $k_{b,b'} \in K$ y $k_{b,b'} = 0$ para casi todo $(b, b') \in B \times B'$. Para cada $b' \in B'$, ponemos $e_{b'} = \sum_{b \in B} k_{b,b'} b \in E$. Como $k_{b,b'} = 0$, para casi todo $(b, b') \in B \times B'$, se tiene que $e_b = 0$ para casi todo $b \in B$. Además y $\sum_{b' \in B} e_{b'} b' = 0$. Como $B'$ es linealmente independiente sobre $E$, se tiene que $e_{b'} = 0$ para todo $b' \in B'$. Utilizando que $B$ es linealmente independiente sobre $K$, deducimos que $k_{b,b'} = 0$ para todo $(b, b') \in B \times B'$, lo que muestra que $A$ es linealmente independiente.

(4) y (5) Ejercicio. □

Si $L/K$ es una extensión y $S$ es un subconjunto de $L$, entonces $K[S]$ denota el menor subanillo de $L$ que contiene a $K$ y lo llamamos *subanillo* de $L$ *generado* por $K$ y $S$. El subcuerpo $K(S)$ descrito en el apartado (5) de la Proposición 2.3 se llama *extensión* de $K$ *generada* $S$. Observando que la intersección de subcuerpos de un cuerpo $L$ es otro subcuerpo de $L$, se tiene que $K(S)$ es la intersección de todos los subcuerpos de $L$ que contienen a $K$ y a $S$. Obsérvese que si $S_1$ y $S_2$ son dos subconjuntos de $L$, entonces

$$K(S_1)K(S_2) = K(S_1 \cup S_2).$$

De la misma forma, si $L_1/K$ y $L_2/K$ son dos subextensiones de $L$, entonces $L_1L_2$ es la intersección de todos los subcuerpos de $L$ que contienen a $L_1 \cup L_2$ y por tanto

$$L_1L_2 = K(L_1 \cup L_2).$$

El concepto de compuesto de dos subextensiones se puede generalizar de forma obvia a una familia arbitraria de subextensiones: Si $\mathcal{C}$ es una familia de subextensiones de $L/K$ entonces el *compuesto* de $\mathcal{C}$ es el menor subcuerpo de $L$ que contiene a todos los elementos de $\mathcal{C}$ y coincide con la intersección de todos los subcuerpos de $L$ que contienen todos los elementos de $\mathcal{C}$ y con $K(\cup_{E \in \mathcal{C}} E)$. Si $\mathcal{C} = \{L_1/K, \ldots, L_n/K\}$, entonces el compuesto de $\mathcal{C}$ se denota por $L_1 \cdots L_n$ y está formado por todos los elementos de la forma

$$\frac{\sum_{i=1}^{m} a_{1i} \cdots a_{ni}}{\sum_{i=1}^{m} b_{1i} \cdots b_{ni}}$$

con $m$ arbitrario, $a_{ji}, b_{ji} \in L_i$ y $\sum_{i=1}^{m} b_{1i} \cdots b_{ni} \neq 0$.

Si $S = \{a_1, \ldots, a_n\}$, entonces escribimos $K[S] = K[\alpha_1, \ldots, \alpha_n]$ y $K(S) = K(a_1, \ldots, a_n)$. Decimos que $L/K$ es una *extensión finitamente generada* si existen $a_1, \ldots, a_n \in L$ tales que $L = K(a_1, \ldots, a_n)$ y que es *simple* si $L = K(a)$ para algún $a \in L$. En este último caso decimos que $a$ es un *elemento primitivo* de $L/K$.

**Lema 2.4** *Sea $L/K$ una extensión. Si $\alpha \in L$ es una raíz de un polinomio irreducible $p$ de grado $n$ $K[X]$ entonces*

*(1)* $K[\alpha] = K(\alpha)$.

*(2) Si $q \in K[X]$, entonces $q(\alpha) = 0$ si y solo si $p$ divide a $q$ en $K[X]$.*

*(3)* $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ *es una base de* $K(\alpha)_K$. *En particular,* $[K(\alpha) : K] = n$.

**Demostración.** (1) y (2) Consideremos el homomorfismo de sustitución $S = S_\alpha : K[X] \to L$ y sea $I = \text{Ker } S = \{q \in K[X] : q(\alpha) = 0\}$. Como obviamente $I$ es un ideal propio de $K[X]$ y $\alpha$ es raíz de $p$ se tiene $(p) \subseteq I \subset K[X]$. Pero $(p)$ es un ideal maximal de $K[X]$, pues $K[X]$ es un DIP. Concluimos que $I = (p)$ y, del Primer Teorema de Isomorfía deducimos que $K[\alpha] = \text{Im } S \simeq K[X]/(p)$, que es un cuerpo pues $(p)$ es un ideal maximal de $K[X]$. Esto implica que $K[\alpha] = K(\alpha)$ y que para todo $q \in K[X]$ se verifica $q(\alpha) = 0$ si y solo si $p|q$ en $K[X]$.

(3) Si $\beta \in K[\alpha]$, entonces $b = f(\alpha)$ para algún $f \in K[X]$. Como el grado define una función euclídea en $K[X]$, existen $q, r \in K[X]$ tales que $f = qp + r$ y $m = \text{gr}(r) < \text{gr}(p) = n$. Entonces $\beta = f(\alpha) = r(\alpha) = r_0 + r_1\alpha + r_2\alpha^2 \cdots + r_m\alpha^m$. Esto prueba que $1, \alpha, \ldots, \alpha^{n-1}$ genera $K(\alpha)_K$. Para demostrar que son linealmente independientes ponemos $\sum_{i=0}^{n-1} a_i\alpha^i = 0$, con $k_i \in K$. Entonces $\alpha$ es raíz del polinomio $a = \sum_{i=0}^{n-1} a_iX^i$, es decir $a \in KerS = (p)$. Como $n = \text{gr}(p) > \text{gr}(a)$, deducimos que $a = 0$, es decir $a_i = 0$ para todo $i$. □

## 2.2 Adjunción de raíces

El siguiente teorema muestra que todos los polinomios no constantes tienen alguna raíz en algún cuerpo.

**Teorema 2.5 (Kronecker)** *Si $K$ es un cuerpo y $p \in K[X] \setminus K$, entonces existe una extensión $L$ de $K$ que contiene una raíz de $p$.*

**Demostración.** Como $p \in K[X] \setminus K[X]^*$ y $K[X]$ es un DFU, $p$ es divisible en $K[X]$ por un polinomio irreducible y todas las raíces de este divisor son raíces de $p$. Por tanto podemos suponer que $p$ es irreducible. Eso implica que $(p)$ es un ideal maximal de $K[X]$, pues este último es un DIP. Entonces $L = K[X]/(p)$ es un cuerpo. La composición de la inclusión $K \to K[X]$ y la proyección $K[X] \to L = K[X]/(p)$ es un homomorfismo (inyectivo) de cuerpos y por tanto podemos considerar $L$ como una extensión de $K$. Para acabar la demostración basta ver que $a = X + (p)$ es una raíz de $p$. En efecto, $p(a) = p(X + (p)) = p + (p) = (p)$, que es el cero del anillo $L$. □

Por tanto, si $p \in K[X]$ es un polinomio no constante entonces existe una extensión $L/K$ que contiene una raíz $\alpha$ de $p$ y $K(\alpha)$ es la menor subextensión de $L/K$ que contiene a $\alpha$.

Decimos que un polinomio $p \in K[X] \setminus K$ es *completamente factorizable* sobre $K$ si es producto de polinomios de grado 1, o lo que es lo mismo si $p = a(X-\alpha_1)\cdots(X-\alpha_n)$ para ciertos $a, \alpha_1, \ldots, \alpha_n \in K$. En tal caso las raíces de $p$ son $\alpha_1, \ldots, \alpha_n$. Por ejemplo

$$X^3 - 1 = (X-1)(X^2+X+1) = (X-1)\left(X - \frac{-1+\sqrt{-3}}{2}\right)\left(X - \frac{-1-\sqrt{-3}}{2}\right)$$

es completamente factorizable sobre $\mathbb{C}$, pero no sobre $\mathbb{Q}$ ni $\mathbb{R}$. El Teorema de Kronecker afirma que cada polinomio no constante tiene una raíz en alguna extensión. De hecho podemos decir algo más.

**Corolario 2.6** *Si $K$ es un cuerpo y $p \in K[X] \setminus K$, entonces $p$ es completamente factorizable en alguna extensión de $K$.*

**Demostración.** Por inducción sobre el grado de $p$. Si el grado de $p$ es 1, no hay nada que demostrar. Si el grado de $p$ es mayor que 1 entonces $p$ tiene una raíz $\alpha$ en alguna extensión $E$ de $K$. Entonces $p = (X-\alpha)q$ para algún $q \in E[X] \setminus E$. Por hipótesis de inducción $q$ es completamente factorizable en alguna extensión $L$ de $E$, es decir $q$ es producto de polinomios de grado menor o igual que 1 en $L[X]$ y por tanto también $p$ es producto de polinomios de grado menor o igual que 1. □

La siguiente definición modela nuestro objetivo principal.

**Definición 2.7** *Una* torre radical *es una torre de cuerpos*

$$E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n$$

*tal que para cada* $i = 1, \ldots, n$, *existen* $n_i \geq 1$ *y* $\alpha_i \in E_i$ *tal que* $E_i = E_{i-1}(\alpha_i)$ *y* $\alpha^{n_i} \in E_{i-1}$.

*Una* extensión *de cuerpos* $L/K$ *se dice que es* radical *si existe una torre radical*

$$K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = L.$$

*Una ecuación polinómica* $P(X) = 0$, *con* $P \in K[X]$, *se dice que es* resoluble por radicales *sobre* $K$ *si existe una extensión radical* $L/K$ *tal que* $P$ *es completamente factorizable en* $L$. *En tal caso también se dice que el polinomio* $P$ *es resoluble por radicales sobre* $K$.

Nuestro objetivo principal es establecer un criterio de cuándo un polinomio es resoluble por radicales que es precisamente cuando sus raíces se puedan expresar en sucesivas extensiones en las que en cada paso se adjunta una raíz $n$-ésima de elementos del cuerpo anterior. O sea si suponemos que $P \in K[X]$ entonces $P$ es resoluble sobre $K$ si $K$ tiene una extensión radical que contiene todas las raíces de $P$. Para llegar a ello tenemos que recorrer un largo camino que se completará en los dos últimos capítulos.

Recordemos que si $\sigma : K \to E$ es un homomorfismo de anillos, entonces $\sigma$ tiene una única extensión a un homomorfismo entre los anillos de polinomios, que seguiremos denotando por $\sigma : K[X] \to E[X]$, tal que $\sigma(X) = X$. Este homomorfismo se comporta bien sobre las raíces.

**Lema 2.8** *Sean* $\sigma : E \to L$ *un homomorfismo de cuerpos y* $p \in E[X]$. *Si* $\alpha$ *es una raíz de* $p$ *en* $E$ *entonces* $\sigma(\alpha)$ *es una raíz de* $\sigma(p)$.

*Si* $E/K$ *y* $L/K$ *son extensiones de un cuerpo* $K$, $p \in K[X]$ *y* $\sigma$ *es un* $K$*-homomorfismo entonces* $\sigma$ *se restringe a una aplicación inyectiva del conjunto de las raíces de* $p$ *en* $E$ *al conjunto de las raíces de* $p$ *en* $L$.

*En particular, si* $E = L$ *(es decir, si* $\sigma \in \mathrm{Gal}(L/K)$*), entonces esta restricción de* $\sigma$ *es una permutación del conjunto de las raíces de* $p$ *en* $L$.

**Demostración.** Si $p = p_0 + p_1X + \cdots + p_nX^n$, entonces

$$\begin{aligned} \sigma(p)(\sigma(\alpha)) &= (\sigma(p_0) + \sigma(p_1)X + \sigma(p_1)X^2 + \cdots + \sigma(p_n)X^n)(\sigma(\alpha)) \\ &= \sigma(p_0) + \sigma(p_1)\sigma(\alpha) + \sigma(p_1)\sigma(\alpha)^2 + \cdots + \sigma(p_n)\sigma(\alpha)^n \\ &= \sigma(p_0 + p_1\alpha + p_1\alpha^2 + \cdots + p_n\alpha^n) \\ &= \sigma(p(\alpha)) = \sigma(0) = 0. \end{aligned}$$

Esto prueba la primera afirmación. Las otras dos afirmaciones son consecuencias inmediatas de la primera. □

**Lema 2.9 (Lema de Extensión)** *Sea* $\sigma : K_1 \to K_2$ *un homomorfismo de cuerpos y sea* $p \in K_1[X]$ *un polinomio irreducible. Sean* $L_1/K_1$ *y* $L_2/K_2$ *dos extensiones de cuerpos y sean* $\alpha_1 \in L_1$ *y* $\alpha_2 \in L_2$ *con* $\alpha_1$ *una raíz de* $p$.

*Entonces existe un homomorfismo* $\widehat{\sigma} : K_1(\alpha_1) \to K_2(\alpha_2)$ *tal que* $\widehat{\sigma}|_{K_1} = \sigma$ *y* $\widehat{\sigma}(\alpha_1) = \alpha_2$ *si y solo si* $\alpha_2$ *es una raíz del polinomio* $\sigma(p)$. *En tal caso sólo hay un homomorfismo* $\widehat{\sigma}$ *que satisfaga la condición indicada y si además,* $\sigma$ *es un isomorfismo, entonces también* $\widehat{\sigma}$ *es un isomorfismo.*

**Demostración.** Si existe el homomorfismo $\widehat{\sigma}$ satisfaciendo la propiedad indicada entonces del Lema 2.8 se tiene que $\alpha_2 = \widehat{\sigma}(\alpha_1)$ es una raíz de $\widehat{\sigma}(p) = \sigma(p)$.

Recíprocamente, supongamos que $\alpha_2$ es una raíz de $\sigma(p)$. Consideremos los homomorfismos de sustitución en $\alpha_1$ y $\alpha_2$: $S_{\alpha_1} : K_1[X] \to K_1(\alpha_1)$ y $S_{\alpha_2} : K_2[X] \to K_2(\alpha_2)$. Por el Lema 2.4, $K_1[\alpha_1] = K_1(\alpha_1)$, $[K(\alpha_1) : K] = \mathrm{gr}(p)$ y $(p) = \mathrm{Ker}\, S_{\alpha_1}$. Además, por el Lema 2.8, $\sigma(p) \in \mathrm{Ker}\, S_{\alpha_2}$. Todo esto implica que la aplicación $\widehat{\sigma} : K_1(\alpha_1) \to K_2(\alpha_2)$, dada por $\widehat{\sigma}(f(\alpha_1)) = \sigma(f)(\alpha_2)$, para $f \in K_1[X]$, está bien definida pues si $f(\alpha_1) = g(\alpha_1)$, con $f, g \in K_1[X]$, entonces $f - g \in \mathrm{Ker}\, S_{\alpha_1}$, con lo que $p$ divide a $f - g$ en $K_1[X]$. Luego $\sigma(p)$ divide a $\sigma(f) - \sigma(g)$ en $K_2[X]$ y por tanto $\sigma(f) - \sigma(g) \in \mathrm{Ker}\, S_{\alpha_2}$, es decir $\sigma(f)(\alpha_2) = \sigma(g)(\alpha_2)$. Una vez que hemos visto que $\widehat{\sigma}$ está bien definida, es trivial ver que es un homomorfismo de cuerpos y que satisface las condiciones del Lema.

Si además $\sigma$ es un isomorfismo, entonces $\widehat{\sigma}$ es un isomorfismo pues todo homomorfismo de cuerpos es inyectivo y además $K_2$ y $\alpha_2$ están en la imagen de $\widehat{\sigma}$, lo que muestra que $\widehat{\sigma}$ es suprayectivo.

Para la unicidad ver el Ejemplo 1.4. □

Si aplicamos el Lema anterior al caso en que $\sigma$ es la aplicación identidad $\sigma : K \to K$ entonces obtenemos que si $\alpha$ es una raíz de un polinomio irreducible $p$ de $K[X]$ en una extensión de $K$ entonces la extensión $K(\alpha)/K$ es única salvo $K$-isomorfismos. Más aún, si $\beta$ es ora raíz de $p$ entonces $K(\alpha)$ y $K(\beta)$ son $K$-isomorfos.

**Proposición 2.10** *Sea $p \in K[X]$ un polinomio irreducible y $\alpha$ y $\beta$ son dos raíces de $p$ en dos extensiones de $K$ (tal vez dos extensiones diferentes). Entonces existe un único $K$-isomorfismo $f : K(\alpha) \to K(\beta)$ tal que $f(\alpha) = \beta$. En particular las dos extensiones $K(\alpha)/K$ y $K(\beta)/K$ son isomorfas.*

Obsérvese que la hipótesis de que el polinomio $p$ sea irreducible en la Proposición 2.10 es imprescindible. Por ejemplo, si $p = X(X^2 + 1)$, entonces 0 e $i$ son dos raíces de $p$ y obviamente $\mathbb{Q}(0) = \mathbb{Q}$ no es isomorfo a $\mathbb{Q}(i)$.

A la vista de la Proposición 2.10, si $p \in K[X]$ es irreducible, hablaremos de *la extensión de $K$ obtenida adjuntando a $K$ una raíz del polinomio irreducible $p$*, como la extensión $K(\alpha)/K$ donde $\alpha$ es cualquier raíz de $p$ es una extensión arbitraria de $K$.

## 2.3 Extensiones algebraicas

**Definición 2.11** *Sea $L/K$ una extensión de cuerpos. Un elemento $\alpha \in L$ se dice que es* algebraico *sobre $K$ si existe un polinomio no nulo $0 \neq p \in K[X]$ tal que $p(\alpha) = 0$. En caso contrario se dice que $\alpha$ es* transcendente *sobre $K$. En otras palabras, $\alpha$ es transcendente sobre $K$ si el homomorfismo de sustitución*

$$\begin{array}{rcl} S_\alpha : K[X] & \to & L \\ p & \to & p(\alpha) \end{array}$$

*es inyectivo y algebraico en caso contrario.*

*Decimos que $L/K$ es una* extensión algebraica *si todo elemento de $L$ es algebraico sobre $K$. En caso contrario decimos que la* extensión *es* transcendente.

La siguiente proposición caracteriza cuándo un elemento es algebraico.

**Proposición 2.12** *Si $L/K$ es una extensión de cuerpos y $\alpha \in L$, entonces las siguientes condiciones son equivalentes:*

*(1) $\alpha$ es algebraico sobre $K$.*

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

*(3) $K[\alpha]$ es un subcuerpo de $L$.*

*(4) $K(\alpha)/K$ es finita.*

**Demostración.** (1) implica (2) y (4) Supongamos que $\alpha$ es algebraico sobre $K$ y sea $0 \neq f \in K[X]$ tal que $f(\alpha) = 0$. Si $f = p_1 \cdots p_n$ es una factorización de $f$ es producto de irreducibles de $K[X]$, entonces $p_1(\alpha) \cdots p_n(\alpha) = f(\alpha) = 0$ y por tanto $p_i(\alpha) = 0$ para algún $i$. Eso implica que $\alpha$ es una raíz de un polinomio irreducible de $K[X]$ y del Lema 2.4 se deduce que $K[\alpha] = K(\alpha)$ y que $K(\alpha)/K$ es finita.

(2) implica (3) es obvio.

Para demostrar (3) implica (1) y (4) implica (1) consideramos el homomorfismo de sustitución $S = S_\alpha : K[X] \to K[\alpha]$. Si $\alpha$ no es algebraico entonces $S$ es un isomorfismo. Como $K[X]$ no es un cuerpo y tiene dimensión infinita entonces no se verifican ni (3) ni (4). □

Sean $L/K$ una extensión y $\alpha$ un elemento de $L$ algebraico sobre $K$. Entonces el núcleo $I$ del homomorfismo de sustitución $S = S_\alpha : K[X] \to L$ es un ideal no nulo que es primo pues $K[X]/I \simeq K[\alpha]$ es un dominio. Por tanto $I = (p)$ para un polinomio irreducible $p$ de $K[X]$. De todos los generadores de $I$, hay uno sólo que sea mónico. Se llama *polinomio irreducible* ó *mínimo* de $\alpha$ sobre $K$, denotado $\mathrm{Min}_K(\alpha)$, al único generador mónico de $I = \mathrm{Ker}\, S_\alpha$. Está claro que $\mathrm{Min}_K(\alpha)$ es el único polinomio mónico de grado mínimo de $I$. Del Lema 2.4 se deduce que si $\mathrm{Min}_K(\alpha)$ tiene grado $n$, entonces $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)/K$. En resumen:

**Lema 2.13** *Si $\alpha$ es algebraico sobre $K$, entonces $[K(\alpha) : K] = \mathrm{gr}(\mathrm{Min}_K(\alpha))$ y si este grado es $n$, entonces $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)_K$.*

**Ejemplos 2.14** (1) $\mathrm{Min}_{\mathbb{Q}}(\sqrt{2}) = X^2 - 2$, $\mathrm{Min}_{\mathbb{R}}(\sqrt{2}) = X - \sqrt{2}$ y $\mathrm{Min}_{\mathbb{Q}}(i) = \mathrm{Min}_{\mathbb{R}}(i) = X^2 + 1$. Más generalmente, si $q \in \mathbb{Q}$ y $\sqrt{q} \notin \mathbb{Q}$, entonces $\mathrm{Min}_{\mathbb{Q}}(\sqrt{q}) = X^2 - q$.

(2) Si $\alpha = \sqrt{5 + \sqrt{5}}$, entonces $\alpha^2 - 5 = \sqrt{5}$, con lo que $5 = (\alpha^2 - 5)^2 = \alpha^4 - 10\alpha^2 + 25$, es decir $\alpha$ es una raíz del polinomio $X^4 - 10X + 20$. Aplicando el Criterio de Eisentein a este polinomio para el primo 5, deducimos que es irreducible sobre $\mathbb{Q}$ y por tanto $\mathrm{Min}_{\mathbb{Q}}(\alpha) = X^4 - 10X + 20$.

(3) El cuerpo de fracciones de $K[X]$ es $K(X)$ y $K(X)/K$ es una extensión de grado infinito pues las potencias de $X$ son linealmente independientes sobre $K$. Por tanto $X$ es transcendente sobre $K$.

(4) Decidir si un número real o complejo es algebraico sobre el cuerpo de los números racionales es un problema normalmente muy difícil. El carácter algebraico o transcendente del número $\pi$ sobre $\mathbb{Q}$ fue un problema sin resolver durante muchos años hasta que Lindemann demostró en 1882 que es transcendente. También es transcendente la base $e$ del logaritmo neperiano, lo que fue demostrado por Hermite en 1873.

Una consecuencia de la Proposición 2.12 es el siguiente corolario que caracteriza las extensiones finitas.

**Corolario 2.15** *Las siguientes condiciones son equivalentes para una extensión de cuerpos.*

*(1) $L/K$ es finita.*

*(2) $L/K$ es algebraica y finitamente generada.*

*(3) Existen $\alpha_1, \ldots, \alpha_n \in L$ algebraicos sobre $K$ tales que $L = K(\alpha_1, \ldots, \alpha_n)$.*

**Demostración.** (1) implica (2). Supongamos que $L/K$ es finita. Entonces $[K(\alpha):K] \leq [L:K] < \infty$ para todo $\alpha \in L$. De la Proposición 2.12 se deduce que $\alpha$ es algebraico sobre $K$. Por otro lado, si $\alpha_1, \ldots, \alpha_n$ es una base de $L_K$, entonces $L = K(\alpha_1, \ldots, \alpha_n)$ y por tanto $L/K$ es finitamente generada.

(2) implica (3) es obvio.

(3) implica (1). Si $\alpha_1, \ldots, \alpha_n$ satisfacen las condiciones de (3), entonces cada $\alpha_i$ es algebraico sobre $K(\alpha_1, \ldots, \alpha_{i-1})$. Por tanto $K(\alpha_1, \ldots, \alpha_i)/K(\alpha_1, \ldots, \alpha_{i-1})$ es una extensión finita por el Lema 2.12. Aplicando que la clase de extensiones finitas es multiplicativa deducimos que $L = K(\alpha_1, \ldots, \alpha_n)/K$ es finita. □

**Corolario 2.16** *La clase de extensiones algebraicas es multiplicativa.*

**Demostración.** Sea $K \subseteq E \subseteq L$ una torre de extensiones. Es obvio que si $L/K$ es algebraica entonces $E/K$ y $L/K$ son algebraicas. Recíprocamente, supongamos que $E/K$ y $L/E$ son algebraicas y sea $\alpha \in L$. Entonces $\alpha$ es algebraico sobre $E$. Sea $p = \mathrm{Min}_E(\alpha)$ y sean $p_0, p_1, \ldots, p_n$ los coeficientes de $p$. Por hipótesis $p_0, p_1, \ldots, p_n$ que son algebraicos sobre $K$, lo que implica que $F = K(p_0, p_1, \ldots, p_n)/K$ es finita, por el Corolario 2.15. Además, $\alpha$ es algebraico sobre $F$ y por tanto $F(\alpha)/F$ es finita. Entonces $[K(\alpha):K] \leq [K(\alpha, p_0, p_1, \ldots, p_n):K] = [F(\alpha):F][F:K] < \infty$. De la Proposición 2.12 deducimos que $\alpha$ es algebraico sobre $K$. □

**Corolario 2.17** *Si $L/K$ es una extensión de cuerpos, entonces el conjunto $C$ de los elementos de $L$ que son algebraicos sobre $K$ es un subcuerpo de $L$ que contiene a $K$, llamado* clausura algebraica *de $L/K$, o* clausura algebraica *de $K$ en $L$..*

*En particular, si $S$ es un subconjunto de $L$ formado por elementos algebraicos sobre $K$, entonces $K(S)$ es algebraico sobre $K$.*

**Demostración.** Obviamente $K \subseteq C$. Si $\alpha, \beta \in C$, entonces $\beta$ es algebraico sobre $K(\alpha)$ y por tanto $K(\alpha)/K$ y $K(\alpha,\beta)/K(\alpha)$, son algebraicas lo que implica que $K(\alpha,\beta)/K$ es también algebraica (Corolario 2.16). Por tanto todo elemento de $K(\alpha,\beta)$ es algebraico sobre $K$ y en particular $\alpha+\beta, \alpha-\beta, \alpha\beta \in C$ y, si $\beta \neq 0$, entonces $\beta^{-1} \in C$. Esto prueba que $C$ es un subcuerpo de $L$. □

Decimos que una clase $\mathcal{C}$ de extensiones de cuerpos es cerrada para *levantamientos* si para cada dos extensiones admisibles $L_1/K$ y $L_2/K$ tales que $L_1/K$ esté en $\mathcal{C}$ se verifica que $L_1L_2/L_2$ también está en $\mathcal{C}$.

**Proposición 2.18** *Cada una de las clases de extensiones finitas, algebraicas, finitamente generadas y simples, son cerradas para levantamientos.*

**Demostración.** Sean $L_1/K$ y $L_2/K$ dos extensiones admisibles. Está claro que si $L_1 = K(\alpha_1, \ldots, \alpha_n)$, entonces $L_2L_1 = L_2(L_1) = L_2(\alpha_1, \ldots, \alpha_n)$, lo que muestra que las clases de extensiones finitamente generadas y de extensiones simples son ambas cerradas para extensiones. Por otro lado si $L_1/K$ es algebraica, entonces todo elemento de $L_1$ es algebraico sobre $K$ y por tanto también sobre $L_2$, lo que implica que $L_1L_2 = L_2(L_1)$ es algebraico sobre $K$, por el Corolario 2.17. Esto prueba que la clase de extensiones algebraicas es cerrada para levantamientos. Como una extensión es finita si y solo si es algebraica y finitamente generada (Proposición 2.12) deducimos que la clase de extensiones finitas también es cerrada para levantamientos. □

Recuérdese que todo endomorfismo de una extensión finita ha de ser un automorfismo (Proposición 2.3). Esta propiedad se verifica de hecho para toda extensión algebraica.

**Proposición 2.19** *Si $L/K$ es una extensión algebraica, entonces todo $K$-endomorfismo de $L$ es un automorfismo.*

**Demostración.** Sea $\sigma$ un $K$-endomorfismo de $L$. Como todo homomorfismo de cuerpos es inyectivo, sólo hay que probar que $\sigma$ es suprayectivo. Sea $\alpha \in L$ y sean $p = \mathrm{Min}_K(\alpha)$, $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ las raíces de $p$ en $L$. Del Lema 2.8 se deduce que $\sigma$ permuta $\{\alpha_1, \ldots, \alpha_n\}$ y por tanto $\alpha = \sigma(\alpha_i)$ para algún $i$. □

# Problemas

En los siguientes ejercicios $K$ es un cuerpo, $L/K$ una extensión de cuerpos y $X$ es una variable.

**2.1** Sea $\alpha$ una raíz real del polinomio $X^3+3X^2-3X+3$. Expresar cada uno de los siguientes elementos como combinación lineal de $1, \alpha, \alpha^2$ con coeficientes en $\mathbb{Q}$:

$$\alpha^7, \quad \alpha^4 + \alpha + 2, \quad (\alpha+1)^{-1}.$$

**2.2** Calcular los grados y una base de las siguientes extensiones.

$$\mathbb{Q}(\sqrt{2})/\mathbb{Q}, \quad \mathbb{Q}(i)/\mathbb{Q}, \quad \mathbb{Q}(i,\sqrt{2})/\mathbb{Q}, \quad \mathbb{Q}(i,\sqrt{2})/\mathbb{Q}(i), \quad \mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}, \quad \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}, \quad \mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}.$$

**2.3** Demostrar que si $n \in \mathbb{Z}$, entonces $[\mathbb{Q}(\sqrt{n}) : \mathbb{Q}] \leq 2$ y decidir cuándo es 1 y cuándo es 2.

**2.4** Calcular el grado y una base de las siguientes extensiones

$$K(X)/K,\ K(X)/K(X^2),\ K(X)/K(X+1),\ K(X)/K(X^6),\ K(X)/K(X^2+X+1),\ K(X^2)/K(X^6),$$

donde $K(X)$ es el cuerpo de fracciones de $K[X]$.

**2.5** Calcular $[K(X) : K(p)]$, donde $p \in K[X]$ es un polinomio irreducible.

**2.6** Demostrar que $\mathbb{Q}(i,\sqrt{2}) = \mathbb{Q}(i+\sqrt{2})$. Calcular $\mathrm{Min}_{\mathbb{Q}}(i+\sqrt{2}), \mathrm{Min}_{\mathbb{Q}}(i+\sqrt{2})$ y $\mathrm{Min}_{\mathbb{Q}(\sqrt{2})}(i+\sqrt{2})$.

**2.7** Demostrar que si $\mathrm{car}K \neq 2$ y $a, b \in K$, entonces $K(\sqrt{a},\sqrt{b}) = K(\sqrt{a}+\sqrt{b})$.

**2.8** Demostrar que si $p$ y $q$ son dos números primos distintos, entonces el polinomio $X^4-2(p+q)X^2+(p-q)^2$ es irreducible sobre $\mathbb{Q}$. (Indicación: El ejercicio 2.7.)

**2.9** Calcular el polinomio mínimo sobre $\mathbb{Q}$ de los siguientes números complejos.

$$\sqrt{2}+1, \quad \sqrt[3]{3}-1, \quad \sqrt[3]{2}-\sqrt[3]{4}, \quad \sqrt[4]{2}+\sqrt[2]{2}+1, \sqrt{3}+\sqrt[5]{3}, \quad \sqrt[5]{2}\sqrt[3]{3},$$
$$\sqrt{2+\sqrt[3]{2}}, \quad \sqrt[3]{2}+i\sqrt[5]{2}, \quad \sqrt{2+\sqrt{2+\sqrt{2}}}, \quad \sqrt[4]{7+4\sqrt{3}}-\sqrt[4]{7-4\sqrt{3}}.$$

**2.10** Demostrar que si $\mathrm{car}K \neq 2$ y $K$ contiene raíces cuadradas de todos los elementos de $K$, entonces todos los polinomios de grado 2 sobre $K$ son reducibles. Mostrar que esto no es así si $\mathrm{car}K = 2$.

**2.11** Dados $a, b \in K^*$, demostrar que $K(\sqrt{a}) = K(\sqrt{b})$ si y solo si $K(\sqrt{ab}) = K$. Utilizar esto para calcular $[Q(\sqrt{n},\sqrt{m}) : \mathbb{Q}]$ para dos números enteros arbitrarios $n$ y $m$.

**2.12** Calcular el grado y una base de $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ sobre $\mathbb{Q}$.

**2.13** Demostrar que si $p_1, \ldots, p_n, q$ son primos distintos, entonces $\sqrt{q} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$.

**2.14** Sea $K$ un cuerpo y sean $P_1, \ldots, P_r$ polinomios de $K[X]$. Demostrar que existe una extensión de cuerpos $K'/K$ tal que cada $P_i$ se descompone totalmente en $K'[X]$.

**2.15** Encontrar un polinomio irreducible $p \in \mathbb{Q}[X]$ y una raíz $\alpha \in \mathbb{R}$ de $p$ tal que $p$ no es completamente factorizable sobre $\mathbb{Q}(\alpha)$.

**2.16** Demostrar que un polinomio $f \in K[X]$ tiene una raíz doble en alguna extensión de $K$ si y solo si $f$ y su derivada $f'$ no son coprimos en $K[X]$.

**2.17** Sea $q = p^n$, con $p$ primo y $n$ un entero positivo y sea $L$ una extensión de $\mathbb{Z}_p$ en la que el polinomio $X^q - X$ factoriza completamente. Demostrar:

(1) El conjunto de las raíces del polinomio $X^q - X$ en $L$ forman un subcuerpo de $L$ de orden $q$.

(2) Si $m$ es un entero positivo entonces existe un cuerpo de orden $m$ si y solo si $m$ es una potencia de un primo.

(3) Para todo $n$ existe un polinomio irreducible de grado $n$ en $\mathbb{Z}_p[X]$.

(4) Dos cuerpos finitos del mismo cardinal son isomorfos.

De este problema deducimos que para cada potencia de un primo $q$ existe al menos un cuerpo con $q$ y que todos los cuerpos con $q$ elementos son isomorfos. Denotaremos por $\mathbb{F}_q$ al cuerpo con $q$ elementos (único salvo isomorfismos). En particular, si $q$ es primo, entonces $\mathbb{F}_p = \mathbb{Z}_p$.

**2.18** Construir cuerpos de 4, 8, 16, 9, 27 y 121 elementos.

**2.19** Sea $q$ una potencia de un primo y sean $n$ y $m$ un enteros positivos. Demostrar que $\mathbb{F}_{q^m}$ tiene un subcuerpo de orden $q^n$ si y solo si $n|m$.

**2.20** Calcular cuántos subcuerpos tiene un cuerpo de order $p^n$, con $p$ primo. Construir un cuerpo $\mathbb{F}_{64}$ con 64 elementos y calcular todos sus subcuerpos. ¿Cuantos elementos $\alpha$ de $\mathbb{F}_{64}$ verifican que $\mathbb{F}_2[\alpha] = \mathbb{F}_{64}$?

**2.21** Demostrar que si $p$ es primo y $K$ es un cuerpo con $p^n$ elementos, entonces cada elemento de $K$ tiene exactamente una raíz $p$-ésima.

**2.22** Sean $E = \mathbb{Z}_2[X]/(X^2 + X + 1)$ y $F = \mathbb{Z}_2[X]/(X^3 + X + 1)$. Calcular los polinomios mínimos de todos los elementos de $E$ y $F$ sobre $\mathbb{Z}_2$. Construir un cuerpo de orden mínimo que contenga subcuerpos isomorfos a $E$ y $F$.

**2.23** Calcular las raíces complejas del siguiente polinomio $X^4 - 2X^2 + 2$ y la extensión de $\mathbb{Q}$ generada por cada dos de ellas.

**2.24** Demostrar que si $[L : K]$ es impar y $\alpha \in L$, entonces $K(\alpha^2) = K(\alpha)$.

**2.25** Decidir sobre la verdad o falsedad de las siguientes afirmaciones, demostrando las afirmaciones verdaderas y dando un contraejemplo de las falsas.

(1) Existe una extensión de $K$ de grado mayor que 1.

(2) Existe una extensión algebraica de $K$ de grado mayor que 1.

(3) Toda extensión simple es algebraica.

(4) Toda extensión es simple.

(5) Todas las extensiones transcendentes simples son isomorfas.

(6) Si $E$ y $F$ son dos subextensiones $K$-isomorfas de $L/K$ entonces $E = F$.

(7) Si $\alpha \in L$ es transcendente sobre $K$ y $p \in K[X]$, entonces $p(\alpha)$ es transcendente sobre $K$.

(8) Si $p \in K[X]$ y $p(\alpha)$ es transcendente sobre $K$, entonces $\alpha \in L$ es transcendente sobre $K$.

(9) El cardinal del conjunto de números complejos que son algebraicos sobre $\mathbb{Q}$ es numerable.

(10) Si $L/K$ es una extensión finita, entonces $L$ y $K$ tienen el mismo cardinal.

(11) Si $L/K$ es una extensión algebraica y $K$ es infinito, entonces $L$ y $K$ tienen el mismo cardinal.

**2.26** Demostrar las siguientes afirmaciones para $E/K$ y $F/K$ dos extensiones admisibles.

(1) $[EF : K]$ es finito si y solo si $[E : K]$ y $[F : K]$ lo son.

(2) Si $[EF : K]$ es finito, entonces $[E : K]$ divide a $[EF : K]$ y $[EF : K] \leq [E : K][F : K]$.

(3) Si $[E : K]$ y $[F : K]$ son finitos y coprimos, entonces $[EF : K] = [E : K][F : K]$.

(4) Si $[EF : K] = [E : K][F : K]$, entonces $E \cap F = K$.

(5) El recíproco de $d$) es cierto si $[E : K]$ ó $[F : K]$ es 2 pero no lo es en general.

**2.27** Para cada número entero $n$ sea $\zeta_n = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i \text{ sen } \left(\frac{2\pi}{n}\right)$.

(1) Calcular $\text{Min}_{\mathbb{Q}}(\zeta_n)$, para $n \leq 6$.

(2) Demostrar que si $p$ es primo, entonces $\text{Min}_{\mathbb{Q}}(\zeta_p) = 1 + X + X^2 + \cdots + X^{p-1}$.

(3) Encontrar todos los automorfismos de $\mathbb{Q}(\zeta_6)$.

(4) ¿Existe un automorfismo de $\mathbb{Q}(\zeta_5)$ que lleve $\zeta_5$ a $\zeta_5^2$?

**2.28** Encontrar todos los automorfismos del cuerpo $\mathbb{Q}(\sqrt{5 + 2\sqrt{5}})$.

**2.29** Utilizando el Teorema de Lindeman que afirma que $\pi$ es transcendente sobre $\mathbb{Q}$ demostrar que si $p$ es un polinomio no constante con coeficientes en $\mathbb{Q}$, entonces $p(\pi)$ es transcendente sobre $\mathbb{Q}$.

**2.30** Probar que $L/K$ es algebraica si y solo si para toda subextensión $E$ de $L/K$, todo $K$-endomorfismo de $E$ es un automorfismo.

# Capítulo 3

# Cuerpos de descomposición

## 3.1 Cuerpos algebraicamente cerrados

Una consecuencia del Teorema de Kronecker es la siguiente proposición.

**Proposición 3.1** *Las siguientes condiciones son equivalentes para un cuerpo $K$.*

*(1) Todo polinomio no constante de $K[X]$ tiene una raíz en $K$.*

*(2) Los polinomios irreducibles de $K[X]$ son precisamente los de grado 1.*

*(3) Todo polinomio no constante de $K[X]$ es completamente factorizable sobre $K$.*

*(4) $K$ contiene un subcuerpo $K_0$ tal que $K/K_0$ es algebraica y todo polinomio de $K_0[X]$ es completamente factorizable sobre $K$.*

*(5) Si $L/K$ es una extensión algebraica, entonces $L = K$.*

*(6) Si $L/K$ es una extensión finita, entonces $L = K$.*

**Demostración.** (1) implica (2), (2) implica (3) y (3) implica (4) son obvios. (5) implica (6) es consecuencia inmediata de la Proposición 2.15.

(4) implica (5). Supongamos que $K$ contiene un subcuerpo $K_0$ satisfaciendo la propiedad (4). Si $L/K$ es una extensión algebraica, entonces $L/K_0$ es también algebraica, por el Corolario 2.16. Si $\alpha \in L$, entonces por hipótesis $p = \mathrm{Min}_{K_0}(\alpha)$ es completamente factorizable sobre $K$, con lo cual todas las raíces de $p$ pertenecen a $K$. En particular $\alpha \in K$ y esto prueba que $L = K$.

(6) implica (1). Supongamos que se verifica (6) y sea $p \in K[X] \setminus K$. Por el Teorema de Kronecker, existe una extensión $L/K$ que contiene una raíz $\alpha$ de $p$. Entonces $K(\alpha)/K$ es finita por la Proposición 2.12. Por hipótesis $K(\alpha) = K$ y deducimos que $\alpha$ es una raíz de $p$ en $K$. □

Se dice que un cuerpo $K$ es *algebraicamente cerrado* cuando verifica las condiciones equivalentes de la Proposición 3.1.

Es fácil encontrar ejemplos de cuerpos que *no* son algebraicamente cerrados. Por ejemplo, $\mathbb{Q}$ y $\mathbb{R}$ no lo son porque el polinomio $X^2 + 1$ no tiene raíces reales y $\mathbb{Z}_2$ tampoco lo es porque $X^2 + X + 1$ no tiene raíces en $\mathbb{Z}_2$. Si $p \geq 3$ es un entero primo entonces $\mathbb{Z}_p$ no es algebraicamente cerrado, pues $X^{p-1} + 1$ no tiene raíces en $\mathbb{Z}_p$ por el Teorema Pequeño de Fermat. Más generalmente, ningún cuerpo finito es algebraicamente cerrado (Problema 3.1). Sin embargo, se tiene:

**Teorema 3.2 (Teorema Fundamental del Álgebra)** $\mathbb{C}$ *¨es algebraicamente cerrado.*

**Demostración.** se trata de ver que, dado un polinomio

$$p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

de grado $n \geq 1$ ($a_n \neq 0$) con coeficientes complejos ($a_i \in \mathbb{C}$ para cada $i = 0, 1, \ldots, n$), existe un número complejo $z$ tal que $p(z) = 0$.

Usaremos propiedades elementales de los números complejos, como las desigualdades entre módulos

$$|z_1| - |z_2| \leq |z_1 + z_2| \leq |z_1| + |z_2|$$

o el hecho de que todos ellos tienen raíces $m$-ésimas para cualquier entero $m \geq 1$ (esto se demuestra considerando la forma polar, o forma módulo-argumento, de un complejo, y aplicando el Teorema de Bolzano al polinomio $X^m - r$ en el intervalo $[0, r + 1]$ para demostrar que todo número real positivo $r$ tiene una raíz $m$-ésima).

También emplearemos los conceptos de límite y continuidad. En particular, el hecho de que toda función continua $\mathbb{C} \to \mathbb{R}$, por ejemplo, $z \mapsto |p(z)| = +\sqrt{p(z)\overline{p(z)}}$, alcanza su mínimo en cualquier subconjunto cerrado y acotado de $\mathbb{C}$, y por tanto en cualquier "bola" $\{z \in \mathbb{C} \ : \ |z| \leq r\}$, donde $r$ es un número real positivo (Teorema de Weierstrass).

El esquema de la demostración, que desarrollaremos de inmediato, es el siguiente: Comenzamos viendo que la función $z \mapsto |p(z)|$ alcanza su mínimo absoluto en $\mathbb{C}$; para ello, se demuestra que $|p(z)|$ "se hace grande" fuera de cierta bola $\{z \in \mathbb{C} \ : \ |z| \leq r\}$, y entonces el mínimo que alcanza $|p(z)|$ en esa bola es de hecho un mínimo absoluto en $\mathbb{C}$. Bastará entonces ver que ese mínimo vale 0, y esto lo hacemos por reducción al absurdo: si el mínimo no es 0, construimos una función $\mathbb{C} \to \mathbb{R}$ cuyo mínimo absoluto vale 1, y sin embargo encontramos un punto en el que la misma función vale menos de 1. Vamos con los detalles:

Veamos, por inducción en el grado $n$, que $|p(z)|$ se hace más grande que cualquier número real positivo fuera de cierta bola; es decir, veamos que:

Para cada real $k \geq 0$, existe un real $r \geq 0$ tal que $|p(z)| > k$ para cada complejo $|z| > r$.

En efecto, la expresión de $p(X)$ se reescribe como

$$p(X) = a_0 + Xq(X), \qquad \text{donde} \quad q(X) = a_1 + a_2X + \cdots + a_nX^{n-1},$$

y entonces

$$|p(z)| = |zq(z) + a_0| \geq |z| \cdot |q(z)| - |a_0| \qquad \text{para cada } z \in \mathbb{C}.$$

Si $n = 1$ entonces $q = a_1$ es constante y distinto de cerpo y podemos tomar $r = \dfrac{k + |a_0|}{|a_1|}$. Si $n > 1$ entonces la hipótesis de inducción aplicada al polinomio $q$ y a $k' = k + |a_0|$ asegura que existe un real $s \geq 0$ tal que $|q(z)| > k + |a_0|$ cuando $|z| > s$, y entonces es claro que $|p(z)| > a_0$ cuando $|z| > r = \max\{s, 1\}$.

En particular, tomando $k = |a_0|$, encontramos $r \geq 0$ con $|p(z)| > |a_0|$ cuando $|z| > r$. Como la función $|p(z)|$ es continua, alcanza un mínimo en la bola $B = \{z \in \mathbb{C} \ : \ |z| \leq r\}$; es decir, existe $z_0 \in B$ tal que $|p(z_0)| \leq |p(z)|$ para cada $z \in B$. La misma desigualdad se tiene cuando $z \notin B$, pues entonces $|z| > r$ y así $p(z) > |a_0| = p(0) \geq |p(z_0)|$. En consecuencia, $|p(z)|$ alcanza un mínimo absoluto en $z_0$; es decir, $|p(z_0)| \leq |p(z)|$ para cada $z \in \mathbb{C}$.

Es claro que $p(X)$ tiene una raíz si y solo si la tiene $p(X + z_0)$, y éste tiene la ventaja de que su módulo alcanza un mínimo absoluto en el 0. Por tanto, sustituyendo $p(X)$ por $p(X + z_0)$, podemos suponer que $z_0 = 0$, y por tanto que $|p(z)| \geq |p(0)| = |a_0|$ para cada $z \in \mathbb{C}$. Si $a_0 = 0$ hemos terminado, así que se trata de ver que la condición $a_0 \neq 0$ nos lleva a una contradicción.

En este caso, dividir $p$ por $a_0$ no va a cambiar el punto en el que se alcanza el mínimo, por lo que podemos suponer que $a_0 = 1$. Excluyendo monomios con coeficiente nulo, podemos escribir

$$p(X) = 1 + a_m X^m + a_{m+1} X^{m+1} + \cdots + a_n X^n \qquad (\text{con } a_m \neq 0)$$

para cierto entero $m$ con $1 \leq m \leq n$. Sea ahora $\omega$ una raíz $m$-ésima de $-a_m^{-1}$ (es decir, $\omega \in \mathbb{C}$ verifica $\omega^m = -a_m^{-1}$). Entonces $p(\omega X) = 1 - X^m +$ (términos de grado mayor que $m$); es decir,

$$p(\omega X) = 1 - X^m + X^m h(X),$$

donde $h(X)$ es cierto polinomio con $h(0) = 0$.

Finalmente, vamos a encontrar un número real $t$ tal que $|p(\omega t)| < 1$, lo que nos dará la contradicción buscada puesto que 1 es el mínimo absoluto de $|p(z)|$. Consideremos la función $\mathbb{R} \to \mathbb{R}$ dada por $t \mapsto |h(t)|$. Considerando su límite en $x = 0$ (que vale 0 por continuidad) encontramos un número $t$ en el intervalo $(0, 1)$ tal que $|h(t)| < 1$ (haciendo $\epsilon = 1$ en la formulación usual del límite). Entonces también $t^m$ y $1 - t^m$ están en el intervalo $(0, 1)$, por lo que

$$|p(\omega t)| \leq |1 - t^m| + |t^m h(t)| < 1 - t^m + t^m \cdot 1 = 1,$$

como queríamos ver. □

## 3.2 Clausura algebraica

Por el Teorema Fundamental del Álgebra, $\mathbb{C}$ es un cuerpo que contiene las raíces de *todos* los polinomios no constantes de $K[X]$ para cualquier subcuerpo $K$ de $\mathbb{C}$. Por otro lado el Corolario 2.6 muestra que para un cuerpo arbitrario $K$ y un polinomio cualquiera $p$ de $K[X]$, se puede encontrar una extensión $L$ de $K$ en la que el polinomio $p$ factoriza completamente, es decir, en lo que atañe al polinomio $p$, $L$ se comporta como si fuera algebraicamente cerrado, aunque para que lo fuera todos los polinomios con coeficientes en $L$ tendrían que ser completamente factorizables sobre $L$, lo que no tiene por qué ser cierto. En vista de esto es natural preguntarse si, todo cuerpo $K$ tiene una extensión algebraicamente cerrada. Por otro lado tenemos la siguiente proposición que nos va a garantizar que si $K$ es subcuerpo de un cuerpo algebraicamente cerrado entonces también va a poderse incluir en un cuerpo que además de ser algebraicamente cerrado es algebraico sobre $K$.

**Proposición 3.3** *Sea $L/K$ una extensión con $L$ algebraicamente cerrado y sea $C$ la clausura algebraica de $K$ en $L$. Entonces $C/K$ es algebraica y $C$ es algebraicamente cerrado.*

**Demostración.** Que $C/K$ es algebraica, es consecuencia de la definición de clausura algebraica de $K$ en $L$. Por otro lado, si $p \in C[X]$, entonces $p$ tiene una raíz $\alpha$ en $L$. Eso implica que $C(\alpha)/C$ es finita y, como la clase de extensiones algebraicas es multiplicativa, se tiene que $C(\alpha)/K$ es algebraica, lo que implica que $\alpha \in C$. Esto prueba que $C$ es algebraicamente cerrado. □

**Definición 3.4** *Una* clausura algebraica *de un cuerpo $K$ es una extensión algebraica $L$ de $K$ formada por un cuerpo algebraicamente cerrado.*

Obsérvese la diferencia entre una clausura algebraica de un cuerpo $K$ y la clausura algebraica de una extensión $L/K$. La primera es una extensión de $K$ que ha de ser algebraica sobre $K$ y algebraicamente cerrada y la segunda es el mayor subcuerpo de $L$ que es algebraico sobre $K$, pero no tiene que ser algebraicamente cerrado, a no ser que $L$ sea algebraicamente cerrado (Proposición 3.3).

**Teorema 3.5** *Todo cuerpo tiene una clausura algebraica.*

**Demostración.** Por la Proposición 3.3, basta demostrar que todo cuerpo está contenido en un cuerpo algebraicamente cerrado. En primer lugar vamos a ver que si $K$ es un cuerpo, entonces existe otro cuerpo $E$ tal que todo polinomio no constante de $K[X]$ tiene una raíz en $E$. Para eso tenemos que considerar anillos con infinitas indeterminadas.

Si $A$ es una anillo y $S$ es un conjunto de símbolos entonces se define el anillo de polinomios en $S$ con coeficientes en $A$ como la unión

$$A[S] = \cup_{T\in\mathcal{F}} A[T]$$

donde $\mathcal{F}$ es el conjunto de todos los subconjuntos finitos de $S$ y para cada $T \in \mathcal{F}$, $A[T]$ es el anillo de polinomios con coeficientes en $A$, con indeterminadas los elementos de $T$. Si $T_1, T_2 \in \mathcal{F}$, entonces $A[T_1]$ y $A[T_2]$ son dos subanillos de $A[T_1 \cup T_2]$. Por tanto cada subconjunto finito de $A[S]$ está dentro de $A[T]$ para algún $T \in \mathcal{F}$, lo que nos permite sumar y multiplicar elementos de $A[S]$ simplemente sumándolos o multiplicándolos en el anillo en un número finito de indeterminadas que los contenga.

Para construir el cuerpo $E$ que contiene raíces de todos los polinomios no constantes de $K[X]$ razonamos de la siguiente forma. A cada polinomio no constante $p \in K[X]$ le asociamos un símbolo $X_p$ y construimos el anillo $K[S]$ donde $S = \{X_p : p \in K[X] \setminus K\}$. Sea $I$ el ideal de $K[S]$ generado por todos los elementos de la forma $p(X_p)$.

Vamos a empezar mostrando que $I$ es un ideal propio de $K[S]$. En caso contrario existirían $g_1, \ldots, g_n \in K[S]$ y $p_1, \ldots, p_n \in K[X] \setminus K$ tales que $g_1 p_1(X_{p_1}) + \cdots + g_n p_n(X_{p_n}) = 1$. Para simplificar la notación vamos a poner $X_i$ en lugar de $X_{p_i}$, con lo que tenemos

$$g_1 p_1(X_1) + \cdots + g_n p_n(X_n) = 1 \tag{3.1}$$

Aplicando el Teorema de Kronecker repetidamente deducimos que existe una extensión $F$ de $K$ en la que cada uno de los polinomios $p_1, \ldots, p_n$ tiene una raíz $\alpha_i$. Sustituyendo $X_i$ por $\alpha_i$ en la ecuación (3.1) obtenemos $0 = 1$, una contradicción.

Una vez que sabemos que $I$ es un ideal propio de $K[S]$ deducimos que $I$ está contenido en un ideal maximal $M$ de $K[S]$ (Proposición 2.8 de GyA). Entonces $E = K(S)/M$ es un cuerpo y la composición de la inclusión $K \to K(S)$ con la proyección $K(S) \to K(S)/M$ proporciona un homomorfismo de cuerpos, con lo que podemos considerar $E$ como una extensión de $K$. Ahora observamos que $p(X_p + M) = p(X_p) + M = 0$, pues $p(X_p) \in M$, con lo que $X_p + M$ es una raíz de $p$ en $E$ para todo $p \in K[X] \setminus K$.

Utilizando que para cada cuerpo $K$ existe una extensión $E$ de $K$ que contiene raíces de todos los polinomios no nulos de $K[X]$ construimos de forma recursiva una sucesión de extensiones

$$K = E_1 \subseteq E_2 \subseteq E_3 \ldots$$

tal que todo polinomio no constante de $E_i[X]$ tiene una raíz en $E_{i+1}$. Entonces $E = \cup_{i\geq 1} E_i$ tiene una estructura de cuerpo en el que la suma y el producto de cada dos elementos se calcula en un $E_i$ que contiene a ambos. Si $f$ es un polinomio no constante de $E[X]$, entonces $f \in E_i[X]$ para algún $i$ y por tanto $f$ tiene una raíz en $E_{i+1}$ que, por supuesto, pertenece a $E$. Esto prueba que $E$ es algebraicamente cerrado. □

**Teorema 3.6** *Si $\sigma : K \to L$ es un homomorfismo de cuerpos con $L$ algebraicamente cerrado y $F/K$ una extensión algebraica, entonces existe otro homomorfismo de cuerpos $F \to L$ que extiende $\sigma$.*

**Demostración.** Sea

$$\Omega = \left\{ (E, \tau) : \begin{array}{l} E/K \text{ es una subextensión de } F/K \text{ y} \\ \tau : E \to L \text{ es un homomorfismo que extiende } \sigma \end{array} \right\}$$

y consideremos el siguiente orden en $\Omega$:

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

Es fácil ver que $(\Omega, \leq)$ es un conjunto ordenado inductivo y, por el Lema de Zorn, tiene un elemento maximal $(E, \tau)$.

Basta con demostrar que $F \subseteq E$. Sean $\alpha \in F$ y $p = \mathrm{Min}_E(\alpha)$. Como $L$ es algebraicamente cerrado, el polinomio $\sigma(f)$ tiene una raíz $\beta$ en $L$. Del Lema 2.9 deducimos que existe un homomorfismo $\tau' : E(\alpha) \to L$ que extiende $\tau$ y tal que $\tau'(\alpha) = \beta$. Entonces $(E(\alpha), \tau') \in \Omega$ y $(E, \tau) \leq (E(\alpha), \tau')$. De la maximalidad de $(E, \tau)$ deducimos que $E = E(\alpha)$, es decir $\alpha \in E$. Esto prueba que $F \subseteq E$. □

El siguiente corolario del Teorema 3.6 muestra que la clausura algebraica de un cuerpo es única salvo isomorfismos, por lo que a partir de ahora utilizaremos el artículo definido para hablar de la clausura algebraica de un cuerpo.

**Corolario 3.7** *Si $\sigma : K_1 \to K_2$ es un isomorfismo de cuerpos y $L_1$ y $L_2$ son clausuras algebraicas de $K_1$ y $K_2$, respectivamente, entonces existe un isomorfismo $L_1 \to L_2$ que extiende $\sigma$.*

**Demostración.** Por el Teorema 3.6 hay un homomorfismo $L_1 \to L_2$ que extiende $\sigma$. Como $L_1$ es algebraicamente cerrado y $\overline{\sigma}$ induce un isomorfismo entre $L_1$ y $\overline{\sigma}(L_1)$, este último también es algebraicamente cerrado. Como $L_2/K_2$ es algebraica, $L_2/\overline{\sigma}(L_1)$ es algebraica y por tanto $L_2 = \overline{\sigma}(L_1)$, lo que muestra que $\overline{\sigma}$ es un isomorfismo. □

## 3.3 Cuerpos de descomposición y extensiones normales

**Definición 3.8** *Sean $K$ un cuerpo y $\mathcal{P}$ un conjunto de polinomios no constantes de $K[X]$. Se llama* cuerpo de descomposición *de $\mathcal{P}$ sobre $K$ a un cuerpo de la forma $K(S)$ donde $S$ es el conjunto de las raíces de los elementos de $P$ en una clausura algebraica de $K$.*

Para cada clausura algebraica $L$ de $K$ hay un cuerpo de descomposición de $\mathcal{P}$ sobre $K$ dentro de $L$ pero la unicidad de la clausura algebraica salvo isomorfismos va a implicar la unicidad del cuerpo de descomposición de una familia de polinomios sobre $K$. Eso es lo que dice la siguiente proposición.

**Proposición 3.9** *Sea $\sigma : K_1 \to K_2$ un isomorfismo de cuerpos y sean $\mathcal{P}_1$ un conjunto de polinomios no constantes de $K_1[X]$ y $\mathcal{P}_2 = \{\sigma(p) : p \in \mathcal{P}\}$. Si $L_1$ es un cuerpo de descomposición de $\mathcal{P}$ sobre $K_1$ y $L_2$ es un cuerpo de descomposición de $\mathcal{P}_2$ sobre $K_2$, entonces existe un isomorfismo $\overline{\sigma} : L_1 \to L_2$ que extiende $\sigma$.*

**Demostración.** Para cada $i = 1, 2$ sean $\overline{K_i}$ una clausura algebraica de $K_i$ y $S_i$ el conjunto formado por las raíces de los elementos de $\mathcal{P}_i$ en $\overline{K_i}$. Del Corolario 3.7 se tiene que existe un isomorfismo $\overline{\sigma} : \overline{K_1} \to \overline{K_2}$, que extiende $\sigma$. Si $\alpha \in S_1$, entonces existe $p \in \mathcal{P}_1$ tal que $\alpha$ es raíz de $p$. Del Lema 2.8 se deduce que $\overline{\sigma}(\alpha)$ es una raíz de $\sigma(p)$. Esto prueba que $\overline{\sigma}(S_1) \subseteq S_2$ y el mismo argumento muestra que $\overline{\sigma}^{-1}(S_2) \subseteq S_1$, de donde deducimos que $\overline{\sigma}(S_1) = S_2$ y por tanto $\overline{\sigma}(K(S_1)) = K(S_2)$, con lo que la restricción de $\overline{\sigma}$ a $K(S_1) \to K(S_2)$ es el isomorfismo buscado. □

**Ejemplos 3.10** (1) El cuerpo de descomposición de $X^2 - 2$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt{2})$ y el de $X^2 + 1$ es $\mathbb{Q}(i)$. Más generalmente, si $q \in \mathbb{Q}$, entonces el cuerpo de descomposición de $X^2 - q$ es $\mathbb{Q}(\sqrt{q})$.

(2) El cuerpo de descomposición $X^3-1=(X-1)(X^2+X+1)$ sobre $\mathbb{Q}$, coincide con el de $X^2+X+1$ que es $\mathbb{Q}\left(\frac{-1+\sqrt{-3}}{2}\right)$.

Pongamos $\omega=\frac{-1+\sqrt{-3}}{2}$. Entonces $\omega^2=\frac{-1-\sqrt{-3}}{2}$ y $\omega^3=1$, lo que muestra que $1,\omega$ y $\omega^2$ son las tres raíces del polinomio $X^3-1$, es decir las tres raíces terceras de la unidad. Obsérvese que si $\alpha^3=a$, entonces $(\alpha\omega)^3=(\alpha\omega^2)^3=a$, con lo que las tres raíces de $X^3-a$ son $\alpha,\alpha\omega$ y $\alpha\omega^2$. Por ejemplo, el cuerpo de descomposición de $X^3-2$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2})=\mathbb{Q}(\sqrt[3]{2},\omega)$.

(3) Más generalmente, si $n$ es un entero positivo, entonces las raíces complejas del polinomio $X^n-1$ se llaman *raíces $n$-ésimas de la unidad* y son los números complejos de la forma

$$\zeta_n^k=e^{\frac{2\pi ik}{n}}\qquad(k=0,1,\ldots,n-1),$$

donde $\zeta_n=e^{\frac{2\pi i}{n}}$. Están situadas en los vértices de un polígono regular de $n$ lados inscrito en una circunferencia de radio 1. Por ejemplo, la Figura 3.1 representa las raíces sextas de la unidad Como las raíces de $X^n-1$ son las potencias de $\zeta_n$, el cuerpo de descomposición de $X^n-1$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\zeta_n)$.

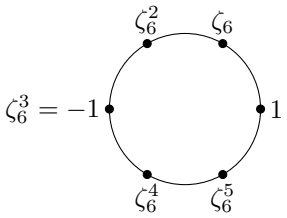



Figura 3.1:

Si $a$ es un número complejo diferente de 0, entonces las raíces complejas del polinomio $X^n-a$ se obtienen multiplicando una de ellas, digamos $\alpha$, por las $n$ raíces $n$-ésimas de la unidad. Por tanto el cuerpo de descomposición de $X^n-a$ es $\mathbb{Q}(\alpha,\zeta_n)$ donde $\alpha$ es una raíz $n$-ésima arbitraria de $a$.

Una *extensión* de cuerpos $L/K$ se dice que es *normal* si satisface cualquiera de las condiciones equivalentes del siguiente teorema:

**Teorema 3.11** *Las siguientes condiciones son equivalentes para una extensión $L/K$.*

*(1) $L$ es un cuerpo de descomposición sobre $K$ de una familia de polinomios no constantes de $K$.*

*(2) $L/K$ es algebraica y para toda clausura algebraica $F$ de $L$ y todo $K$-homomorfismo $\sigma:L\to F$, se verifica $\sigma(L)=L$, es decir, $\sigma\in\mathrm{Gal}(L/K)$.*

*(3) $L/K$ es algebraica y existe una clausura algebraica $F$ de $L$ que satisface (2).*

*(4) $L/K$ es algebraica y para todo $\alpha\in L$, el polinomio $\mathrm{Min}_K(\alpha)$ factoriza completamente en $L$.*

*(5) $L/K$ es algebraica y todo polinomio irreducible $p$ de $K[X]$ que contenga una raíz en $L$ factoriza completamente en $L$.*

**Demostración.** (1) implica (2). Sea $F$ una clausura algebraica de $L$ y sea $\sigma:L\to F$ un $K$-homomorfismo. Supongamos que $L$ es el cuerpo de descomposición de $\mathcal{P}$ sobre $K$, es decir $L=K(S)$, donde $S$ es el conjunto de las raíces de los elementos de $\mathcal{P}$ en $F$. Claramente $L/K$ es algebraica. Además

del Lema 2.8 se deduce que $\sigma$ permuta las raíces de cada elemento de $\mathcal{P}$ y por tanto $\sigma(S) = S$. Esto implica que $\sigma$ es una automorfismo de $L$.

(2) implica (3) es obvio.

(3) implica (4). Supongamos que $F$ es una clausura algebraica de $L$ que satisface las condiciones de (3). Si $\alpha \in L$, entonces $p = \mathrm{Min}_K(\alpha)$ factoriza completamente en $F$ (¿por qué?) y por tanto $p = (X - \alpha_1) \cdots (X - \alpha_n)$ para ciertos $\alpha_1, \ldots, \alpha_n \in F$. De la Proposición 2.10 se deduce que para cada $i = 1, \ldots, n$, existe un $K$-isomorfismo $\sigma : K(\alpha) \to K(\alpha_i)$ tal que $\sigma(\alpha) = \alpha_i$. Podemos considerar $\sigma$ como un homomorfismo de $K(\alpha)$ en $F$ y aplicar que la extensión $L/K(\alpha)$ es algebraica para concluir, con el Teorema 3.6, que $\sigma$ se puede extender a un homomorfismo $L \to F$, que denotaremos también con $\sigma$. Por hipótesis $\alpha_i = \sigma(\alpha) \in L$ y concluimos que $p$ factoriza completamente en $L$.

(4) y (5) son equivalentes pues los polinomios irreducibles de $K[X]$ que tienen raíces en $L$ son los de la forma $a\,\mathrm{Min}_K(\alpha)$, con $0 \neq a \in K$ y $\alpha \in L$.

(5) implica (1). Si se cumple (6), entonces $L$ es el cuerpo de descomposición de los polinomios irreducibles de $K[X]$ que tengan una raíz en $L$. □

**Corolario 3.12** *Una extensión finitamente generada es normal si y solo si es el cuerpo de descomposición de un polinomio.*

**Demostración.** Una implicación es obvia y para demostrar la otra, obsérvese que si $L = K(\alpha_1, \ldots, \alpha_n)/K$ es una extensión normal, entonces $L$ es el cuerpo de descomposición de $\prod_{i=1}^{n} \mathrm{Min}_K(\alpha_i)$. □

**Corolario 3.13** *Si $L$ es una clausura algebraica de $K$ entonces $L/K$ es normal.*

**Ejemplos 3.14** (1) Todas las extensiones que aparecen en los Ejemplos 3.10 son normales pues se trata de cuerpos de descomposición de un polinomio.

(2) En particular $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ es una extensión normal, donde $\omega = \frac{-1+\sqrt{-3}}{2}$. Sin embargo la extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es una normal pues $\mathrm{Min}_{\mathbb{Q}}(\sqrt[3]{2}), \mathbb{Q}) = X^3 - 2$ que tiene tres raíces $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ y $\sqrt[3]{2}\omega^2$. Como todos los elementos de $\mathbb{Q}(\sqrt[3]{2})$ son números reales y $\omega$ no lo es, deducimos que el polinomio $\mathrm{Min}_{\mathbb{Q}}(\sqrt[3]{2})$ no factoriza completamente en $\mathbb{Q}(\sqrt[3]{2})$ y, por tanto, la extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal.

(3) Toda extensión de grado 2 es normal. En efecto, si $L/K$ es una extensión de grado 2 y $\alpha \in L \setminus K$, entonces $L = K(\alpha)$ y por tanto $p = \mathrm{Min}_K(\alpha)$ tiene grado 2. Como $p$ tiene una raíz en $L$, $p$ es completamente factorizable en $L$ y por tanto $L$ es el cuerpo de descomposición de $p$ sobre $K$.

(4) Del ejemplo (3) se deduce que las dos extensiones $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ son normales y sin embargo la extensión $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no lo es, pues $p = \mathrm{Min}_{\mathbb{Q}}(\sqrt[4]{2}) = X^4 - 2$ tiene una raíz en $\mathbb{Q}(\sqrt[4]{2})$ y no es completamente factorizable en $\mathbb{Q}(\sqrt[4]{2})$, ya que $X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2})$ y $X^2 + \sqrt{2}$ no tiene ninguna raíz en $\mathbb{Q}(\sqrt[4]{2})$.

Los Ejemplos (2) y (4) de 3.14 muestran que la clase de extensiones normales no es multiplicativa en torres pues si $K \subseteq E \subseteq L$ es una torre de extensiones, puede ocurrir que $L/K$ sea normal sin que lo sea $E/K$ y también puede ocurrir que $E/K$ y $L/E$ sean normales y no lo sea $L/K$. Para compensar estas propiedades negativas, veamos algunas de las propiedades positivas de la clase de extensiones normales.

**Proposición 3.15** *(1) Si $K \subseteq E \subseteq L$ es una torre de extensiones de cuerpos y $L/K$ es normal, entonces $L/E$ es normal.*

*(2) Si $\{E_i/K : i \in I\}$ es una familia de extensiones normales admisibles, entonces $(\cap_{i\in I} E_i)/K$ y $(\prod_{i\in I} E_i)/K$ son normales.*

*(3) La clase de extensiones normales es cerrada para levantamientos.*

**Demostración.** (1) es obvio.

(2) Por hipótesis todos los $E_i$ son subcuerpos de un cuerpo $L$. Si $E_i/K$ es el cuerpo de descomposición de la familia de polinomios $\mathcal{P}_i$ y $S_i$ es el conjunto de raíces de los elementos de $\mathcal{P}_i$ (en $L$), entonces $E = \prod_{\in I} E_i$ es el menor subcuerpo de $L$ que contiene a $K$ y a todos los $S_i$, es decir que $E = K(\cup_{i\in I} S_i)$ y por tanto $E$ es el cuerpo de descomposición de $\cup_{i\in I}\mathcal{P}_i$ sobre $K$. Esto prueba que $E/K$ es normal.

Si $p$ es un elemento irreducible de $K[X]$ y $\alpha \in \cap_{i\in I} E_i$ es una raíz de $p$, entonces, por el Teorema 3.11, $p$ factoriza completamente en cada $E_i$, con lo que $p$ factoriza completamente en $L$ y las raíces de $p$ están en todos los $E_i$, es decir en $\cap_{i\in I} E_i$. Eso implica que $\cap_{i\in I} E_i/K$ es normal por el Teorema 3.11.

(3) Sean $E/K$ y $F/K$ extensiones admisibles con $E/K$ normal. Sea $\mathcal{P}$ un subconjunto de $K[X]$ tal que $E$ es el cuerpo de descomposición de $\mathcal{P}$ sobre $K$, es decir $E = K(S)$, donde $S$ es el conjunto de las raíces de los elementos de $\mathcal{P}$ en una clausura algebraica que contenga a $EF$. Entonces $EF = F(S)$ y por tanto $EF/F$ es normal. □

**Teorema 3.16 (Clausura Normal)** *Sea $L/K$ una extensión algebraica. Entonces*

*(1) Existe una extensión $N/L$ que verifica:*

*(a) $N/K$ es normal.*

*(b) Si $E$ es una subextensión de $N/L$ y $E/K$ es normal, entonces $E = N$.*

*En tal caso se dice que $N/K$ es una* clausura normal *de $L/K$.*

*(2) Todas las clausuras normales de $L/K$ son $L$-isomorfas.*

*(3) Si $L/K$ es finita y $N/L$ es una clausura normal de $L/K$, entonces $N/K$ es finita.*

**Demostración.** (1) Sea $\overline{L}$ una clausura algebraica de $L$. Como $L/K$ es una extensión algebraica, $\overline{L}$ también es una clausura algebraica de $K$. Sea

$$\Omega = \{E : E \text{ es una subextensión de } \overline{L}/L \text{ tal que } E/K \text{ es normal}\}.$$

Como $\overline{L}$ es algebraicamente cerrado, $\overline{L} \in \Omega$ y por tanto $\Omega \neq \emptyset$. De la Proposición 3.15 se deduce que $N = \cap_{E\in\Omega} E$ es una extensión normal de $K$ y claramente $N$ verifica (a) y (b).

(2) y (3) Sean $N_1/K$ y $N_2/K$ dos clausuras normales de $L/K$. Sea $B$ una base de $L_K$. Para cada $\alpha \in B$ sean $p_\alpha = \mathrm{Min}_K(\alpha)$. Sea $\mathcal{P} = \{p_\alpha : \alpha \in B\}$ y para cada $i = 1, 2$ sea $R_{i,\alpha}$ el conjunto de raíces de $p_\alpha$ en $N_i$. Sea $F_i = K(\cup_{\alpha\in B} R_{i,\alpha})$ $(i = 1, 2)$. Como $N_i/K$ es normal y $N_i$ contiene una raíz de $p_\alpha$, este polinomio es completamente factorizable en $N_i$ y por tanto $F_i$ es el cuerpo de descomposición sobre $K$ de $\mathcal{P}$ (en una clausura algebraica de $N_i$). Por tanto $F_i/K$ es normal de donde se deduce que $F_i = N_i$ pues $N_i/K$ es una clausura normal de $L/K$. Luego $N_1$ y $N_2$ son dos cuerpos de descomposición sobre $K$ del mismo conjunto de polinomios. Como además $K \subseteq L \subseteq N_i$ también $N_1$ y $N_2$ son cuerpos de descomposición de $\mathcal{P}$ sobre $L$. Deducimos que $N_1$ y $N_2$ son $L$-isomorfos de la Proposición 3.9. Esto prueba (2) y también prueba (3) pues si $L/K$ es finita, entonces $B$ es finito y por tanto $\cup_{\alpha\in B} R_{i,\alpha}$ es finito, con lo que cada $N_i/K$ es una extensión finita. □

## Problemas

**3.1** Demostrar que, si $K$ es un cuerpo, entonces $K[X]$ tiene infinitos elementos irreducibles. Deducir que:

(1) Todo cuerpo algebraicamente cerrado es infinito.

(2) Si $K$ es finito, entonces en $K[X]$ existen polinomios irreducibles de grado arbitrariamente grande (es decir, para cada $n \in \mathbb{Z}^+$, existe un polinomio irreducible de grado mayor o igual que $n$).

**3.2** Demostrar que la clausura algebraica de un cuerpo numerable tiene cardinal infinito numerable.

**3.3** Demostrar que si $K/\mathbb{Q}$ es una extensión finita y $\overline{K}$ es un clausura algebraica de $K$, entonces $[K : \mathbb{Q}] = \infty$.

**3.4** Calcular el cuerpo de escisión sobre $\mathbb{Q}$ contenido $\mathbb{C}$ de cada uno de los siguientes polinomios.

$$X^4 + 1, \;\; X^4 - 2, \;\; X^4 + X^2 + 1, \;\; X^4 - 8X^2 + 15, \;\; X^6 + 1, \;\; X^9 + X^3 + 1.$$

**3.5** Sea $K$ un cuerpo arbitrario y $\alpha$ una raíz del polinomio $p = X^3 - 3X + 1$ en una extensión de $K$. Demostrar que $\alpha^2 - 2$ también es raíz $p$ y utilizar esto para demostrar que $K(\alpha)$ es un cuerpo de escisión de $p$ sobre $K$.

**3.6** Calcular un cuerpo de escisión $L$ sobre $K$ (con $K$ tanto $\mathbb{Z}_2$ como $\mathbb{Z}_3$) y el grado $[L : K]$ para cada uno de los siguientes polinomios:

$$X^2 + X + 1, \;\; X^3 + X + 1, \;\; X^3 + X^2 + X + 1, \;\; X^4 + X^2 + 1.$$

**3.7** Sea $a$ un número racional que no es un cubo de un número racional y sea $K$ el cuerpo de descomposición de $X^3 - a$ sobre $\mathbb{Q}$, determinar $[K : \mathbb{Q}]$ y calcular una base de $K$ sobre $\mathbb{Q}$.

**3.8** Dar un ejemplo de dos polinomios irreducibles sobre $\mathbb{Q}$ que tengan el mismo cuerpo de descomposición.

**3.9** Sea $K$ un cuerpo de característica distinta de dos. Demostrar que el cuerpo de descomposición sobre $K$ del polinomio $X^4 - (a + b)X^2 + ab$, donde $a, b \in K$, tiene grado 4 sobre $K$ si y solo si $a$, $b$ y $ab$ no son cuadrados en $K$.

**3.10** Demostrar que si $\alpha$ es transcendente sobre $K$, entonces $K(\alpha)$ no es algebraicamente cerrado.

**3.11** Sea $p \in K[X]$ y $L$ un cuerpo de descomposición de $p$ sobre $K$. Demostrar que si $E$ es una extensión de $K$ admisible con $L$, entonces $LE$ es un cuerpo de descomposición de $p$ sobre $E$.

**3.12** Para cada una de los siguientes subcuerpos $K$ de $\mathbb{C}$, calcular un subcuerpo $N$ de $\mathbb{C}$ que sea una clausura normal de $K/\mathbb{Q}$ y calcular también $[N : K]$:

$$\mathbb{Q}(\sqrt[3]{2}), \;\; \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5}), \;\; \mathbb{Q}(\sqrt[8]{2}, \sqrt{3}), \;\; \mathbb{Q}(\zeta_5), \;\; \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots).$$

**3.13** Demostrar que si $\alpha$ es un número complejo que cumple $\alpha^2 = 1 + i$, entonces $\mathbb{Q}(\alpha, \sqrt{2})$ es una clausura normal de $\mathbb{Q}(\alpha)/\mathbb{Q}$.

**3.14** Sea $K \subseteq L \subseteq N$ una torre de extensiones y supongamos que $N/K$ es normal. Demostrar que $L/K$ es normal si y solo si $\sigma(L) \subseteq L$ para todo $K$-automorfismo $\sigma$ de $N$.

**3.15** Probar que si $p \in K[X]$ tiene grado $n$ y $L$ es un cuerpo de descomposición de $p$ sobre $K$, entonces $[L : K]$ divide a $n!$.

**3.16** Demostrar que si $[L : K] = n$ y $N$ es la clausura normal de $L/K$ entonces $[N : K]$ divide a $n!$

**3.17** Demostrar que las siguientes condiciones son equivalentes para dos extensiones normales finitas $N_1/K$ y $N_2/K$.

(1) Existe un $K$-homomorfismo $L_1 \to L_2$.

(2) Existen polinomios $p_1, p_2 \in K[X]$ tales que $p_2|p_1$ en $K[X]$ y $N_i$ es la clausura normal de $p_i$ sobre $K$ para $i = 1, 2$.

**3.18** Demostrar que toda extensión de cuerpos finitos es normal.

**3.19** Sean $N/K$ una extensión normal, $p \in K[X]$ irreducible y $g, h$ dos divisores irreducibles de $p$ en $N[X]$. Demostrar que existe $\sigma \in \mathrm{Gal}(N/K)$ tal que $\overline{\sigma}(g) = h$. Dar un ejemplo mostrando que el resultado no es válido si la extensión no es normal.

# Capítulo 4

# Extensiones ciclotómicas

## 4.1 Raíces de la unidad

Las raíces del polinomio $X^n - 1$ se llaman *raíces n-ésimas de la unidad*.

Obsérvese que hay un polinomio $P = X^n - 1$ para cada posible característica que puede ser 0 ó un número primo. Si la característica considerada es no es divisor de $n$ (lo que incluye que sea 0), entonces la única raíz de $P' = nX^{n-1}$ es 0, que no es raíz de $p$, con lo que en tal caso $P$ no tiene raíces múltiples y por tanto el polinomio $X^n - 1$ tiene $n$ raíces distintas en cualquier clausura algebraica del cuerpo original. Sin embargo, si la característica considerada es un divisor primo $p$ de $n$, entonces $P' = 0$, con lo que todas las raíces son múltiples. De hecho como $p$ divide a $\binom{p}{i}$ para todo $i = 1, 2, \ldots, p-1$, si $a$ y $b$ son elementos de un anillo de característica $p$, entonces $(a+b)^p = a^p + b^p$. En particular si consideramos $X^n - 1$ como un polinomio con coeficientes en $\mathbb{Z}_p[X]$ y $n = p^k m$, entonces

$$X^n - 1 = (X^m - 1)^{p^k}$$

con lo que, si $p \nmid m$, entonces las raíces de $X^m - 1$ son simples y las raíces de $n$ tienen todas multiplicidad $p^k$. En resumen

**Lema 4.1** *Consideremos $X^n - 1$ como un polinomio con coeficientes en un cuerpo $K$.*

*(1) Si $K$ tiene característica 0, entonces $X^n - 1$ tiene $n$-raíces distintas en cualquier cuerpo de descomposición de $X^n - 1$.*

*(2) Si la característica de $K$ es $p$ y $n = p^k m$, con $p \nmid m$, entonces $X^n - 1$ tiene $m$ raíces en un cuerpo de descomposición suyo, todas con multiplicidad $p^k$.*

Obsérvese que las raíces $n$-ésimas de la unidad son los elementos de orden finito del grupo de unidades de un cuerpo algebraicamente cerrado. Las raíces $n$-ésimas (en una característica fijada) son precisamente los elementos de orden divisible por $n$ y forman un subgrupo finito del grupo de unidades del cuerpo al que pertenecen. De hecho este grupo es cíclico.

**Lema 4.2** *Todo subgrupo finito del grupo de unidades de un cuerpo es cíclico.*

**Demostración.** Sea $G$ un subgrupo finito del grupo de unidades $K^*$ de un cuerpo $K$. Del Teorema de Estructura de los Grupos Abelianos Finitos (Teorema 7.55 de GyA) se deduce que $G \simeq C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}$ para ciertos enteros mayores que 1 tales que $n_1 | n_2 | \cdots | n_k$. Si $p$ es un divisor primo de $n_1$, entonces cada $C_{n_i}$ tiene un subgrupo de orden $p$, con lo que $G$ tiene un subgrupo isomorfo a $C_p^k$. Por

tanto la ecuación $X^p = 1$ tiene al menos $p^k$ soluciones en el cuerpo $K$, lo que implica que $k = 1$. Por tanto $G \simeq C_{n_1}$, es decir $G$ es cíclico. □

Por tanto, el grupo de la raíces $n$-ésimas de la unidad (en una característica) es un grupo cíclico finito. Si la característica es 0, entonces el orden de este grupo es $n$. Si por el contrario la característica es $p > 0$, entonces el orden de este grupo es el mayor divisor de $n$ que no es múltiplo de $p$. Recíprocamente, si $G$ es un subgrupo finito de orden $n$ del grupo de unidades $K^*$ de un cuerpo $K$ entonces, por el Teorema de Lagrange, todos los elementos de $G$ satisfacen la ecuación $X^n = 1$, con lo que $G$ está formado por las $n$-raíces $n$-ésimas de la unidad, lo que implica que la característica de $K$ no divide a $n$. En tal caso $G$ es un grupo cíclico y los generadores de $G$ se llaman *raices n-ésimas primitivas de la unidad.* Es decir, una raíz $n$-ésima primitiva de la unidad es un elemento de orden $n$ de $K^*$, para algún cuerpo $K$. Obsérvese que hay raíces $n$-ésimas primitivas de la unidad en una característica si y solo si $n$ no es múltiplo de la característica. Recuérdese también que si $g$ es un elemento de orden $n$ en un grupo y $r$ es un entero positivo entonces el orden de $g^r$ es $\frac{n}{\mathrm{mcd}(n,r)}$ (Fórmula (4.2) en GyA). Por tanto,

**Lema 4.3** *Supongamos que $\xi$ es una raíz $n$-ésima primitiva de la unidad. Entonces $\xi^r$ es una raíz $\frac{n}{(r,n)}$-ésima primitiva de la unidad. En particular las raíces $n$-ésimas primitivas de la unidad son los elementos de la forma $\xi^r$, con* $\gcd(r, n) = 1$.

*Por tanto, si $n$ no es múltiplo del primo $p$, entonces, en un cuerpo algebraicamente cerrado de característica $p$, hay $\varphi(n)$ raíces $n$-ésimas primitivas de la unidad, donde $\varphi(n) = |\mathbb{Z}_n^*|$, es decir, $\varphi$ es la Función de Euler.*

## 4.2 Extensiones ciclotómicas

**Definición 4.4** *Sea $K$ un cuerpo y $n$ un entero positivo. Se llama $n$-ésima* extensión ciclotómica *de $K$ al cuerpo de descomposición de $X^n - 1$ sobre $K$ (que es único salvo isomorfismos por la Proposición 3.9).*

Como el conjunto de las raíces $n$-ésimas de la unidad forma un grupo cíclico, la extensión $n$-ésima extensión ciclotómica de $K$ es $K(\xi)$ donde $\xi$ es un generador del grupo de raíces $n$-ésimas de la unidad.

Supongamos que la característica de nuestro cuerpo no divide a $n$ y sean $\xi_1, \ldots, \xi_r$ las raíces $n$-ésimas primitivas de la unidad. Entonces el polinomio

$$\Phi_n = (X - \xi_1) \cdots (X - \xi_r)$$

se llama *$n$-ésimo polinomio ciclotómico.*

Recordemos que el *subcuerpo primo* de un cuerpo $K$ es el menor cuerpo contenido en él. El cuerpo primo de $K$ es isomorfo a $\mathbb{Q}$ si $\mathrm{car}(K) = 0$ e isomorfo a $\mathbb{Z}_p$ si $\mathrm{car}(K) = p$. Además el subanillo primo de $K$ es el menor subanillo primo contenido en $K$, que es isomorfo a $\mathbb{Z}$ si $\mathrm{car}(K) = 0$ e igual al cuerpo primo si la característica es diferente de 0. Obsérvese que un anillo primo es o bien un cuerpo o bien isomorfo a $\mathbb{Z}$ y, por tanto, es un DFU.

**Lema 4.5** *Sean $D$ un DFU, $K$ el cuerpo de fracciones de $D$ y sean $p \in D[X]$ y $q \in K[X]$ con $p$ y $q$ polinomios mónicos tales que $q$ divide a $p$ en $K[X]$. Entonces $q \in D[X]$ y $q$ divide a $p$ en $D[X]$.*

**Demostración.** Sea $r \in K[X]$ con $p = qr$. Como $p$ es mónico y tiene coeficientes en $D$, entonces $p$ es primitivo y por tanto $q$ y $r$ tienen contenido 1. Del Lema de Gauss [GyA, Lema 3.19] se deduce que si $c$ y $d$ son los contenidos de $q$ y $r$ entonces $cd = u$ es una unidad de $D$ y $q = cq_1$ y $r = dr_1$ con $q_1, r_1$ polinomios primitivos en $D[X]$. Como $p$ y $q$ son mónicos, también lo es $r$ y por tanto $1 = cc_1 = dd_1$, donde $c_1$ y $d_1$ son los términos principales de $q_1$ y $r_1$ respectivamente. Entonces $c = ud^{-1} = ud_1 \in D$ y por tanto $q = cq_1 \in D[X]$. Análogamente, $r \in D[X]$ y por tanto $q$ divide a $p$ en $D[X]$. □

Recuérdese que si $D$ es un DFU, $K$ es su cuerpo de cocientes y $p \in K[X] \setminus \{0\}$ entonces $p = cq$ con $c \in K$ y $q \in D[X]$ con $q$ primitivo, es decir el máximo común divisor de los coeficientes de $q$ es 1. Por otro lado, si $c, d \in K$ y $q, r \in D[X]$ con $q$ y $r$ primitivos y $p = cq = dr$ entonces existe $u \in D^*$ tal que $c = du$ y $r = qu$.

**Proposición 4.6** *Sean $P$ y $K$ el anillo primo y el cuerpo primo en una característica y sea $n$ un entero positivo que no es múltiplo de* $\mathrm{car}(P)$. *Entonces*

*(1)* $\mathrm{gr}(\Phi_n) = \varphi(n) = |\mathbb{Z}_n^*|$.

*(2)* $X^n - 1 = \prod_{d|n} \Phi_d$.

*(3)* $\Phi_n \in P[X]$.

*(4) Si $\xi$ es una raíz de la unidad en una extensión de $K$, entonces* $\mathrm{Min}_K(\xi) \in P[X]$.

**Demostración.** (1) es consecuencia del Lema 4.3.

(2) Si $G$ es el grupo de la $n$-raíces $n$-ésimas de la unidad, entonces $X^n - 1 = \prod_{\xi \in G}(X - \xi)$. Los órdenes de elementos de $G$ son divisores de $n$ y para cada divisor $d$ de $n$, los elementos de orden $d$ de $G$ son las raíces $d$-ésimas primitivas de la unidad. Por tanto, si $G_d$ denota el conjunto de las raíces $d$-ésimas primitivas de la unidad, entonces $\{G_d : d|n\}$ es una partición de $G$, con lo que

$$X^n - 1 = \prod_{d|n} \prod_{\xi \in G_d} (X - \xi) = \prod_{d|n} \Phi_d.$$

(3) Razonamos por inducción sobre $n$. Si $n = 1$, entonces $\zeta_n = 1$ y $\Phi_1 = X - 1 = \mathrm{Min}_K(\zeta_n) \in P[X]$. Supongamos que $n > 1$ y que (3) y (4) se verifican para todo número menor que $n$. Entonces de (2) se tiene que

$$X^n - 1 = \Phi_n \prod_{n \neq d|n} \Phi_d$$

y tanto $X^n - 1$ como $q = \prod_{n \neq d|n} \Phi_d$ son polinomios mónicos que están en $P[X]$, por la hipótesis de inducción. Si $P$ es un cuerpo, entonces esto implica que $\Phi_n \in P[X]$. En caso contrario la característica es 0, $P = \mathbb{Z}$ y $\Phi_n$ es un polinomio mónico de $\mathbb{Q}[X]$ que divide a $X^n - 1$ en $\mathbb{Q}[X]$. Por el Lema 4.5, $\Phi_n \in \mathbb{Z}[X]$.

(4) El mismo argumento de (3) muestra que $\mathrm{Min}_K(\xi) \in P[X]$. □

La Proposición 4.6 proporciona un método recursivo para calcular $\Phi_n$ como muestra el siguiente ejemplo.

**Ejemplo 4.7** $\Phi_1 = 1$, $\Phi_2 = \frac{X^2-1}{\Phi_1} = \frac{X^2-1}{X-1} = X + 1$, $\Phi_3 = \frac{X^3-1}{\Phi_1} = \frac{X^3-1}{X-1} = X^2 + X + 1$, $\Phi_4 = \frac{X^4-1}{\Phi_1\Phi_2} = \frac{X^4-1}{(X-1)(X+1)} = X^2 + 1$.

Si $q$ es primo (diferente de la característica), entonces $\Phi_q = \frac{X^q-1}{\Phi_1} = 1 + X + X^2 + \cdots + X^{q-1}$. Por ejemplo $\Phi_5 = 1 + X + X^2 + X^3 + X^4$.

Podemos continuar calculando polinomios ciclotómicos:

$$\begin{aligned} \Phi_6 &= \frac{X^6-1}{\Phi_1\Phi_2\Phi_3} = \frac{X^6-1}{(X-1)(X+1)(1+X+X^2)} = X^2 - X + 1, \\ \Phi_{10} &= \frac{X^{10}-1}{\Phi_1\Phi_2\Phi_5} = \frac{X^{10}-1}{(X-1)(X+1)(1+X+X^2+X^3+X^4)} = \frac{X^{10}-1}{(X^5-1)(X+1)} = \frac{X^5+1}{X+1} = X^4 - X^3 + X^2 - X + 1. \end{aligned}$$

Obsérvese que la expresión de $\Phi_n$ no depende de la característica, siempre que esta característica no divida a $n$. Sin embargo que $\Phi_n$ sea irreducible o sí que depende de la característica.

**Teorema 4.8** *Los polinomios ciclotómicos en característica* 0 *son irreducibles sobre* $\mathbb{Q}$.

**Demostración.** Fijemos una raíz $n$-ésima primitiva de la unidad $\xi$ y sean $f = \mathrm{Min}_{\mathbb{Q}}(\xi)$ y $\Phi = \Phi_n$. Tenemos que demostrar que $\Phi$ es irreducible y, como $\xi$ es raíz de $\Phi$ y $\Phi$ es mónico eso equivale a demostrar que $f = \Phi$, o lo que es lo mismo a demostrar que toda raíz $n$-ésima primitiva de la unidad (es decir todo elemento de la forma $\xi^r$ con $\mathrm{mcd}(r, n) = 1$) es raíz de $p$. Eso está claro si $n = 1$.

Supondremos primero que $r = p$ es primo. Sean $g = \mathrm{Min}_{\mathbb{Q}}(\xi^p)$ y $g_1 = g(X^p)$. Como $\xi^p$ es raíz de $g$, $\xi$ es raíz de $g_1$ y por tanto $f$ divide a $g_1$ en $\mathbb{Q}[X]$ y como $g_1 \in \mathbb{Z}[X]$, del Lema 4.5, y de que tanto $f$ como $g_1$ son mónicos deducimos que $f$ divide a $g_1$ en $\mathbb{Z}[X]$. Pongamos $g_1 = fg_2$ con $g_2 \in \mathbb{Z}[X]$. Considerando el proyección canónica $\mathbb{Z} \to \mathbb{Z}_p$, que extendemos de forma canónica a un homomorfismo de anillos $\mathbb{Z}[X] \to \mathbb{Z}_p[X]$. Denotamos por $\overline{f}$ a la imagen de $f \in \mathbb{Z}[X]$ por este homomorfismo. Entonces utilizando el Pequeño Teorema de Fermat y el hecho de que elevar a $p$ es un homomorfismo en un anillo de característica $p$ deducimos

$$\overline{g}(X)^p = \overline{g}(X^p) = \overline{g_1} = \overline{f}\,\overline{g_2}.$$

Por tanto si $q$ es un divisor irreducible de $\overline{f}$ en $\mathbb{Z}_p[X]$, entonces $q$ divide a $\overline{g}$. Si $\xi^p$ no es raíz de $f$, entonces $f$ y $g$ son coprimos en $\mathbb{Z}[X]$ y por tanto $fg$ divide a $X^n - 1$ en $\mathbb{Z}[X]$ lo que implica que $\overline{f}\,\overline{g}$ divide a $X^n - 1$. Entonces $q^2$ divide a $X^n - 1$, en contra de que $X^n - 1$ no tiene raíces múltiples en una extensión de $\mathbb{Z}_p$ pues $\gcd(p, n) = 1$.

Consideremos ahora un caso arbitrario, con $r = p_1 \cdots p_k$ con $p_1, \ldots, p_k$ primos y argumentemos por inducción en $k$. El caso en que $k = 1$ es el caso considerado en el párrafo anterior. Por hipótesis de inducción $\eta = \xi^{p_1 \cdots p_{k-1}}$ es una raíz de $f$, con lo que $\mathrm{Min}_{\mathbb{Q}}(\eta) = f$. Aplicando ahora el caso visto en el párrafo anterior a $\eta$, deducimos que $\xi^r = \eta^{p_k}$ es raíz de $f$. □

**Corolario 4.9** *Si* $\xi$ *es una raíz* $n$*-ésima primitiva de la unidad en característica* 0*, entonces* $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$.

**Ejercicio 4.10** *El Teorema 4.8 no se verifica en característica positiva. Por ejemplo, en característica 2 tenemos* $\Phi_7 = 1 + X + X^2 + X^3 + X^4 + X^5 + X^6 = (X^3 + X + 1)(X^3 + X^2 + 1)$.

# Problemas

Para cada entero positivo, $\xi_n$ denota una raíz $n$-ésima primitiva de la unidad en la clausura algebraica del cuerpo considerado. Por tanto, implícitamente cada vez que aparezca $\xi_n$ estamos suponiendo que $n$ no es múltiplo de la característica del cuerpo

**4.1** Calcular $\Phi_n$ para todos los números enteros entre 1 y 16.

**4.2** Dar una fórmula general para $\Phi_{2p}$ para $p$ un número primo.

**4.3** Demostrar que si $n$ es par, entonces $\mathbb{Q}(\zeta_n)$ tiene exactamente $n$ raíces de la unidad y en caso contrario tiene $2n$. ¿Cuáles son las raíces de la unidad en cada caso?

**4.4** Demostrar que si $n \leq m$, entonces $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)$ si y solo si $n = m$ ó $n$ es impar y $m = 2n$.

**4.5** Demostrar que si $p$ es un número primo y $\alpha^{p^{n-1}} = \xi_p$ entonces que $\alpha$ es una raíz $p^n$-ésima primitiva de la unidad.

**4.6** Calcular las raíces de la unidad que pertenecen a $\mathbb{Q}(\sqrt{d})$ donde $d$ es un número entero.

**4.7** Demostrar las siguiente igualdades para $\zeta = \zeta_n$.

(1) $\prod_{i=0}^{n-1}(X-\zeta^i)=X^n-1$.

(2) $\sum_{i=0}^{n-1}\zeta^i=\begin{cases}1, & \text{si } n=1;\\ 0, & \text{si} n>1\end{cases}$.

(3) $\prod_{i=1}^{n-1}(1-\zeta^i)=n$. (Por convenio, el producto vacío es 1.)

(4) $\prod_{i=1}^{n-1}(1+\zeta^i)=\begin{cases}0 & \text{si } 2|n\\ 1 & \text{si } 2\nmid n\end{cases}$.

**4.8** Sean $m$ y $n$ dos números naturales y $d=\mathrm{mcd}(m,n)$. Demostrar que $\Phi_m$ es el producto de $\varphi(d)$ polinomios irreducibles de $\mathbb{Q}(\zeta_n)$ de grado $\varphi(m)/\varphi(d)$.

**4.9** Demostrar que $F_n=\mathbb{Q}(\zeta_n)\cap\mathbb{R}=\mathbb{Q}(\zeta_n+\zeta_n^{-1})=\mathbb{Q}(\cos\frac{2\pi}{n})$. Calcular $[\mathbb{Q}(\zeta_n):F_n]$ e $\mathrm{Min}_{F_n}(\zeta_n)$ en función de $n$.

**4.10** Demostrar que toda extensión de cuerpos finitos es una extensión ciclotómica.

**4.11** Demostrar que si $E/K$ es una extensión normal y $L/E$ es una extensión ciclotómica entonces $L/K$ es normal.

**4.12** Sea $\mathbb{F}=\mathbb{F}_q$ un cuerpo finito de cardinal $q$ y $n$ un número natural coprimo con $q$. Demostrar

(1) $[\mathbb{F}(\xi_n):\mathbb{F}]$ es el menor entero positivo $r$ tal que $q^r\equiv 1 \bmod n$.

(2) Demostrar que $\Phi_n$ (el $n$-ésimo polinomio ciclotómico en característica $p$) es el producto de $\varphi(n)/r$ polinomios de grado $r$, donde $r$ es como en $a$).

(3) Si $n$ es primo, entonces $\mathrm{Min}_{\mathbb{F}}(\zeta_n)=1+X+X^2+\cdots+X^{n-1}$ si y solo si $n$ no divide a $\prod_{i=1}^{n-2}(q^i-1)$.

(Indicación: Aplicar propiedades de los grupos cíclicos.)

**4.13** Sea $\mathbb{F}=\mathbb{F}_q$ un cuerpo con $q$ elementos y para cada entero $n$ sea $I_d$ el conjunto de los polinomios mónicos e irreducibles de grado $d$ en $\mathbb{F}[X]$. Demostrar que $X^{q^n}-X=\prod_{d|n}\prod_{p\in I_d}p$.

**4.14** Demostrar que si $n$ es un entero mayor o igual que 2 y $p$ es un número primo, entonces la clausura normal de $\mathbb{Q}(\sqrt[n]{p})/\mathbb{Q}$ es $\mathbb{Q}(\sqrt[n]{p},e^{2\pi i/n})$. ¿Para que números $n$ y $p$ se verifica que $\mathbb{Q}(\sqrt[n]{p})/\mathbb{Q}$ es una extensión normal? Calcular $[\mathbb{Q}(\sqrt[n]{p},e^{2\pi i/n}):\mathbb{Q}(\sqrt[n]{p})]$.

**4.15** Demostrar que la aplicación $\mathbb{Z}_n^*\to\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ dada por $i\mapsto\sigma_i$, donde $\sigma_i(\zeta_n)=\zeta_n^i$ es un isomorfismo de grupos.

**4.16** Sea $\zeta=\zeta_p\in\mathbb{C}$, con $p$ primo y sea $\lambda$ un generador de $\mathbb{Z}_p^*$. Para cada $i\in\mathbb{Z}_p^*$, sea $\epsilon_i=\zeta^{\lambda^i}$. Demostrar

(1) $\epsilon_0,\epsilon_1,\ldots,\epsilon_{p-2}$ son las $p-1$ raíces primitivas de la unidad y forman una base de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$.

(2) El grupo de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ es cíclico generado por el automorfismo $\sigma$ de $\mathbb{Q}(\zeta)$ dado por $\sigma(\zeta)=\epsilon_1$.

(3) $\sigma^j(\epsilon_i)=\epsilon_{i+j}$, donde el subíndice hay que leerlo módulo $p-1$.

(4) Para cada $k$ y cada divisor $d$ de $p-1$ se verifica $\sigma^d(\omega_{k,d}) = \omega_{k,d}$, donde

$$\omega_{k,d} = \epsilon_k + \epsilon_{k+d} + \epsilon_{k+2d} + \cdots + \epsilon_{k+\left(\frac{p-1}{d}-1\right)d},$$

pero $\sigma^{d_1}(\omega_{k,d}) \neq \omega_{k,d}$, para todo divisor $d_1$ de $p-1$ menor que $d$. Los elementos de la forma $\omega_{k,d}$, se llaman *periodos de Gauss*.

**4.17** Demostrar las siguientes propiedades de los polinomios ciclotómicos $\Phi_n$.

(1) $\Phi_p(X) = 1+X+X^2+\cdots+X^{p-1}$ y $\Phi_{p^r} = \Phi_p(X^{p^{r-1}})$ donde $p$ es primo y $r$ es un número natural.

(2) $\Phi_n(X) = \Phi_{p_1\cdots p_s}(X^{p_1^{r_1-1}\cdots p_s^{r_s-1}})$, donde $n = p_1^{r_1}\cdots p_s^{r_s}$, $p_1,\ldots,p_r$ son primos distintos y $r_1,\ldots,r_s$ son números naturales.

(3) Si $n$ es impar entonces $\Phi_{2n}(X) = \Phi_n(-X)$.

(4) Si $p$ es un primo que no divide a $n$, entonces $\Phi_{pn}(X)\Phi_n(X) = \Phi_n(X^p)$.

(5) $\Phi_n(X) = \prod_{d|n}(X^{n/d}-1)^{\mu(d)}$, donde $\mu$ es la función de Möbius definida de la siguiente fórmula sobre los números naturales:

$$\mu(n) = \begin{cases} 1, & \text{si } n = 1, \\ (-1)^r, & \text{si n es el producto de } r \text{ primos distintos}, \\ 0, & \text{en cualquier otro caso.} \end{cases}$$

**4.18** Sea $p$ un número primo impar. Para cada entero $n$, ponemos

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } n \equiv 0 \bmod p, \\ 1 & \text{si } n \equiv x^2 \not\equiv 0 \bmod p \text{ para algún entero } x, \\ -1 & \text{si } n \not\equiv x^20 \bmod p \text{ para todo entero } x. \end{cases}$$

Demostrar:

(1) $\left\{n = 1,\ldots,p-1 : \left(\frac{n}{p}\right) = 1\right\}$ tiene $\frac{p-1}{2}$ elementos.

(2) Si $n \equiv m \bmod p$, entonces $\left(\frac{n}{p}\right) = \left(\frac{m}{p}\right)$.

(3) $\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right)$.

(4) Si $\zeta = \zeta_p$ es una raíz $p$-ésima primitiva de la unidad en $\mathbb{C}$ y

$$S = \sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\zeta^n$$

entonces

$$S^2 = \left(\frac{-1}{p}\right)p.$$

(5) $\mathbb{Q}(\zeta)$ contiene a $\mathbb{Q}(\sqrt{p})$ ó a $\mathbb{Q}(\sqrt{-p})$. ¿Cuándo se da cada caso?

(6) $\mathbb{Q}(\sqrt{p})$ está contenido en $\mathbb{Q}(\zeta_{4p})$.

(7) Toda extensión cuadrática de $\mathbb{Q}$ está contenida en una extensión ciclotómica.

# Capítulo 5

# Extensiones separables

## 5.1 Grado de separabilidad

**Definición 5.1** *Sean $E/K$ una extensión algebraica y $\sigma : K \to L$ un homomorfismo de cuerpos con $L$ algebraicamente cerrado. Se llama* grado de separabilidad *de la extensión $E/K$ al cardinal del conjunto $S_\sigma^E$ de las extensiones de $E$ a $L$, es decir los homomorfismos $\tau : E \to L$ tales que $\tau|_K = \sigma$. Denotamos el grado de separabilidad de la extensión $E/K$ por $[E : K]_s$.*

Para que la anterior sea una buena definición el cardinal de $S_\sigma^E$ no debe de depender de $L$ ni de $\sigma$.

**Proposición 5.2** *Si $E/K$ es una extensión algebraica entonces el cardinal $S_\sigma^E$ es el mismo para todos los homomorfismos de cuerpos $\sigma : K \to L$, con $L$ algebraicamente cerrado.*

**Demostración.** En primer lugar vamos a ver que podemos suponer que $L$ es una clausura algebraica de $\sigma(K)$. Obsérvese que si $\tau \in S_\sigma^E$, entonces $\tau(E)$ es algebraico sobre $\tau(K) = \sigma(K)$. Por tanto $\tau(E)$ está incluido en la clausura algebraica de $\sigma(K)$ en $L$, con lo que $S_\sigma^E$ no se ve afectado si cambiamos $L$ por está clausura algebraica, que también es algebraicamente cerrada por la Proposición 3.3. A partir de ahora supondremos que $L$ es una clausura algebraica de $\sigma(K)$.

Sea $\sigma' : K \to L'$ otro homomorfismo con $L'$ una clausura algebraica de $\sigma'(K)$. La aplicación $\sigma(K) \to \sigma'(K)$ dada por $x \to \sigma' \circ \sigma^{-1}(x)$ es un isomorfismo. Por la Proposición 3.7, existe un isomorfismo $\lambda : L \to L'$ tal que $\lambda(\sigma(k)) = \sigma'(k)$ para todo $k \in K$. La aplicación de $S_\sigma^E$ en $S_{\sigma'}^E$ dada por $\tau \mapsto \lambda \circ \tau$ es biyectiva pues su inversa es la aplicación en sentido contrario dada por $\tau' \mapsto \lambda^{-1} \circ \tau'$. En conclusión el cardinal del conjunto $S_\sigma^E$ no depende del cuerpo algebraicamente cerrado $L$ ni del homomorfismo $\sigma$. □

**Ejemplo 5.3** Supongamos que $\alpha$ es algebraico sobre $K$ y sea $L$ una clausura algebraica de $K$ que contenga a $\alpha$. Sea $p = \mathrm{Min}_K(\alpha)$. Por el Lema de Extensión (Lema 2.9) si $\tau : K(\alpha) \to L$ es un $K$-homomorfismo (es decir $\tau \in S_\sigma^{K(\alpha)}$, donde $\sigma : K \to L$ es el homomorfismo de inclusión) entonces $\tau(\alpha)$ es una raíz de $p$ y, recíprocamente para cada raíz $\beta$ de $p$, existe un isomorfismo $K(\alpha) \simeq K(\beta)$, que podemos considerar como un $K$-homomorfismo de $K(\alpha)$ en $L$. Por tanto $[K(\alpha) : K]_s$ es igual al número de raíces de $p$.

Las raíces de $\mathrm{Min}_K(\alpha)$ (en $L$) son llamadas también *conjugados* de $\alpha$ sobre $K$ y, como hemos visto son las imágenes de $\alpha$ por los $K$-automorfismos de $L$. Obsérvese que con esta terminología los conjugados de un número complejo $\alpha$ sobre $\mathbb{R}$ son exactamente $\alpha$ y su conjugado complejo $\overline{\alpha}$.

En muchos aspectos el grado de separabilidad se comporta como el grado.

**Proposición 5.4 (Propiedad Multiplicativa del Grado de Separabilidad)** *Si $K \subseteq E \subseteq F$ es una torre de cuerpos, entonces*

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

**Demostración.** Sea $\sigma : K \to L$ un homomorfismo de cuerpos con $L$ algebraicamente cerrado. Como todo elemento de $S_\sigma^F$ es una extensión de un elemento de $S_\sigma^E$, a saber de su restricción a $E$, se tiene que

$$S_\sigma^F = \bigcup_{\tau \in S_\sigma^E} S_\tau^F.$$

Claramente los conjuntos $S_\tau^F$ son disjuntos y por otro lado de la Proposición 5.2 se tiene que $S_\tau^F = [F : E]_s$ para todo $\tau \in S_\sigma^E$. Concluimos que $[F : K]_s = \sum_{\tau \in S_\sigma^E} |S_\tau^F| = [F : E]_s[E : K]_s$. □

**Lema 5.5** *Si $K$ es un cuerpo de característica $p \neq 0$ entonces la aplicación $\varphi : x \mapsto x^p$ de $K$ en si mismo es un homomorfismo de cuerpos (llamado* homomorfismo de Frobenius*. Si además $K$ es algebraico sobre su cuerpo primo (por ejemplo, si $K$ es finito), entonces $\varphi$ es un automorfismo de $K$ (conocido con el nombre de* automorfismo de Frobenius*.*

*Por tanto, si $\alpha^p = \beta^p$ con $\alpha, \beta \in K$, entonces $\alpha = \beta$.*

**Demostración.** Claramente $\varphi(1) = 1$ y $\varphi(ab) = \varphi(a)\varphi(b)$. Por otro lado, si $1 \leq i < p$ entonces $\binom{p}{i}$ es múltiplo de $p$. Por tanto $\varphi(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i}b^i = a^p + b^p = \varphi(a) + \varphi(b)$. Esto demuestra que $\varphi$ es un homomorfismo de cuerpos, que como todos los homomorfismos entre cuerpos será inyectivo.

Supongamos ahora que $K$ es algebraico sobre su cuerpo primo $P$ y sea $\alpha \in K$ y $E = P(\alpha)$. Entonces $E$ una extensión finita de $P$ y $P \cong \mathbb{Z}_p$. Por tanto $E$ es un cuerpo finito y $\varphi$ se restringe a un homomorfismo de $E$ en si mismo, que será un automorfismo pues $\varphi$ es injectivo y $E$ es finito. Por tanto, si $\alpha$ está en la imagen de $\varphi$. □

**Lema 5.6 (Uniformidad de la Multiplicidad)** *Sea $f \in K[X]$ irreducible.*

*(1) Todas las raíces de $f$ (en un cuerpo de descomposición de $f$) tienen la misma multiplicidad.*

*(2) Si $\mathrm{car}K = 0$ entonces $f$ no tiene raíces múltiples.*

*(3) Si $\mathrm{car}K = p \neq 0$ entonces la multiplicidad de las raíces de $f$ es una potencia de $p$ y la multiplicidad es $p^n$ si y solo si $n$ es el mayor número no negativo tal que $f = g(X^{p^n})$ para algún $g \in K[X]$.*

**Demostración.** Podemos suponer que $f$ es mónico.

(1) Sean $\alpha_1, \ldots, \alpha_n$ las raíces de $f$ y sea $m_i$ la multiplicidad de $\alpha_i$ como raíz de $f$. Fijemos $1 \leq i, j \leq n$. Por el Lema de Extensión (Lemma 2.9), existe un $K$-isomorfismo $\sigma : K(\alpha_i) \to K(\alpha_j)$ tal que $\sigma(\alpha_i) = \alpha_j$. Además $\sigma$ permuta los $\alpha_k$. Por tanto

$$\prod_{k=1}^{n} (X - \alpha_k)^{m_k} = f = \sigma(f) = \prod_{k=1}^{n} (X - \sigma(\alpha_k))^{m_k}$$

De la unicidad de la factorización deducimos que $m_j$ = exponente de $X - \alpha_j$, en la expresión de la izquierda = Exponente de $X - \sigma(\alpha_i) = X - \alpha_j$ es la expresión de la derecha = $m_i$. Esto termina la demostración de (1).

Para demostrar (2) y (3) recordemos que las raíces múltiples son las raíces comunes de $f$ y $f'$. Como $\mathrm{gr}(f') < \mathrm{gr}(f)$, se tiene que $f | f'$ si y solo si $f' = 0$ y en caso contrario $\mathrm{mcd}(f, f') = 1$ y $f$ no tendrá raíces múltiples.

(2) Si car$K \neq 0$, entonces $f' \neq 0$ y por tanto $f$ no tiene raíces múltiples.

(3) Supongamos que car$K = p > 0$ y sea $n$ el mayor entero no negativo de forma que $f(X) = g(X^{p^n})$ para algún $g \in K[X]$. Para ver que este número existe, obsérvese que para $n = 0$, tomando $g = f$ se cumple la igualdad y por otro lado si se cumple la igualdad entonces $\mathrm{gr} f = p^n \mathrm{gr} g$ con lo que $n$ está acotado superiormente. Eso garantiza la existencia de $n$. Además $g$ está unívocamente determinado por $f$ y si $f = \sum_i f_i X^i$ entonces $n > 0$ si y solo si $f_i = 0$ para todo $i$ que no sea múltiplo de $p$ si y solo si $f' = 0$ si y solo si $f$ tiene raíces múltiples.

Como $f$ es irreducible, $g$ también lo es. Si $g' = 0$ entonces $g = h(X^p)$ para algún $h \in K[X]$ y por tanto

$$f = g(X^{p^n}) = h((X^{p^n})^p) = h(X^{p^{n+1}})$$

en contra de la elección de $n$. Por tanto $g$ es irreducible y $g' \neq 0$, lo que implica que $g$ no tiene raíces múltiples. Si $\alpha_1, \ldots, \alpha_k$ son las distintas raíces de $f$, entonces $\alpha_1^{p^n}, \ldots, \alpha_k^{p^n}$ son raíces de $g$ y todas son distintas, por el Lema 5.5. Vamos a ver que estas son las únicas raíces de $g$. En efecto si aparte de éstas, $g$ tuviera otras raíces $\beta_1, \ldots, \beta_l$, entonces

$$g = (X - \alpha_1^{p^n}) \cdots (X - \alpha_k^{p^n})(X - \beta_1) \cdots (X - \beta_l)$$

y por tanto

$$f = (X^{p^n} - \alpha_1^{p^n}) \cdots (X^{p^n} - \alpha_k^{p^n})(X^{p^n} - \beta_1) \cdots (X^{p^n} - \beta_l).$$

Si $\gamma$ es una raíz de $(X^{p^n} - \beta_1) \cdots (X^{p^n} - \beta_l)$, entonces $\gamma$ es una raíz de $f$ y por tanto $\gamma = \alpha_i$ para algún $i = 1, \ldots, k$ y $\gamma^{p^n} = \beta_j^{p^n}$ para algún $j = 1, \ldots, l$. Eso implica que $\alpha_i = \gamma = \beta_j$, en contra de que los $\alpha$ y los $\beta$ son diferentes. En resumen,

$$g = (X - \alpha_1^{p^n}) \cdots (X - \alpha_k^{p^n})$$

y por tanto

$$f = (X^{p^n} - \alpha_1^{p^n}) \cdots (X^{p^n} - \alpha_k^{p^n}) = (X - \alpha_1)^{p^n} \cdots (X - \alpha_k)^{p^n}$$

lo que implica que todas las raíces de $f$ tienen multiplicidad $p^n$. □

**Definición 5.7** *Si $f \in K[X]$ es irreducible, entonces se llama* grado de separabilidad *de $f$ sobre $K$ al número de raíces distintas de $f$ (en un cuerpo de descomposición de $f$) y* grado de inseparabilidad *de $f$ a la multiplicidad de cualquiera de las raíces de $f$.*

*Los grados de separabilidad e inseparabilidad de $f$ los denotamos por* $\mathrm{gr}_s(f)$ *y* $\mathrm{gr}_i(f)$*, respectivamente.*

Obviamente

$$\mathrm{gr}(f) = \mathrm{gr}_s(f)\mathrm{gr}_i(f) \tag{5.1}$$

Del Ejemplo 5.3 se deduce que

**Proposición 5.8** *Si $\alpha$ es algebraico sobre $K$, entonces $[K(\alpha) : K]_s = \mathrm{gr}_s(\mathrm{Min}_K(\alpha))$.*

Además:

**Proposición 5.9** *Si $E/K$ es una extensión finita de cuerpos, entonces $[E : K]_s$ divide a $[E : K]$.*

**Demostración.** Razonamos por inducción sobre $n = [E : K]$, con el caso $n = 1$ trivial. Supongamos que $n > 1$ y la hipótesis de inducción. Sea $\alpha \in E \setminus K$. Entonces $[E : K(\alpha)] < n$ y, por la hipótesis inducción, $[E : K(\alpha)]_s$ divide a $[E : K(\alpha)]$. Pongamos $k = [E : K(\alpha)]/[E : K(\alpha)]_s$. Si $p = \mathrm{Min}_K(\alpha)$, entonces aplicando la Proposición 5.8 y la fórmula (5.1) se deduce que

$$\begin{aligned} [E : K] &= [E : K(\alpha)][K(\alpha) : K] = k[E : K(\alpha)]_s \mathrm{gr}(p) = k[E : K(\alpha)]_s \mathrm{gr}_s(p)\mathrm{gr}_i p \\ &= (k\mathrm{gr}_i(p))[E : K(\alpha)]_s[K(\alpha) : K]_s = (k\mathrm{gr}_i(p))[E : K]_s. \end{aligned}$$

□

Se llama *grado de inseparabilidad* de una extensión finita $E/K$ al cociente

$$[E:K]_i = \frac{[E:K]}{[E:K]_s}.$$

## 5.2 Extensiones separables

**Definición 5.10** *Un polinomio $f \in K[X]$ no constante se dice que es* separable *si no tiene raíces múltiples en una extensión de $K$, o lo que es lo mismo si* $\mathrm{mcd}(f, f') = 1$.

*Si $\alpha$ es un* elemento *de una extensión $L$ de $K$ entonces se dice que $\alpha$ es* separable *sobre $K$ si es algebraico y $\mathrm{Min}_K(\alpha)$ es un polinomio separable.*

*Una* extensión *$L/K$ se dice que es* separable *si todo elemento de $L$ es separable sobre $K$. En particular una extensión separable es algebraica.*

*Una extensión $L/K$ se dice que es* puramente inseparable *si los únicos elementos de $L$ que son separables sobre $K$ son los elementos de $K$.*

Claramente si $f \in K[X]$ es irreducible entonces $f$ es separable si y solo si $\mathrm{gr}_s(f) = \mathrm{gr}(f)$ si y solo si $\mathrm{gr}_i(f) = 1$. Por otro lado como consecuencia del Lema 5.6 se tiene:

**Proposición 5.11** *Si* $\mathrm{car}K = 0$ *entonces todo polinomio irreducible de $K[X]$ es separable y por tanto toda extensión algebraica de $K$ es separable.*

Además de la Proposición 5.8 se deduce que un elemento algebraico $\alpha$ sobre $K$ es separable si y sólo si $[K(\alpha):K] = [K(\alpha):K]_s$ si y solo si $[K(\alpha):K]_i = 1$.

**Teorema 5.12** *Las siguientes condiciones son equivalentes para una extensión finita $L/K$:*

*(1) $L/K$ es separable.*

*(2) $[L:K] = [L:K]_s$.*

*(3) $[L:K]_i = 1$.*

**Demostración.** La equivalencia entre (2) y (3) es obvia.

(2) implica (1) Supongamos que $[L:K] = [L:K]_s$ y sean $\alpha \in L$ y $E = K(\alpha)$. Entonces, de las propiedades multiplicativas del grado y del grado de separabilidad (Proposición 5.4) deducimos

$$[L:E][E:K] = [L:K] = [L:K]_s = [L:E]_s[E:K]_s.$$

Como los dos factores de la derecha son menores o iguales que los de la izquierda y todos son enteros positivos, deducimos que $[L:E] = [L:E]_s$ y $[K(\alpha):K] = [K(\alpha):K]_s$ y ya sabemos que esto último es equivalente a que $\alpha$ sea separable sobre $K$.

(1) implica (2) Supongamos que $L/K$ es separable y razonemos por inducción sobre $n = [L:K]$, con nada que demostrar en el caso en que $n = 1$. Supongamos que $n > 1$ y la hipótesis de inducción. Elegimos $\alpha \in L \setminus K$. Como $\mathrm{Min}_{K(\alpha)}(\beta)$ divide a $\mathrm{Min}_K(\beta)$, para todo $\beta \in L$, tenemos que $L/K(\alpha)$ es separable y como $[L:K(\alpha)] < n$, deducimos que $[L:K(\alpha)] = [L:K(\alpha)]_s$, por la hipótesis de inducción. Además, como $\alpha$ es separable sobre $K$ se tiene que $[K(\alpha):K] = [K(\alpha):K]_s$. Uniendo estas dos igualdades obtenemos

$$[L:K] = [L:K(\alpha)][K(\alpha):K] = [L:K(\alpha)]_s[K(\alpha):K]_s = [L:K]_s.$$

□

Una consecuencia inmediata del Teorema 5.12 y de las propiedades multiplicativas de los grados es el siguiente

**Corolario 5.13** *La clase de extensiones separables es multiplicativa.*

Veamos más consecuencias del Teorema 5.12.

**Corolario 5.14** *Si $L = K(A)$ y todos los elementos de $A$ son separables sobre $K$ entonces $L/K$ es separable.*

**Demostración.** Si $\alpha \in L$, entonces existe $B \subseteq A$ finito tal que $\alpha \in K(B)$, lo que implica que en la demostración podemos suponer que $A$ es finito. Si $A = \{\alpha_1, \ldots, \alpha_n\}$ entonces cada $\alpha_i$ es separable sobre $K$ y por tanto también sobre $K(\alpha_1, \ldots, \alpha_{i-1})$. Aplicando que la clase de extensiones separables es multiplicativa, basta demostrar el corolario para el caso en que $A$ tiene un único elemento $\alpha$. Pero esto está claro pues si $\alpha$ es separable sobre $K$, entonces $[K(\alpha) : K] = [K(\alpha) : K]_s$, es decir $K(\alpha)/K$ es separable. □

Una consecuencia inmediata del Corolario 5.14 es el siguiente

**Corolario 5.15** *Si $L/K$ es una extensión de cuerpos entonces el conjunto de los elementos de $L$ que son separables sobre $K$ es un subcuerpo de $L$ que contiene a $K$. Este subcuerpo se llama* clausura separable *de $K$ en $L$.*

Dos últimos corolarios, el primero de los cuales es obvio:

**Corolario 5.16** *Si $L/K$ es una extensión finita y $S$ es la clausura separable de $L/K$ entonces $[L : K]_s = [S : K]$.*

**Corolario 5.17** *La clase de extensiones separables es cerrada para levantamientos.*

**Demostración.** Sean $E/K$ y $F/K$ extensiones admisibles con $E/K$ separable. Cada elemento de $E$ es separable sobre $K$ y por tanto también es separable sobre $F$, con lo que del Corolario 5.14 deducimos que $EF/F = F(E)/F$ es separable. □

## 5.3 Elementos primitivos

Recordemos que una extensión $L/K$ se dice que es simple si $L = K(\alpha)$ para algún $\alpha \in L$. En tal caso se dice que $\alpha$ es un *elemento primitivo* de la extensión $L/K$.

**Lema 5.18** *Sean $\alpha$ y $\beta$ elementos de una extensión $L$ de $K$ y sean $a$ y $b$ elementos distintos de $K$. Si $E = K(\alpha + a\beta) = K(\alpha + b\beta)$, entonces $E = K(\alpha, \beta)$.*

**Demostración.** Supongamos que $E = K(\alpha + a\beta) = K(\alpha + b\beta)$. La inclusión $E \subseteq K(\alpha, \beta)$ es obvia. Para ver la otra inclusión observemos que $(a - b)\beta \in E$ y por tanto $\beta \in E$, lo que implica que $\alpha \in E$. □

**Teorema 5.19 (Teorema del Elemento Primitivo)** *Toda extensión separable finita es simple (es decir, tiene un elemento primitivo).*

**Demostración.** Ya sabemos que si $K$ es finito, entonces $L/K$ es simple por lo que supondremos que $K$ es infinito.

Sea $L/K$ una extensión separable finita y sea $n$ el menor número de elementos de $L$ necesarios para generar $L$ sobre $K$. Tenemos que demostrar que $n = 1$, con lo que suponemos $n \geq 2$. Pongamos $L = K(\alpha_1, \ldots, \alpha_n)$ y $m = [K(\alpha_1, \alpha_2) : K]$. Sea $\sigma$ la inclusión de $K$ en una clausura algebraica de $L$ y sean $m = [K(\alpha_1, \alpha_2) : K]$. Como $K(\alpha_1, \alpha_2)/K$ es separable, $S_\sigma^{K(\alpha_1,\alpha_2)}$ tiene $m$ elementos, $\sigma_1, \ldots, \sigma_m$. Consideremos el polinomio

$$p = \prod_{i \neq j} (\sigma_i(\alpha_1) - \sigma_j(\alpha_1) + X(\sigma_i(\alpha_2) - \sigma_j(\alpha_2))).$$

Para todo $i \neq j$, $\sigma_i \neq \sigma_j$ y por tanto $\sigma_i(\alpha_1) \neq \sigma_j(\alpha_1)$ ó $\sigma_i(\alpha_2) \neq \sigma_j(\alpha_2)$, con lo que los factores lineales que aparecen en la definición de $p$ son diferentes de 0 y por tanto $p \neq 0$. Como $K$ es infinito existe $a \in K$ tal que $p(a) \neq 0$, o lo que es lo mismo, si $\beta = \alpha_1 + a\alpha_2$, entonces $\sigma_i(\beta) \neq \sigma_j(\beta)$ para todo $i \neq j$. Esto muestra que $[K(\beta) : K]_s \geq m$ y, como todas las subextensiones de $L/K$ son separables, tenemos $m \leq [K(\beta) : K]_s = [K(\beta) : K] \leq [K(\alpha_1, \alpha_2) : K] = m$. Concluimos que $K(\alpha_1, \alpha_2) = K(\beta)$ y por tanto

$$L = K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\alpha_1, \alpha_2)(\alpha_3, \ldots, \alpha_n) = K(\beta)(\alpha_3, \ldots, \alpha_n) = K(\beta, \alpha_3, \ldots, \alpha_n)$$

en contra de la minimalidad de $n$. □

Vamos a denotar con $\mathrm{Sub}(L/K)$ al conjunto de las subextensiones de $L/K$, es decir $\mathrm{Sub}(L/K)$ es el conjunto de los subcuerpos de $L$ que contienen a $K$.

**Teorema 5.20 (Artin)** *Una extensión finita $L/K$ es simple si y solo si $\mathrm{Sub}(L/K)$ es finito.*

**Demostración.** Si $K$ es finito, entonces $L$ es finito (¿por qué?) y por tanto $\mathrm{Sub}(L/K)$ es finito. Además $L^*$ es cíclico (Lema 4.2) y si $\alpha$ es un generador de $L^*$ entonces $L = K(\alpha)$. Esto muestra el Teorema para el caso en que $K$ es finito, por lo que a partir de ahora supondremos que $K$ es infinito.

Supongamos primero que $\mathrm{Sub}(L/K)$ es finito. Como $K$ es infinito y $\mathrm{Sub}(L/K)$ es finito, aplicando el Lema 5.18, deducimos que para todo $\alpha, \beta \in L$ existen dos elementos distintos $a$ y $b$ de $K$ tales que $K(\alpha + a\beta) = K(\alpha + b\beta)$, en cuyo caso del Lema 5.18 se tiene que $K(\alpha, \beta)$ es simple. Si $n$ es el menor número de elementos de $L$ tales que $L = K(\alpha_1, \ldots, \alpha_n)$ y $n \geq 2$ entonces existe $\beta \in L$ tal que $K(\alpha_1, \alpha_2) = K(\beta)$ y por tanto

$$L = K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\alpha_1, \alpha_2)(\alpha_3, \ldots, \alpha_n) = K(\beta)(\alpha_3, \ldots, \alpha_n) = K(\beta, \alpha_3, \ldots, \alpha_n)$$

en contra de la minimalidad de $n$. Por tanto $n = 1$, es decir $L/K$ es simple.

Recíprocamente, supongamos que $L/K$ es simple y sea $\alpha \in L$ con $L = K(\alpha)$. Para cada $E \in \mathrm{Sub}(L/K)$ sea $p_E = \mathrm{Min}_E(\alpha)$. Si $P$ es el conjunto de los divisores mónicos de $p_K$ en $L(X)$ entonces $P$ es finito pues si $\alpha_1, \ldots, \alpha_n$ son las raíces de $p_K$ en una clausura algebraica de $L$, entonces cada elemento de $P$ es de la forma $(X - \alpha_1)^{e_1} \cdots (X - \alpha_n)^{e_n}$ con $\sum_{i=1}^n e_n \leq \mathrm{gr}(p_K)$. Además $E \mapsto p_E$ define una aplicación de $\mathrm{Sub}(L/K)$ a $P$ y para acabar la demostración basta demostrar que esta aplicación es inyectiva. Para ver esto vamos a demostrar que $E$ está generado sobre $K$ por los coeficientes de $p_E$. En efecto, sean $E \in \mathrm{Sub}(L/K)$ y $F$ el elemento de $\mathrm{Sub}(L/K)$ generado sobre $K$ por los coeficientes de $p_E$. Entonces $p_E \in F[X]$ y $p_E(\alpha) = 0$ lo que implica que $p_F$ divide a $p_E$. Luego $[L : E] = [E(\alpha) : E] = \mathrm{gr}(p_E) \geq \mathrm{gr}(p_F) = [F(\alpha) : F] = [L : F]$, o lo que es lo mismo $[E : K] \leq [F : K]$ y $F \subseteq E$ de donde concluimos que $E = F$ como queríamos. □

## Problemas

**5.1** Para cada uno de los siguiente polinomios y los siguientes cuerpos decidir qué polinomios son separables sobre qué cuerpos. Polinomios: $X^3+1$, $X^4+2X-1$ y $X^3-21X^2+147X-343$ sobre $\mathbb{Q}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_7$.

**5.2** Decidir sobre la verdad o falsedad de las siguientes afirmaciones, demostrando las verdaderas y dando un contraejemplo de las falsas.

(1) Todo polinomio irreducible de $K[X]$ es separable.

(2) Toda extensión separable en normal.

(3) Toda extensión normal es separable.

(4) Toda extensión de cuerpos finitos es separable.

(5) Toda extensión finita es separable.

(6) Si la característica de $K$ no divide al grado de la extensión $L/K$, entonces la extensión $L/K$ es separable.

(7) Si $p \in K[X]$ tiene grado $n$, $L$ es un cuerpo de escisión de $p$ sobre $K$ y la característica de $K$ no divide a $n$, entonces $L/K$ es separable.

(8) Si $p \in K[X]$ tiene grado $n$, $L$ es un cuerpo de escisión de $p$ sobre $K$ y la característica de $K$ no divide a $n!$, entonces $L/K$ es separable.

(9) Si $p \in K[X]$ es separable sobre $K$ entonces el cuerpo de escisión de $p$ sobre $K$ es normal sobre $K$.

**5.3** Construir una extensión finita que no sea simple. (Indicación: $\mathbb{F}_p(X,Y)/?$.)

**5.4** Demostrar que las siguientes condiciones son equivalentes para un cuerpo $K$ y un elemento $\alpha$ algebraico sobre $K$.

(1) $[K(\alpha):K]_s = 1$, es decir, la extensión $K(\alpha)/K$ es puramente inseparable.

(2) $\alpha^{p^n} \in K$ para algún $n \geq 0$.

(3) $\mathrm{Min}_K(\alpha) = X^{p^n} - a$, para algún $n \geq 0$ y algún $a \in K$.

Decimos que $\alpha$ es *puramente inseparable* sobre $K$ si se cumplen las condiciones anteriores.

**5.5** Demostrar que una extensión algebraica de cuerpos $L/K$ es puramente inseparable, si todo elemento de $L$ es puramente inseparable sobre $K$.

**5.6** Demostrar que si $K$ es un cuerpo de característica $p > 0$ y $n \geq 0$, entonces $K^{p^n} = \{a^{p^n} : a \in K\}$ es un subcuerpo de $K$ y $K/K^{p^n}$ es una extensión puramente inseparable.

**5.7** Demostrar que la clase de extensiones puramente inseparables es multiplicativa en torres y estable por levantamientos.

**5.8** Demostrar que si $L = K(A)$ y los elementos de $A$ son puramente inseparables sobre $K$, entonces $L/K$ es puramente inseparable.

**5.9** Sea $L/K$ una extensión de cuerpos. Demostrar que $P = \{\alpha \in L : \alpha$ es puramente inseparable sobre $K\}$ es un subcuerpo de $L$. Este cuerpo se llama *clausura puramente inseparable* de $L/K$ (o de $K$ en $L$).

**5.10** Demostrar que si $L/K$ es una extensión finita y puramente inseparable, entonces $[L : K]$ es una potencia de la característica de $K$. (Se entiende que $0^0 = 1$.)

**5.11** Sea $L/K$ una extensión algebraica. Demostrar que existe subextensión $S$ de $L/K$ tal que $S/K$ es separable y $L/S$ es puramente inseparable. Demostrar también que si $E$ es una subextensión de $L/K$, entonces $E \cap S = K$ si y solo si $E/K$ es puramente inseparable.

**5.12** Sea $p = Y^6 - X \in K[Y]$, con $K = \mathbb{F}_3(X)$, y sea $\alpha$ una raíz de $p$, en un clausura algebraica de $K$. Estudiar la separabilidad de $\alpha^n$ sobre $K$, para cada $n \geq 1$ y calcular las clausuras separable y puramente inseparable de $K(\alpha)/K$.

**5.13** Sea $K = \mathbb{F}_2(X)$, el cuerpo de fracciones del anillo de polinomios $\mathbb{F}_2[X]$ y $L = K(\sqrt[4]{X})$. Sean $S$ y $P$ las clausuras separable y puramente separables de $L/K$. Demostrar que $L \neq SP$.

**5.14** Demostrar que las siguientes condiciones son equivalentes para un cuerpo $K$.

(1) Todo polinomio irreducible en $K[X]$ es separable.

(2) Toda extensión algebraica de $K$ es separable.

(3) $\mathrm{car}K = 0$ ó $\mathrm{car}K = p \neq 0$ y $K = K^p$.

Un cuerpo que satisface estas condiciones se dice que es *perfecto*.

**5.15** Demostrar:

(1) Todo cuerpo finito es perfecto.

(2) Si $K$ es perfecto y $L/K$ es una extensión algebraica, entonces $L$ es perfecto.

(3) Si $L$ es perfecto y $L/K$ es una extensión separable, entonces $K$ es perfecto.

(4) Si $L$ es perfecto y $L/K$ es una extensión finita, entonces $K$ es perfecto.

**5.16** Demostrar que el cuerpo de fracciones $K(X)$ del anillo de polinomios $K[X]$ es perfecto si y solo si $\mathrm{car}K = 0$.

**5.17** Sea $K$ un cuerpo de característica $p$ y $\overline{K}$ una clausura algebraica de $K$. Sea

$$\sqrt[p]{K} = \{x \in \overline{K} : x^p \in K\}$$

De forma recursiva definimos $E_n$ para todo $n \geq 0$ poniendo $E_0 = K$ y $E_{n+1} = \sqrt[p]{E_n}$. Demostrar que

$$E_0 \subseteq E_1 \subseteq E_2{}' \subseteq \ldots$$

es una sucesión de subextensiones de $\overline{K}/K$ y que la unión de estos subcuerpos es la menor subextensión de $\overline{K}/K$ que es un cuerpo perfecto. Esta unión se llama *clausura perfecta* de $K$.

**5.18** Dados dos números racionales $a$ y $b$, encontrar un elemento primitivo de $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ sobre $\mathbb{Q}$.

**5.19** Encontrar un elemento primitivo de la extensión $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})/\mathbb{Q}$.

**5.20** Sea $L/K$ una extensión separable de grado $n$ y sea $\alpha \in L$. Demostrar que $\alpha$ es un elemento primitivo de $L/K$ si y solo si $\alpha$ tiene $n$ conjugados.

**5.21** Demostrar que si $K$ un cuerpo de característica $p \neq 0$ y $X$ e $Y$ son dos indeterminadas, entonces la extensión $K(\sqrt[p]{X}, \sqrt[p]{Y})/K(X,Y)$ tiene infinitas subextensiones pero no es simple.

**5.22** Sea $K = \mathbb{F}_2(T)$ el cuerpo de funciones racionales sobre el cuerpo con dos elementos $\mathbb{F}_2$, en la variable $T$ y sean $F = X^2 - T$ y $G = X^2 - (T^2 + T^3)$ y $\alpha$ y $\beta$ raíces de $F$ y $G$ en una extensión de $K$. Demostrar que $K(\alpha, \beta)/K$ es una extensión de grado 4 que no es simple.

**5.23** Sea $f$ un elemento irreducible de $K[X]$ de grado $n$. Demostrar que si la característica de $K$ no divide a $n$ entonces $f$ es separable sobre $K$.

# Capítulo 6

# Extensiones de Galois

## 6.1 La correspondencia de Galois

Recordemos que si $L/K$ es una extensión de cuerpos, entonces el grupo de Galois de $L/K$ es el grupo $\mathrm{Gal}(L/K)$ formado por los automorfismos de $L/K$, es decir los $K$-automorfismos de $L$.

**Ejemplos 6.1** (1) Claramente $\mathrm{Gal}(K/K) = 1$ pero no son éstas las únicas extensiones con grupo de Galois trivial. Por ejemplo, si $a$ es un número racional positivo que no es el cubo de un número racional, entonces $p = X^3 - a$ es irreducible en $\mathbb{Q}[X]$. Las raíces de $p$ son $\alpha = \sqrt[3]{a}, \omega\alpha$ y $\omega^2\alpha$, donde $\omega$ es una raíz tercera primitiva de la unidad. Como $\omega$ no es un número real, la única raíz de $p$ que pertenece a $K(\alpha)$ es $\alpha$ y por tanto $\mathrm{Gal}(K(\alpha)/K) = 1$ (¿por qué?).

(2) Si $L/K$ es una extensión de grado 2 y $\mathrm{car}K \neq 2$, entonces $\mathrm{Gal}(L/K)$ tiene dos elementos. En efecto, si $\alpha \in L \setminus K$, entonces $L = K(\alpha)$ y por tanto $p = \mathrm{Min}_K(\alpha)$ tiene grado 2. Pongamos $p = X^2+aX+b = (X+\frac{a}{2})^2+b-\frac{a^2}{4}$ y sean $\beta = \alpha+\frac{a}{2}$ y $c = \frac{a^2}{4}-b$. Entonces $q = \mathrm{Min}_K(\beta) = X^2-c$ y $L = K(\beta) = K(\sqrt{c})$. Como las raíces de $q$ son $\pm\beta$, si $\sigma \in \mathrm{Gal}(L/K)$ entonces $\sigma(\beta) = \pm\beta$, con lo que efectivamente $\mathrm{Gal}(L/K)$ tiene dos elementos. (¿Seguro que tiene dos?).

En particular, $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ tiene orden 2 y de hecho está formado por la identidad y la conjugación.

(3) Como un automorfismo de $\mathbb{R}$ ha de ser una aplicación creciente (¿por qué?), necesariamente $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = 1$ y por tanto $\mathrm{Gal}(\mathbb{R}/K) = 1$ para todo subcuerpo $K$ de $\mathbb{R}$ (¿por qué?). De hecho el único automorfismo de $\mathbb{R}$ es la identidad (¿por qué?).

(4) Sean $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Entonces $\sigma(\sqrt{2}) = \pm\sqrt{2}$ y $\sigma(\sqrt{3}) = \pm\sqrt{3}$ y por tanto $\mathrm{Gal}(K/\mathbb{Q})$ tiene a lo sumo 4 elementos. De hecho $\mathrm{Gal}(K/\mathbb{Q})$ tiene exactamente cuatro elementos. En efecto, en el Ejemplo (2) hemos visto que $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ tiene 2 elementos. Por otro lado $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ (ver Ejercicio 2.11 del Capítulo 2). Por tanto $K/\mathbb{Q}(\sqrt{2})$ es una extensión separable (¿por qué?) de grado 2, con lo que cada uno de los dos elementos de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ tiene dos extensiones a un homomorfismo de $K$ en una clausura algebraica de $K$ que, como además $K/\mathbb{Q}$ es normal (¿por qué?), estas dos extensiones son elementos de $\mathrm{Gal}(K/\mathbb{Q})$. Por tanto $\mathrm{Gal}(K/\mathbb{Q})$ tiene cuatro elementos: $\sigma_{++}, \sigma_{+-}, \sigma_{-+}, \sigma_{--}$ dados por $\sigma_{ab}(\sqrt{2}) = a\sqrt{2}$ y $\sigma_{ab}(\sqrt{3}) = b\sqrt{3}$.

(5) Sea $\xi$ una raíz $n$-ésima primitiva de la unidad y sea $L = K(\xi)/K$ una extensión ciclotómica. Si $\sigma \in \mathrm{Gal}(L/K)$, entonces $\sigma(\xi) = \xi^i$ para algún entero $i$, coprimo con $n$ y $\sigma$ está completamente determinada por el resto de $i$ módulo $n$. Por tanto tenemos una aplicación $\psi : \mathrm{Gal}(L/K) \to \mathbb{Z}_n^*$ que asocia $\sigma \in \mathrm{Gal}(L/K)$ con la única clase $\mathbb{Z}_n^*$ que contiene a $i$ (con $\sigma(\xi) = \xi^i$). Entonces $\psi$

es un homomorfismo inyectivo de grupos (comprobarlo) y por tanto $\mathrm{Gal}(L/K)$ es isomorfo a un subgrupo de $\mathbb{Z}_n^*$. En particular el grupo de Galois de toda extensión ciclotómica es abeliano.

Si además $K = \mathbb{Q}$, entonces $\mathrm{Min}_{\mathbb{Q}}(\xi) = \Phi_n$, el $n$-ésimo polinomio ciclotómico (Teorema 4.8). Por tanto para cada $i$ coprimo con $n$ existe un elementos $\sigma \in \mathrm{Gal}(L = \mathbb{Q}(\xi)/\mathbb{Q})$ con $\sigma(\xi) = \xi^i$. En otras palabras, $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ es isomorfo a $\mathbb{Z}_n^*$ y un isomorfismo $\tau : \mathbb{Z}_n^* \to \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ viene dado asociando $i \in \mathbb{Z}_n^*$ con el único automorfismo $\tau_i$ de $\mathbb{Q}(\xi)$ tal que $\tau_i(\xi) = \xi^i$.

Obsérvese que si $\phi : L \to L^*$ es un $K$-isomorfismo, entonces la aplicación $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L^*/K)$ dada por $\sigma \mapsto \phi\sigma\phi^{-1}$ es un isomorfismo.

Si $L/K$ es una extensión algebraica y $\overline{L}$ es una clausura algebraica de $L$, entonces podemos ver cada elemento de $\mathrm{Gal}(L/K)$ como un elemento de $S_1^L = \{\sigma : L \to \overline{L} : \sigma|_K = 1_K\}$. Por tanto de la Proposición 5.9 deducimos:

**Proposición 6.2** *Si $L/K$ es una extensión finita entonces $|\mathrm{Gal}(L/K)| \leq [L : K]_s \leq [L : K]$.*

Recordemos que $\mathrm{Sub}(L/K)$ denota el conjunto de las subextensiones de $L/K$. Si $G$ es un grupo, entonces vamos a denotar por $\mathrm{Sub}(G)$ al conjunto de todos los subgrupos de $G$ y si $H$ es un subgrupo de $G$, entonces $\mathrm{Sub}(G/H)$ es el conjunto de los subgrupos de $G$ que contienen a $H$. En realidad esta última notación es ambigua pues si $N$ es un subgrupo normal de $G$, entonces $\mathrm{Sub}(G/N)$ tiene dos significados: El conjunto de los subgrupos de $G$ que contienen a $N$ y el conjunto de los subgrupos de $G/N$. El Teorema de la Correspondencia (Teorema 5.4 de GyA) nos muestra que esta ambigüedad no es muy grave.

Consideramos $\mathrm{Sub}(L/K)$ y $\mathrm{Sub}(G/H)$ como conjuntos ordenados por la inclusión. Una aplicación $f : (A, \leq) \to (B, \leq)$ entre conjuntos ordenados se dice que es un *homomorfismo de conjuntos ordenados* si conserva el orden, es decir si para cada $x, y \in A$ tales que $x \leq y$ se verifica que $f(x) \leq f(y)$; y se dice que es un *anti-homomorfismo de conjuntos ordenados* si $f(x) \geq f(y)$ para todo $x, y \in A$ con $x \leq y$.

Si $L/K$ es una extensión de cuerpos entonces tenemos dos aplicaciones

$$(-)^\circ = \mathrm{Gal}(L/-) : \mathrm{Sub}(L/K) \leftrightarrows \mathrm{Sub}(\mathrm{Gal}(L/K)) : (-)^\circ = L^{(-)}.$$

La aplicación que va para la derecha, asocia $F \in \mathrm{Sub}(L/K)$ con

$$F^\circ = \mathrm{Gal}(L/F) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(x) = x \text{ para todo } x \in F\}$$

y la que va para la izquierda, asocia $H \in \mathrm{Sub}(\mathrm{Gal}(L/K))$ con

$$H^\circ = L^H = \{a \in L : \sigma(x) = x, \text{ para todo } \sigma \in H\}.$$

El par formado por estas aplicaciones se llama *correspondencia de Galois* de la extensión $L/K$. Veamos algunas propiedades de la correspondencia de Galois.

Recordemos que tanto la unidad de un anillo, como el neutro de un grupo como el el subgrupo trivial del grupo lo denotamos siempre como 1. Por el contexto no debería haber confusión. En la siguiente proposición 1 siempre denota el subgrupo trivial de $\mathrm{Gal}(L/K)$.

**Proposición 6.3** *Sea $L/K$ una extensión de cuerpos y sea $G = \mathrm{Gal}(L/K)$. La correspondencia de Galois $(-)^\circ : \mathrm{Sub}(L/K) \rightleftarrows \mathrm{Sub}(G)$ satisface las siguientes propiedades:*

*(1) $L^\circ = 1$, $K^\circ = G$ y $1^\circ = L$.*

*(2) $(-)^\circ = \mathrm{Gal}(L/-)$ y $(-)^\circ = L^{(-)}$ son antihomomorfismos de conjuntos ordenados, es decir si $X \subseteq Y$ entonces $Y^\circ \subseteq X^\circ$.*

*(3) $X \subseteq X^{\circ\circ}$ y $X^\circ = X^{\circ\circ\circ}$, tanto si $X \in \mathrm{Sub}(L/K)$ como si $X \in \mathrm{Sub}(G)$.*

*(4) Las dos aplicaciones que forman la correspondencia de Galois inducen un anti-isomorfismo de conjuntos ordenados entre sus dos imágenes.*

**Demostración.** (1) y (2) y la inclusión $X \subseteq X^{\circ\circ}$ son sencillos ejercicios. Por tanto $X^\circ \subseteq X^{\circ\circ\circ} \subseteq X^\circ$, lo que prueba la igualdad de (3). Finalmente (4) es consecuencia inmediata de (2) y la igualdad de (3). □

Los elementos de las imágenes de las dos aplicaciones de la correspondencia de Galois se dice que son respectivamente *subextensiones cerradas* en $L/K$ y *subgrupos cerrados* en $L/K$. Obsérvese que de la propiedad (3) de la Proposición 6.3 se tiene que

$X$ es cerrado si y solo si $X = X^{\circ\circ}$.

y la propiedad (4) se puede reescribir como

**Corolario 6.4** *Las aplicaciones de la correspondencia de Galois de una extensión de cuerpos $L/K$ se restringen a un anti-isomorfismo de conjuntos ordenados entre las subextensiones cerradas en $L/K$ y los subgrupos cerrados en $L/K$.*

Obsérvese que $L$, 1 y $\mathrm{Gal}(L/K)$ son cerrados en $L/K$, pero $K$ no tiene porque serlo. Por ejemplo, si $L \neq K$ y $\mathrm{Gal}(L/K) = 1$ (ver Ejemplos 6.1) entonces $K^{\circ\circ} = 1^\circ = L \neq K$.

**Proposición 6.5** *Sea $L/K$ una extensión de cuerpos.*

*(1) Si $E_1 \subseteq E_2$ son subextensiones de $L/K$ con $E_2/E_1$ finita entonces $[E_1^\circ : E_2^\circ] \leq [E_2 : E_1]$.*

*(2) Si $H_1 \leq H_2$ son subgrupos de $\mathrm{Gal}(L/K)$ con $[H_2 : H_1] < \infty$, entonces $[H_1^\circ : H_2^\circ] \leq [H_2 : H_1]$.*

**Demostración.** (1) Razonamos por inducción sobre $n = [E_2 : E_1]$, con el caso $n = 1$ obvio. Supongamos pues que $n > 1$ y la hipótesis de inducción. Sean $\alpha \in E_2 \setminus E_1$, $p = \mathrm{Min}_{E_1}(\alpha)$ y $s = \mathrm{gr}(p) > 1$. Entonces $[E_2 : E_1(\alpha)] < n$. Si $s < n$, entonces por la hipótesis de inducción tenemos

$$[E_1^\circ : E_2^\circ] = [E_1^\circ : E_1(\alpha)^\circ][E_1(\alpha)^\circ : E_2^\circ] \leq [E_1(\alpha) : E_1][E_2 : E_1(\alpha)] = [E_2 : E_1].$$

En caso contrario, $E_2 = E_1(\alpha)$. Sean $R$ el conjunto de raíces de $p$ y $\phi : E_1^\circ/E_2^\circ \to R$ la aplicación dada por $\phi(\sigma E_2^\circ) = \sigma(\alpha)$. Es fácil ver que esta aplicación está bien definida y es inyectiva. Por tanto $[E_1^\circ : E_2^\circ] \leq |R| \leq \mathrm{gr}(p) = [E_2 : E_1]$.

(2) Pongamos $H_2/H_1 = \{\tau_1 H_1, \ldots, \tau_n H_n\}$ con $\tau_1 = 1$ y razonemos por reducción al absurdo, es decir, supondremos que $[H_1^\circ : H_2^\circ] > n$. Entonces existen $\alpha_1, \ldots, \alpha_n, \alpha_{n+1} \in H_1^\circ$, linealmente independientes sobre $H_2^\circ$. Consideremos la matriz

$$A = \begin{pmatrix} \tau_1(\alpha_1) & \tau_1(\alpha_2) & \ldots & \tau_1(\alpha_{n+1}) \\ \tau_2(\alpha_1) & \tau_2(\alpha_2) & \ldots & \tau_2(\alpha_{n+1}) \\ \ldots & \ldots & \ldots & \ldots \\ \tau_n(\alpha_1) & \tau_n(\alpha_2) & \ldots & \tau_n(\alpha_{n+1}) \end{pmatrix}$$

y sea $r$ el rango de $A$. Reordenamos los $\alpha_1$ para que las primeras $r$ columnas sean linealmente independientes. Entonces la columna $r+1$ es combinación lineal de las $r$ primeras (obsérvese que $r \leq n < n+1 \leq$ número de columnas de $A$) y por tanto existe $a = (a_1, \ldots, a_r, 1, 0, \ldots, 0) \in L^{n+1}$ tal que $Aa = 0$. Como $\tau_1 = 1$ tenemos

$$\alpha_1 a_1 + \cdots + \alpha_r a_r + \alpha_{r+1} = 0$$

y, como los $\alpha_i$ son linealmente independientes sobre $H_2^\circ$ existe $1 \leq i \leq r$ tal que $a_i \notin H_2^\circ$. Reordenando $a_1, \ldots, a_r$ podemos suponer que $a_1 \notin H_2^\circ$, es decir $\sigma(a_1) \neq a_1$ para algún $\sigma \in H_2$.

La aplicación $H_2/H_1 \to H_2/H_1$ dada por $\tau H_1 \mapsto \sigma\tau H_1$ es inyectiva pues si $\sigma\sigma_1 H_1 = \sigma\sigma_2 H_1$, entonces $\sigma_2^{-1}\sigma_1 = (\sigma\sigma_2)^{-1}(\sigma\sigma_1) \in H_1$, luego $\sigma_1 H_1 = \sigma_2 H_1$. Por tanto existe una permutación $\rho \in S_n$ tal que $\sigma^{-1}\tau_i = \tau_{\rho(i)}$ para todo $i = 1, \ldots, n$, con lo que la matriz

$$B = \begin{pmatrix} \sigma^{-1}\tau_1(\alpha_1) & \sigma^{-1}\tau_1(\alpha_2) & \ldots & \sigma^{-1}\tau_1(\alpha_{n+1}) \\ \sigma^{-1}\tau_2(\alpha_1) & \sigma^{-1}\tau_2(\alpha_2) & \ldots & \sigma^{-1}\tau_2(\alpha_{n+1}) \\ \ldots & \ldots & \ldots & \ldots \\ \sigma^{-1}\tau_n(\alpha_1) & \sigma^{-1}\tau_n(\alpha_2) & \ldots & \sigma^{-1}\tau_n(\alpha_{n+1}) \end{pmatrix}$$

se obtiene permutando las filas de la matriz $A$. Eso implica que $Ba = 0$ y por tanto $A\sigma(a) = 0$, donde

$$\sigma(a) = \begin{pmatrix} \sigma(a_1) \\ \vdots \\ \sigma(a_r) \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Luego $A(a - \sigma(a)) = 0$ y

$$a - \sigma(a) = \begin{pmatrix} a_1 - \sigma(a_1) \\ \vdots \\ a_r - \sigma(a_r) \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

con $a_1 - \sigma(a_1) \neq 0$. Eso implica que las $r$ primeras columnas de $A$ son linealmente dependientes en contra de la elección, lo que proporciona la contradicción deseada. □

**Corolario 6.6** *Sea $L/K$ una extensión de cuerpos.*

*(1) Si $K \subseteq E_1 \subseteq E_2 \subseteq L$ es una torre de cuerpos, con $[E_2 : E_1] < \infty$ y $E_1$ cerrado en $L/K$ entonces $E_2$ es cerrado en $L/K$ y $[E_1^\circ : E_2^\circ] = [E_2 : E_1]$.*

*(2) Si $H_1 \leq H_2 \leq \mathrm{Gal}(L/K)$ son subgrupos de $\mathrm{Gal}(L/K)$ con $[H_2 : H_1] < \infty$ y $H_1$ cerrado en $L/K$ entonces $H_2$ es cerrado en $L/K$ y $[H_1^\circ : H_2^\circ] = [H_2 : H_1]$.*

**Demostración.** (1) Aplicando el primer apartado de la Proposición 6.5 a $E_1 \leq E_2$ obtenemos que $[E_1^\circ : E_2^\circ] \leq [E_2 : E_1]$ y aplicando el segundo apartado a $E_2^\circ \subseteq E_1^\circ$ obtenemos $[E_2^{\circ\circ} : E_1^{\circ\circ}] \leq [E_1^\circ : E_2^\circ]$. Como $E_1$ es cerrado tenemos que $[E_2^{\circ\circ} : E_1] = [E_2^{\circ\circ} : E_1^{\circ\circ}] \leq [E_2 : E_1]$ y como $E_2 \subseteq E_2^{\circ\circ}$, concluimos que $E_2 = E_2^{\circ\circ}$, es decir $E_2^{\circ\circ}$ es cerrado.

(2) Es completamente análoga. □

## 6.2 Extensiones de Galois

**Definición 6.7** *Una* extensión de Galois *es una extensión de cuerpos que es normal y separable.*

La siguiente proposición es consecuencia inmediata de las Proposiciones 3.15 y 5.17.

**Proposición 6.8** *La clase de extensiones de Galois es cerrada para levantamientos.*

El siguiente Teorema caracteriza las extensiones de Galois.

**Teorema 6.9** *Las siguientes condiciones son equivalentes para una extensión de cuerpos $L/K$, con $G = \mathrm{Gal}(L/K)$:*

*(1) $L/K$ es una extensión de Galois.*

*(2) $L/E$ es una extensión de Galois para todo $E \in \mathrm{Sub}(L/K)$.*

*(3) $L/K$ es algebraica y toda subextensión de $L/K$ es cerrada.*

*(4) $L/K$ es algebraica y $K$ es un subcuerpo cerrado de $L/K$.*

*(5) $L/K$ es algebraica y para todo $\alpha \in L \setminus K$ existe $\sigma \in \mathrm{Gal}(L/K)$ tal que $\sigma(\alpha) \neq \alpha$.*

*(6) $L/K$ es algebraica y $G^\circ = K$ o sea, si $\alpha \in L$ satisface $\sigma(\alpha) = \alpha$ para todo $\sigma \in G$ entonces, $\alpha \in K$.*

**Demostración.** (1) implica (2) es consecuencia de la Proposición 6.8.

(2) implica (3). Supongamos que $L/K$ satisface (2) y sea $E \in \mathrm{Sub}(L/K)$. De la Proposición 6.3 se tiene que $E \subseteq E^{\circ\circ}$ y tenemos que demostrar que se verifica la igualdad, o lo que es lo mismo tenemos que demostrar que si $\alpha \in L \setminus E$ entonces existe $\sigma \in \mathrm{Gal}(L/E)$ tal que $\sigma(\alpha) \neq \alpha$. Si $\alpha \in L \setminus E$, entonces $p = \mathrm{Min}_E(\alpha)$ tiene una raíz en $L$ y, como $L/E$ es normal, $p$ es completamente factorizable en $L$. Como además $L/E$ es separable y $\alpha \notin E$, existe $\alpha \neq \beta \in L$ tal que $\beta$ también es raíz de $p$. De la Proposición 2.10 se deduce que existe un $E$-isomorfismo $\sigma : E(\alpha) \to E(\beta)$. Sea $\overline{L}$ una clausura algebraica de $L$. Como $L/E$ es algebraica (y por tanto también lo es $L/E(\alpha)$) $\sigma$ se extiende a un homomorfismo $L \to \overline{L}$, que también denotaremos por $\sigma$, y como $L/E$ es normal, $\sigma(L) \subseteq L$, con lo que $\sigma \in \mathrm{Gal}(L/E)$. Deducimos que $\alpha \neq \beta = \sigma(\alpha)$.

(3) implica (4), (4) implica (5) y que (5) y (6) son equivalentes está claro.

(5) implica (1). Supongamos que $L/K$ verifica (5). Sea $\alpha \in L$ y sean $p = \mathrm{Min}_K(\alpha)$ y $n = \mathrm{gr}(p)$. Tenemos que demostrar que $p$ factoriza completamente en $L$ (para demostrar que $L/K$ es normal) y que $p$ no tiene raíces múltiples (para mostrar que $L/K$ es separable) o lo que es lo mismo que $p$ tiene $n$ raíces (distintas) en $L$. Sea $R = \{\alpha = \alpha_1, \ldots, \alpha_r\}$ el conjunto de las (distintas) raíces de $p$ en $L$ y sea $q = (X - \alpha_1) \cdots (X - \alpha_r)$. Si $\sigma \in \mathrm{Gal}(L/K)$, entonces $\sigma(\alpha_i)$ es una raíz de $p$ en $L$, lo que implica que $\sigma$ induce una permutación de $R$ y por tanto $\sigma(q) = q$, es decir $\sigma(a) = a$ para cada uno de los coeficientes $a$ de $q$. Como estamos suponiendo que $L/K$ satisface la propiedad (5), concluimos que cada uno de estos coeficientes pertenece a $K$, es decir $q \in K[X]$. Como $r = \mathrm{gr}(q) \leq n = \mathrm{gr}(p)$ y $p$ tiene grado mínimo entre los polinomios de $K[X]$ que tienen a $\alpha$ como raíz deducimos que $p = q$, y por tanto $r = n$. □

La siguiente proposición muestra criterios para decidir si una extensión es de Galois para el caso de extensiones finitas.

**Proposición 6.10** *Las siguientes condiciones son equivalentes para una extensión finita $L/K$.*

*(1) $L/K$ es una extensión de Galois.*

*(2) $[L : K] = |\mathrm{Gal}(L/K)|$*

*(3)* $[L : E] = |\operatorname{Gal}(L/E)|$ *para todo* $E \in \operatorname{Sub}(L/K)$.

**Demostración.** (1) implica (3) Supongamos que $L/K$ es de Galois y sea $E \in \operatorname{Sub}(L/K)$. Entonces $L/E$ es de Galois (Teorema 6.10). De que $L/E$ sea normal se deduce que si $\overline{L}$ es una clausura algebraica de $E$, entonces $\operatorname{Gal}(L/E)$ coincide las restricciones a $L$ de los elementos del conjunto $S_1^L$ de extensiones de la inclusión $E \to \overline{L}$ a un homomorfismo $L \to \overline{L}$, con lo que $|\operatorname{Gal}(L/E)| = |S_1^L| = [L : E]_s$ y este número coincide con $[L : E]$ por ser $L/E$ separable.

(3) implica (2) es obvio.

(2) implica (1) Supongamos que $|\operatorname{Gal}(L/K)| = [L : K]$. De la Proposición 6.3 tenemos $[L : K] = |\operatorname{Gal}(L/K)| = |K^\circ| = |K^{\circ\circ\circ}| = |\operatorname{Gal}(L/K^{\circ\circ})| \leq [L : K^{\circ\circ}] \leq [L : K]$ y como $K \subseteq K^{\circ\circ}$ deducimos que $K = K^{\circ\circ}$, es decir $K$ es cerrado en $L/K$ y por tanto $L/K$ es de Galois (Teorema 6.9). □

**Teorema 6.11 (Teorema Fundamental de la Teoría de Galois)** *Sea* $L/K$ *una extensión de Galois finita y sea* $G = \operatorname{Gal}(L/K)$. *Entonces se verifican las siguientes propiedades:*

*(1) La correspondencia de Galois es un anti-isomorfismo de conjuntos ordenados entre* $\operatorname{Sub}(L/K)$ *y* $\operatorname{Sub}(\operatorname{Gal}(L/K))$.

*(2) Si* $E \in \operatorname{Sub}(L/K)$ *entonces* $[L : E] = |E^\circ|$ *y* $[E : K] = [G : E^\circ]$.

*(3) Si* $H \in \operatorname{Sub}(G)$ *entonces* $|H| = [L : H^\circ]$ *y* $[G : H] = [H^\circ : K]$.

*(4) Si* $E \in \operatorname{Sub}(L/K)$ *entonces las siguientes condiciones son equivalentes:*

*(a)* $E/K$ *es de Galois.*

*(b)* $E/K$ *es normal.*

*(c)* $\sigma(E) \subseteq E$ *para todo* $\sigma \in \operatorname{Gal}(L/K)$.

*(d)* $\operatorname{Gal}(L/E)$ *es normal en* $\operatorname{Gal}(L/K)$.

*Además, si estas condiciones se satisfacen, entonces*

$$\operatorname{Gal}(E/K) \simeq \frac{\operatorname{Gal}(L/K)}{\operatorname{Gal}(L/E)}.$$

**Demostración.** (1) A la vista de la Proposición 6.3 y el Teorema 6.9 para demostrar (1), sólo falta demostrar que todo subgrupo $H$ de $G$ es cerrado, pero eso es consecuencia inmediata del Corolario 6.6.

(2) y (3) Por el Teorema 6.9, $L/E$ es de Galois, luego $[L : E] = |\operatorname{Gal}(L/E)| = |E^\circ|$ por el Teorema 6.10, de donde se deduce que

$$[E : K] = \frac{[L : K]}{[L : E]} = \frac{|\operatorname{Gal}(L/K)|}{|\operatorname{Gal}(L/E)|} = [G : E^\circ].$$

Aplicando esto a $E = H^\circ$ tenemos que $|H| = |H^{\circ\circ}| = [L : H^\circ]$ y $[G : H] = [G : H^{\circ\circ}] = [H^\circ : K]$.

(4) La equivalencia entre (a) y (b) es consecuencia inmediata de que la clase de extensiones separables es multiplicativa (Proposición 5.13).

(b) implica (c) Supongamos que $E/K$ es normal y sean $\alpha \in E$ y $\sigma \in \operatorname{Gal}(L/K)$. Entonces $p = \operatorname{Min}_K(\alpha)$ es completamente factorizable en $E$, o sea $p = (X - \alpha_1) \cdots (X - \alpha_n)$ con $\alpha_1, \ldots, \alpha_n \in E$. Entonces $\sigma(\alpha)$ es raíz de $p$ y por tanto $\sigma(\alpha) = \alpha_i \in E$, para algún $i$. Esto prueba que $\sigma(E) \subseteq E$.

(c) implica (d) Supongamos que se verifica (c) y sean $\sigma \in \operatorname{Gal}(L/K)$ y $\tau \in \operatorname{Gal}(L/E)$. Entonces $\sigma(E) \subseteq E$ y por tanto $\tau\sigma(\alpha) = \sigma(\alpha)$, es decir $\sigma^{-1}\tau\sigma(\alpha) = \alpha$, para todo $\alpha \in E$. Esto prueba que

$\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/E)$ para todo $\sigma \in \mathrm{Gal}(L/E)$ y todo $\tau \in \mathrm{Gal}(L/E)$, es decir $\mathrm{Gal}(L/E)$ es normal en $\mathrm{Gal}(L/K)$.

(d) implica (b) Supongamos que $\mathrm{Gal}(L/E)$ es normal en $\mathrm{Gal}(L/K)$. Sea $\rho : E \to \overline{L}$ un $K$-homomorfismo. Como $L/E$ es algebraica, $\rho$ extiende a un $K$-homomorfismo $\sigma : L \to \overline{L}$. Como $L/K$ es normal, $\sigma(L) = L$ (Teorema 3.11), y por tanto podemos considerar $\sigma$ como un elemento de $\mathrm{Gal}(L/K)$. Por hipótesis, $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/E)$ para todo $\tau \in \mathrm{Gal}(L/E)$, con lo que $\tau\sigma(\alpha) = \sigma(\alpha)$, para todo $\tau \in \mathrm{Gal}(L/E)$ y todo $\alpha \in E$. Esto muestra que $\rho(\alpha) = \sigma(\alpha) \in \mathrm{Gal}(L/E)^\circ = E^{\circ\circ} = E$. Como $L/E$ es algebraica, $\overline{L}$ es una clausura algebraica de $E$ con lo que hemos comprobado que $E/K$ satisface las condiciones del Teorema 3.11, es decir $E/K$ es normal.

Supongamos ahora que las condiciones (a)-(d) se verifican. Entonces la aplicación de restricción

$$\begin{array}{rcl} f : \mathrm{Gal}(L/K) & \to & \mathrm{Gal}(E/K) \\ \sigma & \mapsto & \sigma_E \end{array}$$

es un homomorfismo de grupos cuyo núcleo es $\mathrm{Gal}(L/E)$. Aplicando el Primer Teorema de Isomorfía y que todas las extensiones $L/K$, $E/K$ y $L/E$ son de Galois deducimos que

$$|\mathrm{Im}\ f| = \frac{|\,\mathrm{Gal}(L/K)|}{|\,\mathrm{Gal}\, L/E|} = \frac{[L:K]}{[L:E]} = [E:K] = |\,\mathrm{Gal}(E,K)|,$$

lo que implica que $f$ es suprayectiva y $\mathrm{Gal}(E/K) \simeq \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(E/K)}$. □

Sea $K \subseteq L \subseteq F$ una torre de extensiones de cuerpos y supongamos que $L/K$ es normal. Entonces para todo $\sigma \in \mathrm{Gal}(F/K)$ la restricción $\sigma|_L$ de $\sigma$ a $L$ pertenece a $\mathrm{Gal}(L/K)$ y la aplicación

$$\begin{array}{rcl} \mathrm{Res}_L^F : \mathrm{Gal}(F/K) & \to & \mathrm{Gal}(L/K) \\ \sigma & \mapsto & \sigma_L \end{array}$$

es un homomorfismo de grupos cuyo núcleo es $\mathrm{Gal}(F/L)$. Además, si $E$ es otra subextensión de $F/K$, entonces $\mathrm{Res}_L^F$ se restringe a un homomorfismo

$$\mathrm{Res}_E^{LE} : \mathrm{Gal}(LE/E) \to \mathrm{Gal}(L/L \cap E).$$

**Teorema 6.12 (Teorema de las irracionalidades accesorias de Lagrange)** *Sean $L/K$ y $E/K$ dos extensiones admisibles y supongamos que la primera es finita y de Galois. Entonces $LE/E$ y $L/L \cap E$ son extensiones de Galois finitas y el homomorfismo de restricción*

$$\mathrm{Res}_L^{LE} : \mathrm{Gal}(LE/E) \to \mathrm{Gal}(L/L \cap E)$$

*es un isomorfismo de grupos.*

**Demostración.** Como $L/K$ es de Galois, del Teorema 6.9 se deduce que $L/L\cap E$ también es de Galois y de la Proposición 6.8 que lo es $LE/E$. Que la primera es finita es obvio y que lo sea la segunda es consecuencia de la Proposición 2.18. Que $\mathrm{Res}_L^{LE}$ sea inyectiva es obvio ya que un elemento del núcleo es un automorfismo $\sigma$ de $LE$ que verifica $\sigma(x) = x$ para todo $x \in L$ y todo $x \in E$. Finalmente, si $H = \mathrm{Im}\ \mathrm{Res}_L^{LE}$, entonces $L \cap E = \mathrm{Gal}(L/L \cap E)^\circ \subseteq H^\circ$. Por otro lado, si $\alpha \in H^\circ$, entonces para todo $\sigma \in \mathrm{Gal}(LE/E)$ se verifica $\sigma(\alpha) = \sigma_L(\alpha) = \alpha$, con lo que $\alpha \in \mathrm{Gal}(LE/E)^\circ = E$, pues $LE/E$ es de Galois. Eso prueba que $H^\circ \subseteq L \cap E$. En resumen $L \cap E = H^\circ \subseteq L$ y del Teorema Fundamental de la Teoría de Galois se deduce que $\mathrm{Gal}(L/L \cap E) = (L \cap E)^\circ = H^{\circ\circ} = H$, es decir $\mathrm{Res}_L^{LE}$ es suprayectiva. □

## Problemas

**6.1** Demostrar que toda extensión de grado 2 de cuerpos de característica distinta de 2 es de Galois. Encontrar una extensión de grado 2 de cuerpos de característica 2 y una de grado 3 de cuerpos de característica 0 que no sean de Galois.

**6.2** Demostrar que toda extensión ciclotómica es de Galois con grupo de Galois abeliano.

**6.3** Sean $L$ un cuerpo, $G$ un subgrupo finito del grupo de automorfismos de $L$ y $K = L^G = \{x \in L : \sigma(x) = x, \text{ para todo } \sigma \in G\}$. Demostrar que $L/K$ es una extensión de Galois y $G = \mathrm{Gal}(L/K)$.

**6.4** Sean $X_1, \ldots, X_n$ variables independientes sobre $K$ y $S_1, \ldots, S_n$ los polinomios simétricos elementales en las variables $X_1, \ldots, X_n$. Sea $K(X_1, \ldots, X_n)$ el cuerpo de fracciones de $K[X_1, \ldots, X_n]$. Para cada permutación $\sigma \in S_n$ sea $\overline{\sigma}$ el automorfismo de $K[X_1, \ldots, X_n]$ definido en la Sección 1.2. Demostrar

(1) Para cada $\sigma \in S_n$, $\overline{\sigma}$ se extiende de forma única a un automorfismo de $K(X_1, \ldots, X_n)$, que también denotaremos por $\overline{\sigma}$.

(2) $K(X_1, \ldots, X_n)/K(S_1, \ldots, S_n)$ es una extensión de Galois.

(3) El homomorfismo $S_n \to \mathrm{Gal}(K(X_1, \ldots, X_n)/K(S_1, \ldots, S_n))$ que asocia cada permutación $\sigma \in S_n$, con $\overline{\sigma}$ es un isomorfismo.

**6.5** Sea $L/K$ una extensión finita de Galois y sean $E$ y $F$ subextensiones de $L/K$. Demostrar que

$$\mathrm{Gal}(L/EF) = \mathrm{Gal}(L/E) \cap \mathrm{Gal}(L/F) \quad \text{y} \quad \mathrm{Gal}(L/E \cap F) = \langle \mathrm{Gal}(L/E) \cup \mathrm{Gal}(L/F) \rangle.$$

**6.6** Sea $\alpha = \sqrt{5 + 2\sqrt{5}}$.

(1) Calcular $\mathrm{Min}_{\mathbb{Q}}(\alpha)$.

(2) Demostrar que $\sqrt{5 - 2\sqrt{5}} \in \mathbb{Q}(\alpha)$ y deducir que $\mathbb{Q}(\alpha)/\mathbb{Q}$ es una extensión de Galois.

(3) Calcular $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$.

(4) Calcular las subextensiones de $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ y decir cuales de ellas son de Galois sobre $\mathbb{Q}$.

**6.7** Sea $n$ un número entero libre de cuadrados, es decir, $n$ no es divisible por el cuadrado de un entero.

(1) Calcular el cuerpo de descomposición $L$ de $X^4 - n$ sobre $\mathbb{Q}$.

(2) Demostrar que $\mathrm{Gal}(L/\mathbb{Q})$ es isomorfo al grupo diédrico de orden 8.

(3) Calcular todas las subextensiones de $L/\mathbb{Q}$ y decir cuales de ellas son de Galois sobre $\mathbb{Q}$.

(4) Calcular $\mathrm{Gal}(L/K)$ y $\mathrm{Gal}(K/\mathbb{Q})$ para cada subextensión $K$ de $L/\mathbb{Q}$.

**6.8** Calcular el grupo de Galois del cuerpo de descomposición de $X^4 - 2$ sobre $\mathbb{F}_3$ y $\mathbb{F}_7$.

**6.9** Sean $\zeta = \zeta_3 \in \mathbb{C}$ una raíz tercera primitiva de la unidad, $p$ un número primo y $L = \mathbb{Q}(\zeta, \sqrt{p})/\mathbb{Q}$.

(1) Demostrar que $L/\mathbb{Q}$ es una extensión de Galois.

(2) Calcular $\mathrm{Gal}(L/\mathbb{Q})$ y cada uno de sus subgrupos.

(3) Calcular las subextensiones de $L/\mathbb{Q}$.

**6.10** Calcular todas las subextensiones de $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, donde $\zeta_n$ es una raíz $n$-ésima primitiva de la unidad, para $n = 3, 5, 7, 8, 11$ y 16.

**6.11** Sea $L/K$ una extensión de cuerpos y $G$ un subgrupo finito de $\mathrm{Gal}(L/K)$. Demostrar que $T_G(a) = \sum_{\sigma\in G}\sigma(a)$ y $N_G(a) = \prod_{\sigma\in G}\sigma(a)$ pertenecen a $G^\circ$.

Interpretar los Periodos de Gauss del Problema 4.16 del Capítulo 4 en términos de estos elementos.

**6.12** Utilizando el Problema 4.16 del Capítulo 4 describir todos las subextensiones de $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, donde $p$ es un número primo y $\zeta_p$ es una raíz $p$-ésima primitiva de la unidad. Demostrar que cada uno estas subextensiones está generada por uno de los periodos de Gauss. Utilizar esto para mostrar que las subextensiones de $\mathbb{Q}(\zeta_{17})/\mathbb{Q}$ forman una cadena de la forma

$$\mathbb{Q} = L_0 \subset L_1 = L_0(\sqrt{a_0}) \subset L_2 = L_1(\sqrt{a_1}) \subset L_3 = L_2(\sqrt{a_2}) \subset L_4 = L_3(\sqrt{a_3}) = \mathbb{Q}(\zeta_{17})$$

con $a_i \in L_i$.

**6.13** Sea $K$ un cuerpo finito de característica $p$ y cardinal $q = p^n$. Demostrar

(1) La aplicación $\sigma : K \to K$ dada por $\sigma(x) = x^p$ es un automorfismo de $K$. Este automorfismo se llama *automorfismo de Frobenius* de $K$.

(2) $\mathrm{Gal}(K/\mathbb{F}_p)$ es cíclico de orden $n$, generado por el automorfismo de Frobenius.

(3) Si $L/K$ es una extensión finita, entonces $\mathrm{Gal}(L/K)$ es cíclico generado por el automorfismo de $L$ dado por $\sigma(x) = x^q$.

(4) Si $\alpha$ es algebraico sobre $K$ y $[K(\alpha) : K] = m$, entonces

$$\mathrm{Min}_K(\alpha) = (X - \alpha)(X - \alpha^q)\cdots(X - \alpha^{q^{m-1}}).$$

(5) Describir las subextensiones de $L/K$ donde $L$ es una extensión de grado $m$ de $K$.

(6) Demostrar que la aplicación $x \mapsto x^p$ es un endomorfismo no inyectivo de $\mathbb{F}_p(X)$.

**6.14** Sea $K$ un cuerpo y $X$ una indeterminada. Denotamos por $\mathrm{GL}_2(K)$ el grupo de las matrices invertibles

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

con entradas en $K$.

(1) Mostrar que para cada matriz invertible $A \in \mathrm{GL}_2(K)$ existe un único $\sigma_A \in \mathrm{Gal}(K(X)/K)$ tal que

$$\sigma_A(X) = \frac{aX + b}{cX + d}$$

y que la aplicación $\sigma : \mathrm{GL}_2(K) \to \mathrm{Gal}(K(X)/K)$, dada por $\sigma(A) = \sigma_A$ es un homomorfismo de grupos.

(2) Demostrar que $\sigma$ es suprayectiva y que su núcleo es el conjunto de las matrices escalares $\alpha I$ con $\alpha \neq 0$.

(3) Sea $\alpha = f/g \in K(X) \setminus K$ con $f, g \in K[X]$ y $(f, g) = 1$. Demostrar que $X$ es algebraico sobre $K(\alpha)$ y que $[K(X) : K(\alpha)] = max\{\partial(f), \partial(g)\}$. (Indicación. Observa que $\alpha$ es transcendente sobre $K$).

(4) Demostrar que $\mathbb{Q}(X^2)$ es un cuerpo intermedio cerrado de la extensión $\mathbb{Q} \subset \mathbb{Q}(X)$ y que $\mathbb{Q}(X^3)$ no lo es.

(5) Demostrar que $K(X)/K$ es de Galois si y solo si $K$ es infinito.

(6) Demostrar que si $K$ es infinito, entonces los únicos subgrupos cerrados de $\mathrm{Gal}(K(X)/K)$ son él mismo y sus subgrupos finitos.

(7) Calcular $H^\circ$ para cada uno de los siguientes subgrupos $H$ de $\mathrm{Gal}(K(X)/K)$:

- $H = \langle \sigma_A \rangle$ donde $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
- $H = \langle \sigma_A \rangle$ donde $A = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$.
- $H = \langle \sigma_A, \sigma_B \rangle$ donde $A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ y $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
  (Observa que $(X^2 - X + 1)^3/(X^2 - X)^2 \in H^\circ$.)
- $H = \langle \sigma_A, \sigma_B \rangle$ donde $A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ y $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

**6.15** Sea $L$ una subextensión de una extensión ciclotómica $K(\zeta)/K$. Demostrar

(1) $L/K$ es una extensión de Galois.

(2) $\mathrm{Gal}(L/K)$ es abeliano.

(3) Si $\zeta^p = 1$, con $p$ primo, entonces $\mathrm{Gal}(L/K)$ es cíclico.

**6.16** Sea $p \in K[X]$ de grado $n$ y $L$ el cuerpo de descomposición de $p$ sobre $K$. Demostrar que $\mathrm{Gal}(L/K)$ es isomorfo a un subgrupo $G$ de $S_n$, el grupo simétrico en $n$ símbolos. Demostrar que $G$ es transitivo si y solo si $p$ es irreducible y separable. (Un subgrupo $G$ de $S_n$ se dice que es *transitivo* si para todo $1 \leq i, j \leq n$ existe $\sigma \in G$ tal que $\sigma(i) = j$.)

**6.17** Sea $L/K$ es una extensión de Galois con $\mathrm{Gal}(L/K)$ es abeliano. Demostrar que $F/K$ es de Galois para todo cuerpo intermedio $F$ de la extensión $L/K$ y $\mathrm{Gal}(F/K)$ también es abeliano. Demostrar también que si $E/K$ es una extensión admisible con $L/K$ entonces $LE/E$ es de Galois con grupo de Galois abeliano.

**6.18** Dos subgrupos $H_1$ y $H_2$ de un grupo $G$ se dice que son conjugados en $G$ si existe $g \in G$ tal que $H_2 = g^{-1}H_1g$. Dos cuerpos intermedios $F_1$ y $F_2$ de una extensión $L/K$ se dice que son conjugados en la extensión $L/K$ si existe $g \in \mathrm{Gal}(L/K)$ tal que $g(F_1) = F_2$. Sea $L/F$ una extensión de Galois y sean $F_1$ y $F_2$ dos cuerpos intermedios de $L/K$. Demostrar que $F_1$ y $F_2$ son conjugados en $L/K$ si y solo si $F_1^\circ$ y $F_2^\circ$ son conjugados en $G$.

**6.19** Sea $L/K$ una extensión de Galois finita y sean $F_1$ y $F_2$ cuerpos intermedios tales que $F_1F_2 = L$. Demostrar que si $F_1/K$ es de Galois entonces $L/F_2$ es de Galois y $\mathrm{Gal}(L/F_2)$ es isomorfo a un subgrupo de $\mathrm{Gal}(F_1/K)$. Deduce de aquí que si $F_1 \cap F_2 = F$ entonces $\mathrm{Gal}(L/F_2)$ es isomorfo a $\mathrm{Gal}(F_1/K)$.

**6.20** Sean $L_1/K$ y $L_2/K$ extensiones admisibles de Galois finitas y consideremos la aplicación

$$\begin{array}{rcl} \Phi : \mathrm{Gal}(L_1L_2/K) & \to & \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \\ \sigma & \mapsto & (\sigma_{L_1}, \sigma_{L_2}) \end{array}$$

Demostrar

(1) $\Phi$ es un homomorfismo inyectivo de grupos.

(2) Si $L_1 \cap L_2 = K$, entonces $\Phi$ es un isomorfismo de grupos.

(3) Calcular el grupo de Galois de $L = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}$, donde $p_1, \ldots, p_n$ son primos diferentes.

(4) Calcular todas las subextensiones de $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

(5) Calcular el grupo de Galois de $L = \mathbb{Q}(i, \sqrt[4]{2}, \sqrt[4]{3})/Q(i) = K$.

(6) Calcular las subextensiones de $L/K$.

(7) Demostrar que $\mathrm{Gal}(L/\mathbb{Q})$ es isomorfo a un subgrupo de $D_4 \times D_4$, donde $D_4$ es el grupo diédrico de orden 8.

**6.21** Dar extensiones de Galois $L/\mathbb{Q}$ para las que $\mathrm{Gal}(L/\mathbb{Q})$ sea isomorfo a cada uno de los siguientes grupos: $C_6, C_{10}, C_{15}, C_2 \times C_{30}$.

**6.22** Sean $a$ un entero libre de cuadrados diferente de 1 y $-1$, $m = p_1 \cdots p_k$ con $p_1, \ldots, p_k$ primos distintos, $\xi_m$ una raíz $m$-ésima primitiva de la unidad compleja y $K$ el cuerpo de descomposición de $(X^{p_1} - a) \cdots (X^{p_k} - a)$ sobre $\mathbb{Q}$. Demostrar

$$[K : \mathbb{Q}] = \begin{cases} 2m\phi(m), & \text{si } 2|m \text{ y } \sqrt{a} \notin \mathbb{Q}(\xi_m); \\ m\phi(m), & \text{en caso contrario;} \end{cases}$$

donde $\phi$ es la función de Euler.

# Capítulo 7

# Construcciones con regla y compás

## 7.1 Construcciones con regla y compás

**Definición 7.1** *Sea $\mathcal{A}$ un conjunto de puntos del plano euclídeo $\mathbb{R}^2$ y $P \in \mathbb{R}^2$. Decimos que $P$ es* constructible con regla y compás a partir de $\mathcal{A}$ en un paso *si se verifica una de las dos siguientes situaciones.*

*(1) $P$ está en la intersección de dos líneas diferentes, cada una de las cuales pasa por dos puntos distintos de $\mathcal{A}$. (En particular, las líneas no son paralelas).*

*(2) $P$ está en la intersección de una línea $L$ y una circunferencia $C$ tales que $L$ pasa por dos puntos diferentes de $\mathcal{A}$, el centro de $C$ está en $\mathcal{A}$ y el radio de la $C$ coincide con la distancia entre dos puntos de $\mathcal{A}$.*

*(3) $P$ es uno de los puntos de intersección de dos circunferencias cuyos centros están en $\mathcal{A}$ y cuyos radios son las distancias entre puntos de $\mathcal{A}$.*

*Decimos que $P$ es* constructible con regla y compás *a partir de $\mathcal{A}$ si existen*

$$P_1, P_2, \ldots, P_n = P$$

*de forma que para todo $i$, $P_i$ es constructible con regla y compás en un paso a partir de $\mathcal{A} \cup \{P_1, \ldots, P_{i-1}\}$.*

Para acortar nuestro discurso la expresión "constructible con regla y compás" la reduciremos a constructible, y todas las conjugaciones del verbo construir se entenderán como conjugaciones de construir con regla y compás. Diremos que un punto es *constructible (con regla y compás)*, sin especificar el conjunto de partida, si lo es a partir de dos puntos que identificaremos con $(0,0)$ y $(1,0)$.

Obsérvese que para poder construir, a partir de los elementos de un conjunto $\mathcal{A}$ es necesario que $\mathcal{A}$ tenga al menos dos puntos. Si partimos de exactamente dos puntos $\{O, P\}$, podemos considerar que $O$ es el origen de coordenadas, fijar el eje de abscisas como la recta que pasa por $O$ y $P$ y la distancia unidad como la distancia entre $O$ y $P$ de forma que en la práctica cuando $\mathcal{A}$ tiene exactamente dos puntos podemos suponer que esos puntos son $(0,0)$ y $(1,0)$.

Abusando de la notación diremos que un *elemento geométrico* del plano es *constructible* a partir de un conjunto de puntos $\mathcal{A}$ (o constructible a secas si $\mathcal{A} = \{(0,0),(1,0)\}$) si está determinado por un conjunto de puntos constructibles a partir de $\mathcal{A}$. Por ejemplo una recta se dice que es *constructible con regla y compás* a partir de $\mathcal{A}$ si pasa por dos puntos distintos constructibles a partir de $\mathcal{A}$ y se dice que una circunferencia es constructible con regla y compás si el centro es constructible a partir de $\mathcal{A}$ y el radio coincide con la distancia entre dos puntos constructibles a partir de $\mathcal{A}$.

Veamos algunas construcciones elementales con regla y compás.

**Proposición 7.2** *(1) Si $P$ y $Q$ son constructibles a partir de $\mathcal{A}$, entonces la circunferencia con centro $P$ que pasa por $Q$ es constructible a partir de $\mathcal{A}$.*

*(2) El punto medio y la mediatriz entre dos puntos constructibles a partir de $\mathcal{A}$ son constructibles a partir de $\mathcal{A}$.*

*(3) Si un punto $P$ y una recta $L$ son constructibles a partir de $\mathcal{A}$ entonces también son constructibles a partir de $\mathcal{A}$ las rectas perpendicular y paralela a $L$ que pasan por $P$.*

*(4) Las bisectrices de dos rectas constructibles a partir de $\mathcal{A}$ son constructibles a partir de $\mathcal{A}$.*

**Demostración.** En esta demostración constructible significa constructible a partir de $\mathcal{A}$.
(1) es obvio (Figura 7.1).

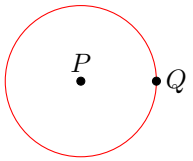



Figura 7.1: Circunferencia con centro $P$ que pasa por $Q$.

(2) La mediatriz entre dos puntos (es decir el conjunto de puntos equidistantes de ambos) es la recta que pasa por la intersección de las dos circunferencias centradas en uno de los puntos y que pasan por el otro y el punto medio es la intersección de la mediatriz con la recta que pasa por los dos puntos (Figura 7.2).

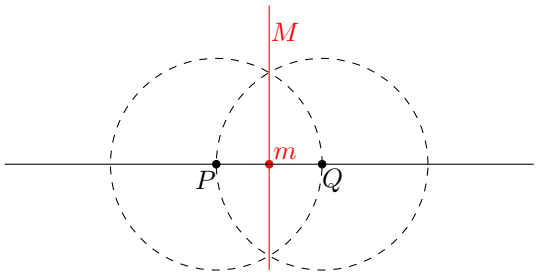



Figura 7.2: Punto medio ($m$) y mediatriz ($M$) entre dos puntos $P$ y $Q$.

(3) Empecemos construyendo la perpendicular a $L$ que pasa por $P$ (Figura 7.3). Como la recta $L$ es constructible, al menos contiene dos puntos constructibles y uno de ellos $Q$ es distinto de $P$. Si $P$ no está en $L$ entonces la circunferencia $C$ centrada en $P$ que pasa por $Q$ corta a $L$ en uno o dos puntos y uno de ellos es $Q$. Si sólo lo corta en $Q$ y entonces la recta que pasa por $P$ y $Q$ es la perpendicular buscada. En caso contrario los dos puntos de corte, $Q$ y $Q'$, son equidistantes de $P$ y por tanto la mediatriz entre estos dos es la perpendicular a $L$ que pasa por $P$. Si $P$ está en $L$ entonces construimos la circunferencia centrada en $P$ que pasa por $Q$ y la mediatriz entre los dos puntos de intersección de esta circunferencia y la recta es la perpendicular buscada.

Para construir la paralela simplemente observamos que la recta que pasa por $P$ y es perpendicular a la perpendicular a $L$ por $P$ es paralela a $L$.

(4) Ejercicio. □

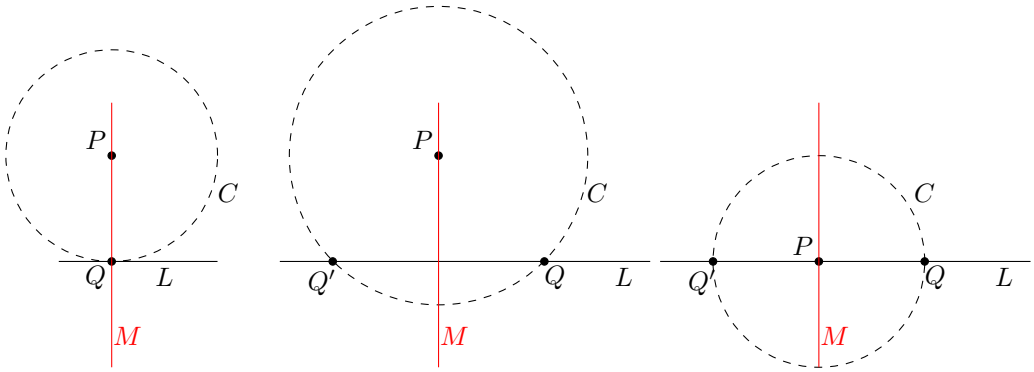



Figura 7.3: Recta $M$ perpendicular a una recta dada $L$ que pasa por un punto dado $P$.

**Corolario 7.3** *Si* $(0,0),(1,0) \in \mathcal{A} \subseteq \mathbb{C}$ *entonces* $(a,b)$ *es constructible a partir de* $\mathcal{A}$ *si y solo si lo son* $a$ *y* $b$.

A partir de ahora es conveniente identificar el plano euclídeo $\mathbb{R}^2$ con el conjunto de los números complejos de la forma habitual, es decir el punto de coordenadas $(a,b)$ se identifica con el número complejo $a+bi$. Con este convenio el Corolario 7.3 toma la siguiente forma:

Si $0,1 \in \mathcal{A} \subseteq \mathbb{C}$ entonces $a+bi$ es constructible a partir de $\mathcal{A}$ si y solo si lo son $a$ y $b$.

Una consecuencia inmediata de la Proposición 7.2 es la siguiente:

**Proposición 7.4** *Sea* $\mathcal{A}$ *un subconjunto de* $\mathbb{C} = \mathbb{R}^2$ *que contiene a* 0 *y* 1 *y* $K$ *el conjunto de los puntos constructibles a partir de* $\mathcal{A}$. *Entonces*

*(1)* $K$ *es un subcuerpo de* $\mathbb{C}$.

*(2) Las raíces de un polinomio de segundo grado con coeficientes en* $K$ *están también en* $K$.

**Demostración.** De nuevo, es esta demostración constructible significa constructible a partir de $\mathcal{A}$.

Como 0 y 1 están en $\mathcal{A}$, la recta real es constructible.

(1) Para empezar mostramos que los elementos de $K \cap \mathbb{R}$ forman un subcuerpo de $\mathbb{R}$. Sean $a,b \in K \cap \mathbb{R}$. Como $0 \in \mathcal{A}$, la distancia $|b|$ de 0 a $b$ es constructible, es decir está en $K$. Entonces $a+b$ y $a-b$ son las intersecciones de la recta real con la circunferencia centrada en $a$ de radio $|b|$, lo que muestra que $a+b$ y $a-b$ pertenecen a $K \cap \mathbb{R}$ (Figura 7.4).

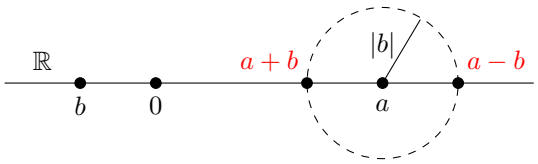



Figura 7.4: Suma y diferencia de dos números reales.

Vamos ahora a demostrar que $ab \in K$ y si $b \neq 0$ entonces $b^{-1} \in K$. En vista de que los opuestos de elementos de $K \cap \mathbb{R}$ están en $K \cap \mathbb{R}$, bastará considerar el caso en que $a$ y $b$ son positivos. Como

$1 = (1,0)$ y $b = (b,0)$ son constructibles, del Corolario 7.3 deducimos que $i = (0,1)$ y $bi = (0,b)$ son constructibles. Por tanto la recta que pasa por 0 y $a$ es constructible y la recta paralela a esta que pasa por $bi$ también es constructible. Aplicando el Teorema de Tales se deduce que la intersección de esta recta con el eje real es $ab = (ab,0)$. Esto prueba que $ab \in K \cap \mathbb{R}$ y esta misma idea sirve para mostrar que entonces $b^{-1} \in K \cap \mathbb{R}$ (Figura 7.5).

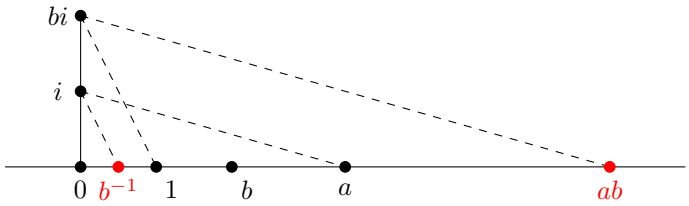



Figura 7.5: Producto e inverso de números reales.

Para demostrar que $K$ es un cuerpo basta recordar que $a + bi$ es constructible si y solo si $a$ y $b$ son constructibles (Corolario 7.3) y que las operaciones aritméticas de números complejos se obtienen mediante operaciones aritméticas con las partes reales y complejas:

$$\begin{aligned}(a+bi)+(c+di) &= (a+c)+(b+d)i\\ -(a+bi) &= (-a)+(-b)i\\ (a+bi)(c+di) &= (ac-bd)+(ad+bc)i\\ (a+bi)^{-1} &= \tfrac{a}{a^2+b^2} - \tfrac{b}{a^2+b^2}i\end{aligned}$$

(2) Como las raíces del polinomio $aX^2 + bX + c$ son $\frac{-b\sqrt{b^2-4ac}}{2a}$, aplicando el apartado (1) basta demostrar que si $a \in K$ entonces $\sqrt{a} \in K$.

Empezamos demostrando esto bajo la hipótesis de que $a$ es un número real mayor que 1. Como $a+1, a-1 \in K$, la recta que pasa por $(a-1)i$ y es paralela a la recta real, y la circunferencia centrada en 0 de radio $a+1$ son constructibles. Por tanto, es constructible el punto $P$ de intersección entre ambas, situado en el primer cuadrante (izquierda de la Figura 7.6). Por tanto también es constructible la recta que pasa por este punto y es perpendicular a la recta real. Sea $Q$ el punto de intersección de esta recta con la recta real. Aplicando el Teorema de Pitágoras al triángulo $0QP$ cuya hipotenusa mide $a+1$ y sus catetos miden $a-1$ y $q$ deducimos que $Q^2 = (a+1)^2 - (a-1)^2 = 4a$. Luego $Q = 2\sqrt{a} \in K$ y por tanto $\sqrt{a} \in K$. Esto demuestra que si $a \in K \cap \mathbb{R}$ con $a > 1$ entonces $\sqrt{a} \in K$.

Si ahora $a \in K \in \mathbb{R}$ con $0 < a < 1$ entonces $a^{-1} > 1$ y por el párrafo anterior, $\sqrt{a^{-1}} \in K$, lo que implica que $\sqrt{a} = (\sqrt{a^{-1}})^{-1} \in K$. Esto demuestra que si $a \in K \cap \mathbb{R}^+$ entonces $\sqrt{a} \in K$.

Finalmente si $a = x + yi \in K \setminus \{0\}$, entonces $x, y \in K$, por la Proposición 7.3. De los párrafos anteriores tenemos que $|a| = \sqrt{x^2+y^2}$ es constructible, con lo que $\sqrt{|a|}$ es constructible. Deducimos que $\sqrt{a}$ es constructible pues pertenece a la intersección de la circunferencia centrada en 0 de radio $\sqrt{|a|}$ con una de las bisectrices de la recta real y la que pasa por 0 y $a$ (derecha de la Figura 7.6). □

## 7.2 Teorema de Wantzel

Hasta ahora hemos visto resultados positivos sobre la constructibilidad con regla y compás. Es el momento de "bajarnos los humos" y mostrar limitaciones sobre la constructibilidad de puntos con regla y compás.

Dado un subconjunto $\mathcal{A}$ de $\mathbb{R}^2$ vamos a denotar por $\overline{\mathcal{A}}$ al conjunto de las coordenadas de los elementos de $\mathcal{A}$. La clave para caracterizar los puntos constructibles es el siguiente lema.

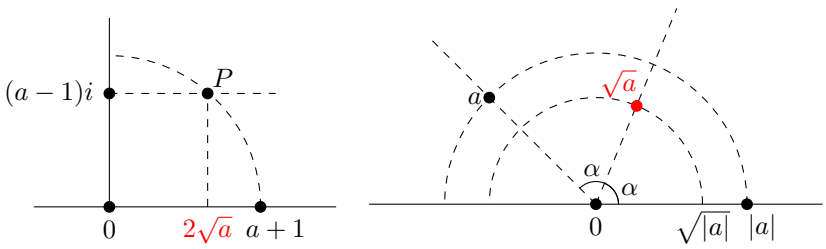



Figura 7.6: Raíz cuadrada de un número complejo.

**Lema 7.5** *Sean $\mathcal{A} \subseteq \mathbb{R}^2$ y $P \in \mathbb{R}^2$. Si $P$ es constructible en un paso a partir de $\mathcal{A}$ entonces $[\mathbb{Q}(\overline{\mathcal{A} \cup \{P\}}) : \mathbb{Q}(\overline{\mathcal{A}})] \leq 2$.*

**Demostración.** Ponemos $K = \mathbb{Q}(\overline{\mathcal{A}})$ y tenemos que demostrar que $z = a + bi$ es constructible en un paso a partir de $\mathcal{A}$ si y solo si $[K(a,b) : K] \leq 2$.

Empezamos suponiendo que $z = a + bi = (a,b)$ es constructible en un paso a partir de $\mathcal{A}$ y consideremos las tres construcciones posibles:

*$z$ está en la intersección de dos rectas distintas que pasan por dos parejas de puntos de $\mathcal{A}$.*

Pongamos que las rectas son $L_1$ y $L_2$ y las parejas de puntos respectivas son $((p_{11}, p_{12}), (q_{11}, q_{12}))$ y $((p_{21}, p_{22}), (q_{21}, q_{22}))$, con lo que las coordenadas de estos cuatro puntos están en $\overline{\mathcal{A}}$. Además las ecuaciones de las rectas $L_1$ y $L_2$ son

$$\frac{X - p_{11}}{q_{11} - p_{11}} = \frac{Y - p_{12}}{q_{12} - p_{12}} \quad \text{y} \quad \frac{X - p_{21}}{q_{21} - p_{21}} = \frac{Y - p_{22}}{q_{22} - p_{22}}$$

que se convierten en dos ecuaciones lineales

$$\begin{aligned} a_{11}X + a_{12}Y &= b_1 \\ a_{21}X + a_{22}Y &= b_2 \end{aligned}$$

con $a_{ij} \in K$ para todo $i, j$. Como las rectas $L_1$ y $L_2$ son distintas el sistema de ecuaciones lineales es compatible determinado, es decir el determinante de la matriz de coeficientes es diferente de 0, y las coordenadas $a$ y $b$ del punto $z = (a,b)$, solución del sistema, se expresa mediante la Regla de Cramer a partir de los coeficientes de la ecuación mediante operaciones suma, resta producto y cociente, con lo que $a$ y $b$ están en $K$ y por tanto $[K(a,b) : K] = 1$.

*$z$ está en la intersección de una recta $L$ que pasa por dos puntos de $\mathcal{A}$ y una circunferencia $C$ centrada en un punto de $\mathcal{A}$ y de radio la distancia entre dos puntos de $\mathcal{A}$.*

Como en el caso anterior la ecuación de la recta $pX + qy = r$ tiene coeficientes en $K$. También tiene coeficientes en $K$ la ecuación de la circunferencia $(X - c_1)^2 + (Y - c_2)^2 = R$, donde $(c_1, c_2)$ es el centro y $R = (p_1 - q_1)^2 + (p_2 - q_2)^2$, siendo $(p_1, q_1)$ y $(p_2, q_2)$ dos puntos de $\mathcal{A}$. Por tanto $(a,b)$ es una de las soluciones del sistema de ecuaciones

$$\begin{aligned} pX + qY &= r \\ (X - c_1)^2 + (Y - c_2)^2 &= R \end{aligned}$$

y sólo hay que mostrar que las soluciones pertenecen a una extensión de grado $\leq 2$ de $K$. Como $p \neq 0$ ó $q \neq 0$, por simetría podemos suponer que $q \neq 0$, con lo que despejando $Y$ en la primera ecuación y sustituyendo en la segunda obtenemos una ecuación de segundo grado $X^2 + hX + k = 0$ cuyas soluciones pertenecen a $E = K(\sqrt{\Delta})$ donde $\Delta = \sqrt{h^2 - 4k}$. Una de esas soluciones es $a$. Por tanto $a \in E$ y entonces $b = \frac{r - pa}{q} \in E$. Concluimos que $[K(a,b) : K] \leq [E : K] \leq 2$.

*$z$ está en la intersección de dos circunferencias con centros en $\mathcal{A}$ y radios las distancias entre parejas de puntos de $\mathcal{A}$.*

En este caso se plantea un sistema de dos ecuaciones cuadráticas con coeficientes en $K$:

$$\begin{aligned}(X-c_{11})^2+(Y-c_{12})^2 &= R_1\\ (X-c_{21})^2+(Y-c_{22})^2 &= R_2\end{aligned}$$

que después de desarrollar se convierten en

$$\begin{aligned}X^2+Y^2+a_{11}X+a_{12}Y+b_1 &= 0\\ X^2+Y^2+a_{21}X+a_{22}Y+b_2 &= 0\end{aligned}$$

que a su vez se puede convertir en el siguiente sistema

$$\begin{aligned}X^2+Y^2+a_{11}X+a_{12}Y+b_1 &= 0\\ (a_{21}-a_{11})X+(a_{22}-b_{12})Y+(b_2-b_1) &= 0\end{aligned}$$

y razonando como en el caso anterior concluimos que $[K(a,b):K]\leq 2$. □

**Proposición 7.6** *Sea $\mathcal{A}$ un subconjunto de $\mathbb{C}$ que contiene a 0 y 1. Si existe una torre de cuerpos $\mathbb{Q}(\mathcal{A})=K_0\subseteq K_1\cdots\subseteq\cdots\subseteq K_n\subseteq\mathbb{C}$ con $[K_i:K_{i-1}]\leq 2$ para todo $i$ entonces todos los elementos de $K_n$ son constructibles con regla y compás a partir de $\mathcal{A}$.*

**Demostración.** Sea $F$ el conjunto de los elementos de $\mathbb{C}$ constructibles a partir de $\mathcal{A}$. Razonamos por inducción en $i$ para demostrar que $K_i\subseteq F$ para todo $i$. Esto está claro si $i=0$ pues $\mathcal{A}\subseteq F$, luego $K_0=\mathbb{Q}(\mathcal{A})\subseteq F$. Por hipótesis de inducción $K_{i-1}\subseteq F$ y como $[K_i:K_{i-1}]\leq 2$, o bien $K_i=K_{i-1}\subseteq F$ o $K_i=K_{i-1}(\alpha)$ con $\mathrm{Min}_{K_{i-1}}(\alpha)$ de grado 2. En el segundo caso $\alpha\in F$, por el segundo apartado de la Proposición 7.4 y por tanto $K_i\subseteq F$. Concluimos que $K_n\subseteq F$, es decir que los elementos de $K_n$ son constructibles a partir de $\mathcal{A}$. □

**Teorema 7.7 (Wantzel)** *Sea $\mathcal{A}$ un subconjunto de $\mathbb{C}$ que contiene 0 y 1 y $z=a+bi\in\mathbb{C}$, entonces las siguientes condiciones son equivalentes:*

*(1) $z$ es constructible a partir de $\mathcal{A}$.*

*(2) Existe una torre de cuerpos*

$$\mathbb{Q}(\overline{\mathcal{A}})=K_0\subset K_1\subset\cdots\subset K_n\subseteq\mathbb{C}$$

*con $[K_i:K_{i-1}]=2$ para todo $i$ y $a,b\in K_n$.*

**Demostración.** (1) implica (2) Supongamos que $z$ es constructible a partir de $\mathcal{A}$ y sean $P_1,\ldots,P_n=z$ en $\mathbb{C}$ tales que $P_i=(p_i,q_i)$ es constructible en un paso a partir de $\mathcal{A}\cup\{P_1,\ldots,P_{i-1}\}$, para cada $i$. Entonces del Lema 7.5 se deduce que si ponemos $K_i=\mathbb{Q}(\overline{\mathcal{A}}\cup\{p_1,q_1,\ldots,p_i,q_i\})$, entonces

$$[K_i:K_{i-1}]\leq 2$$

para todo $i$, con lo que eliminando los $K_i$ repetidos obtenemos una sucesión que satisface la condición (2).

(2) implica (1) Supongamos que la sucesión $K_0\subset K_1\subset\cdots\subset K_n$ satisface la condición (2). Por el Corolario 7.3 los elementos de $\overline{\mathcal{A}}$ son contructibles a partir de $\mathcal{A}$ y por la Proposición 7.6 los elementos de $K_n$ son constructibles a partir de $\mathcal{A}$. Por tanto los elementos de $K_n$ son constructibles a partir de $\mathcal{A}$ y en particular lo es $z$. □

**Corolario 7.8** *Las siguientes condiciones son equivalentes para un número complejo $z$:*

*(1) $z$ es constructible.*

*(2) Existe una torre de cuerpos $\mathbb{Q} = K_0 \subset K_1 \subset \dots K_n$ con $z \in K_n$ y $[K_i : K_{i-1}] = 2$ para todo $i = 1, \dots, n$.*

**Demostración.** (1) implica (2) Supongamos que $z = a + bi$ es constructible. Por el Teorema de Wantzel existe una torre de cuerpos $\mathbb{Q} = K_0 \subset K_1 \subset \dots K_k$ con $a, b \in K_k$ y $[K_i : K_{i-1}] = 2$ para todo $i = 1, \dots, k$. Si $i \in K_k$ entonces $z \in K_k$ y hemos acabado. En caso contrario ponemos $K_{k+1} = K_k(i)$ y tenemos que $z \in K_{k+1}$ y $[K_{k+1} : K_k] = 2$.

(2) implica (1) El mismo argumento de la demostración de (2) implica (1) en la demostración del Teorema de Wantzel sirve para demostrar esto. □

Como consecuencia del Corolario 7.8 deducimos el siguiente corolario.

**Corolario 7.9 (Criterio de Wantzel)** *Si $z \in \mathbb{C}$ es constructible con regla y compás $[\mathbb{Q}(z) : \mathbb{Q}]$ es una potencia de 2.*

A la vista de los resultados anteriores se podría pensar que si $z$ es constructible a partir de $\mathcal{A}$ entonces debería existir una torre $\mathbb{Q}(\mathcal{A}) = K_0 \subset K_1 \subset \cdots \subset K_n \subseteq \mathbb{C}$ con $z \in K_n$ y $[K_i : K_{i-1}] = 2$ para todo $i$. Si eso fuera cierto $z$ sería algebraico sobre $\mathbb{Q}(\mathcal{A})$. Sin embargo el siguiente ejemplo muestra un elemento constructible a partir de $\mathcal{A}$ que no es algebraico sobre $\mathbb{Q}(\mathcal{A})$.

**Ejemplo 7.10** Sea $K$ la clausura algebraica de $\mathbb{Q}$ en $\mathbb{R}$. Como $\mathbb{Q}[X]$ es numerable y $K$ es la unión de los conjuntos de raíces de los $P \in \mathbb{Q}[X] \setminus \{0\}$, $K$ es la unión de un conjunto numerable de conjuntos finitos y por tanto $K$ es numerable. Luego $\mathbb{R}$ tiene algún elemento $\alpha$ trascendente sobre $\mathbb{Q}$. Pero $\mathbb{Q}[X]$ es numerable y por tanto también lo son $\mathbb{Q}[\alpha]$ y $\mathbb{Q}(\alpha)$. El mismo argumento muestra que la clausura algebraica de $\mathbb{Q}(\alpha)$ en $\mathbb{R}$ es numerable. Por tanto, $\mathbb{R}$ tiene un segundo elemento $\beta$ que es trascendente sobre $\mathbb{Q}(\alpha)$. Sean $\gamma = \alpha + \beta i$ y $\mathcal{A} = \{0, 1, \gamma\}$. Entonces $\mathbb{Q}(\mathcal{A}) = \mathbb{Q}(\gamma)$. Por el Lema 7.3 sabemos que $\alpha$ es constructible a partir de $\mathcal{A}$. Sin embargo vamos a ver que $\alpha$ es trascendente sobre $\mathbb{Q}(\gamma)$.

Por reducción al absurdo, suponemos que $\alpha$ es algebraico sobre $\mathbb{Q}(\gamma)$. Luego existe $P \in \mathbb{Q}(\gamma)[X] \setminus \{0\}$ tal que $P(\alpha) = 0$. Los coeficientes de $\mathbb{Q}(\gamma)$ son fracciones de la forma $\frac{a}{b}$ con $a, b \in \mathbb{Q}[\gamma]$, con lo que multiplicando por el producto de los denominadores podemos suponer sin pérdida de generalidad que $P \in \mathbb{Q}[\gamma][X]$. Por tanto existe un polinomio en dos indeterminadas $Q \in \mathbb{Q}[X, Y] \setminus \{0\}$ tal que $Q(\alpha, \gamma) = P(\gamma)(\alpha) = 0$. Escribimos $Q = Q_0 + Q_1 Y + \cdots + Q_k Y^k$ con $Q_i \in \mathbb{Q}[X]$ y ponemos $R = \mathbb{Q}(\alpha, Y) \in K(\alpha)[Y]$. Si $R = 0$ entonces $Q_i(\alpha) = 0$ para todo $i$ y como $\alpha$ es trascendente sobre $\mathbb{Q}$ necesariamente $Q_i = 0$ para todo $i$, en contra de que $Q \neq 0$. Luego $R \in \mathbb{Q}(\alpha)[Y] \setminus \{0\}$ y $R(\gamma) = 0$. Por tanto $\gamma$ es algebraico sobre $\mathbb{Q}(\alpha)$, con lo que $\mathbb{Q}(\alpha, \gamma)/\mathbb{Q}(\alpha)$ es una extensión finita. Entonces $\mathbb{Q}(\alpha, \gamma, i)/\mathbb{Q}(\alpha)$ es finita y como $\beta \in \mathbb{Q}(\alpha, \gamma, i)$ tenemos que $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}(\alpha)$ es finita, en contra de que $\beta$ es trascendente sobre $\mathbb{Q}(\alpha)$.

El Criterio de Wantzel es suficiente para resolver negativamente los tres problemas clásicos sobre constructibilidad con regla y compás, es decir, la trisección del ángulos, la cuadratura de la circunferencia y la duplicación del cubo.

> **Trisección del Ángulos**: Dado un ángulo, construir con regla y compás la tercera parte de ese ángulo.

**Corolario 7.11** *El problema de Trisección del Ángulo no tiene solución general.*

**Demostración.** Para ello basta ver un ángulo constructible que no se pueda trisecar con regla y compás. Obsérvese que que se pueda construir un ángulo $\alpha$, equivale a que el punto $(\cos\alpha, \text{ sen } \alpha)$ se puede construir pues este punto es la intersección de la circunferencia centrada en el origen con la semirecta que parte del origen y forma un ángulo $\alpha$ con la parte positiva de la recta real (Figura 7.7). Como $\text{ sen } \alpha = \sqrt{1-\cos(\alpha)}$, se tiene que el ángulo $\alpha$ es constructible si y solo si $\cos\alpha$ es constructible. Por ejemplo el ángulo $\pi$ es constructible pues $\cos\pi = -1$ es constructible y este ángulo se puede trisecar pues $\cos\frac{\pi}{3} = \frac{1}{2}$. Sin embargo $\frac{\pi}{3}$ no se puede trisecar con regla y compás, o lo que es lo mismo el ángulo $\frac{\pi}{9}$ no es constructible. Para ver esto calculamos el polinomio mínimo de $\alpha = \cos\left(\frac{\pi}{9}\right)$. De las fórmulas del coseno y seno de la suma de ángulos deducimos que si $\alpha = \cos\left(\frac{\pi}{9}\right)$ entonces

$$\begin{aligned}
\tfrac{1}{2} &= \cos\left(\tfrac{\pi}{3}\right) = \cos\left(\tfrac{\pi}{9} + 2\tfrac{\pi}{9}\right) = \cos\left(\tfrac{\pi}{9}\right)\cos\left(2\tfrac{\pi}{9}\right) - \text{ sen } \left(\tfrac{\pi}{9}\right) \text{ sen } \left(2\tfrac{\pi}{9}\right) \\
&= \cos\left(\tfrac{\pi}{9}\right)\left(\cos^2\left(\tfrac{\pi}{9}\right) - \text{ sen }^2\left(\tfrac{\pi}{9}\right)\right) - 2\,\text{sen }^2\left(\tfrac{\pi}{9}\right)\cos\left(\tfrac{\pi}{9}\right) = \cos^3\left(\tfrac{\pi}{9}\right) - 3\cos\left(\tfrac{\pi}{9}\right) \text{ sen }^2\left(\tfrac{\pi}{9}\right) \\
&= \cos^3\left(\tfrac{\pi}{9}\right) - 3\cos\left(\tfrac{\pi}{9}\right)\left(1 - \cos^2\left(\tfrac{\pi}{9}\right)\right) = 4\cos^3\left(\tfrac{\pi}{9}\right) - 3\cos\left(\tfrac{\pi}{9}\right) = 4\alpha^3 - 3\alpha
\end{aligned}$$

Por tanto $\alpha$ es una raíz del polinomio $8X^3 - 6X - 1$ que es irreducible sobre $\mathbb{Q}$ pues no tiene raíces en $\mathbb{Q}$. Eso implica que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, y deducimos que $\alpha$ no es constructible con regla y compás por el Criterio de Wantzel (Corolario 7.9). □

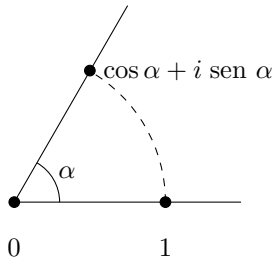



Figura 7.7:

**Cuadratura del Círculo**: Construir con regla y compás un cuadrado que tenga el mismo área que un círculo dado.

**Corolario 7.12** *Es imposible cuadrar un círculo con regla y compás.*

**Demostración.** Para cuadrar un círculo de radio 1, necesitaríamos poder construir con regla y compás un número cuyo cuadrado fuera el área del círculo, es decir $\pi$. Si esto fuera posible, el número $\pi$ sería constructible con regla y compás, en particular $[\mathbb{Q}(\pi) : \mathbb{Q}]$ sería finito, es decir $\pi$ sería algebraico. Sin embargo $\pi$ es transcendente como demostró Lindeman en 1882. □

**Duplicación del Cubo**: Construir un cubo que tenga el doble del volumen de un cubo dado.

**Corolario 7.13** *Es imposible duplicar un cubo arbitrario.*

**Demostración.** Duplicar el cubo de lado 1, equivaldría a construir el lado $\alpha$ de un cubo cuyo volumen fuera 2, es decir eso equivaldría a construir $\sqrt[3]{2}$, que no es constructible con regla y compás pues $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ no es una potencia de 2. □

## 7.3 Construcción de polígonos regulares

En esta sección vamos a tratar el problema de la constructibilidad de polígonos regulares con regla y compás. Se entiende que los datos dados son el centro y uno de los vértices y podemos fijar el sistema de coordenadas de forma que el centro sea $0 = (0, 0)$ y uno de los vértices sea $1 = (1, 0)$. Entonces los vértices de un polígono regular de $n$ lados centrado en el origen y uno de cuyos vértices sea 1, son las $n$-raíces $n$-ésimas de la unidad. Como estas raíces son las potencias de una raíz $n$-ésima primitiva de la unidad, por ejemplo

$$\zeta_n = e^{2\pi i/n} = \left(\cos\frac{2\pi}{n},\ \text{sen}\ \frac{2\pi}{n}\right),$$

el polígono regular de $n$ lados es constructible con regla y compás si y solo si $\zeta_n$ es constructible con regla y compás, lo que equivale a que $\cos\frac{2\pi}{n}$ sea constructible. Por ejemplo, es fácil construir con regla y compás los polígonos regulares de tres, cuatro, cinco y seis lados. El de cuatro lados es el más fácil pues $\zeta_4 = i$. También podemos utilizar que $\cos\frac{2\pi}{4} = 0$. Para construir el de tres lados observamos que $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ o que $\cos\frac{2\pi}{3} = -\frac{1}{2}$. Para el de seis observamos que $-\zeta_3$ y $-\zeta_3^2$ son dos raíces sextas primitiva de la unidad de orden 6 con lo que una de ellas es $\zeta_6$. De hecho $\zeta_6 = -\zeta_3^2$ (Figura 7.8).

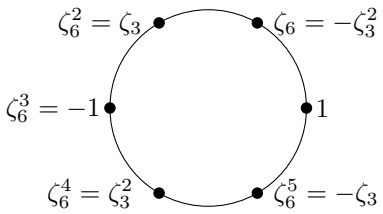



Figura 7.8:

Para construir el de 5 lados observamos que $\zeta_5$ no es número real y que $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$. Sea $\alpha = 2\cos\left(\frac{2\pi}{5}\right) = \zeta_5 + \zeta_5^{-1}$. Utilizando que $1+\zeta_5+\zeta_5^2+\zeta_5^3+\zeta_5^4 = 0$ obtenemos que $\alpha^2 = \zeta_5^2+2+\zeta_5^{-2} = 1-\alpha$, con lo que $\alpha$ es raíz del polinomio $X^2 + X - 1$ y por tanto

$$\alpha = \frac{-1+\sqrt{5}}{2}.$$

Luego tenemos la torre de extensiones de grado 2

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta_5),$$

y aplicando el Teorema de Wantzel (Teorema 7.7) deducimos que $\zeta_5$ es constructible y por tanto también lo es el polígono regular de cinco lados. Es un ejercicio educativo y divertido hacer la construcción de este polígono siguiendo las indicaciones de la Proposición 7.4.

Para caracterizar los polígonos regulares que son constructibles necesitaremos la siguiente proposición cuya demostración utiliza la Proposición 5.15 de GyA que nos asegura que todo grupo de orden potencia de un primo tiene centro no trivial.

**Proposición 7.14** *Si $G$ es un grupo cuyo orden es una potencia de un primo $p$, entonces existe una sucesión de subgrupos de $G$*

$$1 = G_0 < G_1 < \cdots < G_n = G$$

*tal que $[G_i : G_{i-1}] = p$ para todo $i$.*

**Demostración.** Supongamos que $|G| = p^n$ y razonemos por inducción sobre $n$. No hay nada que demostrar si $n = 0$, es decir, si $G = 1$, por lo que supongamos que $n > 0$ y la hipótesis de inducción para $n$ menor. De la Proposición 5.15 de GyA deducimos que $Z(G) \neq 1$. Sea $a \in \mathbb{Z}(G) \setminus \{1\}$. Entonces $\langle a \rangle$ tiene un subgrupo $G_1$ de orden $p$ (¿por qué?), y como $G_1 \subseteq Z(G)$, se tiene que $G_1 \trianglelefteq G$. Por hipótesis de inducción $G/G_1$ tiene una cadena de subgrupos

$$1 = \overline{G_1} \leq \overline{G_2} \leq \cdots \leq \overline{G_n} = G/G_1$$

tales que $[\overline{G_i} : \overline{G_{i-1}}] = p$. Por el Teorema de la Correspondencia, para cada $i$, se tiene que $\overline{G_i} = G_i/G_1$, para algún $G_1 \leq G_i \leq G$. Entonces

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

satisface la propiedad deseada pues $[G_i : G_{i-1}] = [\overline{G_i} : \overline{G_{i-1}}] = p$. □

Recordemos que $\phi : \mathbb{N} \to \mathbb{N}$ denota la función de Euler, es decir $\phi(n)$ es el cardinal de $\mathbb{Z}_n^*$, o sea el número de enteros entre 1 y $n$ que son coprimos con $n$. Recordemos también que si $n = p_1^{e_1} \cdots p_k^{e_k}$ es la factorización de un número natural $n$, es decir $p_1, \ldots, p_k$ son primos distintos y $e_1, ¨, e_k$ son enteros positivos, entonces

$$\phi(n) = (p_1 - 1) \cdots (p_k - 1) p_1^{e_1 - 1} \cdots p_k^{e_k - 1} = n \frac{p_1 - 1}{p_1} \cdots \frac{p_k - 1}{p_k}.$$

**Teorema 7.15 (Gauss)** *Las siguientes condiciones son equivalentes para un un entero positivo $n$.*

*(1) El polígono regular de $n$ lados es constructible con regla y compás.*

*(2) $\zeta_n = e^{2\pi i/n}$ es constructible con regla y compás.*

*(3) $\cos \frac{2\pi}{n}$ es constructible con regla y compás.*

*(4) $\phi(n)$ es una potencia de 2.*

*(5) $n = 2^k p_1 p_2 \cdots p_m$ para $k \geq 0$ y cada $p_i$ un primo tal que $p_i - 1$ es una potencia de 2 y todos los $p_i$ son distintos dos a dos.*

**Demostración.** Ya hemos visto al principio de la sección que (1), (2) y (3) son equivalentes.

(2) implica (4) Si $\zeta_n$ es constructible entonces $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ es una potencia de 2, por el Criterio de Wantzel (Corolario 7.9). Aplicando el Corolario 4.9 deducimos que $\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ es una potencia de 2.

(4) implica (2) Supongamos que $\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ es una potencia de 2. Como $\mathbb{Q}(\zeta_n)$ es el cuerpo de descomposición de $X^n - 1$ sobre $\mathbb{Q}$, la extensión $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es normal, y por tanto es de Galois (¿por qué?). Eso implica que $|\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ es una potencia de 2. De la Proposición 7.14 deducimos que existe una sucesión

$$1 = G_0 < G_1 < \cdots < G_n = \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

de subgrupos de $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ tales que $[G_i : G_{i-1}] = 2$, para todo $i$. Aplicando el Teorema Fundamental de la Teoría de Galois deducimos que

$$\mathbb{Q} = K_0 = G_n^\circ \subset K_1 = G_{n-1}^\circ \subset \cdots \subset K_{n-1} = G_1^\circ \subset K_n = G_0^\circ = \mathbb{Q}(\zeta_n)$$

es una torre de cuerpos con $[K_i : K_{i-1}] = 2$, para todo $i$. Aplicando el Corolario 7.8 deducimos que $\zeta_n$ es constructible.

Finalmente demostramos que (4) y (5) son equivalentes. En efecto, sea $n = 2^k p_1^{\alpha_1} \dots p_m^{\alpha_m}$ con $2, p_1, \dots, p_m$ primos distintos, $k \geq 0$, y $\alpha_i \geq 1$. Entonces

$$\phi(n) = 2^{\max\{0,k-1\}} p_1^{\alpha_1 - 1} \cdots p_m^{\alpha_m - 1}(p_1 - 1) \cdots (p_m - 1)$$

con lo que $\phi(n)$ es una potencia de 2 si y solo si $\alpha_i = 1$, para todo $i$ y $p_i - 1$ es una potencia de 2. □

En realidad se puede decir algo más de un primo $p$ tal que $p - 1$ sea potencia de 2. En concreto $p = 2^a + 1$ y $a$ ha de ser una potencia de 2. En efecto, en caso contrario $a$ es divisible por un número impar $q > 1$. Consideremos la igualdad

$$X^q + 1 = (X + 1)(X^{q-1} - X^{q-2} + \cdots + X^2 - X + 1)$$

en la que sustituimos $X$ por $2^{a/q}$ para obtener

$$p = 2^a + 1 = (2^{a/q} + 1)(2^{a(q-1)/q} - X^{a(q-2)/q} + \cdots + X^{2a/q} - X^{a/q} + 1)$$

Como $1 < 2^{a/q} + 1 < 2^a + 1$, deducimos que $p$ no es primo en contra de la hipótesis. Por tanto los primos $p_i$ que aparecen en la condición 5 del Teorema 7.15 son de la forma $F_m = 2^{2^m} + 1$ para algún $m \geq 0$. El número $F_m$ se llama $m$-ésimo número de Fermat pues Fermat conjeturó que $F_m$ es primo para todo $m$. Fermat había comprobado que los primeros números de Fermat

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537,$$

son en efecto primos. Sin embargo, Euler mostró que el siguiente no lo es al mostrar que

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417.$$

De hecho todavía no se conoce ningún número de Fermat que sea primo a añadir a los cinco primeros.

# Problemas

**7.1** Dado un triángulo mostrar cómo construir con regla y compás el incentro (centro de una circunferencia inscrita), circuncentro (centro de una circunferencia circunscrita) y el baricentro (punto de intersección de las alturas).

**7.2** Explicar cómo construir con regla y compás los polígonos regulares de 3, 4, 5, 6, 8 y 10 lados.

**7.3** Demostrar, sin utilizar el Teorema 7.15, que si se pueden construir un polígono regular de $n$ lados y otro de $m$ lados, entonces también se puede construir otro de $\text{mcm}(n, m)$ lados. ¿Se podría construir otro de $nm$ lados? Mostrar cómo construir con regla y compás un polígono regular de 15 lados.

**7.4** ¿Se puede trisecar con regla y compás el ángulo $2\pi/5$?

**7.5** ¿Se puede trisecar con regla y compás un segmento de longitud $\pi$?

**7.6** Determinar el conjunto de puntos del plano constructibles con regla y compás a partir de los puntos del eje de abscisas.

**7.7** ¿Son constructibles con regla y compás los ángulos de 1 y 3 grados?

**7.8** Vamos a explicar cómo trisecar con regla y compás un ángulo dado $\alpha$ siguiendo los siguientes pasos:

(1) Supongamos que el ángulo $\alpha$ es el formado por dos semirectas $S_1$ y $S_2$ que parten del punto $O$.

(2) Construimos una circunferencia centrada en $O$ de radio $r$ arbitrario.

(3) Sean $A_1$ y $A_2$ las intersecciones de esta circunferencia con las semirectas $S_1$ y $S_2$ y sea $L_1$ la recta que pasa por $O$ y $A_1$ (es decir $L_1$ es la prolongación de $S_1$).

(4) Colocamos la regla de forma que pase por $A_2$ y la distancia entre los puntos $B$ y $C$ de corte de la regla con la recta $L_1$ y la circunferencia (diferente de $A_2$) están a distancia $r$ y dibujamos la recta $L$ que marca la regla. Es decir, la recta $L$ pasa por $A_2$, $B$ y $C$.

Entonces el ángulo formado por $L$ y $L_1$ es $\alpha/3$ pues (Figura 7.9)

$$\begin{aligned}\alpha &= \widehat{A_1OA_2} = \pi - \widehat{A_2OB} = \widehat{OBA_2} + \widehat{OA_2B} = \widehat{OBC} + \widehat{OA_2C} = \widehat{OBC} + \widehat{OCA_2} \\ &= \widehat{OBC} + \pi - \widehat{OCB} = \widehat{OBC} + \widehat{BOC} + \widehat{OBC} = 3 \cdot \widehat{OBC}\end{aligned}$$

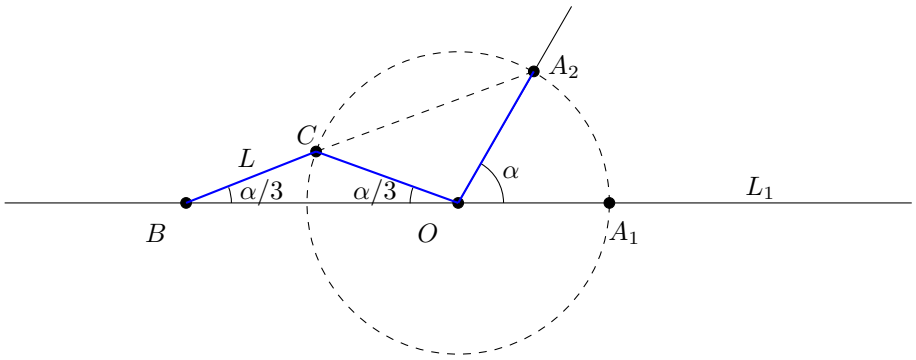



Figura 7.9:

¿Te imaginas qué pide el problema? ¿Cuál es tu solución?

**7.9** Coge una regla y un compás, dibuja un segmento de longitud 1, construye un heptágono de lado $3/5 = 0.6$, como el de la Figura 7.10 y explica que está pasando aquí.

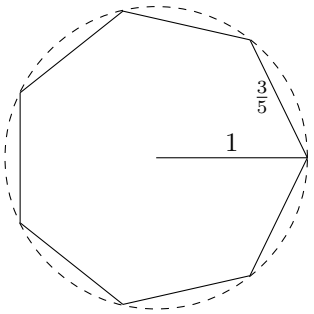



Figura 7.10:

**7.10** Demostrar que un ángulo $\alpha$ se puede trisecar con regla con regla y compás si y solo si el polinomio $4X^3 - 3X - \cos(\alpha)$ es reducible sobre $\mathbb{Q}(\cos(\alpha))$.

**7.11** Demostrar que un número complejo $\alpha \neq 0$ es constructible con regla y compás si y solo si $\alpha + \alpha^{-1}$ lo es.

**7.12** Demostrar que si $\alpha$ es una raíz del polinomio $8X^3 + 4X^2 - 4X - 1$, entonces $\alpha$ no es constructible con regla y compás.

**7.13** Demostrar que las raíces de un polinomio del tipo $aX^4 + bX^2 + c$, con $a, b, c \in \mathbb{Q}$ son constructibles con regla y compás.

**7.14** Sea $p$ un polinomio de grado 3, cuyos coeficientes son números complejos constructibles con regla y compás. Demostrar que si una de las raíces de $p$ es constructible con regla y compás, entonces lo son todas las raíces de $p$.

**7.15** Demostrar que las raíces del polinomio $X^4 + X + 1$ no son constructibles con regla y compás. (Indicación: Calcular $\mathrm{Min}_{\mathbb{Q}}(\alpha\overline{\alpha} + \beta\overline{\beta})$, donde $\alpha$ y $\beta$ son dos raíces no conjugadas del polinomio.)

**7.16** Desde la antigüedad se sabían construir con regla y compás polígonos regulares de 3, 4, 5, 6, 8, 12, 15 y 16 lados y ya sabemos que esto es imposible para los polígonos de 7, 9, 10, 11, 13 y 14 grados (¿por qué?). El 30 de marzo de 1796, Gauss escribió su primer descubrimiento en un cuaderno que le acompañaría el resto de su vida y en el que consignaría sus más importantes resultados matemáticos. El descubrimiento era un método para construir con regla y compás un polígono heptadecágono regular, o sea un polígono regular de 17 lados. Gauss contaba con 19 años y debió ser uno de sus descubrimientos favoritos pues por un lado fue el que le decidió a dedicarse a las matemáticas (hasta entonces dudaba entre matemáticas o lengua) y por otro pidió que en su tumba se esculpiera un polígono regular de 17 lados. El deseo de Gauss no se cumplió por que el cantero que tenía que esculpir la lápida argumento que el resultado no se distinguiría de una circunferencia.

El problema consiste en construir un heptadecágono regular con regla y compás, para lo cual habrá que mezclar los siguientes pasos algebraicos con los métodos geométricos explicados en el capítulo.

(1) Calcular las 16 primeras potencias de 3 módulo 17, es decir completar la siguiente tabla:

| $m$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $3^m$ | 1 | 3 | 9 | 10 | 13 | | | | | | | | | | | |

(2) Sean $\theta = 2\pi/17$, $\zeta = \zeta_{17} = e^{\theta i}$. Observa que 3 es un generador de $\mathbb{Z}_{17}$ y por tanto $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \langle\sigma\rangle$, donde $\sigma(\zeta) = \zeta^3$. Pongamos $\epsilon_i = \zeta^{3^i}$.

Utilizar la tabla anterior para construir los periodos de Gauss (ver Ejercicio 4.16 del Capítulo 4)

$$\begin{aligned} x_1 &= \omega_{0,2} = \epsilon_0 + \epsilon_2 + \cdots + \epsilon_{14}, \\ x_2 &= \omega_{1,2} = \epsilon_1 + \epsilon_3 + \cdots + \epsilon_{15}, \\ y_1 &= \omega_{0,4} = \epsilon_0 + \epsilon_4 + \epsilon_8 + \epsilon_{12}, \\ y_2 &= \omega_{1,4} = \epsilon_1 + \epsilon_5 + \epsilon_9 + \epsilon_{13}, \\ y_3 &= \omega_{2,4} = \epsilon_2 + \epsilon_6 + \epsilon_{10} + \epsilon_{14}, \\ y_4 &= \omega_{3,4} = \epsilon_3 + \epsilon_7 + \epsilon_{11} + \epsilon_{15}. \end{aligned}$$

Demostrar:

$$\begin{aligned} x_1 &= 2(\cos\theta + \cos 8\theta + \cos 4\theta + \cos 2\theta), \\ x_2 &= 2(\cos 3\theta + \cos 7\theta + \cos 5\theta + \cos 6\theta), \\ y_1 &= 2(\cos\theta + \cos 4\theta), \\ y_2 &= 2(\cos 8\theta + \cos 2\theta), \\ y_3 &= 2(\cos 3\theta + \cos 5\theta), \\ y_4 &= 2(\cos 7\theta + \cos 6\theta). \end{aligned}$$

(3) Demostrar que $x_1$ y $x_2$ son las raíces del polinomio $X^2 + X - 4$ y construir $x_1$ y $x_2$ con regla y compás. Observa que $x_1 > 0 > x_2$

(4) Demostrar que $y_1$ e $y_2$ son las raíces del polinomio $X^2 - x_1X - 1$ e $y_3$ e $y_4$ son las raíces del polinomio $X^2 - x_2X - 1$ y construir $y_1, y_2, y_3$ e $y_4$ con regla y compás. Observa que $y_1 > y_2$ e $y_3 > y_4$.

(5) Demostrar que $z_1 = 2\cos\theta$ y $z_2 = 2\cos 4\theta$ son las raíces del polinomio $T^2 - y_1T - y_3$ y construir $z_1$ y $z_2$ con regla y compás.

(6) Construir $\zeta = \cos\theta + i \operatorname{sen}\theta$ con regla y compás.

(7) Demostrar la siguiente igualdad

$$\cos\theta = \frac{1}{16}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{68 + 12\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}} - 2(1 - \sqrt{17})\sqrt{34 - 2\sqrt{17}}}\right).$$

# Capítulo 8

# Extensiones cíclicas

## 8.1 Polinomio característico, norma y traza

En esta sección $L/K$ va a ser una extensión finita y vamos a definir tres aplicaciones

$$\chi_K^L : L \to K[X], \qquad \mathrm{N}_K^L : L \to K, \qquad \mathrm{T}_K^L : L \to K$$

de la siguiente forma: Para cada $\alpha \in L$ consideramos la aplicación

$$\begin{array}{rccc} \rho_\alpha^L : & L & \to & L \\ & x & \mapsto & \alpha x \end{array}$$

como un endomorfismo del espacios vectorial $L_K$. (Obsérvese que también podemos considerar $\rho_\alpha^L$ como endomorfismo de $L_L$ ó como endomorfismo de $L_E$ para cualquier subcuerpo de $E$, pero nosotros lo consideramos como endomorfismo de $L_K$.) Entonces $\chi_K^L(\alpha)$, $\mathrm{N}_K^L(\alpha)$ y $\mathrm{T}_K^L(\alpha)$ son respectivamente el polinomio característico, la norma y la traza de este endomorfismo y se llaman respectivamente *polinomio característico*, *norma* y *traza* de $\alpha$ en la extensión $L/K$. (Recuérdese que el polinomio característico, el determinante y la norma de un endomorfismo $f$ del espacio vectorial de dimensión finita $V$ son respectivamente el polinomio característico, el determinante y la traza de $A$, donde $A$ es cualquiera de las matrices asociadas a $f$ en una base de $V$, y que el resultado de este cálculo no depende de la base elegida.)

Obsérvese que la norma y la traza coinciden con dos de los coeficientes del polinomio característico, salvo en el signo. Más concretamente

$$\begin{array}{rcl} \mathrm{N}_K^L(\alpha) & = & (-1)^{[L:K]} \text{ Término independiente de } \chi_K^L(\alpha) \\ \mathrm{T}_K^L(\alpha) & = & - \text{ Coeficiente de } X^{[L:K]-1} \text{ en } \chi_K^L(\alpha). \end{array} \tag{8.1}$$

La siguiente proposición reúne las propiedades principales del polinomio característico, la norma y la traza.

**Proposición 8.1** *Sea $L/K$ una extensión de cuerpos finita y sean $\alpha, \beta \in L$, $a \in K$ y $E \in \mathrm{Sub}(L/K)$.*

*(1) $\mathrm{T}_K^L : L \to K$ es una aplicación $K$-lineal y $\mathrm{T}_K^L(a) = [L:K]a$.*

*(2) $\mathrm{N}_K^L(\alpha\beta) = \mathrm{N}_K^L(\alpha)\mathrm{N}_K^L(\beta)$ y $\mathrm{T}_K^L(a) = a^{[L:K]}$.*

*(3) Si $\alpha \in E$, entonces*

$$\chi_K^L(\alpha) = \chi_K^E(\alpha)^{[L:E]}, \quad \mathrm{N}_K^L(\alpha) = \mathrm{N}_K^E(\alpha)^{[L:E]} \quad y \quad \mathrm{T}_K^L(\alpha) = [L:E]\,\mathrm{T}_K^E(\alpha).$$

*(4)* $\chi_K^L(\alpha) = \mathrm{Min}_K(\alpha)^{[L:K(\alpha)]}$. *En particular* $\alpha$ *es una raíz de* $\chi_K^L(\alpha)$ *y* $\alpha$ *es un elemento primitivo de* $L$ *si y solo si* $\chi_K^L = \mathrm{Min}_K(\alpha)$.

*(5) Si* $\sigma_1, \ldots, \sigma_n$ *son los* $K$*-homomorfismos de* $L$ *en una clausura algebraica de* $K$*, entonces*

$$\chi_K^L(\alpha) = \left(\prod_{i=1}^n (X - \sigma_i(\alpha))\right)^{[L:K]_i}, \quad \mathrm{N}_K^L(\alpha) = \left(\prod_{i=1}^n \sigma_i(\alpha)\right)^{[L:K]_i} \quad y \quad \mathrm{T}_N^L(\alpha) = [L:K]_i \sum_{i=1}^n \sigma_i(\alpha).$$

*En particular, si* $L/K$ *es separable, entonces*

$$\chi_K^L(\alpha) = \prod_{i=1}^n (X - \sigma_i(\alpha)), \quad \mathrm{N}_K^L(\alpha) = \prod_{i=1}^n \sigma_i(\alpha) \quad y \quad \mathrm{T}_N^L(\alpha) = \sum_{i=1}^n \sigma_i(\alpha).$$

*(6) Si* $\sigma : L \to L'$ *es un* $K$*-isomorfismo de cuerpos, entonces*

$$\chi_K^L(\alpha) = \chi_K^{L'}(\sigma(\alpha)), \quad \mathrm{N}_K^L(\alpha) = \mathrm{N}_{L'}^E(\sigma(\alpha)) \quad y \quad \mathrm{T}_K^L(\alpha) = \mathrm{T}_K^{L'}(\sigma(\alpha)).$$

*(7) (Transitividad de la norma y la traza) Si* $E \in \mathrm{Sub}(L/K)$*, entonces*

$$\mathrm{N}_K^L(\alpha) = \mathrm{N}_K^E(\mathrm{N}_E^L(\alpha)) \quad y \quad \mathrm{T}_K^L(\alpha) = \mathrm{T}_K^E(\mathrm{T}_E^L(\alpha)).$$

**Demostración.** (2) y (1) son consecuencias inmediatas de las propiedades del determinante y la traza de una matriz.

En las demostraciones de (3) y (5) basta comprobar las propiedades sobre el polinomio característico pues las propiedades sobre la norma y la traza son consecuencias inmediatas de las del polinomio característico y de la relación (8.1).

(3) Si $B_1 = \{b_1, \ldots, b_n\}$ es una base de $E_K$ y $B_2 = \{c_1, \ldots, c_m\}$ es una base de $L_E$, entonces $B = \{b_i c_j : i = 1, \ldots, n, j = 1, \ldots, m\}$ es una base de $L/K$. Si $A = (a_{ij})$ es la matriz asociada a $\rho_\alpha^E : E \to E$ en la base $B$ entonces

$$\alpha b_i = \rho_\alpha^E(b_i) = \sum_{k=1}^n a_{ki} b_k$$

Por tanto

$$\rho_\alpha^L(b_i c_j) = \alpha b_i c_j = \sum_{k=1}^n a_{ki} b_k c_j$$

con lo que la matriz asociada a $\rho_\alpha^L$ en la base $B$ tiene siguiente la forma en $m \times m$ bloques de matrices cuadradas de tamaño $n$,

$$\overline{A} = \begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix}$$

donde la matriz $A$ aparece $m = [L:E]$ veces en la diagonal y donde no se escribe nada es por que hay ceros. Por tanto $\chi_K^L(\alpha) = \det(XI - \overline{A}) = \prod_{i=1}^m \det(XI - A) = \chi_K^E(\alpha)^m$.

(4) En vista del apartado (3), sólo hay que demostrar que $\chi_K^{K(\alpha)}(\alpha) = \mathrm{Min}_K(\alpha)$. Pongamos $p = \mathrm{Min}_K(\alpha) = p_0 + p_1 X + \cdots + p_{n-1} X^{n-1} + X^n$. Entonces $1, \alpha, \alpha^2, \ldots, \alpha_{n-1}$ es una base de $K(\alpha)_K$ y la

matriz asociada a $\rho_\alpha^{K(\alpha)}$ es

$$A = \begin{pmatrix} & & & -p_0 \\ 1 & & & -p_1 \\ & 1 & & -p_2 \\ & & \ddots & \vdots \\ & & 1 & -p_{n-1} \end{pmatrix}.$$

Esta matriz se llama *matriz de compañía del polinomio* $p$ y vamos a ver que su polinomio característico es $p$ por inducción sobre el grado. Esto es obvio para grados pequeños por lo que podemos suponer que $n > 1$ y la hipótesis de inducción. Entonces

$$\begin{aligned} \chi_K^{K(\alpha)}(\alpha) &= \det(XI - A) = \begin{vmatrix} X & & & & p_0 \\ -1 & X & & & p_1 \\ & -1 & X & & p_2 \\ & & \ddots & & \vdots \\ & & & -1 & X + p_{n-1} \end{vmatrix} \\ &= X \begin{vmatrix} X & & & & p_1 \\ -1 & X & & & p_2 \\ & -1 & X & & p_3 \\ & & \ddots & & \vdots \\ & & & -1 & X + p_{n-1} \end{vmatrix} + (-1)^{n+1} p_0 \begin{vmatrix} -1 & X & & \\ & -1 & X & \\ & & \ddots & \ddots \\ & & & -1 \end{vmatrix} \\ &= X \begin{vmatrix} X & & & & p_1 \\ -1 & X & & & p_2 \\ & -1 & X & & p_3 \\ & & \ddots & & \vdots \\ & & & -1 & X + p_{n-1} \end{vmatrix} + p_0 \end{aligned}$$

Obsérvese que el determinante que aparece multiplicada por $X$ es el de la matriz de compañía del polinomio $q = p_1 + p_2 X + \cdots + p_{n-1} X^{n-2} + X^{n-1}$. Aplicando la hipótesis de inducción tenemos que

$$\chi_K^{K(\alpha)} = p_0 + Xq = p.$$

(5) Sean $p = \mathrm{Min}_K(\alpha)$, $\alpha_1, \ldots, \alpha_r$ las diferentes raíces de $p$ en una clausura algebraica $\overline{K}$ de $K$. Por la Uniformidad de las Raíces (Lema 5.6), se tiene que $p = \prod_{i=1}^r (X - \alpha_i)^{[K(\alpha):K]_i}$. Además el número de $K$-homomorfismos de $K(\alpha)$ en $\overline{K}$ es $r = [K(\alpha) : K]_s$ y estos $r$ homomorfismos $\tau_1, \ldots, \tau_r$ vienen dados por $\tau_i(\alpha) = \alpha_i$. Cada uno de estos $\tau_i$ tiene $s = [L : K(\alpha)]_s$ extensiones a homomorfismos $\rho_{i,j} : L \to \overline{K}$, con lo que $\{\sigma_1, \ldots, \sigma_n\} = \{\rho_{i,j} : i = 1, \ldots, r, j = 1, \ldots, s\}$ y cada $\alpha_i$ aparece $s$ veces en la lista $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$. Por tanto, aplicando (3) tenemos

$$\begin{aligned} \chi_K^L(\alpha) &= p^{[L:K(\alpha)]} = \left(\textstyle\prod_{i=1}^r (X - \alpha_i)^{[K(\alpha):K]_i}\right)^{[L:K(\alpha)]} \\ &= \left(\textstyle\prod_{i=1}^r (X - \alpha_i)\right)^{[K(\alpha):K]_i [L:K(\alpha)]_i [L:K(\alpha)]_s} \\ &= \left(\textstyle\prod_{i=1}^r (X - \alpha_i)^s\right)^{[L:K]_i} \\ &= \left(\textstyle\prod_{i=1}^n (X - \sigma_i(\alpha))\right)^{[L:K]_i}. \end{aligned}$$

(6) Es consecuencia inmediata de (5).

(7) Sea $\overline{L}$ una clausura algebraica de $L$ y sean $F$ la clausura normal de $L/K$.

$\tau_1, \ldots, \tau_r : E \to \overline{K}$ los $K$-homomorfismos de $E$ a $\overline{L}$,
$\sigma_1, \ldots, \sigma_s : L \to \overline{K}$, los $E$-homomorfismos de $L$ a $\overline{L}$,
$\overline{\tau}_1, \ldots, \overline{\tau}_r : F \to \overline{L}$ donde $\overline{\tau}_i$ es una extensión de $\tau_i$.

Entonces $\sigma_i(L) \subseteq F$ y $\overline{\tau}_i$ es un automorfismo de $F$ para cada $i = 1, \ldots, r$ (¿por qué?). Los elementos de $X = \{\overline{\tau}_i\sigma_j : i = 1, \ldots, r, j = 1, \ldots, \}$ son $K$-homomorfismos y de hecho es el conjunto de los diferentes $K$-homomorfismos de $L$ en $\overline{K}$ ya que si $\rho : L \to \overline{K}$ es un $K$-homomorfismo, entonces $\rho|_E = \tau_i = \overline{\tau}_i|_E$, para algún $i$, con lo que $\overline{\tau}_i^{-1}\rho$ es un $E$-homomorfismo y por tanto $\overline{\tau}_i^{-1}\rho = \sigma_j$, para algún $j$. Entonces

$$\begin{aligned} \mathrm{N}_K^L(\alpha) &= \textstyle\prod_{i,j} \overline{\tau}_i\sigma_j(\alpha)^{[L:K]_i} = \prod_i \overline{\tau}_i \left(\prod_j \sigma_j(\alpha)^{[L:E]_i}\right)^{[E:K]_i} \\ &= \textstyle\prod_i \overline{\tau}_i(\mathrm{N}_E^L(\alpha))^{[E:K]_i} = \mathrm{N}_K^E(\mathrm{N}_E^L(\alpha)) \end{aligned}$$

Esto muestra la transitividad de la norma y la transitividad de la traza se demuestra de forma similar. □

## 8.2 Teorema 90 de Hilbert

En esta sección veremos un teorema fundamental de Hilbert para cuya demostración utilizaremos el siguiente teorema.

**Teorema 8.2 (Artin)** *Si $K$ y $L$ son dos cuerpos, entonces el conjunto de los homomorfismos no nulos $K \to L$ es linealmente independiente sobre $L$.*

**Demostración.** Sean $\sigma_1, \ldots, \sigma_n : K \to L$ homomorfismos distintos (y diferentes de 0). Tenemos que demostrar que la dimensión $d$ de $V = L\sigma_1 + \cdots + L\sigma_n$ coincide con $n$. Razonemos por reducción al absurdo, suponiendo que $d < n$ y reordenemos los $\sigma_i$ para que los $d$ primeros formen una base de $V$. Entonces $\sigma = \sigma_n$ es distinto de 0 y de $\sigma_i$ para $i = 1, \ldots, d$ y existen $a_1, \ldots, a_d \in L$ tales que

$$\sigma = a_1\sigma_1 + \cdots + a_d\sigma_d.$$

Como $\sigma \neq 0$, algún $a_i \neq 0$ y reordenando los $\sigma_1, \ldots, \sigma_d$, podemos suponer que $a_1 \neq 0$. Sea $\alpha \in K$ tal que $\sigma(\alpha) \neq \sigma_1(\alpha)$. Entonces para todo $\beta \in K$ tenemos

$$\begin{aligned} &\sigma(\alpha)(a_1\sigma_1(\beta) + \cdots + a_d\sigma_d(\beta)) = \sigma(\alpha)\sigma(\beta) \\ &= \sigma(\alpha\beta) = a_1\sigma_1(\alpha\beta) + \cdots + a_d\sigma_d(\alpha\beta) \\ &= a_1\sigma_1(\alpha)\sigma_1(\beta) + \cdots + a_d\sigma_d(\alpha)\sigma_d(\beta) \end{aligned}$$

y por tanto

$$[(\sigma(\alpha) - \sigma_1(\alpha))a_1\sigma_1 + \cdots + (\sigma(\alpha) - \sigma_d(\alpha))a_d\sigma_d](\beta) = 0$$

para todo $\beta \in K$, es decir

$$(\sigma(\alpha) - \sigma_1(\alpha))a_1\sigma_1 + \cdots + (\sigma(\alpha) - \sigma_d(\alpha))a_d\sigma_d = 0$$

y como el primer coeficiente de la anterior combinación lineal es diferente de 0, esto contradice la independencia lineal de $\{\sigma_1, \ldots, \sigma_d\}$ sobre $L$. □

**Lema 8.3** *Las siguientes condiciones son equivalentes para una extensión finita $L/K$:*

*(1)* $\mathrm{T}_K^L(\alpha) \neq 0$ *para algún* $\alpha \in L$.

*(2)* $\mathrm{T}_K^L(\alpha) = 1$ *para algún* $\alpha \in L$.

*(3)* $L/K$ *es separable.*

**Demostración.** (2) implica (1) es obvio.

(1) implica (2) Si $\mathrm{T}_K^L(\alpha) \neq 0$, entonces $\mathrm{T}_K^L\left(\frac{\alpha}{\mathrm{T}_K^L(\alpha)}\right) = 1$.

(3) si y solo si (1) Elegimos una clausura algebraica $\overline{L}$ de $L$. Si $\sigma_1, \ldots, \sigma_n$ son los $K$-homomorfismos de $L$ en $\overline{L}$, entonces $\sigma_1, \ldots, \sigma_n$ son linealmente independientes por el Teorema 8.2 y $\mathrm{T}_K^L = [L:K]_i(\sigma_1 + \cdots + \sigma_n)$, por la propiedad 5 de la Proposición 8.1. Por tanto $\mathrm{T}_K^L = 0$ si y solo si $[L:K]_i$ es cero en el cuerpo $L$, es decir, si ponemos $t = [L:K]_i 1_L$. Entonces $\mathrm{T}_K^L = 0$ si y solo si $t = 0$ si y solo si $[L:K]_i$ es múltiplo de la característica de $L$. Recordando que $[L:K]_i$ es una potencia de la característica de $K$, resulta que $L/K$ es separable si y solo si $[L:K]_i = 1$, si y solo si $t \neq 0$ si y solo si $\mathrm{T}_K^L \neq 0$. □

**Definición 8.4** *Una* extensión cíclica *es una extensión de Galois cuyo grupo de Galois es cíclico.*

**Ejemplos 8.5** (1) Toda extensión de Galois de grado primo es cíclica pues todo grupo de orden primo es cíclico.

(2) Si $p$ es un número primo y $\zeta_p$ es una raíz compleja $p$-ésima primitiva de la unidad, entonces $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es una extensión de Galois y su grupo de Galois es isomorfo al grupo de unidades $\mathbb{Z}_p^*$ del cuerpo $\mathbb{Z}_p$. Del Lema 4.2 se deduce que $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es cíclico. De hecho si $K$ es cualquier cuerpo y $\zeta_p$ es una raíz $p$-ésima primitiva de la unidad en una extensión de $K$ entonces $K(\zeta_p)/K$ es también una extensión cíclica pues su grupo de Galois es isomorfo a un subgrupo de $\mathbb{Z}_p^*$.

Supongamos que $L/K$ es una extensión cíclica de grado $n$ con grupo de Galois $G$ y sea $\sigma$ un generador de $G$. Entonces para cada divisor $d$ de $n$, $G_d = \langle \sigma^d \rangle$ es el único subgrupo de $G$ de orden $\frac{n}{d}$ y, del Teorema Principal de la Teoría de Galois, $L_d = L^{G_d} = \{x \in L : \sigma^d(x) = x\}$ es el único elemento de $\mathrm{Sub}(L/K)$ tal que $[L_d : L] = d$.

**Teorema 8.6 (Teorema 90 de Hilbert)** *Sea* $L/K$ *una extensión cíclica finita con* $\mathrm{Gal}(L/K) = \langle \sigma \rangle$ *y sea* $\alpha \in L$. *Entonces*

*(1)* $\mathrm{T}_K^L(\alpha) = 0$ *si y solo si* $\alpha = \beta - \sigma(\beta)$ *para algún* $\beta \in L$.

*(2)* $\mathrm{N}_K^L(\alpha) = 1$ *si y solo si* $\alpha = \beta\sigma(\beta)^{-1}$ *para algún* $\beta \in L^*$.

**Demostración.** Para simplificar la notación pondremos $N = \mathrm{N}_K^L$ y $T = \mathrm{T}_K^L$. La condición suficiente es obvia en ambos casos pues $T(\beta) = T(\sigma(\beta))$ y $N(\beta) = N(\sigma(\beta))$.

(1) Supongamos que $T(\alpha) = 0$ y para cada $i = 1, \ldots, n$ consideramos

$$\gamma_i = \alpha + \sigma(\alpha) + \cdots + \sigma^{i-1}(\alpha).$$

Podemos considerar los $\gamma_i$ como trazas parcial donde la primera sería $\gamma_1 = \alpha$ y la última $\gamma_n = \mathrm{T}_K^L(\alpha)$, la traza total. Consideremos un elemento $\theta \in L$ tal que $T(\theta) = 1$ cuya existencia está garantizada por el Lema 8.3. Vamos a ver que, si $n = [L:K]$, entonces

$$\beta = \gamma_1\sigma(\theta) + \gamma_2\sigma^2(\theta) + \cdots + \gamma_{n-1}\sigma^{n-1}(\theta)$$

cumple la propiedad deseada, o sea $\alpha = \beta - \sigma(\beta)$. Teniendo en cuenta que, para $i = 1, \ldots, n-1$, se tiene que $\sigma(\gamma_i\sigma^i(\theta)) = \gamma_{i+1}\sigma^{i+1}(\theta) - \alpha\sigma^{i+1}(\theta)$ deducimos que

$$\begin{aligned} \beta - \sigma(\beta) &= \gamma_1\sigma(\theta) + \gamma_2\sigma^2(\theta) + \cdots + \gamma_{n-1}\sigma^{n-1}(\theta) \\ &\quad -\gamma_2\sigma^2(\theta) - \cdots - \gamma_{n-1}\sigma^{n-1}(\theta) - \gamma_n\sigma^n(\theta) \\ &\quad +\alpha(\sigma^2(\theta) + \cdots + \sigma^n(\theta)) \\ &= \alpha(\sigma(\theta) + \cdots + \sigma^{n-1}(\theta) + \sigma^n(\theta)) = \alpha\, T(\theta) = \alpha. \end{aligned}$$

(2) Supongamos ahora que $N(\alpha) = 1$ y consideremos ahora normas parciales

$$\gamma_i = \alpha\sigma(\alpha)\cdots\sigma^{i-1}(\alpha)$$

de forma que

$$\gamma_0 = 1, \gamma_1 = \alpha, \ldots, \gamma_n = N(\alpha) = 1.$$

Por el Lema de Artin (Teorema 8.2) el siguiente endomorfismo de $L_K$ es diferente de 0

$$f = \gamma_0 1 + \gamma_1\sigma + \gamma_2 + \sigma^2 + \cdots + \gamma_{n-1}\sigma^{n-1}$$

y por tanto existe $\theta \in K$ tal que

$$\beta = f(\theta) = \theta + \gamma_1\sigma(\theta) + \gamma_2\sigma^2(\theta) + \cdots + \gamma_{n-1}\sigma^{n-1}(\theta) \neq 0.$$

Como $\alpha\sigma(\gamma_i) = \gamma_{i+1}$ tenemos

$$\alpha\sigma(\beta) = \gamma_1\sigma(\theta) + \gamma_2\sigma^2(\theta) + \cdots + \gamma_{n-1}\sigma^{n-1}(\theta) + \gamma_n\sigma^n(\theta) = \beta$$

pues $\sigma^n = 1$. □

## 8.3 Caracterización de las extensiones cíclicas

**Proposición 8.7** *Sean $n$ un entero positivo, $K$ un cuerpo que contiene una raíz $n$-ésima primitiva de la unidad y $a \in K$. Si $L$ es el cuerpo de descomposición de $X^n - a$ sobre $K$, entonces $L/K$ es una extensión cíclica.*

**Demostración.** Si $a = 0$ entonces $L = K$ y no hay nada que demostrar. Por tanto supongamos que $a \neq 0$. Como $K$ tiene una raíz $n$-ésima primitiva de la unidad, $n$ no es múltiplo de la característica de $K$ y por tanto el polinomio $X^n - a$ es separable, lo que implica que $L/K$ es una extensión de Galois. Sea $\alpha$ una raíz de $X^n - a$. Entonces las raíces de $X^n - a$ son $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha$, donde $\zeta \in K$ es una raíz $n$-ésima primitiva de la unidad. Por tanto $L = K(\alpha)$ y $\sigma(\alpha) = \zeta^{i_\sigma}\alpha$, para un $i_\sigma \in \mathbb{Z}_n$. Esto implica que la aplicación $\sigma \mapsto i_\sigma$ es un homomorfismo de grupos inyectivo de $\mathrm{Gal}(L/K)$ al grupo aditivo de $\mathbb{Z}_n$. Como este último es cíclico, también $\mathrm{Gal}(L/K)$ es cíclico. □

**Teorema 8.8** *Sean $n$ un entero positivo y $K$ un cuerpo que contiene una raíz $n$-ésima primitiva de la unidad. Las siguientes condiciones son equivalentes para una extensión $L/K$ de grado $n$.*

*(1) $L/K$ es cíclica.*

*(2) Existe $a \in K$ tal que $p = X^n - a$ es irreducible en $K[X]$ y tiene una raíz en $L$.*

*(3) Existe $\alpha \in L$ tal que $L = K(\alpha)$ y $\alpha^n \in K$.*

*(4) $L$ es un cuerpo de descomposición de $X^n - a$ sobre $K$ para algún $a \in K$.*

**Demostración.** Fijemos una raíz $n$-ésima primitiva de la unidad $\zeta \in K$.

(1) implica (2) Supongamos que $L/K$ es cíclica y $\sigma$ es un generador de $\mathrm{Gal}(L/K)$. Como $\zeta \in K$, se tiene que $N(\zeta) = \zeta^n = 1$ y del Teorema 90 de Hilbert se deduce que existe $\alpha \in L$ tal que $\sigma(\alpha) = \zeta\alpha$. Si $p = \mathrm{Min}_K(\alpha)$, entonces

$$\alpha, \sigma(\alpha) = \zeta\alpha, \sigma^2(\alpha) = \zeta^2\alpha, \ldots, \sigma^{n-1}(a) = \zeta^{n-1}\alpha$$

son raíces de $p$, y todas son distintas. Como $\mathrm{gr}(p) = [K(\alpha) : K] \leq n$, estas son las $n$ raíces de $p$ y por tanto

$$p = (X - \alpha)(X - \zeta\alpha)(X - \zeta^2\alpha) \cdots (X - \zeta^{n-1}\alpha)$$

Aplicando la Fórmula de Cardano-Vieta deducimos que el coeficiente de $X^{n-i}$ $(i = 1, 2, \ldots, n)$ de $p$ es

$$p_{n-i} = (-1)^{n-i} S_i(\alpha, \zeta\alpha, \zeta^2\alpha, \ldots, \zeta^{n-1}\alpha) = \alpha^i S_i(1, \zeta, \zeta^2, \ldots, \zeta^{n-1})$$

donde $S_i$ es el $i$-ésimo polinomio simétrico elemental en $n$ variables. Como $1, \zeta, \zeta^2, \zeta^{n-1}$ son las raíces de $X^n - 1$, aplicando de nuevo la Fórmula de Cardano-Vieta obtenemos que $p_{n-i} = 0$, si $i \neq n$ y $p_n = -\alpha^n$, con lo que $p = X^n - \alpha^n$. Por tanto, $a = \alpha^n \in K$, $p = X^n - a$ es irreducible en $K[X]$ y tiene una raíz en $L$.

(2) implica (3) Supongamos que $p = X^n - a$ es irreducible en $K[X]$ y $\alpha$ es una raíz de $p$ en $L$. Entonces $\alpha^n = a \in K$ y $n = [L : K] \geq [K(\alpha) : K] = \mathrm{gr}(p) = n$, con lo que $L = K(\alpha)$.

(3) implica (4) Si $a = \alpha^n$, entonces las raíces de $X^n - a$ son $\alpha, \zeta\alpha, \zeta^2\alpha, \ldots, \zeta^{n-1}\alpha$ y por tanto $L$ es es cuerpo de descomposición de $X^n - a$ sobre $K$.

(4) implica (1) es consecuencia de la Proposición 8.7. □

# Problemas

**8.1** Demostrar que la traza de la extensión $K(\sqrt{X})/K = \mathbb{F}_2(X)$ es idénticamente nula.

**8.2** Sea $\zeta = \zeta_p \in \mathbb{C}$ con $p$ primo. Demostrar que si $a_0, a_1, \ldots, a_{p-2} \in \mathbb{Q}$, entonces

$$\mathrm{T}_{\mathbb{Q}}^{\mathbb{Q}(\zeta)}\left(\sum_{i=0}^{p-2} a_i\zeta^i\right) = (p-1)a_0 - \sum_{i=1}^{p-2} a_i.$$

**8.3** Decir cuáles de las siguientes extensiones son cíclicas.

(1) $L/K$, donde $L$ es el cuerpo de descomposición de $X^p - 1$ sobre $K$ para un primo $p$.

(2) Una extensión de cuerpos finitos.

(3) $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, para cada uno de los números $n \leq 25$.

(4) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

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

(6) El cuerpo de descomposición de $X^3 - 2$ sobre $\mathbb{Q}$, $\mathbb{F}_3$ y $\mathbb{F}_5$.

**8.4** Sea $L/K$ una extensión cíclica de cuerpos de característica $p \neq 0$ y sea $\sigma$ un generador de $L/K$. Demostrar que para todo elemento $\beta \in L$ tal que $\mathrm{T}_K^L(\beta) = 0$ existe $\alpha \in L$ tal que $\sigma(\alpha) - \alpha = \beta^p - \beta$.

**8.5** Sea $K$ un cuerpo de característica $p \neq 0$ y $f = X^p - X - a$ con $a \in K$. Demostrar:

(1) Si $\alpha$ es una raíz de $f$, entonces $\alpha + 1$ también es raíz de $f$.

(2) $f$ es o irreducible o completamente indescomponible sobre $K$.

(3) Si $f$ es irreducible sobre $K$ y $\alpha$ es una raíz de $f$ en una extensión de $K$, entonces $K(\alpha)/K$ es una extensión cíclica.

(4) (Teorema de Artin-Schreier) Si $L/K$ es una extensión cíclica de grado $p$, entonces existen $a \in K$ y una raíz $\alpha$ de $f = X^p - X - a$ tal que $L = K(\alpha)$. En tal caso $L/K$ es el cuerpo de descomposición de $f$ sobre $K$.

**8.6** Sea $K$ un cuerpo que contiene una raíz $n$-ésima primitiva de la unidad y $L/K$ una extensión cíclica de grado $n$. Demostrar que si $L = K(\beta_1) = K(\beta_2)$ con $\beta_i^n \in K$, entonces existe un entero $m$, coprimo con $n$ tal que $\beta_2\beta_1^m \in K$.

**8.7** Sea $L/K$ una extensión cíclica de grado $p$ de cuerpos de característica $p$. Demostrar que si $L = K(\beta_1) = K(\beta_2)$ con $\beta_i^p - \beta_i \in K$ , entonces existe un entero $0 < m < p$ tal que $\beta_2 - m\beta_1 \in K$.

**8.8** Demostrar que si $L/K$ es una extensión cíclica de grado $p^n$ con $p$ primo y $E/K$ es una subextensión de grado $p^{n-1}$ de $L/K$ entonces $L = K(\alpha)$ para todo $\alpha \in L \setminus E$.

**8.9** Sea $L/K$ una extensión cíclica de grado $p^n$ de cuerpos de característica $p$, sea $\sigma$ un generador de $\mathrm{Gal}(L/K)$ y sea $E/K$ una subextensión de grado $p$ de $L/K$. Demostrar que existen $a \in E$ y $\beta \in L \setminus E$ tales que:

(1) $\beta^p - \beta = a$

(2) $L = K(\beta)$.

(3) $\sigma^{p^{n-1}}(\beta) = \beta + 1$.

(4) $\alpha^p - \alpha = \sigma(a) - a$, para $\alpha = \sigma(\beta) - \beta$.

**8.10** Sea $L/K$ una extensión finita. Para cada $\alpha, \beta \in L$ sea

$$(\alpha, \beta) = \mathrm{T}_K^{L'}(\alpha\beta).$$

Para cada lista $\alpha_1, \ldots, \alpha_n$ de elementos de $L$ ponemos

$$\Delta_K^L(\alpha_1, \ldots, \alpha_n) = \Delta(\alpha_1, \ldots, \alpha_n) = \begin{vmatrix} (\alpha_1,\alpha_1) & (\alpha_1,\alpha_2) & \ldots & (\alpha_1,\alpha_n) \\ (\alpha_2,\alpha_1) & (\alpha_2,\alpha_2) & \ldots & (\alpha_2,\alpha_n) \\ \ldots & \ldots & \ldots & \ldots \\ (\alpha_n,\alpha_1) & (\alpha_n,\alpha_2) & \ldots & (\alpha_n,\alpha_n) \end{vmatrix}.$$

Demostrar

(1) $(-,-)$ es una forma bilineal simétrica del espacio vectorial $L_K$, es decir, satisface las siguientes condiciones.

   (a) Para todo $\alpha \in L$, la aplicación $(\alpha, -) : L \to K$, dada por $(\alpha, -)(\beta) = (\alpha, \beta)$, es $K$-lineal.

   (b) $(\alpha, \beta) = (\beta, \alpha) \in K$, para todo $\alpha, \beta \in L$.

(2) Si $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$ entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base de $L_K$.

(3) Si $\{\alpha_1, \ldots, \alpha_n\}$ y $\{\beta_1, \ldots, \beta_n\}$ son dos bases de $L_K$, entonces existe $\lambda \in K^*$ tal que $\Delta(\alpha_1, \ldots, \alpha_n) = \lambda^2\Delta(\beta_1, \ldots, \beta_n)$.

(4) Si $s = [L : K]_s$ y $\{\sigma_1, \ldots, \sigma_s\}$ son los $K$-homomorfismos de $L$ en una clausura algebraica de $K$ entonces

$$\Delta(\alpha_1, \ldots, \alpha_s) = [L : K]_i^s \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_n) \\ \ldots & \ldots & \ldots & \ldots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{vmatrix}.$$

(5) Sean $p \in K[X]$ un polinomio irreducible separable de grado $n$, $\alpha$ una raíz de $p$ y $L = K(\alpha)$. Demostrar que $\Delta(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_K^L(\alpha)$.

(6) Las siguientes condiciones son equivalentes, donde $\phi : L \to \mathrm{Hom}_K(L, K)$ es la aplicación que asocia $\alpha \in L$ con la forma lineal $(\alpha, 0)$.

(a) $(-,-)$ es no degenerada, es decir $\phi$ es inyectiva.

(b) $\phi$ suprayectiva.

(c) $\phi$ biyectiva.

(d) $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$, para alguna base $\{\alpha_1, \ldots, \alpha_n\}$ de $L_K$.

(e) $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$, para toda base $\{\alpha_1, \ldots, \alpha_n\}$ de $L_K$.

(f) $\mathrm{T}_K^L(\alpha) \neq 0$, para algún $\alpha \in L$.

(g) $L/K$ es separable.

**8.11** Sea $L/K$ una extensión finita. Una *base normal* de $L/K$ es una base de $L_K$ de la forma $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}$, para un $\alpha \in L$. En tal caso se dice que $\alpha$ genera una base normal de $L/K$.

(1) Demostrar que si $L/K$ tiene una base normal, entonces es de Galois.

(2) Decir cuáles de los siguientes elementos generan bases normales de las extensiones que se indican.

(a) $\sqrt{a}$ de $K(\sqrt{a})/K$ para $a \in K \setminus K^2$.

(b) $1 + \sqrt{a}$ de $K(\sqrt{a})/K$ para $a \in K \setminus K^2$.

(c) $\zeta_n$ para $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

(3) Sea $\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$ y $\alpha \in L$. Demostrar que $\alpha$ genera una base normal de $L/K$ si y solo si el determinante de la siguiente matriz es diferente de cero.

$$\begin{pmatrix} \sigma_1^{-1}\sigma_1(\alpha) & \sigma_1^{-1}\sigma_2(\alpha) & \ldots & \sigma_1^{-1}\sigma_n(\alpha) \\ \sigma_2^{-1}\sigma_1(\alpha) & \sigma_2^{-1}\sigma_2(\alpha) & \ldots & \sigma_2^{-1}\sigma_n(\alpha) \\ \ldots & \ldots & \ldots & \ldots \\ \sigma_n^{-1}\sigma_1(\alpha) & \sigma_n^{-1}\sigma_2(\alpha) & \ldots & \sigma_n^{-1}\sigma_n(\alpha) \end{pmatrix}.$$

(4) Demostrar que toda extensión de Galois tiene una base normal.

(5) Supongamos que $\alpha \in L$ genera una base normal de $L/K$ y sean $G = \mathrm{Gal}(L/K)$, $H$ un subgrupo de $G$ y $F = L^H = \{x \in L : \sigma(x) = x, \text{ para todo } \sigma \in H\}$. Recordemos que $\mathrm{T}_F^L(x) = \sum_{\sigma \in H} \sigma(x)$, para cada $x \in L$. Supongamos que $\sigma_1, \ldots, \sigma_m$ es un conjunto de representantes de las clases laterales por la derecha de $H$ en $G$, es decir cada elemento de $H\backslash G$ contiene exactamente un $\sigma_i$. Para cada $i = 1, \ldots, m$ ponemos $H_i = \sigma_i^{-1} H \sigma_i$. Demostrar

(a) $\mathrm{T}_F^L(\alpha)$ es un elemento primitivo de $E$ sobre $K$.

(b) $\{\sigma_1(\mathrm{tr}_{H_1}(\alpha)), \ldots, \sigma_m(\mathrm{tr}_{H_m}(\alpha))\}$ es una base de $F$.

(c) Si $H$ es normal en $G$, entonces $\mathrm{tr}_H(\alpha)$ genera una base normal de $F/K$.

**8.12** Sea $P \in K[X]$ irreducible de grado primo $p \neq \mathrm{car}(K)$ y $\alpha$ una raíz de $P$. Demostrar que si $K(\alpha)$ contiene una raíz de $P$ diferente de $\alpha$, entonces $K(\alpha)$ es el cuerpo de descomposición de $P$ sobre $K$ y $\mathrm{Gal}(K(\alpha)/K)$ es cíclico.

# Capítulo 9

# Grupos resolubles

## 9.1 El subgrupo derivado y la serie derivada

**Definición 9.1** *Sea $G$ un grupo. Si $x, y \in G$, entonces el* conjugado *de $x$ por $y$ es*

$$x^y = x^{-1}yx$$

*y el* conmutador *de $x$ e $y$ es*

$$(x, y) = x^{-1}x^y = x^{-1}y^{-1}xy.$$

*Se llama* subgrupo derivado *o* subgrupo conmutador *de $G$ al subgrupo $G'$ de $G$ generado por los conmutadores de los elementos de $G$. O sea*

$$G' = \langle (x, y) : x, y \in G \rangle.$$

**Ejemplo 9.2** Si $(a_1\ a_2\ \dots\ a_k)$ es un $k$-ciclo en $S_n$ y $\sigma \in S_n$ entonces

$$(a_1\ a_2\ \dots\ a_k)^\sigma = (\sigma^{-1}(a_1)\ \sigma^{-1}(a_2)\ \dots\ \sigma^{-1}(a_k)). \tag{9.1}$$

Si $a, b$ y $c$ son tres elementos distintos de $\{1, 2, ..., n\}$ entonces

$$((a\ b), (a\ c)) = (a\ b)(a\ b)^{(a\ c)} = (b\ c)(a\ c) = (a\ b\ c).$$

Eso implica que todos los tres ciclos de $S_n$ están en $A_n$, y como $A_n$ está generado por los 3-ciclos tenemos que $A_n \subseteq S_n'$. De hecho se verifica la igualdad pues si $\sigma, \tau \in S_n$ entonces $\sigma^\tau$ tiene la misma paridad que $\sigma$ y $\sigma^{-1}$, lo que implica que $(\sigma, \tau) = \sigma^{-1}\sigma^\tau \in A_n$.

El siguiente lema recopila las propiedades fundamentales de los conmutadores y el subgrupo derivado. La demostración es un sencillo ejercicio.

**Lema 9.3** *Dados un grupo $G$ y elementos $a, b \in G$, entonces*

*(1) $(a, b) = 1$ si y solo si $ab = ba$.*

*(2) $G$ es abeliano si y solo si $G' = 1$.*

*(3) $(a, b)^{-1} = (b, a)$.*

*(4) $G'$ consiste en los productos finitos de conmutadores.*

*(5) Si $f : G \to H$ es un homomorfismo de grupos entonces $f((a,b)) = (f(a), f(b))$.*

*(6) En particular, si $N$ es normal en $G$, entonces $(a,b)N = (aN, bN)$ en $G/N$.*

*(7) $(a,b)^x = (a^x, b^x)$ para cada $x \in G$.*

**Teorema 9.4** *Dado un grupo $G$, su subgrupo derivado $G'$ es el menor subgrupo normal de $G$ que da un cociente abeliano; es decir, se verifican:*

*(1) $G'$ es un subgrupo normal de $G$.*

*(2) El cociente $G/G'$ es abeliano.*

*(3) Si $N$ es un subgrupo normal de $G$ tal que el cociente $G/N$ es abeliano, entonces $G' \subseteq N$.*

**Demostración.** 1. Vemos que, si $g \in G'$ y $x \in G$, entonces $g^x \in G'$. En efecto, por el Lema 9.3, se tiene $g = (a_1, b_1) \cdots (a_n, b_n)$ para ciertos elementos $a_1, \ldots, a_n, b_1, \ldots, b_n$ de $G$, y por tanto

$$g^x = (a_1, b_1)^x \cdots (a_n, b_n)^x = (a_1^x, b_1^x) \cdots (a_n^x, b_n^x) \in G'.$$

2. Es una consecuencia inmediata de los apartados 2 y 6 del Lema 9.3.

3. Si $N$ es como en el enunciado y $a, b \in G$, entonces $(a,b)N = (aN, bN) = N$, luego $(a,b) \in N$. Es decir, $N$ contiene a cada conmutador de $G$ y en consecuencia contiene a $G'$. □

El Teorema 9.4 nos dice que, en cierto sentido, $G'$ convierte a $G$ en un grupo abeliano perdiendo la menor información posible (si entendemos que al hacer el cociente por un subgrupo normal $N$ se pierde la información sobre $N$, pues sus elementos representan al neutro en el cociente). En consecuencia, cuanto más pequeño es $G'$, más cerca está $G$ de ser abeliano. En la próxima sección consideraremos una manera más precisa de medir lo lejos que está $G$ de ser abeliano. Concluimos ésta con un ejemplo.

**Ejemplo 9.5** *El subgrupo derivado del grupo diédrico $D_n$.*

Si ponemos $D_n = \{1, a, a^2, \ldots, a^n, b, ab, \ldots, a^{n-1}b\}$, entonces $A = \langle a \rangle$ es un subgrupo de índice 2 de $D_n$, con lo que $A$ es normal en $D_n$ y $D_n/A$ es abeliano. Por tanto $D_n' \subseteq A$. Además $(b,a) = (a,b)^{-1} = (a^{-1}a^b)^{-1} = a^2$, con lo que $B = \langle a^2 \rangle \subseteq D_n' \subseteq A$. Si $n$ es impar, entonces $B = A$, con lo que en tal caso $D_n' = A$. En caso contrario, es decir si $n$ es par, entonces $B = \langle a^2 \rangle$ es un subgrupo normal de orden $n/2$ (¿por qué?) y por tanto $D_n/B$ es también abeliano (¿por qué?). Por tanto, si $n$ es par entonces $D_n' \subseteq B$. En resumen

$$D_n' = \begin{cases} \langle a \rangle & \text{si } 2 \nmid n \\ \langle a^2 \rangle & \text{si } 2 | n \end{cases}$$

## 9.2 Grupos resolubles

Recordemos que $N \trianglelefteq G$ (ó $G \trianglerighteq N$) significa que $N$ es un subgrupo normal de $G$, mientras que $N \triangleleft G$ (ó $G \triangleright N$) significa que $N$ es un subgrupo normal propio de $G$.

**Definición 9.6** *Sea $G$ un grupo. Se define por recurrencia el $t$-ésimo* derivado *del grupo $G$, denotado $G^{(t)}$ (donde $t \in \mathbb{Z}^+$) del modo siguiente:*

- *$G^{(1)} = G'$, el derivado de $G$.*
- *$G^{(t+1)} = (G^{(t)})'$, el derivado de $G^{(t)}$.*

*La cadena de subgrupos*

$$G \trianglerighteq G' \trianglerighteq G^{(2)} \trianglerighteq \cdots$$

*se conoce como la* serie derivada *de $G$, y se dice que $G$ es* resoluble *si su serie derivada alcanza al grupo trivial; es decir, si existe $t \geq 1$ tal que $G^{(t)} = 1$.*

Es evidente que todo grupo abeliano $G$ es resoluble pues $G' = 1$. Un ejemplo de grupo resoluble no abeliano es el grupo diédrico $D_n$, con $n \geq 3$, pues $D_n'$ es abeliano como vimos en el Ejemplo 9.5 y por tanto $D_n'' = 1$. En los siguientes ejemplos veremos otros grupos resolubles, y también otros que no lo son. Usaremos el hecho obvio de que, en cuanto un término se repite en la serie derivada, ésta *se estabiliza* en ese término; es decir, si $G^{(t)} = G^{(t+1)}$ entonces $G^{(t)} = G^{(t+k)}$ para cualquier $k \geq 1$.

**Ejemplos 9.7** *Resolubilidad de los grupos simétricos*

(1) Por el Ejemplo 9.2, tenemos que $S_n' = A_n$. Cuando $n \leq 3$ tenemos $A_n$ es abeliano. Por tanto, si $n \leq 3$ entonces $S_n'' = 1$, con lo que $S_n$ es resoluble.

(2) $A_4$ tiene orden 12 y aplicando (9.1) es fácil ver que el siguiente es un subgrupo normal de $A_4$:

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

Como $A_4$ no es abeliano y $A_4/V$ sí lo es (tiene orden 3), del Teorema 9.4 se deduce que $V = A_4' = S_4^{(2)}$. Como $V$ es abeliano, deducimos que $S_4^{(3)} = 1$. En consecuencia, $S_4$ es resoluble con serie derivada $S_4 \rhd A_4 \rhd V \rhd 1$.

(3) Si $n \geq 5$, por el Teorema de Abel (Teorema 6.24 de GyA) $A_n$ es simple, es decir no tiene ningún subgrupo normal propio no trivial. Por tanto $A_n' = 1$ ó $A_n' = A_n$. Pero como $A_n$ no es abeliano, necesariamente $A_n' = A_n$. Es decir, la serie derivada de $S_n$ se estabiliza en $A_n$ y nunca alcanza al grupo trivial. En consecuencia, ni $S_n$ ni $A_n$ son resolubles cuando $n \geq 5$.

Vamos a estudiar las propiedades básicas de los grupos resolubles, y comenzamos con un lema.

**Lema 9.8** *Sea $f : G \to H$ un homomorfismo de grupos. Entonces:*

*(1) $f(G^{(t)}) \subseteq H^{(t)}$ para cada $t \geq 1$.*

*(2) Si $f$ es suprayectiva entonces $f(G^{(t)}) = H^{(t)}$ para cada $t \geq 1$.*

**Demostración.** 1. Razonamos por inducción en $t$. Como $f((a,b)) = (f(a), f(b))$ para cualesquiera $a, b \in G$, se tiene $f(G') \subseteq H'$. El caso general lo vemos por inducción en $t$, con el caso $t = 1$ resuelto por lo anterior. Si el resultado vale para cierto entero positivo $t$ entonces $f$ se restringe a un homomorfismo $f : G^{(t)} \to H^{(t)}$, y aplicando a éste el caso $t = 1$ deducimos que $f(G^{(t+1)}) = f((G^{(t)})') \subseteq (H^{(t)})' = H^{(t+1)}$, lo que completa la demostración.

2. Supongamos ahora que $f$ es suprayectiva, y sea $(u, v)$ un conmutador en $H$. Tomando $a, b \in G$ con $f(a) = u$ y $f(b) = v$ se tiene $f((a,b)) = (u,v)$, lo que prueba que $(u,v) \in f(G')$; es decir, $H' \subseteq f(G')$, y el apartado anterior nos da la igualdad. El caso general se demuestra por inducción como antes. □

**Proposición 9.9** *Sea $G$ un grupo con un subgrupo $H$ y un subgrupo normal $N$. Se verifican:*

*(1) Si $G$ es resoluble entonces $H$ es resoluble (los subgrupos de resolubles son resolubles).*

*(2) Si $G$ es resoluble entonces $G/N$ es resoluble (los cocientes de resolubles son resolubles).*

*(3) Si $N$ y $G/N$ son resolubles entonces $G$ es resoluble.*

**Demostración.** 1. Aplicando el Lema 9.8 a la inclusión $H \hookrightarrow G$, tenemos $H^{(t)} \subseteq G^{(t)}$ para cada $t \geq 1$. Si $G$ es resoluble entonces existe un $t$ tal que $G^{(t)} = 1$ y por tanto $H^{(t)} = 1$, por lo que $H$ es resoluble.

2. El Lema 9.8 aplicado a la proyección canónica $p : G \to G/N$ nos dice que $p(G^{(t)}) = (G/N)^{(t)}$ para cada $t \geq 1$. Si $G$ es resoluble entonces existe un $t$ tal que $G^{(t)}$ es trivial, y por tanto $(G/N)^{(t)} = p(G^{(t)}) = p(1) = 1$ también es trivial, por lo que $G/N$ es resoluble.

3. Supongamos que $N$ y $G/N$ son resolubles. Como $G/N$ es resoluble, existe $t \geq 1$ tal que $(G/N)^{(t)} = 1$. Aplicando como antes el Lema 9.8 deducimos que $p(G^{(t)})$ es trivial, lo que significa que $G^{(t)} \subseteq \operatorname{Ker} p = N$. Como $N$ es resoluble, por el apartado 1, $G^{(t)}$ es resoluble; es decir, existe $s \geq 1$ tal que $(G^{(t)})^{(s)} = 1$. Como es claro que $(G^{(t)})^{(s)} = G^{(t+s)}$, deducimos que $G$ es resoluble. □

Esto nos permite encontrar otros ejemplos de grupos resolubles:

**Proposición 9.10** *Todo p-grupo finito $G$ es resoluble.*

**Demostración.** Razonamos por inducción sobre el orden de $G$. No hay nada que demostrar si $|G| = 1$, con lo que supongamos que $G$ no es trivial y la hipótesis de inducción. De la Proposición 5.15 de GyA, se deduce que $Z(G) \neq 1$ y de la hipótesis de inducción que $G/Z(G)$ es resoluble. Como $Z(G)$ también es resoluble, del tercer apartado de la Proposición 9.9 deducimos que $G$ es resoluble. □

La serie derivada de un grupo resoluble sugiere la siguiente definición más general:

**Definición 9.11** *Sea $G$ un grupo arbitrario. Una* serie subnormal *de $G$ es una cadena de subgrupos de $G$ de la forma*

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_{n-1} \trianglerighteq G_n = 1$$

*(es decir, es una cadena finita que empieza en $G$ y termina en 1 (o viceversa) y en la que cada subgrupo es normal en el anterior). Los grupos $G_i$ se llaman* términos *de la serie, el número $n$ es la* longitud *de la serie, y cada grupo cociente $G_{i-1}/G_i$ (para $i = 0, 1, \ldots, n$) se llama un* factor *de la serie.*

*Obsérvese que la longitud $n$ mide el número de factores, y no el de términos (que es $n + 1$).*

*Si cada $G_i$ es normal en $G$ entonces se dice que se trata de una* serie normal.

*Una* serie abeliana *es una serie subnormal cuyos factores son abelianos y una* serie cíclica *es una serie subnormal con factores cíclicos.*

Obsérvese que la serie derivada es una serie normal abeliana (tal vez infinita). Por definición un grupo es resoluble si su serie derivada es una serie subnormal de $G$, que resulta ser abeliana. De hecho esta propiedad caracteriza los grupos resolubles.

**Teorema 9.12** *Un grupo $G$ es resoluble si y solo si admite una serie subnormal abeliana.*

**Demostración.** Si $G$ es resoluble entonces su serie derivada es una serie normal con factores abelianos, lo que nos da el "sólo si". Recíprocamente, supongamos que $G$ tiene una serie subnormal como la de la Definición 9.11 con todos los factores abelianos, y veamos que $G$ es resoluble por inducción en la longitud $n$ de la serie. Si $n = 1$ entonces $G$ es el único factor de la serie, por lo que es abeliano y en consecuencia resoluble. En el caso general, la hipótesis de inducción aplicada a $G_1$ nos dice que éste es resoluble (tiene una serie de longitud $n - 1$ con factores abelianos), y como $G/G_1$ también es resoluble (de hecho es abeliano, por ser un factor de la serie inicial), la Proposición 9.9 nos dice que $G$ es resoluble, como queríamos ver. □

**Teorema 9.13** *Las siguientes condiciones son equivalentes para un grupo finito $G$.*

*(1) $G$ es resoluble.*

*(2) $G$ admite una serie abeliana.*

*(3) $G$ admite una cíclica.*

*(4) $G$ admite una serie normal con todos sus factores de orden primo.*

**Demostración.** Ya sabemos que 1 y 2 son equivalentes. 3 implica 2 es evidente y 4 implica 3 es consecuencia de que todo grupo de orden primo es cíclico. Sólo falta demostrar 1 implica 4.

Supongamos pues que $G$ es resoluble y razonamos por inducción sobre el orden de $G$, con el caso en que este orden es 1 trivial. Supongamos pues que $G \neq 1$ y la hipótesis de inducción. Distinguiremos dos casos.

Supongamos primero que $G$ es simple. Eso implica que $G' = 1$ y por tanto $G = 1$ o $G$ es abeliano simple lo que implica que $G$ tiene orden primo.

En caso contrario $G$ tiene un subgrupo normal propio no trivial $N$. De la Proposición 9.9 deducimos que $N$ y $G/N$ son resolubles y por tanto admiten series normales con factores de orden primo:

$$N = N_0 \trianglerighteq N_1 \trianglerighteq N_2 \trianglerighteq \cdots \trianglerighteq N_n = 1$$

y

$$G/N = G_0/N \trianglerighteq G_1/N \trianglerighteq G_2/N \trianglerighteq \cdots \trianglerighteq G_m/N = 1.$$

Entonces

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_m = N = N_0 \trianglerighteq N_1 \trianglerighteq N_2 \trianglerighteq \cdots \trianglerighteq N_n = 1$$

es una serie normal con factores de orden primo. □

# Problemas

**9.1** Obtener una expresión para los conmutadores $(a, bc)$ y $(ab, c)$ en términos de los conmutadores $(a, b), (a, c)$ y $(b, c)$, donde $a, b$ y $c$ son elementos de un grupo

**9.2** Recuérdese que un subgroup $H$ de un grupo $G$ se dice que es *característico* si $\alpha(H) = H$ para todo automorfismo de $G$. Demostrar que el subgrupo derivado de un grupo $G$ es un subgrupo característico de $G$. Deducir que todos los términos de la serie derivada de $G$ son característicos, y por tanto normales, en $G$.

**9.3** Probar que si $G$ es resoluble y no trivial entonces $G' \neq G$.

**9.4** Probar que si $G$ es simple y resoluble entonces $G$ es cíclico de orden

primo.

**9.5** Formar todas las series con factores de orden primo para un grupo cíclico de orden 20.

**9.6** Probar que, si $H$ y $K$ son dos subgrupos normales de $G$, entonces $(H, K) = \langle (h, k) : h \in H, k \in K \rangle$ es un subgrupo normal de $G$ que está contenido en $H \cap K$.

**9.7** Dados un grupo finito $G$ y un entero positivo primo $p$, demostrar la equivalencia de las siguientes condiciones:

(1) El orden de $G$ es una potencia de $p$.

(2) El orden de cada elemento de $G$ es una potencia de $p$.

**9.8** Sea $n \geq 5$ un entero. Encontrar $\sigma, \tau \in A_n$ tales que $(\sigma, \tau) = (1, 2, 3)$, y usar esto para demostrar que $A_n$ no es resoluble sin utilizar el Teorema de Abel.

**9.9** Demostrar que $G \times H$ es resoluble precisamente si $G$ y $H$ lo son.

**9.10** Demostrar que para cada $n \in \mathbb{N}$ existe un grupo resoluble $G$ tal que $G^{(n)} \neq \{1\}$. Utilizar esto para mostrar que el producto directo infinito de grupos resolubles puede no ser resoluble. (Indicación: En la primera parte, usar el isomorfismo $S_3 \simeq \mathrm{Aut}(S_3)$).

**9.11** Probar que si un grupo $G$ es resoluble y $G/Z(G)$ es simple entonces $G$ es abeliano.

**9.12** Probar que si $G$ es un grupo no abeliano de orden $p^3$ (con $p$ primo), entonces $G' = Z(G)$ y $G/G' \simeq C_p \times C_p$.

**9.13** Demostrar que un grupo finito abeliano tiene una única serie con factores de orden primo si y solo si es un $p$-grupo cíclico, para algún primo $p$. ¿Es cierto esto si el grupo no es abeliano?

**9.14** Sean $H$ y $K$ dos subgrupos normales de un grupo $G$. Demostrar que si $G/H$ y $G/K$ son resolubles, entonces $G/H \cap K$ es resoluble.

**9.15** Demostrar que si $G$ es un grupo cuyo orden es una potencia de un primo, entonces $G$ es resoluble.

**9.16** Sea $G$ un grupo. Para cada $n \in \mathbb{N}$ definimos el *$n$-ésimo centro* $Z_n(G)$ de $G$ por recurrencia de la siguiente forma: $Z_0(G) = \{1\}$. Supongamos que hemos definido $Z_n(G)$ que resulta ser un subgrupo normal de $G$. Entonces $Z_{n+1}(G)$ es el único subgrupo (normal) de $G$ que verifica

$$Z_{n+1}(G)/Z_n(G) = Z(G/Z_n(G)).$$

En particular, $Z_1(G)$ es el centro de $G$. La cadena de subgrupos

$$\{1\} = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \cdots$$

se conoce como la *serie central (ascendente)* de $G$. Se dice que $G$ es *nilpotente* si $Z_n(G) = G$ para algún $n$; es decir, si la serie central alcanza al grupo $G$ en algún paso. Demostrar:

(1) Todo grupo abeliano es nilpotente.

(2) $Z_n(G) = \{x \in G : (x, y) \in Z_{n-1}(G) \text{ para todo } y \in G\}$.

(3) Todo $p$-grupo finito ($p$ primo) es nilpotente.

(4) Un grupo $G$ es nilpotente precisamente si tiene una serie normal

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

tal que $G_i/G_{i-1} \subseteq Z(G/G_{i-i})$ para todo $i = 1, 2, \ldots, n$.

(5) Todo grupo nilpotente es resoluble.

(6) Dar un ejemplo de un grupo resoluble que no sea nilpotente.

(7) Si $G$ es nilpotente y $H$ es un subgrupo de $G$, entonces $H$ es nilpotente.

(8) Si $G$ es nilpotente y $N$ es un subgrupo normal de $G$, entonces $G/N$ es nilpotente.

(9) Dar un ejemplo de un grupo $G$ con un subgrupo normal $N$ tales que $N$ y $G/N$ sean nilpotentes y $G$ no lo sea.

(10) Demostrar que si $G$ y $H$ son dos grupos nilpotentes, entonces $G \times H$ es un grupo nilpotente.

**9.17** Sea $n$ un entero positivo. En lugar de la habitual interpretación del grupo simétrico $S_n$ como el grupo de las permutaciones de $\{1, 2, \ldots, n\}$ lo vamos a ver como el grupo de las permutaciones del anillo $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ de restos módulo $n$.

(1) Demostrar que $\mathcal{A}_n = \mathbb{Z}_n^* \times \mathbb{Z}_n$ es un grupo con el siguiente producto.

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1).$$

(2) Demostrar que si $n = p$ es primo y $(a, b) \in \mathcal{A}_n$ tiene orden $p$, entonces $a = 1$.

(3) Demostrar que para cada $(a, b) \in \mathcal{A}_n$, la aplicación $\sigma_{a,b} : \mathbb{Z}_n \to \mathbb{Z}_n$ dada por

$$\sigma_{a,b}(x) = ax + b$$

es un elemento de $S_n$. (Las operaciones suma y producto son las operaciones en el anillo $\mathbb{Z}_n$.

(4) Demostrar que si $\sigma \in S_n$ y $b \in \mathbb{Z}_n$ verifican $\sigma_{1,1}\sigma = \sigma\sigma_{1,b}$, entonces $\sigma(x) + 1 = \sigma(x + b)$. Utilizar esto para demostrar que si $n = p$ es primo, entonces $b \in \mathbb{Z}_p^*$ y $\sigma = \sigma_{b^{-1},\sigma(0)}$.

(5) Mostrar que la aplicación $(a, b) \mapsto \sigma_{a,b}$ es un homomorfismo inyectivo $\mathcal{A}_n \to S_n$.

(6) Consideramos el grupo $\mathrm{GL}_2(\mathbb{Z}_n)$ de matrices invertibles cuadradas de tamaño 2 con entradas en $\mathbb{Z}_n$, es decir:

$$\mathrm{GL}_2(\mathbb{Z}_n) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_n, ad - bc \neq 0\}$$

Demostrar que la aplicación

$$(a, b) \to \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

es un homomorfismo inyectivo de $\mathcal{A}_n$ en $\mathrm{GL}_2(\mathbb{Z}_n)$.

En el resto del ejercicio vamos a identificar $\mathcal{A}_n$ con las imágenes de los dos homomorfismos inyectivos $\mathcal{A}_n \to S_n$ y $\mathcal{A}_n \to \mathrm{GL}_2(\mathbb{Z}_n)$. Este grupo (visto de cualquiera de las tres formas) lo llamamos *$n$-ésimo grupo afín*. Un subgrupo de $S_n$ se dice que es un *grupo afín* si es conjugado en $S_n$ de un subgrupo de $\mathcal{A}_n$, es decir, un subgrupo afín de $S_n$ es un grupo de la forma $\sigma^{-1}H\sigma$, donde $\sigma \in S_n$ y $H$ es un subgrupo de $\mathcal{A}_n$.

(7) Demostrar que si $\sigma$ es un $n$-ciclo, entonces $\langle\sigma\rangle$ es un subgrupo afín de $S_n$.

(8) Demostrar que todo grupo afín es resoluble.

**9.18** Sea $G$ un subgrupo de $S_n$ que seguimos viendo como el grupo de las biyecciones de $\mathbb{Z}_n$ y lo consideramos actuando en $\mathbb{N}_n$ de la forma habitual $\sigma \cdot n = \sigma(n)$. Las órbitas de esta acción las llamamos $G$-órbitas y forman una partición de $\mathbb{Z}_n$.

Decimos que $G$ es transitivo si para todo $x, y \in \mathbb{Z}_n$ existe $\sigma \in G$ tal que $\sigma(x) = y$.

Demostrar:

(1) $G$ es transitivo si y solo si hay una única $G$-órbita.

(2) Si $G$ es transitivo, entonces $n$ es un divisor de $|G|$.

(3) Si $G$ es transitivo y $N$ es un subgrupo normal de $G$, entonces cada $N$-órbita tiene un cardinal divisor de $n$.

(4) Supongamos que $p$ es primo y

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = 1$$

es una serie normal con factores primos para todo $i = 1, 2, \ldots, n$. Demostrar que si $G$ es transitivo, entonces $G_1, \ldots, G_{n-1}$ son transitivos y $G_{n-1}$ tiene orden $p$. (Indicación: Razonar por inducción sobre $i$, para demostrar que $G_i$ es transitivo, si $i < n$.)

(5) Demostrar que si $p$ es primo y $G$ es un subgrupo transitivo de $S_p$, entonces $G$ es resoluble si y solo si $G$ es afín.

# Capítulo 10

# Extensiones radicales

En este capítulo sentamos las bases para poder resolver el problema que nos planteamos desde el principio o sea ¿es posible obtener una expresión de las raíces de un polinomio en términos de los coeficientes utilizando solamente las cuatro operaciones aritméticas elementales, suma, producto, división y resta, además de la extracción de raíces $n$-ésimas? Si llamamos $K$ a un cuerpo que contenga los coeficientes del polinomio las raíces buscadas estarían en un cuerpo $L$ de forma que se podría pasar desde $K$ hasta $L$ en un número finito de pasos de forma que en cada paso pasamos de un cuerpo más pequeño $E$ a otro de la forma $E(\alpha)$ con $\alpha^n \in E$ para algún entero positivo $n$. Esto es la base del siguiente tipo de extensiones que vamos a estudiar.

## 10.1 Extensiones radicales

Comenzamos recordando la definición de torre radical y polinomio resoluble.

**Definición 10.1** *Una* torre radical *es una torre de cuerpos*

$$E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n$$

*tal que para cada $i = 1, \ldots, n$, existen $n_i \geq 0$ y $\alpha_i \in E_i$ tales que $E_i = E_{i-1}(\alpha_i)$ y $\alpha^{n_i} \in E_{i-1}$.*

*Una* extensión *de cuerpos $L/K$ se dice que es* radical *si existe una torre radical*

$$K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = L. \tag{10.1}$$

*Una ecuación polinómica $P(X) = 0$, con $P \in K[X]$, se dice que es* resoluble por radicales *sobre $K$ si existe una extensión radical $L/K$ tal que $P$ es completamente factorizable en $L$. En tal caso también se dice que el polinomio $P$ es resoluble por radicales sobre $K$.*

Veamos algunas propiedades elementales de las extensiones radicales.

**Lema 10.2** *Sea $L/K$ una extensión de cuerpos y sean $E, F \in \mathrm{Sub}(L/K)$.*

*(1) Si $E/K$ y $L/E$ son radicales entonces $L/K$ es radical.*

*(2) Si $E/K$ es radical, entonces $EF/F$ es radical, es decir, la clase de extensiones radicales es cerrada para levantamientos.*

*(3) Si $L/K$ es radical, entonces $L/E$ es radical.*

*(4) Si $E/K$ y $F/K$ son radicales, entonces $EF/K$ es radical.*

*(5) Si $L/K$ es radical y $N$ es la clausura normal de $L$ sobre $K$, entonces $N/K$ es radical.*

**Demostración.** (1) es obvio.

(2) Si $E/K$ admite una torre radical como en (10.1) entonces

$$F = E_0F \subseteq E_1F \subseteq \cdots \subseteq E_nF = EF$$

es una torre radical, pues si $E_i = E_{i-1}(\alpha_i)$ y $\alpha_i^{r_i} \in E_{i-1}$, entonces $E_iF = E_{i-1}F(\alpha_i)$.

(3) es consecuencia de (2), pues $L = LE$.

(4) es consecuencia de (1) y (2).

(5) Supongamos que $L/K$ es radical con torre radical como en (10.1). Para cada $i = 1, \ldots, n$ sean $\beta_{i1}, \ldots, \beta_{ik_i}$ las raíces de $\mathrm{Min}(\alpha_i, K)$ en una clausura algebraica de $L$. Entonces $N = K(\beta_{ij} : 1 \leq i \leq n, 1 \leq j \leq k_i)$ es una clausura normal de $L/K$. Entonces $E_{i-1}(\beta_{ij})$ es $E_{i-1}$-isomorfo a $E_{i-1}(\alpha_i) = E_i$ y $\beta_{ij}^{n_i} = \alpha_i^{n_i} \in E_{i-1}$ para todo $j$ y por tanto la torre

$$K = F_0 \subseteq F_{11} = F_0(\beta_{11}) \subseteq F_{12} = F_{11}(\beta_{12}) \subseteq \ldots F_{1k_1} = F_{1(k_1-1)}(\beta_{1k_1}) \subseteq F_{21} = F_{1k_1}(\beta_{21}) \subseteq \cdots \subseteq F_{nk_n} = N$$

es una torre radical. Luego $N/K$ es una extensión radical. □

## 10.2 Caracterización de extensiones radicales

**Lema 10.3** *Si $L = K(\alpha)$ con $\alpha$ separable sobre $K$ y $\alpha^r \in K$ para algún entero positivo $r$, entonces existe un entero positivo $s$ tal que $\alpha^s \in K$ y $s$ no es múltiplo de* $\mathrm{car}(K)$.

**Demostración.** Si $\mathrm{car}(K) = 0$ no hay nada que demostrar, con lo que podemos suponer que $\mathrm{car}(K) = p \neq 0$. Pongamos $r = p^t s$, con $p \nmid s$, $a = \alpha^r \in K$ y $\beta = \alpha^s$. Entonces $a = \beta^{p^t}$, es decir $\beta$ es raíz del polinomio $f = X^{p^t} - a$. De hecho $\beta$ es la única raíz de $f$ pues $f = X^{p^t} - \beta^{p^t} = (X - \beta)^{p^t}$. Si $g = \mathrm{Min}(\beta, K)$, entonces $g$ divide a $f$, con lo que $g$ sólo tiene una raíz. Sin embargo, como $\alpha$ es separable sobre $K$, $K(\alpha)/K$ es separable (Corolario 5.14), con lo que $\beta$ es separable sobre $K$ y por tanto $[K(\beta) : K] = [K(\beta) : K] = 1$, es decir $\alpha^s = \beta \in K$. □

**Teorema 10.4** *Si $L/K$ es una extensión radical, entonces* $\mathrm{Gal}(E/K)$ *es resoluble para todo $E \in$* $\mathrm{Sub}(L/K)$.

**Demostración.** Supongamos que $L/K$ es una extensión radical y sea $E \in \mathrm{Sub}(L/K)$. Vamos a considerar varios casos cada vez más generales y utilizaremos repetidamente las propiedades de los grupos resolubles que vimos en la Proposición 9.9.

*Caso 1. $E = L$ y $L/K$ es de Galois.*

Sea

$$K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_r = L$$

una torre radical y supongamos $E_i = E_{i-1}(\alpha_i)$ con $\alpha_i^{s_i} \in E_{i-1}$. Por el Lema 10.3, podemos suponer que $s_i$ no es múltiplo de la característica de $K$. Entonces $n = s_1 \cdots s_r$ no es múltiplo de la característica de $K$ y por tanto existe una raíz $n$-ésima primitiva de la unidad $\xi$ en una extensión de $L$. Entonces $L(\xi)/K(\xi)$ es una extensión radical de Galois (Lema 10.2) y de hecho

$$\overline{K} = K(\xi) = \overline{E_0} = E_0(\xi) \subseteq \overline{E_1} = E_1(\xi) \subseteq \cdots \subseteq \overline{E_r} = E_r(\xi) = L(\xi) = \overline{L}$$

es una torre radical. Como $L/K$ es de Galois, de la Proposición 3.15 y el Corolario 5.14 deducimos que $\overline{L}/K$ es de Galois. Por otro lado, $E_i$ es el cuerpo de descomposición de $X^{s_i} - \alpha_i^{s_i}$ sobre $E_{i-1}$ y de la Proposición 8.7 deducimos que $\overline{E_i}/\overline{E_{i-1}}$ es una extensión cíclica para todo $i$. Por tanto la última torre de cuerpos da lugar, por el Teorema Principal de la Teoría de Galois, a una sucesión de subgrupos de $\mathrm{Gal}(\overline{L}/\overline{K})$:

$$\mathrm{Gal}(\overline{L}/\overline{K}) = \mathrm{Gal}(\overline{L}/\overline{E_0}) \geq \mathrm{Gal}(\overline{L}/\overline{E_1}) \geq \cdots \geq \mathrm{Gal}(\overline{L}/\overline{E_r}) = 1.$$

Como $\overline{E_i}/\overline{E_{i-1}}$ es de Galois, $\mathrm{Gal}(\overline{L}/\overline{E_i}) \trianglelefteq \mathrm{Gal}(\overline{L}/\overline{E_{i-1}})$, . Además

$$\mathrm{Gal}(\overline{L}/\overline{E_{i-1}})/\mathrm{Gal}(\overline{L}/\overline{E_i}) \simeq \mathrm{Gal}(\overline{E_i}/\overline{E_{i-1}})$$

es cíclico. Esto demuestra que $\mathrm{Gal}(\overline{L}/\overline{K})$ es resoluble. Como $\mathrm{Gal}(\overline{L}/K)/\mathrm{Gal}(\overline{L}/\overline{K}) \simeq \mathrm{Gal}(\overline{K}/K)$ y $\overline{K}/K = K(\xi)/K$ es de Galois, con grupo de Galois abeliano, de la Proposición 9.9 deducimos que $\mathrm{Gal}(\overline{L}/K)$ es resoluble. Por otro lado $L/K$ es de Galois, por hipótesis, y aplicando una vez más el Teorema 6.11 deducimos que $\mathrm{Gal}(\overline{L}/L) \trianglelefteq \mathrm{Gal}(\overline{L}/K)$ y $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\overline{L}/K)/\mathrm{Gal}(\overline{L}/L)$, que es resoluble por serlo $\mathrm{Gal}(\overline{L}/K)$.

*Caso 2. $E = L$.*

Sea $F = \{x \in L : \sigma(x) = x, \text{ para todo } \sigma \in \mathrm{Gal}(L/K)\}$. Entonces $L/F$ es de Galois, por el Teorema 6.9, y radical, por el Lema 10.2. Por el Caso 1, $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/F)$ es resoluble.

*Caso 3. $E/K$ es de Galois.*

Sea $N$ la clausura normal de $L$ sobre $K$. Del Lema 10.2 deducimos que $N/K$ es radical, con lo que del Caso 2, deducimos que $\mathrm{Gal}(N/K)$ es resoluble. Por otro lado, como $E/K$ es normal, para todo $\sigma \in \mathrm{Gal}(N/K)$ se verifica que la restricción $\sigma|_E$ de $\sigma$ a $E$ es un elemento de $\mathrm{Gal}(E/K)$ (Teorema 3.11) y la aplicación

$$\begin{array}{rccc} \phi: & \mathrm{Gal}(N/K) & \to & \mathrm{Gal}(E/K) \\ & \sigma & \mapsto & \sigma|_E \end{array}$$

es un homomorfismo de grupos. Además, como $N/K$ es normal, todo elemento de $\mathrm{Gal}(E/K)$ extiende a un elemento de $\mathrm{Gal}(N/K)$, o lo que es lo mismo $\phi$ es suprayectiva. Esto muestra que $\mathrm{Gal}(E/K)$ es isomorfo a un cociente de $\mathrm{Gal}(N/K)$ y como este último es resoluble, aquel también lo es.

*Caso General.* De forma similar a como lo hicimos en el Caso 2, ponemos $F = \{x \in E : \sigma(x) = x, \text{ para todo } \sigma \in \mathrm{Gal}(E/K)\}$. Entonces $E/F$ es de Galois y $L/F$ es radical. Por el Caso 3 deducimos que $\mathrm{Gal}(E/K) = \mathrm{Gal}(E/F)$ es resoluble. □

El siguiente teorema es una especie de recíproco del Teorema 10.4.

**Teorema 10.5** *Si $L/K$ es una extensión finita de Galois con grupo de Galois resoluble y $[L : K]$ no es múltiplo de la característica de $K$, entonces existe una extensión $R$ de $L$ tal que $R/K$ es radical.*

**Demostración.** Vamos a razonar por inducción sobre $n = [L : K]$, con el caso $n = 1$ trivial. Supongamos pues que $L/K$ satisface las hipótesis del teorema con $n = [L : K] > 1$ y la hipótesis de inducción. Pongamos $G = \mathrm{Gal}(L/K)$. Como $G$ es resoluble, del Teorema 9.13 se deduce que $G$ tiene un subgrupo normal $N$ de índice primo $p$. Como $n$ no es múltiplo de la característica de $K$, $p$ es diferente de esta característica, y por tanto una extensión de $L$ contiene una raíz $p$-ésima primitiva de la unidad $\xi$. Como $L/K$ es de Galois, también lo es $L(\xi)/K(\xi)$ (¿por qué?). Además, la restricción $\sigma \mapsto \sigma|_L$ induce un homomorfismo de grupos

$$\Phi : \overline{G} = \mathrm{Gal}(L(\xi)/K(\xi)) \to G = \mathrm{Gal}(L/K)$$

que es inyectivo, pues si $\sigma, \tau \in \overline{G}$ satisface $\sigma|_L = \tau|_L$, como además, $\sigma(\xi) = \tau(\xi) = \xi$ se tiene que $\sigma = \tau$.

Si $\Phi$ no fuera suprayectiva tendríamos $[L(\xi) : K(\xi)] = |\overline{G}| < |G| = [L : K]$ y, por la hipótesis de inducción deducimos que $L(\xi)/K(\xi)$ es radical. Como $K(\xi)/K$ también es radical, deducimos que $L(\xi)/K$ es radical y en este caso ya hemos acabado.

En caso contrario, $\Phi$ es un isomorfismo de grupos, con lo que $\overline{N} = \Phi^{-1}(N)$ es un subgrupo normal de índice $p$ de $\overline{G}$. Por tanto $F = L(\xi)^N = \{x \in L(\xi) : \sigma(x) = x, \text{ para todo } \sigma \in N\}$ es un subcuerpo de $L(\xi)$ tal que $\mathrm{Gal}(L(\xi)/F) = \overline{N}$. Por tanto, por el Teorema 6.11 se tiene que $L(\xi)/F$ es de Galois y $\mathrm{Gal}(L(\xi)/F) = \overline{N}$ es resoluble y tiene orden $n/p$. Por hipótesis de inducción $L(\xi)$ tiene una extensión $R$ tal que $R/F$ es radical. Por la misma razón, como $\overline{N}$ es normal en $\overline{G}$, $F/K(\xi)$ es de Galois y como su grupo de Galois tiene orden primo, $F/K(\xi)$ es una extensión cíclica, de donde se deduce que $F = K(\xi)(\alpha)$ para algún $\alpha \in F$ tal que $\alpha^p \in K(\xi)$ (Teorema 8.8). Por tanto $F/K(\xi)$ es radical. Como $K(\xi)/K$ también es radical, deducimos que $R/K$ es radical. □

## 10.3 El Teorema de Galois

Esta sección culmina los resultados principales de Evariste Galois que caracterizan las ecuaciones resolubles por radicales. Aunque se pueden obtener resultados algo más generales sin suponer que la característica del cuerpo sea 0, nos vamos a restringir a est caso que simplificará algunos argumentos e hipótesis.

**Definición 10.6** *Si $P \in K[X]$, entonces se llama* grupo de Galois *de $P$ sobre $K$ al grupo de Galois de $L/K$, donde $L$ es un cuerpo de descomposición de $P$ sobre $K$.*

Obsérvese que el grupo de Galois de $P$ sobre $K$, en principio depende del cuerpo de des-composición de $P$ elegido, sin embargo, como todos los cuerpos de descomposición de $P$ sobre $K$ son $K$-isomorfos (Proposición 3.9), el grupo de Galois de $P$ sobre $K$, está bien definido salvo isomorfismos y lo denotaremos por $\mathrm{Gal}_K(P)$.

**Teorema 10.7 (Galois)** *Sea $K$ un cuerpo de característica 0 y $P \in K[X]$. Entonces $P$ es resoluble por radicales sobre $K$ si y solo si $\mathrm{Gal}_K(P)$ es resoluble.*

**Demostración.** Supongamos que $P$ es resoluble por radicales sobre $K$. Entonces $P$ es completamente factorizable en una extensión radical $L$ de $K$. Por tanto, $L$ contiene un cuerpo de descomposición $E$ de $P$ y $\mathrm{Gal}_K(P) = \mathrm{Gal}(E/K)$ es resoluble por el Teorema 10.4.

Recíprocamente, supongamos que $\mathrm{Gal}_K(P)$ es resoluble y sea $E$ un cuerpo de descomposición de $P$ sobre $K$. Entonces $\mathrm{Gal}(E/K) = \mathrm{Gal}_K(P)$ es resoluble y, del Teorema 10.5, se deduce que $E$ tiene una extensión $R$ tal que $R/K$ es radical. Entonces $P$ factoriza completamente en $R$, lo que muestra que $P$ es resoluble por radicales. □

# Problemas

Salvo que se diga lo contrario, todos los cuerpos tienen característica 0.

**10.1** Demostrar el Teorema 10.7 cambiando la hipótesis de que $K$ tenga característica 0 por la de que la característica de $K$ no divide a $n!$

**10.2** Sea $L/K$ una extensión de Galois finita tal que para cada dos subcuerpos intermedios $E, F \in \mathrm{Sub}(L/K)$ se verifica que $E \subseteq F$ ó $F \subseteq E$. Demostrar que $L$ está contenido en una extensión radical de $K$.

**10.3** Demostrar que si $L/K$ es una extensión de Galois finita cuyo grado es potencia de un primo, entonces $L$ está contenido en una extensión radical de $K$.

**10.4** Sea $P \in \mathbb{Q}[X]$ irreducible de grado 3 y $L$ el cuerpo de descomposición de $P$ sobre $\mathbb{Q}$.

(1) Demostrar que $\mathrm{Gal}(L/K)$ es cíclico de orden 3 o isomorfo a $S_3$.

(2) Demostrar que $L$ está contenido en una extensión radical $R$ de $K$.

(3) Demostrar que si $R \subseteq \mathbb{R}$, entonces $R/K$ no es normal.

(4) Demostrar que si $L \subseteq \mathbb{R}$, entonces $L/K$ no es radical.

(5) Dar un ejemplo de una extensión $L/K$ que no sea radical pero que esté contenida en una extensión radical de $K$.

# Capítulo 11

# Resolubilidad de ecuaciones por radicales

El Teorema 10.7 resuelve de forma teórica el problema planteado inicialmente sobre la resolubilidad por radicales de las ecuaciones polinómicas pero en la práctica no proporciona las soluciones en los casos en los que sea posible ni una forma efectiva de decidir sobre la resolubilidad. Eso es lo que vamos a ver en este capítulo en el que para simplificar argumentos vamos a suponer que la característica de todos los cuerpos es 0. De esta forma garantizamos que todas las extensiones son separables. En realidad podríamos no utilizar esta hipótesis, pero eso nos obligaría a imponer la condición de que la característica no dividiera al grado de ninguna de las extensiones consideradas. En la práctica las extensiones que consideramos en este capítulo son subextensiones de $L/K$ donde $L$ es el cuerpo de descomposición de un polinomio $p \in K[X]$. Si $n$ es el grado de $p$, entonces $[L : K]$ es un divisor de $n!$, con lo que para garantizar la separabilidad de las extensiones consideradas a partir de un polinomio de grado $n$, bastaría exigir que la característica no dividiera a $n!$. La razón de imponer como hipótesis que la característica sea siempre 0 es evitar resultados sobrecargados de hipótesis. Los alumnos deberían hacer el ejercicio de comprobar en cada caso que se puede cambiar la hipótesis de que $K$ tiene característica 0, por la de que la característica de $K$ no divide a $n!$.

Por otro lado supondremos que $K$ tiene "suficientes" raíces de la unidad, que en la práctica significa que contiene una raíz $n!$-ésima primitiva de la unidad.

## 11.1 La ecuación general de grado $n$

Si $X_1, \ldots, X_n$ son variables independientes, entonces el cuerpo de fracciones de $K[X_1, \ldots, X_n]$ se llama *cuerpo de funciones racionales* de $K$ en $n$ indeterminadas y se denota $K(X_1, \ldots, X_n)$. Si $L/K$ es una extensión de cuerpos y $\alpha_1, \ldots, \alpha_n \in L$. Se dice que $\alpha_1, \ldots, \alpha_n$ son *algebraicamente independientes* sobre $K$ si el homomorfismo de sustitución

$$\begin{array}{rccc} S : S_{\alpha_1,\ldots,\alpha_n} : & K[X_1, \ldots, X_n] & \to & L \\ & f & \mapsto & f(\alpha_1, \ldots, \alpha_n) \end{array}$$

es inyectivo. En tal caso $S$ se puede extender de forma única a un homomorfismo de cuerpos

$$S : K(X_1, \ldots, X_n) \to L.$$

¿Por qué?

**Definición 11.1** *Sean $X, C_1, \ldots, C_n$, $n+1$ variables independientes. El* polinomio general de grado $n$ *es el siguiente polinomio en la variable $X$ con coeficientes en $E = K(C_1, \ldots, C_n)$*

$$G_n = X^n - C_1X^{n-1} + C_2X^{n-2} + \cdots + (-1)^{n-2}C_{n-2}X^2 + (-1)^{n-1}C_{n-1}X + (-1)^nC_n$$

*y la* ecuación general de grado $n$ *es la ecuación $G_n = 0$.*

Obsérvese que hay un polinomio general de grado $n$, para cada característica y que los coeficientes de $G_n$ están en $K_0[C_1, \ldots, C_n]$, donde $K_0$ es el cuerpo primo de la característica dada. Pongamos $E = K(C_1, \ldots, C_n)$, $T_1, \ldots, T_n$ las raíces de $G_n$ en una clausura algebraica de $E$, es decir

$$G_n = (X - T_1) \ldots (X - T_n)$$

y $F = K(T_1, \ldots, T_n) = E(T_1, \ldots, T_n)$. Es decir, $F$ es el cuerpo de descomposición de $G_n$ sobre $E$. En principio pudiera darse que dos de los $T_i$ fueran iguales, pero de hecho eso no se da, lo cual es consecuencia de la siguiente proposición que dice todavía más.

**Teorema 11.2** *El polinomio general $G_n = X^n - C_1X^{n-1} + C_2X^{n-2} + \cdots + (-1)^{n-2}C_{n-2}X^2 + (-1)^{n-1}C_{n-1}X + (-1)^nC_n$ de grado $n$ es separable y* $\mathrm{Gal}(G_n, K(C_1, \ldots, C_n)) \simeq S_n$.

**Demostración.** Consideremos variables independientes arbitrarias $X_1, \ldots, X_n$ sobre $K$, sean $S_1, \ldots, S_n$ los polinomios simétricos en estas variables y sea

$$\begin{array}{rccc} \varphi = S_{S_1,\ldots,S_n}: & K[C_1, \ldots, C_n] & \to & F = K(X_1, \ldots, X_n) \\ & f & \mapsto & f(S_1, \ldots, S_n) \end{array}$$

el homomorfismo de sustitución. Como $S_1, \ldots, S_n$ son variables independientes sobre $K$, el Teorema 1.9 asegura que $\varphi$ es inyectiva y su imagen que es claramente $K[S_1, \ldots, S_n]$, es el conjunto de los polinomios simétricos en las variables $X_1, \ldots, X_n$ con coeficiente en $K$. Por tanto $K[C_1, \ldots, C_n] \simeq K[S_1, \ldots, S_n]$, con lo que $\varphi$ se extiende a un isomorfismo entre sus cuerpos de fracciones $\varphi : E = K(C_1, \ldots, C_n) \simeq E' = K(S_1, \ldots, S_n)$, por la Propiedad Universal del Cuerpo de Fracciones. Aplicando la Proposición 3.9 deducimos que $\varphi$ se extiende a un isomorfismo entre los cuerpos de descomposición de $G_n$ sobre $E$ y de $\varphi(G_n)$ sobre $E'$. Como $T_1, \ldots, T_n$ son las raíces de $G_n$ y $X_1, \ldots, X_n$ son las raíces de $\varphi(G_n)$, estos cuerpos de descomposición son $F = K(T_1, \ldots, T_n)$ y $F' = K(X_1, \ldots, X_n)$. Por tanto $\mathrm{Gal}(F/E) \simeq \mathrm{Gal}(F'/E')$. Por el Ejercicio 6.4 del Capítulo 6, la extensión $F'/E'$ es de Galois y su grupo de Galois es isomorfo a $S_n$. Por tanto $F/E$ es una extensión de Galois (en particular $G_n$ es separable) y $\mathrm{Gal}(E/F) \simeq S_n$. □

Sea

$$p = p_n + p_{n-1}X + p_{n-2}X^2 + \cdots + p_1X^{n-1} + X^n = (X - \alpha_1) \cdots (X - \alpha_n) \in K[X]$$

con $\alpha_1, \ldots, \alpha_n$ en una extensión $L$ de $K$. Consideremos el homomorfismo de sustitución

$$\begin{array}{rccc} S = S_{\alpha_1,\ldots,\alpha_n}: & K[T_1, \ldots, T_n] & \to & L \\ & f(T_1, \ldots, T_n) & \mapsto & f(\alpha_1, \ldots, \alpha_n) \end{array}$$

Entonces la restricción de $S$ a $K(C_1, \ldots, C_n)$ es el homomorfismo de sustitución

$$\begin{array}{rccc} S = S_{p_1,\ldots,p_n}: & K[C_1, \ldots, C_n] & \to & K \\ & f(C_1, \ldots, C_n) & \mapsto & f(p_1, \ldots, p_n) \end{array}$$

y por tanto $p = S(G_n)$. Eso implica que si cada $T_i$ se puede poner como una expresión radical de elementos de $E$, entonces $S(T_i)$ se podrá obtener como una expresión radical de elementos de $K$. Por tanto resolver por radicales sobre $K$ todas ecuaciones de grado $n$ equivale a resolver sobre $K$ la ecuación general de grado $n$. Por desgracia la conclusión del Teorema 11.2 es que esto sólo es posible en pocos casos.

**Corolario 11.3** *Si $K$ tiene característica 0, entonces el polinomio general de grado $n$ sobre $K$ es resoluble por radicales sobre $K$ si y sólo si $n \leq 4$.*

**Demostración.** Es una consecuencia inmediata de los Teoremas 10.7 y 11.2 y de que $S_n$ es resoluble si y solo si $n \leq 4$ (Ejemplos 9.7). □

**Corolario 11.4** *Si $K$ tiene característica 0, entonces todo polinomio de $K[X]$ de grado $\leq 4$ es resoluble por radicales sobre $K$. De hecho todo polinomio que sea producto de polinomios de grado $\leq 4$ de $K[X]$ es resoluble por radicales sobre $K$.*

El Teorema 11.3 proporciona un ejemplo de ecuación que no es resoluble por radicales: La ecuación general de grado $n \geq 5$. Sin embargo este ejemplo es algo artificial, pues se trata de ecuaciones con coeficientes en el cuerpo de fracciones racionales en $n$ variables. Cuando Lagrange, Ruffini, Abel ó Galois consideraban el problema de resolver ecuaciones por radicales, las ecuaciones solían tener coeficientes racionales y éstas son las ecuaciones que se pretendía resolver por radicales sobre $\mathbb{Q}$. Por tanto, esta introducción artificial de variables, no resuelve el problema que interesaba a los clásicos y, por tanto, todavía cabría la esperanza de que esto fuera posible. Sin embargo vamos a ver que esto no es así.

Si $P \in K[X]$ y $A = \{\alpha_1, \ldots, \alpha_n\}$ es el conjunto de las raíces de $P$, entonces $\sigma(A) = A$ para todo $\sigma \in \mathrm{Gal}_K(P)$. Además cada $\sigma \in \mathrm{Gal}_K(P)$ está completamente determinado por la restricción de $\sigma$ a $A$. Por tanto $\mathrm{Gal}_K(P)$ es isomorfo a un subgrupo de $S_A$ y a partir de ahora vamos a identificar $\mathrm{Gal}_K(P)$ con este subgrupo de $S_A$, que a menudo identificaremos con $S_n$.

Sea $G$ un subgrupo del grupo de permutaciones $S_A$ de un conjunto finito $A$ (por ejemplo, $G$ puede ser el grupo de Galois de un polinomio sobre $K$ y $A$ el conjunto de raíces de este polinomio en una clausura algebraica). Se dice que $G$ es *transitivo* si para todo $a, b \in A$, existe $\sigma \in G$ tal que $\sigma(a) = b$.

**Lema 11.5** *Si $p$ es primo y $G$ es un subgrupo transitivo de $S_p$ que contiene una trasposición, entonces $G = S_p$.*

**Demostración.** Definimos en $\mathbb{N}_p = \{1, \ldots, p\}$ la relación de equivalencia siguiente:

$$i \sim j \Leftrightarrow \text{ la trasposición } (i, j) \text{ pertenece a } G.$$

(Aquí entendemos que $(i, i) = 1$, para simplificar la notación). Vamos a ver que es efectivamente una relación de equivalencia. Si $i \sim j$ y $j \sim k$, entonces $(i, j), (j, k) \in G$ y, por tanto, $(i, k) = (j, k)(i, j)(j, k) \in G$. Esto prueba que la relación es transitiva y que es reflexiva y simétrica es obvio.

Vamos ahora a ver que todas las clases de equivalencia tienen el mismo número de elementos. En efecto, si $A$ y $B$ son dos clases de equivalencia con $a \in A$ y $b \in B$, entonces de la transitividad de $G$ se tiene que $b = \sigma(a)$ para algún $\sigma \in G$. Si $a_1 \in A$, entonces $(a, a_1) \in G$ y por tanto $(b, \sigma(a_1)) = \sigma(a, a_1)\sigma^{-1} \in G$. Esto muestra que $\sigma$ se restringe a una aplicación de $A$ en $B$ y, claramente $\sigma^{-1}(B) \subseteq A$. Luego $\sigma(A) = B$ y concluimos que $|A| = |B|$.

Por tanto, si $n$ es el cardinal de cada una de las clases de equivalencia, entonces $n|p$ y $n \neq 1$, pues, como $G$ contiene una transposición, al menos una de las clase de equivalencia tiene más de un elemento. Luego $n = p$, es decir, para todo $i, j \in \mathbb{N}_p$ se tiene que $(i, j) \in G$. Esto muestra que $G$ contiene todas las trasposiciones y por tanto $G = S_p$ (Proposición 6.12 de GyA). □

**Lema 11.6** *Si $P \in K[X]$ es separable, entonces $\mathrm{Gal}_K(P)$ es transitivo si y solo si $P$ es irreducible sobre $K$.*

**Demostración.** Si $P$ no es irreducible y $P = fg$, entonces ninguna de las raíces de $f$ puede ser raíz de $g$, con lo que si $\alpha$ es raíz de $f$ y $\beta$ es raíz de $g$, entonces $\sigma(\alpha) \neq \beta$, para todo $\sigma \in \mathrm{Gal}_K(P)$. Esto muestra que $\mathrm{Gal}_K(P)$ no es transitivo.

Por otro lado, si $\mathrm{Gal}_K(P)$ es irreducible y $\alpha$ y $\beta$ son dos raíces de $\mathrm{Gal}_K(P)$, entonces, por la Proposición 2.10, existe un $K$-isomorfismo $K(\alpha) \to K(\beta)$ que, como $L/K$ es normal, donde $L$ es el cuerpo de escisión de $\mathrm{Gal}_K(P)$ sobre $K$, se puede extender a un elemento $\sigma$ de $\mathrm{Gal}(L/K) = \mathrm{Gal}_K(P)$. Por tanto $\sigma(\alpha) = \beta$ y esto prueba que $\mathrm{Gal}(L/K)$ es resoluble. □

**Proposición 11.7** *Sean $K$ un subcuerpo de los números reales y $P \in K[X]$ un polinomio irreducible de grado primo $p$. Si $P$ tiene $p-2$ raíces reales y 2 no reales, entonces* $\mathrm{Gal}_K(P) \simeq S_p$.

**Demostración.** Identificamos $G = \mathrm{Gal}_K(P)$ con un subgrupo del grupo $S_A$ de permutaciones de las $p$ raíces de $P$ en $\mathbb{C}$ (que forman el conjunto $A$). Como $G$ es transitivo, para demostrar que $G = S_A$ (y por tanto isomorfo a $S_p$) basta ver que tiene una trasposición y aplicar el Lema 11.5. Pero esto está claro pues la conjugación compleja es un elemento $\sigma$ de $\mathrm{Gal}_K(P)$, ya que $K \subseteq \mathbb{R}$ y este elemento deja invariantes exactamente $p-2$ elementos de $A$, es decir es una transposición. □

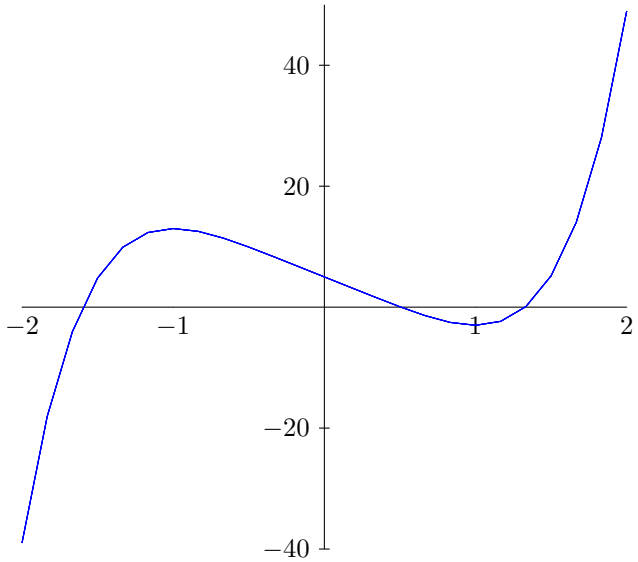



Figura 11.1: Gráfica de la función $f(x) = 2x^5 - 10X + 5$.

**Ejemplo 11.8** La Figura 11.1 representa la gráfica de $y = P(x)$ con $P(X) = 2X^5 - 10X + 5$, un polinomio irreducible sobre $\mathbb{Q}$ (Eisentein). La derivada de $p$ es $p' = 10X^4 - 10$, que tiene dos raíces reales: 1 y -1, que son respectivamente un máximo y mínimo relativo de $p$. Por otro lado $f(1) = -3$ y $f(-1) = 13$. Eso implica que la gráfica de la curva $y = p(x)$ corta al eje real en al menos tres puntos, uno en cada uno de los tres intervalos $(-\infty, -1)$, $(-1, 1)$ y $(1, \infty)$. Como ninguna de las raíces de $P$ es raíz de $P'$, entre cada dos raíces de $P$ hay un extremo relativo con lo que si hubiera más de tres raíces al menos $P'$ tendría tres raíces reales que no es el caso. Por tanto, $P$ tiene exactamente tres raíces reales. De la Proposición 11.7 se deduce que $\mathrm{Gal}_{\mathbb{Q}}(p) \simeq S_5$ y por tanto $P$ no es resoluble por radicales sobre $\mathbb{Q}$.

## 11.2 Resolución efectiva

El Teorema 10.7 transfiere el problema de la resolubilidad de ecuaciones por radicales a un problema de Teoría de Grupos e indica el camino para resolver una ecuación por radicales si es que esto es posible. Los pasos serían los siguientes para un polinomio $P \in K[X]$ con $K$ un cuerpo de característica 0. Recordemos que estamos suponiendo que $K$ tiene tantas raíces de la unidad como sea necesario.

(1) Calcular $G = \mathrm{Gal}_K(P)$ y decidir si $G$ es resoluble o no. Si la respuesta es negativa concluimos que el polinomio no es resoluble por radicales sobre $K$, por el Teorema 10.7.

(2) En caso contrario calculamos una serie cíclica (tal vez con factores de orden primo)

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_k = 1.$$

(3) Aplicando la correspondencia de Galois a esta serie obtenemos una torre de extensiones cíclicas

$$K = L_0 = L^G = L^{G_0} \subset L_1 = L^{G_1} \subset L_2 = L^{G_2} \subset \cdots \subset L_n = L^{G_k} = L^1 = L$$

donde $L$ es el cuerpo de escisión de $P$ sobre $K$.

(4) Si $[L_i : L_{i-1}] = n_i$, entonces, como estamos suponiendo que $K$ contiene tantas raíces de la unidad como sea necesario, tendremos que $L_i = L_{i-1}(\sqrt[n_i]{a_i})$, para algún $a_i \in L_{i-1}$ (Teorema 8.8).

(5) Los elementos de $L$, y en particular las raíces de $P$, se pueden expresar en la forma

$$b_0 + b_1 \sqrt[n_k]{a_k} + b_2 \sqrt[n_k]{a_k}^2 + \cdots + b_{n_k-1} \sqrt[n_k]{a_k}^{n_k-1},$$

con $b_0, b_1, \ldots, b_{n_k-1} \in L_{k-1}$. Entonces $a_k, b_0, b_1, \ldots, b_{n_k-1}$ son expresables de una forma similar a partir de $\sqrt[n_{k-1}]{a_{k-1}}$, y repitiendo el proceso se podrá obtener las raíces de $P$ mediante una expresión radical de elementos de $K$.

Obsérvese también que los radicales $\sqrt[n]{a}$ no están unívocamente determinadas pues ya sabemos que una ecuación del tipo $X^n - a$ tiene $n$ raíces: $\alpha, \xi_n\alpha, \ldots, \xi_n^{n-1}\alpha$. Por tanto, las expresiones radicales tienen un cierto grado de ambigüedad y será necesario a menudo indicar en una expresión radical cuál de las raíces $n$-ésimas es la que estamos eligiendo. Por ejemplo, en la fórmula escolar $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$ de la resolución de la ecuación de segundo grado, la expresión $\sqrt{b^2-ac}$ toma los dos valores posibles y la expresión $\pm$ que aparece en la fórmula, implica que podemos elegir cualquiera de los dos posibles valores. Sin embargo en las expresiones radicales, que al final obtendremos, para resolver las ecuaciones de tercer y cuarto grado aparecerán raíces terceras, que supondrán una ambigüedad de elección entre tres raíces terceras que habrá que precisar porque, a diferencia de la solución de la ecuación de segundo grado, no será cierto que las tres raíces terceras sean válidas.

Parece obvio que, a pesar de que teóricamente el proceso está claro, no tiene porque resultar fácil obtener la expresión radical de las raíces de $p$. Esta sección se dedica a resolver ecuaciones por radicales de forma efectiva. En la sección anterior vimos que las ecuaciones de grado $\leq 4$ son resolubles por radicales y que para resolver todas las ecuaciones de un cierto grado $n \leq 4$ basta con obtener una expresión radical de las raíces del polinomio general de grado $n$. Por supuesto que para $n = 1$ el problema es trivial. A pesar de qué sabemos perfectamente cómo resolver ecuaciones de grado 2 y también vimos en la Introducción cómo resolver ecuaciones de grado 3, es ilustrativo volver a estas ecuaciones desde el punto de vista del programa planteado en el párrafo anterior.

## Ecuaciones cuadráticas

Consideremos un polinomio de grado 2, $P = X^2+aX+b \in K[X]$ y recordemos que estamos considerando $\mathrm{Gal}_K(P)$ como un grupo de permutaciones de las raíces de $P$. Entonces $\mathrm{Gal}_K(P)$ es isomorfo a un subgrupo de $S_2$, con lo que $G = \mathrm{Gal}_K(P)$ es isomorfo a $S_2$ o es un grupo trivial. En el segundo caso el cuerpo de descomposición de $P$ es $K$ y por tanto $P$ es completamente descomponible en $K$. Para evitar casos triviales supondremos que $G \simeq S_2$ y de hecho identificamos $G$ y $S_2$. La única serie cíclica de $S_2$ es

$$S_2 \rhd 1$$

con lo que si el cuerpo de descomposición de $P$ sobre $K$ es $L$, entonces $L/K$ es una torre cíclica y

$$K \subset L$$

es la torre de subextensiones cíclicas de $L/K$ que andamos buscando. Luego $L = K(\sqrt{c})$ para algún $c \in K$. Con la fórmula que aprendimos en la escuela sabemos que $L = K(\sqrt{a^2-4b})$, es decir $c$ puede ser tomado como $a^2-4b$. Sin embargo para que este ejemplo sea de verdad ilustrativo debemos olvidarnos de lo que aprendimos en la escuela y obtener esto de forma directa. Supongamos que $P = (X-\alpha_1)(X-\alpha_2)$, es decir $\alpha_1$ y $\alpha_2$ son las raíces de $P$. Vamos a poner

$$\Delta = \alpha_1 - \alpha_2.$$

Recuérdese que si $P$ es el polinomio general de grado 2, entonces $a$ y $b$ son dos variables independientes sobre $K$ y entonces $\alpha_1$ y $\alpha_2$ también son variables independientes sobre $K$, de forma que $a = -(\alpha_1+\alpha_2)$ y $b = \alpha_1\alpha_2$. Por otro lado $\Delta^2$ es un polinomio simétrico en las variables $\alpha_1, \alpha_2$, con lo que $\Delta^2$ es un polinomio en los coeficientes de $P$. De hecho $\Delta^2 = (\alpha_1+\alpha_2)^2-4\alpha_1\alpha_2 = a^2-4b$, con lo que efectivamente $L = K(\Delta) = K(\sqrt{a^2-4b})$, pues $\alpha_1$ y $\alpha_2$ son las soluciones del siguiente sistema lineal de ecuaciones

$$\begin{array}{rcrl} \alpha_1 & + & \alpha_2 & = -a \\ \alpha_1 & - & \alpha_2 & = \Delta. \end{array} \tag{11.1}$$

Por tanto

$$\alpha_1 = \frac{-a+\Delta}{2} \quad \text{y} \quad \alpha_2 = \frac{-a-\Delta}{2},$$

que proporciona la fórmula escolar de la resolución de la ecuación de segundo grado.

Vamos a analizar este ejemplo con calma pues tiene dos elementos importantes que nos servirán para ecuaciones de grado mayor.

## Resolventes de Galois

La primera enseñanza de la forma cómo hemos resuelto la ecuaciones cuadráticas es que hemos introducido un término $\Delta = \alpha_1 - \alpha_2$ del cuerpo de descomposición sobre $K$ del polinomio $p$. En principio $\Delta$ es un elemento desconocido. Vamos a hacer algo similar para un polinomio arbitrario

$$P = X^n - p_1X^{n-1} + p_2X^{n-2} + \cdots + (-1)^{n-2}p_{n-2}X^2 + (-1)^{n-1}p_{n-1}X + (-1)^n p_n \in K[X],$$

cuyas desconocidas raíces llamamos $\alpha_1, \ldots, \alpha_n$. Es decir $L = K(\alpha_1, \ldots, \alpha_n)$ es el cuerpo de descomposición de $P$ sobre $K$. Como estamos suponiendo que la característica es 0 $L/K$ es una extensión de Galois. Vamos a considerar $G = \mathrm{Gal}_K(P)$ como un subgrupo de $S_n$, identificando la restricción de cada $\sigma$ a $\{\alpha_1, \ldots, \alpha_n\}$ con una permutación de los subíndices, es decir de $\mathbb{N}_n = \{1, 2, \ldots, n\}$. Para cada $\sigma \in S_n$, consideramos el $K$-automorfismo $\overline{\sigma}$ de $K[X_1, \ldots, X_n]$ dado por $\sigma(X_i) = X_{\sigma(i)}$. Obsérvese que si $\sigma \in G$ y $f \in K[X_1, \ldots, X_n]$, entonces

$$\sigma(f(\alpha_1, \ldots, \alpha_n)) = \overline{\sigma}(f)(\alpha_1, \ldots, \alpha_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}). \tag{11.2}$$

Si fijamos $\theta \in L$, entonces $\theta = f(\alpha_1, \ldots, \alpha_n)$ para algún $f \in K[X_1, \ldots, X_n]$ y vamos a poner

$$\begin{array}{rcl} \mathrm{Estab}_{S_n}(f) & = & \{\sigma \in S_n : \overline{\sigma}(f) = f\} \\ \mathrm{Estab}_G(f) & = & \{\sigma \in G : \overline{\sigma}(f) = f\}. \end{array}$$

Como consecuencia de (11.2) se tiene que si $\theta = f(\alpha_1, \ldots, \alpha_n)$, entonces

$$\mathrm{Estab}_G(f) = G \cap \mathrm{Estab}_{S_n}(f) \subseteq \{\sigma \in G : \sigma(\theta) = \theta\} = \mathrm{Gal}(L/K(\theta)). \tag{11.3}$$

Sea $E = \mathrm{Estab}_{S_n}(f)$, con $f \in K[X_1, \ldots, X_n]$ y sea $S_n(f) = \{\overline{\sigma}(f) : \sigma \in S_n\}$. Es fácil ver que la aplicación

$$\begin{array}{rcl} S_n/E & \to & S_n(f) \\ \sigma E & \mapsto & \overline{\sigma}(f) \end{array}$$

está bien definida y es una biyección. Por tanto $|S_n(f)| = [G : \mathrm{Estab}_{S_n}(F)]$.

Se llama *resolvente de Galois* de $f$ y $P$ a

$$R_{f,P} = \prod_{g \in S_n(f)} (X - g(\alpha_1, \ldots, \alpha_n)).$$

**Lema 11.9** *Si $P$ es un polinomio mónico de grado $n$ y $f \in K[X_1, \ldots, X_n]$, entonces $R_{f,P} \in K[X]$.*

**Demostración.** Para cada $\sigma \in S_n$ la aplicación $\tau \mapsto \sigma\tau$ es una biyección de $S_n$ en si mismo y por tanto

$$\overline{\sigma}(S_n(f)) = \{\overline{\sigma\tau}(f) : \tau \in S_n\} = \{\overline{\tau}(f) : \tau \in S_n\} = S_n(f).$$

En particular, si $\sigma \in G$, entonces

$$\begin{array}{rcl} \sigma(\{q(\alpha_1, \ldots, \alpha_n) : q \in S_n(f)\}) & = & \{\sigma(q(\alpha_1, \ldots, \alpha_n)) : q \in S_n(f)\} \\ & = & \{\overline{\sigma}(q)(\alpha_1, \ldots, \alpha_n) : q \in S_n(f)\} \\ & = & \{q(\alpha_1, \ldots, \alpha_n) : q \in S_n(f)\}, \end{array}$$

es decir, $\sigma$ permuta las raíces de $R_{f,P}$, lo que implica que $\sigma(R_{f,P}) = R_{f,P}$ y como $L/K$ es una extensión de Galois tenemos que $R_{f,P} \in K[X]$. □

**Teorema 11.10** *Sea $P \in K[X]$ un polinomio separable de grado $n$ con raíces $\alpha_1, \ldots, \alpha_n$ en una extensión de $K$, y sean $G = \mathrm{Gal}_K(P)$, $f \in K[X_1, \ldots, X_n]$, $E = \mathrm{Estab}_{S_n}(f)$, $\sigma \in S_n$ y $\theta = f(\alpha_1, \ldots, \alpha_n)$. Entonces*

*(1) $\sigma(\theta)$ es una raíz de $R_{f,P}$.*

*(2) Si $\sigma^{-1}G\sigma \subseteq E$, entonces $\sigma(\theta) \in K$.*

*(3) Si $\sigma(\theta) \in K$ y es raíz simple de $R_{f,P}$, entonces $\sigma^{-1}G\sigma \subseteq E$.*

**Demostración.** (1) es consecuencia de la propia definición de $R_{f,P}$.

(2) Supongamos que $\sigma^{-1}G\sigma \subseteq E$. Entonces $G \subseteq \sigma E\sigma^{-1} = \mathrm{Estab}_{S_n}(\overline{\sigma}(f))$. Aplicando esto y (11.3) tenemos $G = G \cap \mathrm{Estab}_{S_n}(\overline{\sigma}(f)) \subseteq \mathrm{Gal}(L/K(\sigma(\theta))) \subseteq G$. Luego $\mathrm{Gal}(L/K(\sigma(\theta))) = G = \mathrm{Gal}(L/K)$ y aplicando el Teorema Fundamental de la Teoría de Galois tenemos que $K = K(\sigma(\theta))$.

(3) Supongamos ahora que $\sigma(\theta) \in K$ y que su multiplicidad en $R_{f,p}$ es 1. Como $\sigma(\theta) \in K$, se tiene que $\tau\sigma(\theta) = \sigma(\theta)$, para todo $\tau \in G$. Si $\tau\sigma(f) \neq \sigma(f)$, entonces

$$\begin{array}{rcl} R_{t,f} & = & \prod_{g \in S_n(f)}(X - g(\alpha_1, \ldots, \alpha_n)) \\ & = & (X - \sigma(\theta))(X - \tau\sigma(\theta)) \prod_{g \in S_n(f) \setminus \{\sigma(\theta), \tau\sigma(\theta)\}}(X - g(\alpha_1, \ldots, \alpha_n)) \\ & = & (X - \sigma(\theta))^2 \prod_{g \in S_n(f) \setminus \{\sigma(\theta), \tau\sigma(\theta)\}}(X - g(\alpha_1, \ldots, \alpha_n)) \end{array}$$

en contra de que $\sigma(\theta)$ es una raíz simple de $R_{f,p}$. Por tanto $\tau\sigma(f) = \sigma(f)$, para todo $\tau \in G$, o lo que es lo mismo $\sigma^{-1}\tau\sigma \in E$, para todo $\tau \in G$, es decir $\sigma^{-1}G\sigma \subseteq E$. □

**Ejemplo 11.11 (Discriminante)** Sea $\Delta = \prod_{1\leq i<j\leq n}(X_i - X_j)$. Claramente $\mathrm{Estab}_{S_n}(\Delta) = A_n$, el grupo alternado y se tiene que $S_n(\Delta) = \{\Delta, -\Delta\}$. Por tanto, si $P(X) = (X-\alpha_1)\cdots, (X-\alpha_n) \in K[X]$, entonces

$$R_{\Delta,P} = (X - \Delta(\alpha_1, \ldots, \alpha_n))(X + \Delta(\alpha_1, \ldots, \alpha_n)) = X^2 - \Delta(\alpha_1, \ldots, \alpha_n)^2 = X^2 - D.$$

Si $K$ tiene característica diferente de 2, entonces $R_{\Delta,p}$ no tiene raíces múltiples. Aplicando el Teorema de Factorización de Resolventes (Teorema 11.10) deducimos que si $P$ es separable y $G = \mathrm{Gal}_K(P)$, entonces $G \subseteq A_n$ si y solo si $\sigma^{-1}G\sigma \subseteq A_n$ si y solo si $G \subseteq A_n$ si y solo si $R_{\Delta,p}$ tiene una raíz en $K$ si y solo si $D$ es un cuadrado en $K$.

El elemento $D = \Delta(\alpha_1, \ldots, \alpha_n)^2 = \prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j)^2$ se llama *discriminante* de $P$. Obsérvese que $D \neq 0$ si y solo si $P$ es separable. En tal caso, la extensión $L = K(\alpha_1, \ldots, \alpha_n)/K$ es de Galois y, si $G = \mathrm{Gal}_K(L) = \mathrm{Gal}(L/K)$, entonces $L^{G\cap A_n} = K(\sqrt{D})$, es decir, la correspondencia de Galois asocia $G \cap A_n$ con $K(\sqrt{D})$.

**Ejemplo 11.12 (Resolvente cúbica)** Consideremos ahora el polinomio

$$f_1 = X_1X_2 + X_3X_4 \in K[X_1, X_2, X_3, X_4].$$

Entonces

$$\mathrm{Estab}_{S_4}(f_1) = \langle (1\ 2), (3\ 4), (1\ 3)(2\ 4)\rangle$$

que es un subgrupo de orden 8 de $S_4$ y

$$S_4(f) = \{f_1, f_2 = X_1X_3 + X_2X_4, f_3 = X_1X_4 + X_2X_3\}.$$

Si $\Sigma_1, \Sigma_2, \Sigma_3, \Sigma_4$ son los polinomios simétricos elementales en $X_1, X_2, X_3, X_4$, entonces

$$R = (T - f_1)(T - f_2)(T - f_3) = T^3 - P_1T^2 + P_2X - P_3$$

donde

$$\begin{array}{lllllll} P_1 & = & f_1 + f_2 + f_3 & = & S_4(X_1X_2) & = & \Sigma_2 \\ P_2 & = & f_1f_2 + f_1f_3 + f_2f_3 & = & S_4(X_1^2X_2X_3) & = & \Sigma_1\Sigma_3 - 4\Sigma_4 \\ P_3 & = & f_1f_2f_3 & = & S_4(X_1^2X_2^2X_3^2) + \Sigma_4\ S_4(X_1^2) & = & \Sigma_3^2 + \Sigma_1^2\Sigma_4 - 4\Sigma_2\Sigma_4. \end{array}$$

En resumen

$$R = T^3 - \Sigma_2T^2 + (\Sigma_1\Sigma_3 - 4\Sigma_4)T + (4\Sigma_2 - \Sigma_1^2)\Sigma_4 - \Sigma_3^2$$

y, por tanto, si $P = X^4 - aX^3 + bX^2 - cX + d$, entonces

$$R_{f_1,P} = T^3 - bT^2 + (ac - 4d)T + (4b - a^2)d - c^2.$$

Este polinomio se llama *resolvente cúbica de la cuártica* $P$. Si $P = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4)$, entonces las raíces de $S = R_{f,p}$ son

$$\theta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \quad \theta_1 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \quad \theta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

Es fácil ver que si $P$ es separable, entonces $S$ también es separable. En tal caso, la extensión $L = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)/K(\theta_1, \theta_2, \theta_3)$ es de Galois pues $L$ es el cuerpo de descomposición de $P$ sobre $K$ (y sobre $F$). Por tanto, si $G = \mathrm{Gal}_F(P)$, entonces $\sigma(\theta_i) \in F$, para todo $\sigma \in S_4$. Aplicando el Teorema de Factorización de Resolventes (Teorema 11.10) deducimos que

$$\sigma^{-1}G\sigma \subseteq \mathrm{Estab}_{S_4}(f_1) \cap \mathrm{Estab}_{S_4}(f_2) \cap \mathrm{Estab}_{S_4}(f_3) = V = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle.$$

y, como $V \lhd S_4$ tenemos que $G \subseteq V$ y, de hecho $G = V \cap \mathrm{Gal}(L/K)$ (¿por qué?), o en otras palabras, la correspondencia de Galois entre las subextensiones de $L/K$ y los subgrupos de $\mathrm{Gal}(L/K)$ asocia $K(\theta_1, \theta_2, \theta_3)$ con $V \cap \mathrm{Gal}(L/K)$.

## Resolventes de Lagrange

La segunda enseñanza que podemos sacar de la resolución por radicales de la ecuación de segundo grado es la relación entre las raíces $\alpha_1, \alpha_2$ de un polinomio de segundo grado y la raíz cuadrada del discriminante, $\Delta = \sqrt{D} = \alpha_1 - \alpha_2$, que en este caso resulta ser el generador del cuerpo de descomposición sobre $K$. Obsérvese que esta relación está regida por el sistema lineal de ecuaciones (11.1) cuya matriz de coeficientes es

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} \xi^{0\cdot 0} & \xi^{1\cdot 0} \\ \xi^{0\cdot 1} & \xi^{1\cdot 1} \end{pmatrix},$$

donde $\xi = -1$ es una raíz segunda primitiva de la unidad.

Supongamos que $L$ es una extensión cíclica de grado $n$ con $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Suponemos que $K$ tiene una raíz $n$-ésima primitiva de la unidad $\xi = \xi_n$ y queremos obtener una expresión radical de un elemento $\alpha \in L$ en términos de $K$. Se llaman *resolventes de Lagrange* de $\alpha$ a los elementos de $L$ de la forma

$$(\xi^i, \alpha) = \sum_{i=0}^{n-1} \xi^{ij} \sigma^j(\alpha).$$

Dados $\lambda_1, \ldots, \lambda_n$, vamos a denotar por $V(\lambda_1, \ldots, \lambda_n)$ a la matriz de Vandermonde definida por $\lambda_1, \ldots, \lambda_n$, es decir

$$V(\lambda_1, \ldots, \lambda_n) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \lambda_1 & \lambda_2 & \ldots & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & \ldots & \lambda_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \ldots & \lambda_n^{n-1} \end{pmatrix}.$$

Recuérdese que el determinante de $V(\lambda_1, \ldots, \lambda_n)$ es invertible si y solo si los $\lambda_i$ son diferentes dos a dos, ya que su determinante es $\prod_{i<j}(\lambda_i - \lambda_j)$.

**Proposición 11.13** *Sea $L/K$ es una extensión cíclica de grado $n$, con $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ y supongamos que $K$ contiene una raíz $n$-ésima primitiva de la unidad $\xi = \xi_n \in K$. Sean $\alpha \in L$ y*

$$r_0 = (1, \alpha), \quad r_1 = (\xi, \alpha), \quad \ldots, \quad r_{n-1} = (\xi^{n-1}, \alpha)$$

*las resolventes de Lagrange de $\alpha$. Entonces*

*(1) $r_i^n \in K$ para todo $i$ y*

*(2) $(\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha))$ es la solución (única) del siguiente sistema de ecuaciones de Cramer*

$$V(1, \xi, \xi^2, \ldots, \xi^{n-1}) \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = \begin{pmatrix} r_0 \\ \vdots \\ r_{n-1} \end{pmatrix}.$$

**Demostración.** Como $1, \xi, \xi^2, \ldots, \xi^{n-1}$ son distintos dos a dos, el sistema es un sistema de Cramer y por la propia definición de las resolventes de Lagrange, se tiene que $(\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha))$ es la solución del sistema de ecuaciones dado. Por tanto, sólo falta demostrar que $r_i^n \in K$. Cómo $L/K$ es una extensión de Galois y $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ demostrar que $r_i^n \in K$ es equivalente a demostrar que $\sigma(r_i^n) = r_i^n$. Pero

$$\begin{aligned} \sigma(r_i) &= \sigma(\alpha + \xi^i\sigma(\alpha) + \xi^{2i}\sigma^2(\alpha) + \cdots + \xi^{(n-1)i}\sigma^{n-1}(\alpha)) \\ &= \sigma(\alpha) + \xi^i\sigma^2(\alpha) + \xi^{2i}\sigma^3(\alpha) + \cdots + \xi^{(n-1)i}\sigma^n(\alpha). \end{aligned}$$

Como $\sigma^n = 1$ y $\xi^{(n-1)i} = \xi^{-i}$, pasando el último sumando al principio tenemos

$$\begin{array}{rcl}\sigma(r_i) & = & \xi^{-i}\alpha + \sigma(\alpha) + \xi^i\sigma^2(\alpha) + \cdots + \xi^{(n-2)i}\sigma^{n-1}(\alpha) \\ & = & \xi^{-i}(\alpha + \xi^i\sigma(\alpha) + \xi^{2i}\sigma^2(\alpha) + \cdots + \xi^{(n-1)i}\sigma^{n-1}(\alpha)) = \xi^{-i}r_i\end{array}.$$

Por tanto,

$$\sigma(r_i^n) = \sigma(r_i)^n = (\xi^{-i}r_i)^n = \xi^{-in}r_i^n = r_i^n.$$

□

## 11.3 La ecuación cúbica

Consideremos el polinomio general de grado 3: $G_3 = X^3 - C_1X^2 + C_2X - C_3 \in K[X]$ (donde $K = F(C_1, C_2, C_3)$ para algún cuerpo), sus raíces $T_1, T_2, T_3$, $L = K(T_1, T_2, T_3)$, el cuerpo de descomposición de $G_3$ sobre $K$, $G = \mathrm{Gal}(G_3/K) = \mathrm{Gal}(L/K) \simeq S_3$. La raíz cuadrada del discriminante es

$$\Delta = (T_1 - T_2)(T_1 - T_3)(T_2 - T_3).$$

Sabemos que la serie normal $S_3 \rhd A_3 \rhd 1$ se corresponde mediante la correspondencia de Galois con

$$K \subseteq K(\Delta) \subseteq L$$

y que $D = \Delta^2 \in K$. Suponemos que $K$ contiene una raíz tercera primitiva de la unidad $\xi = \xi_3$, y por tanto $L/K(\Delta)$ es una extensión cíclica de grado 1 ó 3.

Vamos a obtener una expresión para $D$. Para ello expresamos $D$ en términos de los polinomios simétricos elementales en $T_1, T_2$ y $T_3$ que son precisamente $C_1, C_2$ y $C_3$:

$$\begin{array}{rcl}D & = & (T_1 - T_2)^2(T_1 - T_3)^2(T_2 - T_3)^2 \\ & = & T_1^4T_2^2 + T_1^2T_2^4 + T_1^4T_3^2 + T_2^4T_3^2 + T_1^2T_3^4 + T_2^2T_3^4 \\ & & -2(T_1^3T_2^3 + T_1^3T_3^3 + T_2^3T_3^3) \\ & & -2(T_1^4T_2T_3 + T_1T_2^4T_3 + T_1T_2T_3^4) \\ & & +2(T_1^3T_2^2T_3 + T_1^2T_2^3T_3 + T_1^3T_2T_3^2 + T_1T_2^3T_3^2 + T_1^2T_2T_3^3 + T_1T_2^2T_3^3) \\ & & -6T_1^2T_2^2T_3^2 \\ & = & S_3(T_1^4T_2^2) - 2S_3(T_1^3T_2^3) - 2C_3S_3(T_1^3) + 2C_3S_3(T_1^2T_2) - 6C_3^2.\end{array}$$

Aplicando el algoritmo explicado en la Sección 1.2 tenemos

$$\begin{array}{rcl}S_3(T_1^4T_2^2) & = & C_1^2C_2^2 - 2C_2^3 - 2C_1^3C_3 + 4C_1C_2C_3 - 3C_3^2, \\ S_3(T_1^3T_2^3) & = & C_2^3 - 3C_1C_2C_3 + 3C_3^2, \\ S_3(T_1^3) & = & C_1^3 - 3C_1C_2 + 3C_3, \\ S_3(T_1^2T_2) & = & C_1C_2 - 3C_3.\end{array}$$

con lo que

$$\begin{array}{rcl}D & = & C_1^2C_2^2 - 2C_2^3 - 2C_1^3C_3 + 4C_1C_2C_3 - 3C_3^2 \\ & & -2(C_2^3 - 3C_1C_2C_3 + 3C_3^2) - 2C_3(C_1^3 - 3C_1C_2 + 3C_3) \\ & & +2C_3(C_1C_2 - 3C_3) - 6C_3^2 \\ & = & C_1^2C_2^2 - 4C_2^3 - 4C_1^3C_3 + 18C_1C_2C_3 - 27C_3^2.\end{array}$$

Sustituyendo $C_1, C_2$ y $C_3$ por $-a, b$ y $-c$, para un polinomio $p = X^3 + aX^2 + bX + c$ obtenemos el siguiente lema.

**Lema 11.14** *Si $\Delta$ es el discriminante del polinomio $p = X^3 + aX^2 + bX + c$, entonces*

$$D = \Delta^2 = a^2b^2 + 18abc - (4b^3 + 4a^3c + 27c^2).$$

*En consecuencia, si $P$ es separable e irreducible sobre $K$, entonces*

$$\mathrm{Gal}_K(P) \simeq \begin{cases} A_3 \simeq C_3, & \text{si } a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2 \text{ es un cuadrado en } K; \\ S_3, & \text{en caso contrario} \end{cases}$$

*y $\mathrm{Gal}_{K(\Delta)}(P)$ es cíclico de orden 3.*

El grupo $\mathrm{Gal}(G_3/K(\Delta))$ está generado por el 3-ciclo $\sigma = (T_1, T_2, T_3)$, con lo que las resolventes de Lagrange de $T = T_1$ son

$$\begin{array}{rcccl} r_0 & = & (1,T) & = & T_1 + T_2 + T_3 = -a \\ r_1 & = & (\xi,T) & = & T_1 + \xi T_2 + \xi^2 T_3 \\ r_2 & = & (\xi^2,T) & = & T_1 + \xi^2 T_2 + \xi T_3 \end{array} \tag{11.4}$$

Resolviendo el sistema de ecuaciones tenemos

$$T_1 = \frac{\begin{vmatrix} r_0 & 1 & 1 \\ r_1 & \xi & \xi^2 \\ r_2 & \xi^2 & \xi \end{vmatrix}}{\begin{vmatrix} 1 & 1 & 1 \\ 1 & \xi & \xi^2 \\ 1 & \xi^2 & \xi \end{vmatrix}} = \frac{r_0 + r_1 + r_2}{3}. \tag{11.5}$$

Ahora observamos que

$$(T_1 + \xi T_2 + \xi^2 T_3)^3 = T_1^3 + T_2^3 + T_3^3 + 6T_1T_2T_3 + 3\xi(T_1^2T_2 + T_2^2T_3 + 3\xi T_1T_3^2) + 3\xi^2(T_1T_2^2 + T_1^2T_3 + T_2T_3^2).$$

Escribiendo $T_1^3 + T_2^3 + T_3^3 + 6T_1T_2T_3$ en términos de los polinomios simétricos elementales obtenemos

$$T_1^3 + T_2^3 + T_3^3 + 6T_1T_2T_3 = C_1^3 - 3C_1C_2 + 9C_3.$$

con lo que

$$(T_1 + \xi T_2 + \xi^2 T_3)^3 = C_1^3 - 3C_1C_2 + 9C_3 + 3\xi(T_1^2T_2 + T_2^2T_3 + 3\xi T_1T_3^2) + 3\xi^2(T_1T_2^2 + T_1^2T_3 + T_2T_3^2).$$

Análogamente

$$(T_1 + \xi^2 T_2 + \xi T_3)^3 = C_1^3 - 3C_1C_2 + 9C_3 + 3\xi^2(T_1^2T_2 + T_2^2T_3 + 3\xi T_1T_3^2) + 3\xi(T_1T_2^2 + T_1^2T_3 + T_2T_3^2).$$

Sumando las dos expresiones tenemos

$$(T_1 + \xi T_2 + \xi^2 T_3)^3 + (T_1 + \xi^2 T_2 + \xi T_3)^3 = 2C_1^3 - 6C_1C_2 + 18C_3 + 3(\xi + \xi^2)S_3(T_1^2T_2)$$

Teniendo en cuenta que $\xi + \xi^2 = -1$ y $S_3(T_1^2T_2) = C_1C_2 - 3C_3$ obtenemos

$$(T_1 + \xi T_2 + \xi^2 T_3)^3 + (T_1 + \xi^2 T_2 + \xi T_3)^3 = 2C_1^3 - 6C_1C_2 + 18C_3 - 3(C_1C_2 - 3C_3) = 2C_1^3 - 9C_1C_2 + 27C_3.$$

Por otro lado

$$(T_1^2T_2 + T_1T_3^2 + T_2^2T_3) - (T_1T_2^2 + T_1^2T_3 + T_2T_3^2) = (T_1 - T_2)(T_1 - T_3)(T_2 - T_3),$$

y por tanto

$$(T_1+\xi T_2+\xi^2T_3)^3-(T_1+\xi^2T_2+\xi T_3)^3=3(\xi-\xi^2)(T_1-T_2)(T_1-T_3)(T_2-T_3)=3\sqrt{-3}\Delta.$$

Luego

$$\begin{array}{rcl} r_1^3 & + & r_2^3 = 2C_1^3-9C_1C_2+27C_3, \\ r_1^3 & - & r_2^3 = 3\sqrt{-3}\Delta \end{array}$$

y resolviendo el sistema tenemos

$$\begin{array}{rcl} r_1 & = & \sqrt[3]{\frac{1}{2}(2C_1^3-9C_1C_2-27C_3+3\sqrt{-3}\Delta)}, \\ r_2 & = & \sqrt[3]{\frac{1}{2}(2C_1^3-9C_1C_2-27C_3-3\sqrt{-3}\Delta)}. \end{array}$$

Sustituyendo en (11.5) los valores obtenidos para $r_0, r_1$ y $r_2$ obtenemos

$$T_1=\frac{1}{3}\left(-C_1+\sqrt[3]{\frac{1}{2}(2C_1^3-9C_1C_2-27C_3+3\sqrt{-3}\Delta)}+\sqrt[3]{\frac{1}{2}(2C_1^3-9C_1C_2-27C_3-3\sqrt{-3}\Delta)}\right).$$

Esto proporciona una de las raíces de $G_3$, excepto que ya sabemos que tenemos tres posibilidades para elegir las raíces cúbicas, con lo que tenemos tres posibilidades para $r_1$ y $r_2$, lo que podría dar lugar a seis raíces distintas de $G_3$ que sabemos que es imposible. Es realidad $r_1$ y $r_2$ se determinan una a la otra por la siguiente fórmula:

$$\begin{array}{rcl} r_1r_2 & = & (T_1+\xi T_2+\xi^2T_3)(T_1+\xi^2T_2+\xi T_3) \\ & = & (T_1^2+T_2+T_3^2)+(\xi+\xi^2)(T_1T_2+T_1T_3+T_2T_3) \\ & = & (T_1+T_2+T_3)^2-3(T_1T_2+T_1T_3+T_2T_3) \\ & = & C_1^2-3C_2. \end{array}$$

Por tanto las tres raíces cúbicas que se pueden elegir como valores para $r_1$ determinan el valor de $r_2$ y esto proporciona tres posibles valores para $T_1$. Obsérvese que en realidad estos son los tres valores de $T_1, T_2$ y $T_3$ pues los tres valors posibles para $r_1$ son de la forma $\alpha, \xi\alpha, \xi^2\alpha$ y si elegimos $r_1=\alpha$, para calcular $T_1$, entonces al cambiar $\alpha$ por $\xi\alpha$ y $\xi^2\alpha$ obtenemos los valores de $T_2$ y $T_3$ tal como aparecen en (11.4).

En resumen, cambiando de nuevo $C_1, C_2$ y $C_3$ por $-a, b$ y $-c$ obtenemos:

**Teorema 11.15** *Las raíces de $X^3+aX^2+bX+c$ son los tres elementos de la forma*

$$\frac{1}{3}\left(-a+\sqrt[3]{\frac{1}{2}(-2a^3+9ab-27c+3\sqrt{-3D})}+\sqrt[3]{\frac{1}{2}(-2a^3+9ab-27c-3\sqrt{-3D})}\right)$$

*donde*

$$D=a^2b^2+18abc-(4b^3+4a^3c+27c^2).$$

*y las dos raíces cúbicas hay que elegirlas de forma que el producto sea $a^2-3b$.*

## 11.4 La cuártica

Consideremos ahora el polinomio general de grado 4 sobre un cuerpo $F$ arbitrario

$$G_4=X^4-C_1X^3+C_2X^2-C_3X+C_4=(X-T_1)(X-T_2)(X-T_3)(X-T_4)\in K[X].$$

con $K = F(C_1, C_2, C_3, C_4)$ y $L = F(T_1, T_2, T_3, T_4)$. Recordemos que $S_4 \simeq \mathrm{Gal}(G_4/K) = \mathrm{Gal}(L/K)$ y este isomorfismo viene dado por la aplicación $\sigma \mapsto \overline{\sigma}$ que asocia cada $\sigma \in S_4$ con el $K$-automorfismo de $L$ dado por $\overline{\sigma}(T_i) = T_{\sigma(i)}$. Recordemos también que la serie derivada de $S_4$ es

$$S_4 \rhd A_4 \rhd V \rhd 1$$

donde $V = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle$. Pongamos

$$f_1 = T_1T_2 + T_3T_4, \quad f_2 = T_1T_3 + T_2T_4, \quad f_3 = T_1T_4 + T_2T_3.$$

Del Ejemplo 11.12 tenemos que $F^V = K(C_1, C_2, C_3, C_4, f_1, f_2, f_3)$ y $f_1, f_2, f_3$ son las raíces de la resolvente cúbica

$$R = (X - f_1)(X - f_2)(X - f_3) = X^3 - C_2X^2 + (C_1C_3 - 4C_4)X + (4C_2 - C_1^2)C_4 - C_3^2.$$

La clave de la resolución de la ecuación de grado 4 por radicales consiste en que podemos calcular $f_1, f_2, f_3$ utilizando el Teorema 11.15 y es fácil expresar las raíces $T_1, T_2, T_3, T_4$ en términos $f_1, f_2, f_3$.

Veamos esto último. Si ponemos

$$\begin{array}{rcl} \beta_1 & = & T_1 + T_2 - T_3 - T_4 = 2(T_1 + T_2) + C_1, \\ \beta_2 & = & T_1 - T_2 + T_3 - T_4 = 2(T_1 + T_3) + C_1, \\ \beta_3 & = & T_1 - T_2 - T_3 + T_4 = 2(T_1 + T_4) + C_1 \end{array}$$

concluimos que $(T_1, T_2, T_3, T_4)$ es la solución del siguiente sistema lineal de ecuaciones

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} T_1 \\ T_2 \\ T_3 \\ T_4 \end{pmatrix} = \begin{pmatrix} C_1 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}.$$

Observando que si $A$ es la matriz de los coeficientes del sistema anterior tenemos que $A^2 = 4I$, tenemos que

$$\begin{array}{rcl} T_1 & = & \frac{1}{4}(C_1 + \beta_1 + \beta_2 + \beta_3) \\ T_2 & = & \frac{1}{4}(C_1 + \beta_1 - \beta_2 - \beta_3) \\ T_3 & = & \frac{1}{4}(C_1 - \beta_1 + \beta_2 - \beta_3) \\ T_4 & = & \frac{1}{4}(C_1 + \beta_1 - \beta_2 + \beta_3) \end{array}$$

y sólo falta calcular los $\beta_i$. Para ello observamos que $\sigma(\beta_i) = \pm\beta_i$ para todo $\sigma \in V$, con lo que los cuadrados de los $\beta_i$ pertenecen a $F^V = K(C_1, C_2, C_3, f_1, f_2, f_3)$. Más concretamente

$$\begin{array}{rcl} \beta_1^2 & = & C_1^2 - 4C_2 + 4f_1, \\ \beta_2^2 & = & C_1^2 - 4C_2 + 4f_2, \\ \beta_3^2 & = & C_1^2 - 4C_2 + 4f_3. \end{array}$$

Esto determina los $\beta_i$ salvo el signo. Para determinar el signo observamos que $\overline{\sigma}(\beta_1\beta_2\beta_3) = \beta_1\beta_2\beta_3$ para todo $\sigma \in S_4$, con lo que $\beta_1\beta_2\beta_3 \in K(C_1, C_2, C_3, C_4)$. Aplicando una vez más el método de escribir un polinomio en términos de los polinomios simétricos elementales obtenemos

$$\beta_1\beta_2\beta_3 = C_1^3 - 4C_1C_2 + 8C_3$$

lo que muestra que el signo de dos de los $\beta_i$ determina el del tercero. La elección de dos de los signos de los $\beta_i$, no afecta al resultado pues sólo produce una permutación en las soluciones $T_i$.

Si ahora partimos de un polinomio de cuarto grado $p = X^4 + aX^3 + bX^2 + cX + d \in K[X]$, podemos encontrar sus raíces cambiando en las cuentas anteriores los coeficientes de la ecuación general de grado cuatro por los de este polinomio y obtenemos el siguiente teorema.

**Teorema 11.16** *Las raíces de* $p = X^4 + aX^3 + bX^2 + cX + d \in K[X]$ *son*

$$\begin{aligned}
\alpha_1 &= \tfrac{1}{4}(\beta_1 + \beta_2 + \beta_3 - a),\\
\alpha_2 &= \tfrac{1}{4}(\beta_1 - \beta_2 - \beta_3 - a),\\
\alpha_3 &= \tfrac{1}{4}(-\beta_1 + \beta_2 - \beta_3 - a),\\
\alpha_4 &= \tfrac{1}{4}(-\beta_1 - \beta_2 + \beta_3 - a);
\end{aligned}$$

*para*

$$\beta_1 = \sqrt{a^2 - 4b + 4\theta_1}, \quad \beta_2 = \sqrt{a^2 - 4b + 4\theta_2} \quad y \quad \beta_3 = \sqrt{a^2 - 4b + 4\theta_3}$$

*donde* $\theta_1, \theta_2, \theta_3$ *son las raíces de la resolvente cúbica*

$$X^3 - bX^2 + (ac - 4d)X + (4b - a^2)d - c^2.$$

*con una elección de los signos de* $\beta_i$ *de forma que se cumpla*

$$\beta_1\beta_2\beta_3 = 4ab - a^3 - 8c$$

Obsérvese que en la resolución de la ecuación de cuarto grado proporcionada por el Teorema 11.16 tenemos dos elecciones posibles para los signos de cada uno de los $\beta_i$. Combinando estas tres parejas de elecciones tenemos ocho elecciones posibles de los signos de los $\beta_i$, de las cuales cuatro satisfacen la última condición $\beta_1\beta_2\beta_3 = 4ab - a^3 - 8c$ y las otras cuatro no. Cualquiera de las cuatro que satisfacen la condición es válida pues al cambiar de una a otra lo único que cambia es el orden en el que se obtienen las raíces $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ del polinomio original.

## 11.5 Resolubilidad de las ecuaciones de grado primo

Sea $n$ un número natural. En esta sección vamos a identificar $S_n$ con el conjunto de las permutaciones del conjunto $\mathbb{Z}_n$ de clases de restos módulo $n$.

Para cada $(a, b) \in \mathbb{Z}_n^* \times \mathbb{Z}_n$ sea $\sigma_{a,b} : \mathbb{Z}_n \to \mathbb{Z}_n$ la aplicación dada por $\sigma_{a,b}(x) = ax + b$ y sea

$$\mathcal{A}f_n = \{\sigma_{a,b} : a \in \mathbb{Z}_n^*, b \in \mathbb{Z}_n\}.$$

Obsérvese que $\mathcal{A}f_n$ es un subgrupo de $S_n$. En efecto, por un lado $\sigma_{1,0}$ es la aplicación identidad, con lo que $1 \in \mathcal{A}f_n$. Por otro, si $a_1, a_2 \in \mathbb{Z}_n^*$ y $b_1, b_2 \in \mathbb{Z}_n$, entonces $a_1a_2 \in \mathbb{Z}_n^*$ y

$$\sigma_{a_1,b_1}\sigma_{a_2,b_2}(x) = a_1(a_2x + b_2) + b_1 = a_1a_2x + a_1b_2 + b_1 = \sigma_{a_1a_2,a_1b_2+b_1}(x)$$

con lo que

$$\sigma_{a_1,b_1}\sigma_{a_2,b_2} = \sigma_{a_1a_2,a_1b_2+b_1} \in \mathcal{A}f_n.$$

Finalmente, si $(a, b) \in \mathbb{Z}_n^* \times \mathbb{Z}_n$, entonces existe $a_1 \in \mathbb{Z}_n^*$ tal que $aa_1 = 1$, con lo que

$$\sigma_{a,b}\sigma_{a_1,-a_1b} = \sigma_{aa_1,-aa_1b-b} = \sigma_{1,0} = 1$$

y

$$\sigma_{a_1,-a_1b}\sigma_{a,b} = \sigma_{a_1a,a_1b-a_1b} = \sigma_{1,0} = 1.$$

Es decir $\sigma_{a,0}^{-1} = \sigma_{a_1,-a_1b} \in \mathcal{A}f_n$.

Un subgrupo de $S_n$ se dice que es *afín* en $S_n$ si es conjugado en $S_n$ de un subgrupo de $\mathcal{A}f_n$. En otras palabras los subgrupos afines de $S_n$ son los de la forma $\sigma^{-1}G\sigma$ para $G$ un subgrupo de $\mathcal{A}f_n$ y $\sigma \in S_n$.

**Ejemplo 11.17** Todo subgrupo de $S_n$ generado por un $n$-ciclo es afín. En efecto, si $\sigma$ es un $n$-ciclo, entonces $\sigma$ es conjugado en $S_n$ de $\sigma_{1,1} = (0, 1, 2, \ldots, n-1)$ (Teorema 6.9 de GyA). Por tanto $\langle\sigma\rangle$ es conjugado de $\langle\sigma_{1,1}\rangle$ en $S_n$.

**Proposición 11.18** *Todo subgrupo afín de $S_n$ es resoluble.*

**Demostración.** Como dos grupos conjugados son isomorfos y un subgrupo de uno resoluble es resoluble, para demostrar que todo grupo afín de $S_n$ es resoluble basta demostrar que $\mathcal{A}f_n$ es resoluble. Consideremos el subgrupo $N = \langle\sigma_{1,1}\rangle$ de $\mathcal{A}f_n$. Obsérvese que $\sigma_{1,1}^b = \sigma_{1,b}$, para todo $b \in \mathbb{Z}_n$ y por tanto $N = \{\sigma_{1,b} : b \in \mathbb{Z}_n\}$. Además $N$ es normal en $\mathcal{A}f_n$ pues

$$\sigma_{a,b}^{-1}\sigma_{1,1}\sigma_{a,b} = \sigma_{a^{-1},-a^{-1}b}\sigma_{a,b+1} = \sigma_{a^{-1}a,a^{-1}(b+1)-a^{-1}b} = \sigma_{1,a^{-1}} \in N$$

Por otro lado $H = \{\sigma_{a,0} : a \in \mathbb{Z}_n^*\}$ es un subgrupo abeliano de $\mathcal{A}f_n$ pues es isomorfo a $\mathbb{Z}_n^*$. Además la aplicación $\Phi : \mathcal{A}f_n \to H$ dada por $\Phi(\sigma_{a,b}) = \sigma_{a,0}$ es un homomorfismo suprayectivo cuyo núcleo es precisamente $N$. Por tanto $\mathcal{A}f_n/N \cong H$ y por tanto $\mathcal{A}f_n/N$ es abeliano. Como $N$ también es abeliano, de la Proposición 9.9 deducimos que $\mathcal{A}f_n$ es resoluble. □

Recordemos que el grupo de Galois de un polinomio irreducible separable es transitivo (Lema 11.6). Nuestro siguiente objetivo es caracterizar los subgrupos transitivos resolubles de $S_p$ para $p$ primo. Pero antes necesitamos alguna notación y un lema.

Si $\sigma \in S_n$ entonces

$$F(\sigma) = \{x \in \mathbb{Z}_n : \sigma(x) = x\} \quad \text{y} \quad M(\sigma) = \mathbb{Z}_n \setminus F(\sigma).$$

Sea $G$ un subgrupo de $S_n$. Consideramos $G$ actuando en $\mathbb{Z}_n$ de la forma obvia, es decir $\sigma \cdot x = \sigma(x)$. Entonces

$$G \cdot x = \{\sigma(x) : \sigma \in G\} \quad \text{y} \quad \text{Estab}_G(x) = \{\sigma \in G : \sigma(x) = x\}.$$

Llamaremos $G$-órbitas a las órbitas $G \cdot x$ de esta acción que forman una partición de $\mathbb{Z}_n$, y para todo $x \in \mathbb{Z}_n$ tenemos

$$|G \cdot x| = [G : \text{Estab}_G(x)].$$

Obsérvese que $G$ es transitivo si y solo si $G \cdot x = \mathbb{Z}_n$, para todo $x \in \mathbb{Z}_x$ si y solo si $G \cdot x = \mathbb{Z}_n$, para algún $x \in \mathbb{Z}_x$.

**Lema 11.19** *Sea $G$ un subgrupo de $S_n$ y $\sigma \in S_n$.*

*(1) Si $\sigma^{-1}G\sigma = G$ y $x \in \mathbb{Z}_n$, entonces $\text{Estab}_G(\sigma(x)) = \sigma\text{Estab}_G(x)\sigma^{-1}$, y en particular, $|G \cdot x| = |G \cdot \sigma(x)|$.*

*(2) Si $G$ es un subgrupo transitivo de $S_n$ y $N$ es un subgrupo normal de $G$, entonces todas las $N$-órbitas tienen el mismo cardinal.*

*(3) Si $G$ es un subgrupo afín de $S_p$, con $p$ primo y $1 \neq \sigma \in G$, entonces $|F(\sigma)| \leq 1$.*

*(4) Si $\sigma^{-1}\sigma_{1,1}\sigma \in \mathcal{A}f_p$, con $p$ primo, entonces $\sigma \in \mathcal{A}f_p$.*

**Demostración.** (1) se deja como ejercicio.

(2) Si $x, y \in \mathbb{Z}_n$, entonces existe $\sigma \in G$ tal que $y = \sigma(x)$. Como $N \trianglelefteq G$, $\sigma^{-1}N\sigma = N$ y por tanto $|N \cdot x| = |N \cdot \sigma(x)| = |N \cdot y|$, por (1).

(3) Sea $\sigma \in G$ con $G$ un subgrupo afín de $S_p$ y supongamos que $F(\sigma)$ tiene al menos dos elementos distintos. Tenemos que demostrar que $\sigma = 1$. Como $G$ es afín, $\tau^{-1}\sigma\tau = \sigma_{a,b}$ para algún $(a, b) \in \mathbb{Z}_p^* \times \mathbb{Z}_p$ y $\tau \in S_p$. Luego $\sigma$ y $\sigma_{a,b}$ son permutaciones del mismo tipo (Teorema 6.9 de GyA) y por tanto $|F(\sigma_{a,b})| = |F(\sigma)|$ por tanto $F_{\sigma_{a,b}}$ tiene dos elementos distintos $x$ e $y$. Entonces

$$ax + b = x \quad \text{y} \quad ay + b = y.$$

Luego $(a - 1)(x - y) = 0$, lo que implica que $a = 1$ y por tanto $b = 0$. Es decir $\tau^{-1}\sigma\tau = \sigma_{1,0} = 1$ y concluimos que $\sigma = 1$.

(4) Sea $(a, b) \in \mathbb{Z}_p^* \times \mathbb{Z}_p$ tal que $\sigma^{-1}\sigma_{1,1}\sigma = \sigma_{a,b}$. Como $\sigma_{1,1}$ tiene orden $p$, $\sigma_{a,b}$ también tiene orden $p$. Del Pequeño Teorema de Fermat tenemos que $a^p = a$ y, como $\sigma_{a,b}$ tiene orden $p$ deducimos $1 = \sigma_{a,b}^p = \sigma_{a^p,c} = \sigma_{a,c}$, para algún $c \in \mathbb{Z}_n$. Eso implica que $a = 1$, y por tanto $b \neq 0$. En resumen $\sigma_{1,1}\sigma = \sigma\sigma_{1,b}$ para $b \in \mathbb{Z}_p^*$. Si $x \in \mathbb{Z}_p$ entonces

$$\sigma(x + b) = \sigma\sigma_{1,b}(x) = \sigma_{1,1}\sigma(x) = \sigma(x) + 1.$$

Por tanto, para todo $k \in \mathbb{Z}_p$ tenemos que $\sigma(kb) = \sigma((k - 1)) + 1$ y para $k = xb^{-1}$ tenemos que

$$\sigma(x) = \sigma(kb) = \sigma((k-1)b) + 1 = \sigma((k-2)b) + 2 = \cdots = \sigma(0) + k = b^{-1}x + \sigma(0) = \sigma_{b^{-1},\sigma(0)}(x)$$

es decir $\sigma = \sigma_{b^{-1},\sigma(0)} \in \mathcal{A}f_p$. □

**Teorema 11.20** *Las siguientes condiciones son equivalentes para un subgrupo transitivo $G$ de $S_p$, con $p$ un número primo.*

*(1) $G$ es resoluble.*

*(2) $G$ es afín.*

*(3) $|F(\sigma)| \leq 1$ para todo $1 \neq \sigma \in G$.*

*(4) $G$ tiene un subgrupo normal de orden $p$.*

*(5) $|G| \leq p(p - 1)$.*

*(6) $p$ divide a $|G|$ y $|G| < p^2$.*

**Demostración.** (2) implica (1) es consecuencia de la Proposición 11.18.

(1) implica (2). Sea $G$ un subgrupo resoluble de $S_p$ y sea

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = 1$$

una serie normal con factores de orden primo.

Empezamos demostrando por inducción sobre $i$, que $G_i$ es transitivo en $S_p$ para todo $i < n$. Esto es cierto para $i = 0$ por hipótesis. Supongamos que $0 < i < n$ y $G_{i-1}$ es transitivo. Aplicando el Lema 11.19 a $N = G_i$, un subgrupo normal de $G_{i-1}$, se deduce que los conjuntos de la forma $G_i \cdot x$, tienen todos el mismo cardinal y forman una partición de $\mathbb{Z}_p$, con lo que el cardinal de estos conjuntos es un divisor de $p$. Como $G_i \neq 1$, $|G_i \cdot x| > 1$ para algún $x$ (y por tanto para todos), de donde se deduce que $G_i \cdot x = \mathbb{Z}_p$, es decir $G_i$ es transitivo.

Luego $G_{n-1} = \langle\sigma\rangle$ es cíclico y transitivo y por tanto $\sigma$ es un $p$-ciclo (¿por qué?). Como $\sigma_{1,1}$ es otro $p$-ciclo, $\tau^{-1}\sigma\tau = \sigma_{1,1}$ para algún $\tau \in S_p$. Sea $H = \tau^{-1}G\tau \simeq G$. Como $G$ es resoluble, $H$ también es resoluble y

$$H = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_n = 1$$

es una serie normal con factores de orden primo, donde $H_i = \tau^{-1}G_i\tau$ para cada $i$.

Vamos ahora a demostrar que $H_{n-i} \subseteq \mathcal{A}f_p$ por inducción sobre $i$. Esto es obvio si $i = 0$ y también se verifica para $i = 1$, pues $H_{n-1} = \tau^{-1}\langle\sigma\rangle\tau = \langle\tau^{-1}\sigma\tau\rangle = \langle\sigma_{1,1}\rangle \subseteq \mathcal{A}f_p$. Supongamos que $1 < i \leq n$ y que $H_{n-i-1} \subseteq \mathcal{A}f_p$. Sea $\sigma \in H_{n-i}$. Como $\sigma_{1,1} \in H_{n-1} \subseteq H_{n-(i-1)} \lhd H_{n-i}$, tenemos que $\sigma^{-1}\sigma_{1,1}\sigma \in H_{n-i-1} \subseteq \mathcal{A}f_p$. Del Lema 11.19 deducimos que $\sigma \in \mathcal{A}f_p$ y esto demuestra que $H_{n-i} \subseteq \mathcal{A}f_p$.

(2) implica (3) es consecuencia del Lema 11.19.

(3) implica (4). Supongamos que $|F(\sigma)| \leq 1$, para todo $1 \neq \sigma \in G$, o lo que es lo mismo $|\mathrm{Estab}_G(x) \cap \mathrm{Estab}_G(y)| = 1$, para cada dos elementos distintos $x, y$ de $\mathbb{Z}_p$. Como $G$ es transitivo, $p = |G \cdot x| = [G : \mathrm{Estab}_G(x)]$, es decir $|\mathrm{Estab}_G(x)| = |G|/p$ para todo $x \in \mathbb{Z}_p$. Pongamos

$$n = |G|, \quad \Omega = \bigcup_{x\in\mathbb{Z}_p} (\mathrm{Estab}_G(x) \setminus \{1\}) \quad \text{y} \quad N = G \setminus \Omega.$$

Entonces $\Omega$ es la unión de $p$ subconjuntos disjuntos de $G$, cada uno de cardinal $\frac{n}{p} - 1$. Luego $|N| = n - p\left(\frac{n}{p} - 1\right) = p$. Por tanto existe $1 \neq \sigma \in N$, es decir $G$ tiene un elemento $\sigma$ tal que $F_\sigma = \emptyset$. Supongamos que $\sigma$ es de tipo $[k_1, \ldots, k_r]$, o sea $2 \leq k_1 \leq k_2 \leq \ldots k_r$, $\sigma = \tau_1 \cdot \tau_r$ con $\tau_1, \ldots, \tau_i$ ciclos disjuntos y $\tau_i$ de longitud $k_r$. Entonces $p = k_1 + \ldots k_r$ con lo que o bien $\sigma$ es un $p$-ciclo o no todos los $k_i$ son iguales. En el segundo caso $F(\sigma^{k_1}) \geq 2$ y $\sigma^{k_1} \neq 1$, en contra de la hipótesis. Por tanto $\sigma$ es un $p$-ciclo y $N = \langle\sigma\rangle$ tiene orden $p$. Del Lema 11.19 deducimos que si $g \in G$ entonces $g^{-1}\mathrm{Estab}_G(x)g = \mathrm{Estab}_G(g \cdot x)$ y como $G$ es transitivo $g^{-1}\Sigma g = \cup_{x\in\mathbb{Z}_p}(\mathrm{Estab}_G(g \cdot x) \setminus \{1\}) = \cap_{x\in\mathbb{Z}_p}(\mathrm{Estab}_G(g \cdot x) \setminus \{1\}) = \Sigma$ y por tanto $N$ es un subgrupo normal.

(4) implica (2). Si $G$ tiene un subgrupo normal $N$ de orden $p$ y $1 \neq \sigma \in N$, entonces del Lema 11.19.(2) se deduce que $\sigma$ es un $p$-ciclo. Por tanto existe $\tau \in S_p$ tal que $\tau^{-1}\sigma\tau = \sigma_{1,1} \in \mathcal{A}f_p$. Si $G_1 = \tau^{-1}G\tau$, entonces $N_1 = \langle\sigma_{1,1}\rangle$ es un subgrupo normal de $G_1$ y del Lema 11.19.(4) deducimos que $G_1 \subseteq \mathcal{A}f_n$.

(2) implica (5) es obvio pues $|\mathcal{A}f_p| = p(p-1)$.

(5) implica (6). Supongamos que $|G| \leq p(p-1)$. Entonces $|G| < p^2$. Por otro lado aplicando el Lema 11.19 y que $G$ es transitivo deducimos que $p = |G \cdot x| = [G : \mathrm{Estab}_G(x)]$ un divisor de $|G|$.

(6) implica (4). Esta parte de la demostración utiliza los Teoremas de Sylow.

Supongamos que $n = pm < p^2$. Entonces $p \nmid m$ y, por el Tercer Teorema de Sylow (Teorema A.10), el número $n_p$ de $p$-subgrupos de $G$ de orden $p$ ($p$-subgrupos de Sylow) satisface $n_p|m$ y $n_p \equiv 1 \bmod p$. O sea $n_p = 1 + kp|m < p$ para algún entero $k$, de donde se deduce que $n_p = 1$. Por tanto, $G$ tiene un único subgrupo de orden $p$, que ha de ser normal en $G$. □

**Corolario 11.21** *(Galois) Si $f \in K[X]$ es irreducible de grado primo entonces $f$ es resoluble por radicales sobre $K$ si y solo si $K(\alpha, \beta)$ es un cuerpo de descomposición de $f$ para cada dos raíces distintas de $\alpha, \beta$ de $f$ en una extensión de $f$.*

**Demostración.** Sea $L$ el cuerpo de descomposición de $f$ sobre $K$. Obsérvese que $G = \mathrm{Gal}(f/K) = \mathrm{Gal}(L/K)$ es un subgrupo transitivo de $S_A$, donde $A$ es el conjunto de las raíces de $f$. De los Teoremas 10.7 y 11.20 se deduce que $f$ es resoluble por radicales sobre $K$ si y solo si $G$ es resoluble por radicales si y sólo $|F(\sigma)| \leq 1$, para todo $1 \neq \sigma \in G$, si y solo si $\mathrm{Gal}(L/K(\alpha, \beta)) = 1$, para cada elementos diferentes $\alpha, \beta \in A$ si y solo si $L = K(\alpha, \beta)$. □

## 11.6 Calculo efectivo del grupo de Galois

Si intentamos enfrentarnos al problema de si un polinomio $p$ es resoluble por radicales sobre un cuerpo $K$ de característica 0 nos encontraremos con que la solución proporcionada por el Teorema 10.7 no termina de ser satisfactoria pues necesitamos calcular $\mathrm{Gal}_K(p) = \mathrm{Gal}(L/K)$, donde $L$ es el cuerpo de descomposición de $p$ sobre $K$, y a primera vista puede parecer que esto requiere calcular $L$, lo que nos lleva a calcular las raíces de $L$, que es el problema inicial. Por tanto, tenemos la impresión de encontrarnos en un círculo vicioso. En esta sección vamos a ver un algoritmo que teóricamente proporciona un método para calcular el grupo de Galois de un polinomio irreducible separable arbitrario.

Sea $P = X^n - p_1X^{n-1} + p_2X^{n-2} + \cdots + (-1)^{n-1}p_{n-1} + (-1)^n p_n \in K[X]$, un polinomio irreducible y separable sobre $K$. Supongamos que $\alpha_1, \ldots, \alpha_n$ son las raíces de $P$ y $L = K(\alpha_1, \ldots, \alpha_n)$, el cuerpo de descomposición de $P$ sobre $K$. Vamos a considerar

$$\beta = T_1\alpha_1 + \cdots + T_n\alpha_n,$$

donde $T_1, \ldots, T_n$ son variables independientes y, para cada $\sigma \in S_n$, ponemos

$$\begin{array}{rcl} \sigma_T(\beta) & = & T_{\sigma(1)}\alpha_1 + \cdots + T_{\sigma(n)}\alpha_n \\ \sigma_\alpha(\beta) & = & T_1\alpha_{\sigma(1)} + \cdots + T_n\alpha_{\sigma(n)}. \end{array}$$

Obsérvese que hemos vuelto a la versión clásica en la que los elementos de $S_n$ son permutaciones de $\mathbb{N}_n = \{1, 2, \ldots, n\}$. Por otro lado para cada $\sigma \in S_n$, $\sigma_T$ denota el único automorfismo de $L[T_1, \ldots, T_n, X]$ que actúa como la identidad en $L[X]$ y $\sigma_T(T_i) = T_{\sigma(i)}$ para todo $i = 1, \ldots, n$. Esto define una acción de $S_n$ en $L[T_1, \ldots, T_n, X]$. O sea $\sigma_T(\beta)$ no es más que la aplicación de este automorfismo a $\beta$. Sin embargo, no es verdad que $\sigma \mapsto \sigma_\alpha$ se pueda considerar como una acción de $S_n$ en $L[T_1, \ldots, T_n, X]$ pues no es verdad que tenga por qué existir un automorfismo de $L$ que permute los $\alpha_i$ como $\sigma$. Pero si $\sigma \in \mathrm{Gal}(L/K)$ entonces $\sigma$ permuta los $\alpha_i$ con lo que consideramos $G$ como un subgrupo de $S_n$ y cada $\sigma \in G$ se extiende a un automorfismo de $L[T_1, \ldots, T_n, X]$ que denotaremos como $\sigma_\alpha$ de forma que $\sigma_\alpha(T_i) = T_i$ y $\sigma_\alpha(X) = X$.

Obsérvese que $\sigma_T(\beta) = \sigma_\alpha^{-1}(\beta)$ con lo que el siguiente polinomio podemos calcularlo de las dos siguientes formas alternativas que se indican

$$Q = \prod_{\sigma \in S_n} (X - \sigma_T(\beta)) = \prod_{\sigma \in S_n} (X - \sigma_\alpha(\beta)).$$

Si desarrollamos la segunda forma y lo ponemos como un polinomio en $X, T_1, \ldots, T_n$, observamos que cada uno de sus coeficientes se obtiene al sustituir $\alpha_1, \ldots, \alpha_n$ en un polinomio simétrico en $n$ variables y por tanto dichos coeficientes están en $K$. Vemos esto primero con un ejemplo y más adelante en general.

**Ejemplo 11.22** Si $n = 2$, entonces

$$\begin{array}{rcl} Q & = & (X - (T_1\alpha_1 + T_2\alpha_2))(X - (T_1\alpha_2 + T_2\alpha_1)) \\ & = & X^2 - (\alpha_1 + \alpha_2)(T_1 + T_2)X + \alpha_1\alpha_2(T_1^2 + T_2^2) + (\alpha_1^2 + \alpha_2^2)T_1T_2 \\ & = & X^2 - p_1(T_1 + T_2)X + p_2(T_1^2 + T_2^2) + (p_1^2 - 2p_2)T_1T_2. \end{array}$$

Para ver la afirmación anterior en general observamos que cada factor $X - \sigma_\alpha(\beta)$ es un polinomio homogéneo de grado 1 en las variables $X, T_1, \ldots, T_n$, deducimos que $Q$ es un polinomio homogéneo de grado $n!$. Por tanto, cada monomio de $Q$ en dichas variables tiene la forma $a_{(e)}T_1^{e_1} \ldots T_n^{e_n}X^{n! - \sum_{i=1}^n e_i}$ con $0 \leq e_i$ para todo $i$ y $\sum_{i=1}^n e_i \leq n!$. Para describir $a_{(e)}$ denotamos por $\Omega(e)$ el conjunto de las aplicaciones $f : S_n \to \mathbb{N}_n \cup \{\infty\}$ donde $|f^{-1}(i)| = e_i$ para todo $i$. Entonces

$$a_{(e)} = \sum_{f \in \Omega(e)} \prod_{\sigma \in f^{-1}(\mathbb{N}_n)} \alpha_{\sigma(f(i))}.$$

Por tanto $a_{(e)} = A_{(e)}(\alpha_1, \ldots, \alpha_n)$ donde

$$A_{(e)} = \sum_{f \in \Omega(e)} \prod_{\sigma \in f^{-1}(\mathbb{N}_n)} X_{\sigma(f(i))} \in K_0[X_1, \ldots, X_n],$$

donde $K_0$ es el anillo primo de $K$. Sea $\rho \in S_n$ y $f \in \Omega(e)$ y sea $f^\rho : S_n \to \mathbb{N}_n \cup \{\infty\}$ dada por $f^\rho(\sigma) = f(\rho^{-1}\sigma)$. Entonces $(f^\rho)^{-1}(i) = \{\sigma \in S_n : \rho^{-1}\sigma \in f^{-1}(i)\}$ y por tanto $\sigma \mapsto \rho^{-1}\sigma$ define biyección de $(f^\rho)^{-1}(i)$ a $f^{-1}(i)$. Eso implica que $f^\rho \in \Omega(e)$. Como además $f^{\rho\tau} = (f^\rho)^\tau$ y $f^1 = f$, deducimos que $f \mapsto f^\rho$ define una biyección de $\Omega(e)$ en si mismo. Entonces

$$\begin{aligned} \rho(A_{(e)}) &= \sum_{f \in \Omega(e)} \prod_{\sigma \in f^{-1}(\mathbb{N}_n)} X_{\rho\sigma(f(i))} = \sum_{f \in \Omega(e)} \prod_{\rho^{-1}\sigma \in f^{-1}(\mathbb{N}_n)} X_{\sigma(f(i))} \\ &= \sum_{f \in \Omega(e)} \prod_{\sigma \in (f^\rho)^{-1}(\mathbb{N}_n)} X_{\sigma(f(i))} = \sum_{f \in \Omega(e)} \prod_{\sigma \in f^{-1}(\mathbb{N}_n)} X_{\sigma(f(i))} = A_{(e)}. \end{aligned}$$

Es decir $A_{(e)}$ es un polinomio simétrico en las variables $X_1, \ldots, X_n$. Luego $A_{(e)}$ es un polinomio simétrico en los polinomios simétricos elementales en dichas variables, o sea $A_{(e)} = f_{(e)}(S_1, \ldots, S_n)$ con $P \in K_0[X_1, \ldots, X_n]$. Entonces

$$a_{(e)} = A_{(e)}(\alpha_1, \ldots, \alpha_n) = f_{(e)}(S_1(\alpha_1, \ldots, \alpha_n), \ldots, S_n(\alpha_1, \ldots, \alpha_n)) = P(p_1, \ldots, p_n).$$

En resumen

$$Q = \sum_{j=0}^{n!} \left( \sum_{(e), j + \sum_{i=1}^n e_j = n!} f_{(e)}(p_1, \ldots, p_n) T_1^{e_1} \cdots T_n^{e_n} \right) X^j,$$

donde cada $f_{(e)}(p_1, \ldots, p_n)$ es calculable en términos de los coeficientes de $P$. Esta expresión es teóricamente calculable, utilizando el método de expresión de un polinomio simétrico en términos de los polinomios simétricos elementales, por tanto teóricamente podemos calcular $Q$ sin necesidad de conocer las raíces $\alpha_1, \ldots, \alpha_n$ de $P$, como lo hemos hecho en el Ejemplo 11.22.

El siguiente paso consiste en factorizar $Q$ en el anillo $K[X, T_1, \ldots, T_n]$:

$$Q = Q_1 \ldots Q_k.$$

Como el conjunto de las raíces de $Q$, como polinomio en $X$, es $A = \{\sigma_T(\beta) : \sigma \in S_n\}$, hay una partición $S_n = A_1 \cup \cdots \cup A_k$ de forma que

$$Q_i = \prod_{\sigma \in A_i} (X - \sigma_X(\beta)).$$

Supondremos que $1 \in A_1$. Si consideramos $S_n$ actuando en las variables $T_1, \ldots, T_n$, se tiene que $\sigma_T(Q) = Q$ y por tanto cada $\sigma \in S_n$ produce una permutación de los $Q_i$. El siguiente teorema proporciona la clave para calcular el grupo de Galois de $P$ sobre $K$.

**Teorema 11.23** *Si $P \in K[X]$ es irreducible y separable sobre $K$, entonces $\mathrm{Gal}_K(P) \simeq \mathrm{Estab}^T_{S_n}(Q_1)$, donde $Q_1$ es como antes y $\mathrm{Estab}^T_{S_n}(Q_1)$ corresponde a la acción de $S_n$ en las variables $T_i$.*

**Demostración.** Obsérvese que

$$\begin{aligned} A_1 &= \{\sigma \in S_n : X - \sigma_T(\beta) \text{ divide a } Q_1\} = \{\sigma \in S_n : X - \beta \text{ divide a } \sigma_T^{-1}(Q_1)\} \\ &= \{\sigma \in S_n : Q_1 = \sigma_T^{-1}(Q_1)\} = \mathrm{Estab}^T_{S_n}(Q_1). \end{aligned}$$

Sean $G = \mathrm{Gal}_K(P)$ y

$$Q_G = \prod_{\sigma \in G} (X - \sigma_\alpha(\beta)) = \prod_{\sigma \in G} (X - \sigma_T(\beta)).$$

Entonces $Q_G$ divide a $Q$, con lo que $Q_G$ es el producto de algunos de los $Q_i$. Además $\beta$ es una raíz de $Q_G$, con lo que uno de los divisores irreducibles de $Q_G$ es $Q_1$. Por tanto $Q_1$ divide a $Q_G$. Esto prueba que $A_1 \subseteq G$.

Recíprocamente, si $\tau \in G$, entonces $\tau^{-1}(Q_1) = Q_1$ pues $Q_1 \in K[X]$. Luego

$$\begin{aligned} \tau_T(Q_1) &= \textstyle\prod_{\sigma\in A_1}(X - \tau_T\sigma_T(\beta)) = \prod_{\sigma\in A_1}(X - \tau_\alpha^{-1}\sigma_T(\beta)) = \tau_\alpha^{-1}\left(\prod_{\sigma\in A_1}(X - \sigma_T(\beta))\right) \\ &= \tau_\alpha^{-1}(Q_1) = Q_1, \end{aligned}$$

es decir $\tau \in \mathrm{Estab}^T_{S_n}(Q_1)$. □

Está claro que el método proporcionado a pesar de ser algorítmico es poco satisfactorio ya que requiere unos cálculos enormes. Sin embargo, para el caso en que $P$ sea un polinomio irreducible separable de grado primo el Teorema 11.20, junto con el Teorema de Factorización de Resolvente proporciona un método alternativo para estudiar si $P$ es resoluble.

**Proposición 11.24** *Sean $P$ sea un polinomio irreducible de grado primo $p$ sobre un cuerpo $K$ de característica 0, $f \in K[X_1, \ldots, X_p]$ un polinomio tal que $\mathrm{Estab}_{S_p}(f) = \mathcal{A}f_p$ y $R = R_{f,P}$.*

*(1) Si $K$ no contiene ninguna raíz de $R$, entonces $P$ no es resoluble por radicales sobre $K$.*

*(2) Si $K$ tiene una raíz simple de $R$, entonces $P$ es resoluble por radicales sobre $K$.*

**Demostración.** Sean $\alpha_1, \ldots, \alpha_p$ las raíces de $P$ en un cuerpo de descomposición de $P$ sobre $K$ y sea $\theta = f(\alpha_1, \ldots, \alpha_p)$.

1. Si $P$ es resoluble por radicales sobre $K$, entonces $G = \mathrm{Gal}_K(P)$ es resoluble (Teorema 10.7) y por tanto $G$ es afín (Teorema 11.20), es decir existe $\sigma \in G$ tal que $\sigma^{-1}G\sigma \subseteq \mathcal{A}f_p = \mathrm{Estab}_{S_p}(f)$. Aplicando el Teorema de Factorización de Resolventes (Teorema 11.10) deducimos que $\sigma(\theta)$ es una raíz de $R$ que pertenece a $K$.

2. Si $\beta \in K$ es una raíz simple de $R$ entonces $\beta = \sigma(\theta)$ para algún $\sigma \in S_p$. Del Teorema de Factorización de Resolventes deducimos que $\sigma^{-1}G\sigma \subseteq \mathcal{A}f_p$, con lo que $G$ es un subgrupo afín de $S_p$. Del Teorema 11.20 deducimos que $G$ es resoluble y, del Teorema 10.7, concluimos que $P$ es resoluble por radicales sobre $K$. □

Para fijar ideas supongamos que $P$ tiene grado 5 y sea

$$\begin{aligned} f &= \textstyle\sum_{\sigma\in\mathcal{A}f_5}\overline{\sigma}(x_1^3x_2^2x_3) \\ &= x_1^3x_2^2x_3 + x_1x_2^2x_3^3 + x_2^3x_3^2x_4 + x_1^2x_3^3x_4 + x_1^3x_2x_4^2 + x_1x_2^3x_4^2 + x_1^2x_3x_4^3 + \\ &\quad x_2x_3^2x_4^3 + x_1^2x_2^3x_5 + x_1^3x_3^2x_5 + x_3^3x_4^2x_5 + x_2^2x_4^3x_5 + x_2^3x_3x_5^2 + x_2x_3^3x_5^2 + \\ &\quad x_1^3x_4x_5^2 + x_1x_4^3x_5^2 + x_1^2x_2x_5^3 + x_1x_3^2x_5^3 + x_2^2x_4x_5^3 + x_3x_4^2x_5^3 \end{aligned}$$

Entonces $\mathrm{Estab}_{S_5}(f) = \mathcal{A}f_5$. Podemos ahora calcular $R_{f,P}$, que es un polinomio de grado 6 cuyos coeficientes son polinomios en los coeficientes de $P$, observando que los coeficientes de $R_{f,P}$ son polinomios simétricos en las raíces de $P$. Por tanto $R_{f,P}$ es un polinomio de grado 6 cuyos coeficientes se pueden expresar en términos de los coeficientes de $P$. Más concretamente, si

$$P = X^5 + a_1X^4 + a_2X^3 + a_3X^2 + a_4X + a_5$$

entonces $R_{f,P}$ es igual a un polinomio de grado 6 en $X$ cuyos coeficientes dependen de los de $P$. Por desgracia este polinomio que se puede ver en el Apéndice ocupa varías páginas. Puede parecer que esto es bastante inútil por dos razones. En primer lugar por la longitud del polinomio y en segundo lugar porque reducimos el problema de decidir sobre la resolubilidad de una ecuación de grado 5 a la búsqueda de una raíz de un polinomio de grado 6. Sin embargo, el polinomio proporciona un método rápido para descubrir si un polinomio de grado 5 es resoluble por radicales en algunos casos. Por supuesto será necesario utilizar un ordenador para calcular la resolvente. Veamos algunos ejemplos.

**Ejemplos 11.25** Si $P = X^5 + X^2 - 1$, entonces aplicando la expresión en el apéndice podemos obtener que $R_{f,P} = 1 + 6T + 15T^2 + 20T^3 + 15T^4 + 6T^5 + T^6$. Como este polinomio no tiene ninguna raíz en $\mathbb{Q}$, de la Proposición 11.24 deducimos que $P$ no es resoluble por radicales sobre $\mathbb{Q}$.

Sin embargo si ponemos $P = -1 + 5X + 10X^2 + 10X^3 + 5X^4 + X^5$, entonces $R_{f,P} = -256000000 - 60800000T - 5600000T^2 - 240000T^3 - 4000T^4 + 20T^5 + T^6 = (T - 80)(T + 20)^5$. Como $R_{f,P}$ tiene una raíz simple en $\mathbb{Q}$, de la Proposición 11.24 deducimos que $P$ es resoluble por radicales sobre $\mathbb{Q}$.

# Problemas

**11.1** Demostrar el Corolario 11.4 y los Teoremas 11.15 y 11.16, cambiando la hipótesis de que $K$ tenga característica 0 por la de que $K$ tenga característica diferente de 2 y 3; y el Corolario 11.21, cambiando la hipótesis de que $K$ tenga característica 0 por la de que la característica de $K$ sea mayor que el grado de $f$.

**11.2** Sean $K$ un subcuerpo de los números reales, $p \in K[X]$ irreducible de grado 3. Demostrar que el discriminante de $p$ es negativo si y solo si $p$ tiene una única raíz real y que en caso contrario $p$ tiene 3 raíces reales.

**11.3** Demostrar que para todo cuerpo $K$ el polinomio $X^3 - 3X + 1$ es irreducible o se descompone completamente sobre $K$.

**11.4** Sean $K$ un cuerpo de característica diferente de 2 y $p \in K[X]$ un polinomio separable irreducible con discriminante $D$ tal que $\mathrm{Gal}(p/K)$ es cíclico. Demostrar que $\sqrt{D} \in K$ si y solo si $|\mathrm{Gal}_K(p)|$ es impar.

**11.5** Sea $L$ el cuerpo de descomposición de $X^3 - X + 1$ sobre $\mathbb{Q}$. Hacer un diagrama de los subcuerpos de $L$ y describir el grupo de Galois de $L$ sobre cada uno de estos cuerpos.

**11.6** Sea $L$ el cuerpo de descomposición de un polinomio irreducible de grado 3 sobre un cuerpo $K$ de característica 0. Demostrar que $L/K$ tiene tres o ninguna subextensión de índice 2.

**11.7** Sean $K$ un cuerpo de característica 0, $f \in K[X]$ irreducible de grado 4, $L$ el cuerpo de descomposición de $f$ sobre $K$, $F$ el cuerpo de descomposición de la resolvente cúbica de $f$ sobre $K$, $m = [F : K]$ y $G = \mathrm{Gal}(L/K)$. Demostrar

(1) $m = 1, 2, 3$ ó 6.

(2) Si $m = 6$, entonces $G \simeq S_4$.

(3) Si $m = 3$, entonces $G \simeq A_4$.

(4) Si $m = 1$, entonces $G \simeq C_2 \times C_2$ (el producto directo de dos grupos cíclicos de orden 2).

(5) Si $m = 2$ y $f$ es irreducible sobre $F$, entonces $G \simeq D_8$, el grupo diédrico de orden 8.

(6) Si $m = 2$ y $f$ es reducible sobre $F$, entonces $G$ es cíclico de orden 4.

**11.8** Sea $P$ un polinomio irreducible de grado 4 sobre un cuerpo $K$ de característica 0 y sea $\alpha$ una raíz de $K$ en una extensión de $K$. Demostrar que $K$ y $K(\alpha)$ son las únicas subextensiones de $K(\alpha)/K$ si y solo si $\mathrm{Gal}_K(P)$ is isomorfo a $A_4$ ó $S_4$.

**11.9** Demostrar que si $K$ es un subcuerpo del cuerpo de los números reales, $p \in K[X]$ es irreducible de grado 4 y $K$ tiene exactamente dos raíces de $p$, entonces $\mathrm{Gal}(f/K) \simeq S_4$ ó $D_4$.

**11.10** Sean $K$ un cuerpo de característica cero, $p = X^4 + aX^2 + b \in K[X]$ irreducible y $G = \mathrm{Gal}_K(p)$. Demostrar

(1) Si $b$ es un cuadrado en $K$, entonces $G \simeq C_2 \times C_2$.

(2) Si $b$ no es un cuadrado en $K$ pero $b(a^2 - 4b)$ es un cuadrado en $K$, entonces $G$ es cíclico de orden 4.

(3) Si ninguna de las dos condiciones anteriores se verifica entonces $G \simeq D_4$.

**11.11** Sean $K$ un cuerpo de característica cero, $p = X^4 + bX^3 + cX^2 + bX + 1 \in K[X]$ irreducible, $G = \mathrm{Gal}_K(p)$, $\alpha = c^2 + 4c + 4 - 4b$ y $\beta = b^2 - 4c + 8$. Demostrar

(1) Si $\alpha$ es un cuadrado en $K$, entonces $G \simeq C_2 \times C_2$.

(2) Si $\alpha$ no es un cuadrado en $K$ pero $\alpha\beta$ es un cuadrado en $K$, entonces $G$ es cíclico de orden 4.

(3) Si ninguna de las dos condiciones anteriores se verifica, entonces $G \simeq D_4$.

**11.12** Determinar el grupo de Galois del polinomio $X^4 - 5$ sobre cada uno de los siguientes cuerpos: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$ y $\mathbb{Q}(i\sqrt{5})$.

**11.13** Determinar el grupo de Galois sobre los cuerpos indicados de cada uno de los siguientes polinomios:

| | | |
|---|---|---|
| $X^3 + 2X + 2$ sobre $\mathbb{Z}_3$. | $X^4 + 6X^2 + 9$ sobre $\mathbb{Q}$. | $X^4 - 4X^2 + 2$ sobre $\mathbb{Q}$. |
| $X^5 + 4X^3 + X$ sobre $\mathbb{Q}$. | $X^4 + X^2 - 6$ sobre $\mathbb{Q}$. | $X^4 - 4X^2 + 16$ sobre $\mathbb{Q}$. |
| $X^4 - X^2 - 2$ sobre $\mathbb{Q}$. | $X^6 - 9$ sobre $\mathbb{Q}$. | $4X^4 - 8X^2 + 1$ sobre $\mathbb{Q}$. |
| $X^5 - 3x^3 - 2X^2 + 6$ sobre $\mathbb{Q}$. | $X^3 - 10$ sobre $\mathbb{Q}(\sqrt{-3})$. | $X^4 - 5$ sobre $\mathbb{Q}(\sqrt{5})$. |
| $X^4 - 2$ sobre $\mathbb{Q}(i)$. | | |

**11.14** Demostrar que si $p \in K[X]$ es irreducible, $K$ tiene característica 0 y $p$ es resoluble por radicales, entonces $|\mathrm{Gal}_K(p)|$ divide a $p(p-1)$.

**11.15** Sea $f \in K[X]$ irreducible de grado impar y resoluble por radicales sobre $K$, donde $K$ es un subcuerpo de $\mathbb{R}$. Demostrar que el número de raíces reales de $f$ es 1 ó $p$.

**11.16** Demostrar que el discriminante del polinomio $p = X^4 + aX^3 + bX^2 + cX + d$ es

$$D = a^2b^2c^2 - 4b^3c^2 - 4a^3c^3 + 18abc^3 - 27c^4 - 4a^2b^3d + 16b^4d + 18a^3bcd - 80ab^2cd \\ -6a^2c^2d + 144bc^2d - 27a^4d^2 + 144a^2bd^2 - 128b^2d^2 - 192acd^2 + 256d^3$$

y que si $p$ es irreducible y separable sobre $K$ entonces $\mathrm{Gal}_K(p)$ es isomorfo a $A_4$ ó $C_2 \times C_2$ si y sólo si $D$ es un cuadrado en $K$.

**11.17** Sea $f$ un polinomio separable con coeficientes reales y $n$ el número raíces no reales de $f$. Demostrar que el discriminante de $f$ es positivo si y solo si $n$ es múltiplo de 4. (Indicación: Obsérvese que si $\alpha$ y $\beta$ son dos raíces de $f$ que no son iguales ni conjugadas, entonces $(\alpha - \beta)(\overline{\alpha} - \overline{\beta}) \in \mathbb{R}$ y que $(\alpha - \overline{\alpha})^2 < 0$.)

**11.18** Demostrar las siguientes propiedades para $E/K$ una extensión de cuerpos (no necesariamente finita) y $f \in K[X]$ un polinomio irreducible de grado primo $p \geq 5$.

(1) Si $f$ es resoluble por radicales sobre $K$, entonces el número de raíces de $f$ en $E$ es 1 ó $p$. (Indicación: Utilizar el Teorema 11.21.)

(2) Si $f = X^p - aX + b \in \mathbb{Q}[X]$ con $a > 0$ entonces $f$ no es resoluble por radicales sobre $\mathbb{Q}$.

(3) Si $E = \mathbb{R}$, $p \equiv 1 \bmod 4$ y el discriminante de $f$ es negativo entonces $f$ no es resoluble por radicales sobre $K$. (Indicación: Utilizar el Ejercicio 11.17).

**11.19** Sean $p = \sum_{i=1}^{n} p_i X^i$ y $q = \sum_{i=1}^{n} q_i X^i$ dos polinomios de grado $n$ tales que $q_i = p_{n-i}$ para todo $i$. Demostrar que $p$ es resoluble por radicales si y solo si lo es $q$.

**11.20** Decidir cuáles de los siguientes polinomios son resolubles por radicales sobre $\mathbb{Q}$ y si es posible encontrar una extensión radical que contenga su cuerpo de escisión.

$X^5 - 2X^4 + 2, \quad X^5 - 4X^2 + 2, \quad X^5 - 4X + 2, \quad X^5 - 4X + 10, \quad x^6 - 10x^2 + 5, X^7 - 10X^5 + 15X + 5.$

# Apéndice A

# Teoremas de Cauchy y de Sylow

Sea $X$ un conjunto y $G$ un grupo y sea $S_X$ el grupo de las permutaciones de los elementos de $X$. Recordemos que una acción de $G$ en $X$ es un homomorfismo de grupos $\sigma : G \to S_X$. Dada una acción $\sigma$ de $G$ en $X$ definimos

$$g \cdot x = \sigma(g)(x), \quad (g \in G, x \in X).$$

Entonces se verifican las siguientes condiciones para todo $g, h \in G$ y $x \in X$:

(1) $g \cdot (h \cdot x) = (gh) \cdot x$.

(2) $1 \cdot x = x$.

Recíprocamente, si tenemos una aplicación $G \times X \to X$ de forma que la imagen de $(g, x)$ la denotamos $g \cdot x$ y se verifican las condiciones 1 y 2 anteriores entonces para cada $g \in G$ la aplicación $\sigma(g) : X \to X$ es una biyección (con inversa $\sigma(g^{-1})$ y $\sigma : G \to S_X$ es un homomorfismo de grupos.

Si tenemos una acción de $G$ en $X$ y $x \in X$ entonces definimos

$$G \cdot x = \{g \cdot x : g \in G\} \quad \text{y} \quad \text{Estab}_G(x) = \{g \in G : g \cdot x = x\}.$$

Entonces $\text{Estab}_G(x)$ es un subgrupo de $G$ que llamamos *estabilizador* de $x$ en $G$ y tenemos una aplicación:

$$\begin{array}{rcl} G/\text{Estab}_G(x) & \to & G \cdot x \\ g\text{Estab}_G(x) & \mapsto & g \cdot x \end{array}$$

Por tanto,

$$|G \cdot x| = [G : \text{Estab}_G(x)] \quad (x \in X). \tag{A.1}$$

Los conjuntos $\{G \cdot x : x \in X\}$ forman una partición de $X$ y se llaman *órbitas* de $x$. De (A.1) se deduce que si $G$ es finito entonces los cardinales de las órbitas dividen al orden de $G$. Por otro lado si $R$ es un conjunto de representantes de las órbitas, es decir $R$ tiene exactamente un elemento de cada órbita, entonces $\{G \cdot r : r \in R\}$ es una partición de $G$ y por tanto, si $X$ es finito entonces la Ecuación de Órbitas toma la siguiente forma:

$$|X| = \sum_{r \in R} |G \cdot r| = \sum_{r \in R} [G : \text{Estab}_G(r)]. \tag{A.2}$$

Esta ecuación se llama la *Ecuación de Órbitas*.

**Ejemplos A.1** (1) *Acción por conjugación de un grupo en si mismo.*

Sea $G$ un grupo. Definimos la siguiente acción de $G$ en si mismo:

$$g \cdot x = gxg^{-1}.$$

Las órbitas de esta acción son las clases de conjugación de $G$ y el estabilizador de un elemento $x$ de $G$ es su centralizador $\mathrm{Cen}_G(x)$. Denotaremos la clase de conjugación de $g$ en $G$ con $g^G$. De la fórmula (A.1) deducimos que

$$|x^G| = [G : \mathrm{Cen}_G(x)], \quad (x \in G).$$

Las clases de conjugación de $G$ con un único elemento son las formadas por los elementos del centro $Z(G)$ de $G$. Sea $X$ un conjunto de representantes de las clases de conjugación de $G$ que no están en $Z(G)$. Entonces los conjuntos $Z(G)$ y $x^G$ con $x \in G$ forman una partición de $G$ y por tanto, si $G$ es finito entonces

$$|G| = |Z(G)| + \sum_{x \in X} [G : \mathrm{Cen}_G(x)]. \tag{A.3}$$

Esta fórmula se llama la *Ecuación de Clases*.

(2) *Acción por conjugación de un grupo en el conjunto de sus subgrupos.*

Consideremos ahora el conjunto $\Omega$ formado por todos los subgrupos de $G$ y definimos la siguiente acción de $G$ en $\Omega$:

$$g \cdot H = gHg^{-1}, \quad (g \in G, H \leq G).$$

La órbita de un subgrupo $H$ de $G$ es el conjunto formado por todos los conjugados de $H$ en $G$ y su estabilizador es el normalizador $N_G(H) = \{g \in G : gHg^{-1} = H\}$, que es el mayor subgrupo de $G$ en el que $H$ es normal. Por tanto el número de subgrupos de $G$ que son conjugados a $H$ es $[G : N_G(H)]$. Las órbitas con un solo elemento son las formadas por un subgrupo normal.

**Teorema A.2 (Cauchy)** *Sea $G$ un grupo finito. Si $p$ es un divisor primo de $|G|$, entonces $G$ posee un elemento de orden $p$.*

**Demostración.** Sea $\Omega$ el conjunto de las $p$-tuplas de elementos de $G$ cuyo producto es 1:

$$\Omega = \{(x_1, \ldots, x_p) : x_i \in G \text{ para cada } i \text{ y } x_1 \cdots x_p = 1\}.$$

Es claro que una $p$-tupla $(x_1, \ldots, x_p)$ de elementos de $G$ está en $\Omega$ si y sólo si $x_p = (x_1 x_2 \cdots x_{p-1})^{-1}$. Por tanto, para dar un elemento de $\Omega$ podemos elegir sus $p-1$ primeras componentes arbitrariamente en $G$, y la última queda entonces determinada por éstas. En consecuencia se tiene $|\Omega| = |G|^{p-1}$, y en particular $p$ divide a $|\Omega|$.

Sea $C = \langle c \rangle$ un grupo cíclico de orden $p$, y consideremos su acción por la izquierda en $\Omega$ dada por

$$(c, (x_1, \ldots, x_p)) \mapsto (x_p, x_1, x_2 \ldots, x_{p-1}).$$

Los puntos fijos para esta acción son los elementos de $\Omega$ de la forma $(x, x, \ldots, x)$, que se corresponden con los elementos de $G$ tales que $x^p = 1$. Por tanto, el resultado quedará demostrado si vemos que $\Omega$ contiene algún punto fijo distinto del $(1, 1, \ldots, 1)$.

Sea pues $k \geq 1$ el número de órbitas unitarias (o de puntos fijos) para la acción dada, y sea $q$ el número de órbitas no unitarias. Por (A.1), cada órbita no unitaria tiene cardinal $p$, y así $|\Omega| = k + pq$. Como $p$ divide a $|\Omega|$ deducimos que $p$ divide a $k$, y como $k \neq 0$ deducimos que hay puntos fijos diferentes del $(1, 1, \ldots, 1)$, como queríamos ver. □

Sea $p$ un número primo. Un *$p$-grupo* es un grupo en el que todos los elementos tienen orden potencia de $p$. Por el Teorema de Cauchy y el Teorema de Lagrange un grupo finito es un $p$-grupo si y solo su orden es una potencia de $p$. Otra consecuencia notable del Teorema de Cauchy es la siguiente:

**Proposición A.3** *Los p-grupos verifican el recíproco del Teorema de Lagrange. Es decir, un p-grupo G posee un subgrupo de orden d para cada divisor d de |G|.*

**Demostración.** Sea $|G| = p^n$ con $n \geq 1$, y procedamos por inducción en $n$, con el caso $n = 1$ trivial. En el caso general, el divisor $d$ ha de ser de la forma $p^m$ con $m \leq n$. Por la Proposición 2.25 de GyA¿, el centro $Z = Z(G)$ no es trivial, y por tanto contiene un elemento $g$ de orden $p$. El subgrupo $N = \langle g \rangle$ es normal en $G$ (¿por qué?), y el cociente $G/N$ tiene orden $p^{n-1}$. Por tanto $p^{m-1}$ divide a $|G/N|$, y la hipótesis de inducción nos dice que $G/N$ posee un subgrupo $X$ de orden $p^{m-1}$. Por el Teorema de la Correspondencia, existe un subgrupo $H$ de $G$ que contiene a $N$ y tal que $X = H/N$, y entonces se tiene $|H| = |X| \cdot |N| = p^{m-1}p = p^m$, luego $H$ es el subgrupo que buscábamos. □

**Definición A.4** *Sea G un grupo finito y sea p un entero primo positivo. Un subgrupo de G que sea un p-grupo se llama un p-*subgrupo *de G. Por los Teoremas de Lagrange y de Cauchy, G tiene algún p-subgrupo no trivial si y solo si p divide a|G|.*

*Si $|G| = p^n r$ con $p \nmid r$, un subgrupo de G de orden $p^n$ (es decir, un p-subgrupo del mayor orden posible) se llama un p-*subgrupo de Sylow *de G.*

## El Primer Teorema de Sylow

**Teorema A.5 (Primer Teorema de Sylow)** *Sea G un grupo finito y sea p un divisor primo de |G|. Entonces G contiene algún p-subgrupo de Sylow.*

**Demostración.** Sea $m = |G|$ y pongamos $m = p^n r$ con $p \nmid r$. Se trata de demostrar que $G$ tiene un subgrupo de orden $p^n$, y lo hacemos por inducción sobre $m$. Como $p$ divide a $m$, el menor caso posible es $m = p$ y el resultado es entonces trivial. Así, supondremos que $m > p$ y que el enunciado del teorema es válido para cualquier grupo de orden menor que $m$. Distinguiremos dos casos:

Si existe $g \in G \setminus Z(G)$ tal que $p$ no divide a $[G : \mathrm{Cen}_G(g)]$ entonces, por el Teorema de Lagrange y el Teorema Fundamental de la Aritmética, $p^n$ divide a $|\mathrm{Cen}_G(g)|$. Como éste es un subgrupo propio de $G$, la hipótesis de inducción implica que $\mathrm{Cen}_G(g)$ posee un subgrupo de orden $p^n$, y por tanto $G$ también.

En otro caso, se tiene que $p$ divide a $[G : \mathrm{Cen}_G(g)]$ para cada $g \in G \setminus Z(G)$. Aplicando la Ecuación de Clases (A.3) se deduce que $p$ ha de dividir a $Z(G)$. Por el Teorema de Cauchy (A.2), $Z(G)$ contiene un subgrupo $N$ de orden $p$, que será normal en $G$. Como $|G/N| = m/p < m$ y $p^{n-1}$ es la mayor potencia de $p$ que divide a $|G/N|$, la hipótesis de inducción nos dice que existe un subgrupo $X$ de $G/N$ tal que $|X| = p^{n-1}$. Por el Teorema de la Correspondencia se tiene $X = H/N$ para algún subgrupo $H$ de $G$ que contiene a $N$. Entonces $|H| = |N| \cdot |X| = p^n$, y por tanto $H$ es el subgrupo que buscábamos. □

Aplicando ahora la Proposición A.3 a un subgrupo de Sylow de $G$ se tiene:

**Corolario A.6** *Un grupo finito posee p-subgrupos de todos los órdenes posibles. Es decir, si G es un grupo finito y k es un entero tal que $p^k$ divide a |G|, entonces G contiene algún subgrupo de orden $p^k$.*

Estos resultados nos dan información sobre la existencia de ciertos subgrupos de los grupos finitos. Por ejemplo, sea $G$ un grupo del que sabemos que $|G| = 28.600 = 2^3 \cdot 5^2 \cdot 11 \cdot 13$. Entonces $G$ tiene subgrupos de cualquiera de los órdenes 2, 4, 8, 5, 25, 11 ó 13.

¿Qué pasa con los subgrupos de otros órdenes? Los resultados anteriores no afirman nada sobre su existencia, y de hecho no es posible hacer ninguna afirmación general en ese sentido. Por ejemplo, si $|G| = 12$, lo anterior nos dice que $G$ tiene subgrupos de órdenes 2, 3 y 4 (y por supuesto 1 y 12); en cuanto a los subgrupos de orden 6, existen para el grupo cíclico $\mathbb{Z}_{12}$ o para el grupo diédrico $D_6$, pero no existen para el grupo alternado $A_4$.

## El Segundo Teorema de Sylow

A lo largo de este párrafo suponemos que $|G| = p^n r$ con $p \nmid r$. Por el Primer Teorema (A.5) podemos fijar un $p$-subgrupo de Sylow $P$ de $G$; es decir, un subgrupo tal que $|P| = p^n$.

Denotaremos por $S_P$ el conjunto de todos los subgrupos de $G$ que son conjugados de $P$; es decir, los elementos de la órbita de $P$ en la acción de $G$ en el conjunto $\Omega$ de sus subgrupos. Como "conjugar por $x$" es un automorfismo de $G$, todos los elementos de $S_P$ tienen el mismo cardinal que $P$ y, en consecuencia, son $p$-subgrupos de Sylow de $G$. Una parte del Segundo Teorema de Sylow afirma que, recíprocamente, todo $p$-subgrupo de Sylow de $G$ está en $S_P$ (es decir, es conjugado de $P$). Para ver esto primero observamos que $|S_P| = [G : N_G(P)]$ y $P \subseteq N_G(P)$. Por tanto $|S_P|$ divide a $[G : P] = r$.

Consideremos ahora un subgrupo $H$ de $G$ y consideremos la restricción de la acción de $G$ en $\Omega$ por conjugación a una acción de $H$ en $S_p$. Las órbitas de esta acción tienen cardinal divisor del orden de $H$ y por tanto si $H$ es un $p$-grupo, todas ellas tienen orden una potencia de $p$.

**Lema A.7** *Sea $P$ un subgrupo de Sylow de $G$, $H$ un $p$-subgrupo de $G$ y consideramos $H$ actuando por conjugación en el conjunto $S_P$ de los conjugados de $P$ en $G$:*

*(1) $S_P$ tiene una órbita con un único elemento.*

*(2) La órbita $H \cdot Q$ de un elemento $Q$ de $S_P$ tiene un único elemento si y solo si $H \subseteq Q$.*

**Demostración.** 1. Aplicando la Ecuación de Órbitas (A.2) a esta acción: tenemos

$$|S_P| = \sum |Q^H| = \sum [H : \mathrm{Estab}_H(Q)],$$

donde $Q$ recorre un conjunto de representantes de las órbitas. Como $|S_P| \mid r$ tenemos que $p \nmid |S_p|$ y en consecuencia $p$ no divide a $[H : \mathrm{Estab}_H(Q)]$ para algún $Q \in S_P$. Como $H$ es un $p$-grupo, ese índice debe valer 1 y así $\mathrm{Estab}_H(Q) = H$ con lo que $|H \cdot Q| = [H : H] = 1$.

2. Si $x \in Q$ entonces $xQx^{-1} = Q$. Por tanto, si $H \subseteq Q$ entonces $H = \mathrm{Estab}_H(Q)$ y por tanto $|H \cdot Q| = 1$. Recíprocamente, supongamos que $|H \cdot Q| = 1$. Sea $N = N_G(Q)$. La hipótesis nos dice que $xQ = Qx$ para cada $x \in H$, es decir $H \subseteq N_G(Q)$. Por tanto $H$ es un subgrupo de $N$. Como además $Q$ es un subgrupo normal de $N$, del Tercer Teorema de Isomorfía tenemos que $HQ$ es un subgrupo de $N$ con cardinal $|HQ| = \frac{|H| \cdot |Q|}{|Q \cap H|}$. Como tanto $H$ como $Q$ son $p$-grupos tenemos que $HQ$ es un $p$-subgrupo de $G$ que contiene a $Q$, pero como $Q$ es un $p$-subgrupo de Sylow de $G$ tenemos que $HQ = Q$, o sea $H \subseteq Q$. □

Podemos ya demostrar el Segundo Teorema de Sylow.

**Teorema A.8 (Segundo Teorema de Sylow)** *Sean $G$ un grupo finito, $p$ un divisor primo de $|G|$, $P$ un $p$-subgrupo de Sylow de $G$ y $H$ un $p$-subgrupo de $G$. Entonces $H$ está contenido en algún subgrupo conjugado de $P$.*

*En particular, todos los $p$-subgrupos de Sylow de $G$ son conjugados entre sí.*

**Demostración.** Por el Lema A.7, la acción del $H$ en $S_P$ tiene una órbita $\{Q\}$ con un único elemento y $H \subseteq Q$. Como $P$ y $Q$ son conjugados en $G$ se tiene que $H$ está contenido en un conjugado de $P$. En el caso de que $H$ sea un $p$-subgrupo necesariamente $H = Q$ y por tanto $H$ es conjugado de $P$. □

El siguiente corolario se usa a menudo para contar elementos de un grupo.

**Corolario A.9** *Sea $G$ un grupo finito y sea $p$ un divisor primo de $|G|$. La unión de todos los $p$-subgrupos de Sylow de $G$ coincide con el conjunto de todos los elementos de $G$ cuyo orden es una potencia de $p$.*

**Demostración.** Es claro que el orden de cualquier elemento de esa unión es una potencia de $p$ (incluyendo al neutro, cuyo orden es $p^0$). Recíprocamente, si $o(x) = p^k$ entonces $x$ está en el $p$-subgrupo $\langle x \rangle$, y por tanto está en algún $p$-subgrupo de Sylow por el Segundo Teorema de Sylow. □

## El Tercer Teorema de Sylow

Sea $n_p$ el número de $p$-subgrupos de Sylow de $G$. Del Segundo Teorema de Isomorfía tenemos que si $P$ es un subgrupo de Sylow de $G$ entonces $n_p$ es el número de conjugados de $P$ en $G$. Ya hemos visto que $|S_p|$ divide a $r$. Por tanto $n_p \mid r$ y $n_p = 1$ si y solo si $P$ es normal en $G$.

**Teorema A.10 (Tercer Teorema de Sylow)** *Sea $G$ un grupo finito, sea $p$ un divisor primo de $|G|$ y sea $|G| = p^n r$ con $p \nmid r$. Entonces el número $n_p$ de $p$-subgrupos de Sylow de $G$ verifica:*

*(1) $n_p$ divide a $r$.*

*(2) $n_p \equiv 1 \bmod p$.*

*(3) $n_p = 1$ si y solo si algún $p$-subgrupo de Sylow de $G$ es normal en $G$.*

**Demostración.** 1 y 3 ya los hemos visto.

2. Sea $P$ un $p$-subgrupo de Sylow de $G$. Por el Lema A.7, la acción de $P$ en $S_P$ por conjugación tiene exactamente una órbita con 1 elementos. Las demás órbitas tendrán que tener orden distinto de 1 y divisor de $|P|$, con lo que serán potencias de $p$. Por tanto, en la Ecuación de Órbitas (A.2)

$$n_p = |S_P| = \sum |H \cdot Q^H|,$$

exactamente uno de los sumandos vale 1, y cada uno de los otros es múltiplo de $p$. En consecuencia, $n_p \equiv 1 \bmod p$. □

## Criterios de no simplicidad

En este párrafo usaremos los Teoremas de Sylow para obtener un criterio que nos permite afirmar que ciertos grupos no son simples. Este resultado, junto con otros del mismo tipo que se han visto antes, nos permitirá demostrar que no hay grupos simples no abelianos con menos de 60 elementos.

**Proposición A.11** *Sea $G$ un grupo finito con $|G| = pq$ ó $|G| = pq^2$, donde $p, q$ son dos primos distintos. Entonces se tiene $n_p = 1$ ó $n_q = 1$, y en consecuencia $G$ no es un grupo simple.*

**Demostración.** Usaremos en varias ocasiones el Tercer Teorema de Sylow (A.10). Si $|G| = pq$ podemos asumir que $p < q$, luego $p \not\equiv 1 \bmod q$ y en consecuencia $n_q \neq p$, por lo que $n_q = 1$. Suponemos pues que $|G| = pq^2$, y distinguimos tres casos:

Si $p < q$ entonces $p \not\equiv 1 \bmod q$, y por tanto $n_q = 1$.

Si $p > q^2 (> q)$ entonces $q, q^2 \not\equiv 1 \bmod p$ y en consecuencia $n_p \neq q, q^2$, por lo que $n_p = 1$.

Por último, si $q < p < q^2$ entonces $q \not\equiv 1 \bmod p$ y en consecuencia $n_p \neq q$. Por tanto o bien $n_p = 1$, y hemos terminado, o bien $n_p = q^2$, y basta ver que esta última opción implica que $n_q = 1$. Supongamos pues que $n_p = q^2$. Entonces el número de elementos de orden $p$ que hay en el grupo $G$ es $q^2(p-1)$, pues cada subgrupo de orden $p$ aporta $p-1$ elementos de orden $p$ que no se repiten, ya que dos subgrupos distintos de orden $p$ tienen intersección trivial. Por tanto, el número de elementos de $G$ cuyo orden no es $p$ es

$$pq^2 - q^2(p-1) = q^2.$$

Sea ahora $K$ un $q$-subgrupo de Sylow de $G$; como $|K| = q^2$ y $K$ no contiene elementos de orden $p$, $K$ debe consistir en los $q^2$ elementos de orden distinto de $p$, lo que muestra que $K$ es el único $q$-subgrupo de Sylow de $G$ y así $n_q = 1$. □

**Lema A.12** *Si $G$ es un grupo de orden $n$ y tiene un subgrupo propio $H$ de índice $m$ en $G$, tal que $n$ no divide a $m!$ entonces $G$ no es simple.*

**Demostración.** Consideremos $G$ actuando en $G/H$ por traslación, o sea $g \cdot xH = gxH$. Está claro que $\text{Estab}_G(H) = H$ y por tanto $\text{Estab}_G(xH) = xHx^{-1}$. Por tanto el núcleo de la acción es $c_G(H) = \cap_{x\in G} xHx^{-1}$. Este grupo es el mayor subgrupo normal de $G$ contenido en $H$ y se conoce con el nombre de core de $H$ en $G$. Entonces existe un homomorfismo inyectivo $G/c(G) \to S_m$ y por tanto $[G : c(G)]$ divide a $m!$. Por hipótesis $n = |G|$ no divide a $m!$ y por tanto $c_G(H) \neq 1$ como $c_G(H) \subseteq H \subset G$, concluimos que $c_G(H)$ es un subgrupo normal propio no trivial de $G$ y por tanto $G$ no es simple. □

**Teorema A.13** *El menor entero positivo $n$ para el que existe un grupo simple no abeliano de orden $n$ es $n = 60$.*

**Demostración.** Si $p$ y $q$ son primos distintos, ya sabemos que los grupos de orden $p$ son abelianos y que los de órdenes $p^n$ (con $n > 1$), $pq$ y $pq^2$ no son simples (Proposición 15 de GyA y Proposición A.11). Esto resuelve todos los casos excepto los de órdenes 24, 30, 36, 40, 42, 48 y 56.

Por el Tercer Teorema de Sylow A.10, si si $|G| = 40$ entonces $n_5 = 1$, y si $|G| = 42$ entonces $n_7 = 1$, por lo que ningún grupo de esos órdenes puede ser simple.

Por el Primer Teorema de Sylow A.5, todo grupo de orden 24 tiene un subgrupo de índice 3; todo grupo de orden 36 tiene un subgrupo de índice 4; y todo grupo de orden 48 tiene un subgrupo de índice 3. Por el último apartado del Lema A.12, ningún grupo de esos órdenes puede ser simple.

Supongamos ahora que $|G| = 30 = 2 \cdot 3 \cdot 5$. Del Tercer Teorema de Sylow se deduce que $n_3$ puede valer 1 ó 10, y que $n_5$ puede valer 1 ó 6. Si $n_3 = 10$ entonces, como cada par de 3-subgrupos de Sylow tiene intersección trivial, la unión de todos ellos tiene $10 \cdot 2 = 20$ elementos distintos del neutro, todos de orden 3. Análogamente, si $n_5 = 6$ entonces hay $6 \cdot 4 = 24$ elementos de orden 5 en $G$. Por tanto, no puede tenerse a la vez $n_3 = 10$ y $n_5 = 6$, por lo que uno de ellos vale 1 y por tanto $G$ no es simple.

Sólo nos queda por estudiar el caso $|G| = 56 = 2^3 7$, que estará resuelto si vemos que o bien $n_7 = 1$ o bien $n_2 = 1$. Supongamos que $n_7 \neq 1$ y veamos que $n_2 = 1$. Del Tercer Teorema de Sylow se deduce que $n_7 = 8$. Como en el párrafo anterior, $G$ contiene $8 \cdot 6 = 48$ elementos de orden 7. Sólo quedan pues el neutro y 7 elementos de orden 2 para formar los 2-subgrupos de Sylow (de orden $2^3 = 8$), por lo que ha de ser $n_2 = 1$. □

# Problemas

**A.1** Clasificar los grupos de orden menor que 16 salvo isomorfismos.

**A.2** Demostrar que todo grupo de orden 45 es abeliano.

**A.3** Demostrar que si $p, q, r$ son primos distintos tales que $pq < r$ entonces todo grupo finito de orden $pqr$ es resoluble.

**A.4** Demostrar que todo grupo de orden 63, 440 ó 765 es resoluble.

**A.5** Dado un grupo $G$ de orden $3^3 \cdot 13$, probar que es resoluble y dar una serie normal con factores cíclicos.

**A.6** Demostrar que todo grupo de orden $p^2q$ con $p$ y $q$ primos es resoluble.

**A.7** Demostrar que si $G$ es un grupo no resoluble de orden $n < 300$, entonces $n = 60, 120, 168, 180$ ó 240.

# Índice Terminológico