Ecuaciones algebraicas

Ángel del Río Mateos

Índice general

Introducción

En la escuela aprendimos a resolver ecuaciones lineales

$$aX + b = 0 \tag{1}$$

y cuadráticas

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

donde a, b y c son números y suponemos que $a \neq 0$. Es bien sabido que la única solución de la ecuación (1) es $-\frac{b}{a}$ y que la ecuación (2) tiene a lo sumo dos soluciones que se obtienen al elegir el signo de la raíz cuadrada en la siguiente expresión:

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{3}$$

En realidad, si $b^2 = 4ac$, entonces la ecuación (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 (1) y (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 Hieronymo 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

$$aX^3 + bX^2 + cX + d \quad (a \neq 0). \tag{4}$$

Está claro que dividiendo por a podemos suponer que $a = 1$. Además podemos suponer que $b = 0$ haciendo el cambio $X \mapsto X + \lambda$ para un valor de λ apropiado. Más concretamente, si ponemos

$$\begin{aligned} X^3 + bX^2 + cX + d &= (X + \lambda)^3 - 3\lambda X^2 - 2\lambda^2 X - \lambda^3 + bX^2 + cX + d \\ &= (X + \lambda)^3 + (b - 3\lambda)X^2 + (c - 3\lambda^2)X + d - \lambda^3. \end{aligned}$$

Por tanto, si elegimos $\lambda = \frac{b}{3}$ y ponemos $Y = X + \frac{b}{3}$, entonces la ecuación (4) es equivalente a la siguiente

$$Y^3 + \left(c - 3\left(\frac{b}{a}\right)^2\right)\left(Y - \frac{b}{3}\right) + d - \left(\frac{b}{a}\right)^3. \tag{5}$$

Es decir, para resolver la ecuación (4) podemos primero resolver la ecuación (5) y después calcular las soluciones de la ecuación (4) poniendo $X = Y - \frac{b}{a}$. La ecuación (5) tiene la forma

$$X^3 + pX + q = 0. \tag{6}$$

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

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

Para resolver la ecuación (6) del Ferro y Tartaglia ponían

$$X = u + v$$

con lo que la ecuación (6) 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

$$u^6 + qu^3 - \left(\frac{p}{3}\right)^3 = 0 \tag{7}$$

que parece más complicada que la ecuación original de grado 3 ya que tiene grado 6. Sin embargo la ecuación (7) 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 (7) 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

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

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 (7) 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 (6):

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

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

$$X = \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\left(\frac{p}{3}\right)^3}}, \tag{8}$$

lo que efectivamente nos servirá para calcular las tres soluciones de (6), 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 (3) y (8) parece natural considerar como operaciones algebraicas elementales son 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 (6) lo que hemos hecho es empezar resolviendo la ecuación (7) que se llama *resolvente* de la ecuación (6). 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 α_1, α_2 y α_3 de la ecuación (6) y las soluciones $u_1 = u, u_2 = \omega u, u_3 = \omega^2 u, u_4 = v = -\frac{p}{3}, u_5 = \omega v$ 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 (7) , en términos de las soluciones de la ecuación original (6):

$$\begin{aligned} u_1 &= \tfrac{1}{3}(\alpha_1 + \omega\alpha_3 + \omega^2\alpha_2) \\ u_2 &= \tfrac{1}{3}(\alpha_2 + \omega\alpha_1 + \omega^2\alpha_3) \\ u_3 &= \tfrac{1}{3}(\alpha_3 + \omega\alpha_2 + \omega^2\alpha_1) \\ u_4 &= \tfrac{1}{3}(\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3) \\ u_5 &= \tfrac{1}{3}(\alpha_3 + \omega\alpha_1 + \omega^2\alpha_2) \\ u_6 &= \tfrac{1}{3}(\alpha_2 + \omega\alpha_3 + \omega^2\alpha_1). \end{aligned} \tag{9}$$

Lagrange observó que para pasar de una solución de la resolvente a otra bastaba con permutar los papeles representados por las tres raíces α_1, α_2 y α_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

$$X^4 - pX^3 + qX^2 - rX + s = 0 \tag{10}$$

y sean $\alpha_1, \alpha_2, \alpha_3$ y α_4 las soluciones de (10). Las potencias de ω utilizadas en las expresiones (9) 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

$$u_{i,j,k,l} = \frac{1}{4}(\alpha_i + i\alpha_j + i^2\alpha_k + i^3\alpha_l) \tag{11}$$

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 (10) 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 α_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 (11) obtenemos las cuatro soluciones de la ecuación (10).

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 Grupo. 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

Anillos

1.1. Anillos

Definición 1.1. *Un* anillo (conmutativo y con identidad) *es una terna*[1] $(A, +, \cdot)$ *formada por un conjunto no vacío* A *y dos operaciones* $+$ *y* $\cdot$ *en* A*; la primera llamada usualmente* suma *y la segunda* producto *o* multiplicación*, que verifican:*

1. Conmutativa. $a + b = b + a$ *y* $ab = ba$*, para todo* $a, b \in A$.
2. Asociativa. $a + (b + c) = (a + b) + c$ *y* $a \cdot (b \cdot c) = (ab)c$*, para todo* $a, b, c \in A$.
3. Neutro. *Existen dos elementos* 0 *y* 1 *en* A *tales que* $a + 0 = a$ *y* $a \cdot 1 = a$*, para todo* $a \in A$.
4. Opuesto. *Para todo* $a \in A$ *existe otro elemento de* A *que llamamos opuesto de* a *y denotamos por* $-a$ *tal que* $a + (-a) = 0$.
5. Distributiva $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *para todo* $a, b, c \in A$.

A menudo no se exige que el producto de los elementos de un anillo satisfaga la propiedad conmutativa y se dice que un anillo que sí la satisfaga es un anillo conmutativo. Sin embargo todos los anillos considerados en estos apuntes son conmutativos y por tanto hablaremos de anillo con el significado de anillo conmutativo.

Si a y b son elementos de un anillo A, usualmente escribiremos ab en vez de $a \cdot b$. Además asumiremos que, en ausencia de paréntesis, los productos se realizan antes que las sumas (y que las restas). Así, por ejemplo, la propiedad distributiva se reescribe como $a(b+c) = ab+ac$. Se define la resta de a y b como $a - b = a + (-b)$. Los elementos 0 y 1 de A se llaman *cero* y *unidad* de A.

En general, no se asume que cada elemento a de un anillo A tenga simétrico para el producto. Cuando lo tiene, lo denotamos por a^{-1} (de modo que $aa^{-1} = 1$ y $(a^{-1})^{-1} = a$), le llamamos el *inverso* de a y decimos que a es *invertible* o una *unidad* en A. Si b es invertible, escribiremos a veces a/b ó $\frac{a}{b}$ en lugar de ab^{-1}. Denotaremos por A^* al conjunto de todas las unidades de A.

De los axiomas de anillo se pueden deducir algunas propiedades elementales:

Lema 1.2. *Sea* A *un anillo y sean* $a, b, c \in A$*. Entonces se verifican las siguientes propiedades:*

1. $0a = 0 = a0$.
2. $a(-b) = (-a)b = -(ab)$.

[1] Cuando no haya riesgo de confusión con las operaciones diremos simplemente que A es un anillo.

3. $a(b-c) = ab - ac$.
4. *ab es invertible precisamente si a y b son invertibles. En tal caso* $(ab)^{-1} = a^{-1}b^{-1}$.
5. *Si* $a + b = a + c$ *entonces* $b = c$.
6. *Si a es invertible y* $ab = ac$, *entonces* $b = c$.
7. *El cero y uno son únicos, es decir, si* $x + a = a$, *entonces* $x = 0$ *y si* $xa = a$ *para todo* a, *entonces* $x = 1$.
8. *El opuesto de a es único y si a es invertible, entonces a tiene un único inverso.*
9. *Si* $0 = 1$, *entonces* $A = \{0\}$.

Dados un anillo A, un elemento $a \in A$ y un entero positivo n, la notación na (respectivamente a^n) representa el resultado de sumar (respectivamente multiplicar) a consigo mismo n veces, y si $n = 0$ convenimos que $0a = 0$ y $a^0 = 1$. Más rigurosamente, a partir de estas últimas igualdades se definen na y a^n de forma recurrente poniendo $(n+1)a = a + na$ y $a^{n+1} = aa^n$ para $n \geq 0$. Por último, si $n \geq 1$ se define $(-n)a = -(na)$, y si además a es invertible se define $a^{-n} = (a^{-1})^n$.

Lema 1.3. *Dados un anillo A, elementos $a, b \in A$ y enteros $m, n \in \mathbb{Z}$, se verifican las siguientes propiedades:*

1. $n(a + b) = na + nb$.
2. $(n + m)a = na + ma$.
3. *Si* $n \geq 0$ *entonces* $(ab)^n = a^n b^n$.
4. *Si* $n, m \geq 0$ *entonces* $a^{n+m} = a^n a^m$.
5. *Si a y b son invertibles, las dos propiedades anteriores valen también para exponentes negativos.*

Ejemplos 1.4. *Anillos.*

1. Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos con la suma y el producto usuales. Nótese que todo elemento no nulo es invertible en $\mathbb{Q}$, pero en $\mathbb{Z}$ sólo hay dos elementos invertibles.
2. Sea n un número entero positivo y sea

   $$\mathbb{Z}_n = \{0, 1, 2, \ldots, n\}.$$

   Definimos una suma y producto en $\mathbb{Z}_n$ realizando la correspondiente operación como números enteros y quedándonos con el resto de dividir por n. Por ejemplo, en $\mathbb{Z}_6$ tenemos

   $$2 + 3 = 5, \quad 3 + 5 = 2, \quad 3 + 3 = 0, \quad 2 \cdot 3 = 0, \quad 2 \cdot 4 = 2, \quad 3^2 = 3, \quad 5^2 = 1.$$

   En general, las propiedades de un elemento dependerán del anillo en el que lo estemos considerando. Por ejemplo, 2 no es invertible en $\mathbb{Z}$ ni en $\mathbb{Z}_6$ pero sí que lo es en $\mathbb{Q}$ y en $\mathbb{Z}_5$.
3. Sean A y B dos anillos. Entonces el producto cartesiano $A \times B$ tiene una estructura de anillo con las operaciones

   $$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \quad \text{y} \quad (a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$$

   (se dice que las operaciones en $A \times B$ se definen *componente a componente*). Obsérvese que $A \times B$ es conmutativo precisamente si lo son A y B, y que esta construcción se puede generalizar a productos cartesianos de cualquier familia (finita o no) de anillos.

4. Dados un anillo A y un conjunto X, el conjunto A^X de las aplicaciones de X en A es un anillo con las siguientes operaciones:

$$(f+g)(x) = f(x) + g(x) \qquad (f \cdot g)(x) = f(x) \cdot g(x).$$

¿Cuál es la relación entre este ejemplo y el anterior?

5. Dado un anillo A, un *polinomio* en la *indeterminada* una expresión del tipo

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

donde n es un número entero no negativo y $a_i \in A$ para todo i. Para cada i, a_i se llama *coeficiente* de *grado* i de P, a_0 se llama *coeficiente independiente* de P y, si $a_n \neq 0$, entonces n es el *grado* de P y a_n es su *coeficiente principal*. Dos polinomios son iguales si y sólo si lo son coeficiente a coeficiente. Denotaremos por $A[X]$ al conjunto de los polinomios en la indeterminada X con coeficientes en A.

Utilizando la estructura de anillo de A se puede dotar a $A[X]$ de una estructura de anillo definiendo la suma y el producto de la forma usual:

$$(a_0 + a_1X + a_2X^2 + \cdots) + (b_0 + b_1X + b_2X^2 + \cdots) = c_0 + c_1X + c_2X^2 + \cdots,$$

donde cada $c_n = a_n + b_n$, y

$$(a_0 + a_1X + a_2X^2 + \cdots) \cdot (b_0 + b_1X + b_2X^2 + \cdots) = d_0 + d_1X + d_2X^2 + \cdots,$$

donde cada $d_n = a_0b_n + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0 = \sum_{i=0}^{n} a_ib_{n-i}$ (si un coeficiente no aparece en la expresión de un polinomio se considera que vale 0).

6. Dado un anillo A, denotamos por $A[[X]]$ el conjunto de las sucesiones $(a_0, a_1, a_2, \ldots)$ de elementos de A. En $A[[X]]$ consideramos la suma y el producto dados por

$$\begin{aligned}(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) &= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)\\ (a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots) &= (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \ldots).\end{aligned}$$

Obsérvese la similitud con la definición de las operaciones en el anillo de polinomios; de hecho, el elemento $(a_0, a_1, a_2, \ldots)$ se suele denotar por $\sum_{i=0}^{\infty} a_iX^i$. Con estas operaciones, $A[[X]]$ es un anillo llamado el *anillo de series de potencias* con coeficientes en A.

Si A es un conjunto con una operación $*$ y B es un subconjunto de A, decimos que B es *cerrado para la operación* $*$ si se tiene $x * y \in B$ cuando $x, y \in B$. Esto implica que $* : A \times A \to A$ se restringe a una aplicación $* : B \times B \to B$, y por lo tanto podemos considerar $*$ como una operación en B que se dice *inducida* por la operación en A.

Definición 1.5. *Si $(A, +, \cdot)$ es un anillo, un* subanillo *de A es un subconjunto B de A cerrado para ambas operaciones, que contiene al 1 y tal que $(B, +, \cdot)$ es un anillo.*

La siguiente proposición nos dice cómo comprobar si un subconjunto es un un subanillo.

Proposición 1.6. *Las condiciones siguientes son equivalentes para un subconjunto B de un anillo A:*

1. *B es un subanillo de A.*
2. *B contiene al 1 y es cerrado para sumas, productos y opuestos.*
3. *B contiene al 1 y es cerrado para restas y productos.*

Demostración. 1 implica 2. Si B es un subanillo de A entonces B contiene al 1 y es cerrado para sumas y productos, por definición. Por otro lado, como B es un anillo, cada elemento $b \in B$ tiene un opuesto. Por la unicidad del elemento simétrico (Lema 1.2), este opuesto ha de ser el de A, con lo que B es cerrado para opuestos.

2 implica 3 es evidente.

3 implica 1. Sea B un subconjunto de A que contiene al uno y es cerrado para restas y productos. Entonces $0 = 1 - 1 \in B$, con lo que si $b \in B$, entonces $-b = 0 - b \in B$; es decir, B es cerrado para opuestos. Si $a, b \in B$, entonces $-b \in B$ y, por tanto, $a + b = a - (-b) \in B$; es decir, B es cerrado para sumas. Ahora es evidente que B es un subanillo de A. □

Ejemplos 1.7. *Subanillos.*

1. Todo anillo A es un subanillo de sí mismo, al que llamamos *impropio* por oposición al resto de subanillos, que se dicen *propios*.

2. Cada uno de los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ es un subanillo de los posteriores (y de si mismo).

3. Si A es un anillo, el subconjunto $\{0\}$ es cerrado para sumas, productos y opuestos. Sin embargo, no contiene al 1 (salvo que $A = \{0\}$), con lo que no es un subanillo de A.

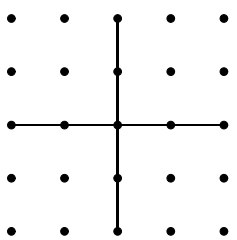
4. Si A es un anillo, el conjunto
$$\mathbb{Z}1 = \{n1 : n \in \mathbb{Z}\}$$
de los múltiplos enteros de 1 es un subanillo de A contenido en cualquier otro subanillo de A; es decir, $\mathbb{Z}1$ es el menor subanillo de A, y se conoce como el *subanillo primo* de A.

   Es claro que $\mathbb{Z}$ y los $\mathbb{Z}_n$ son sus propios subanillos primos, y por lo tanto no tienen subanillos propios.

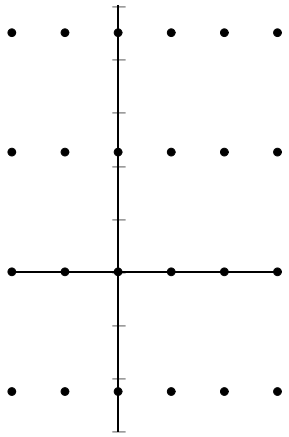
5. Si A y B son anillos y $B \neq 0$ entonces $A \times 0 = \{(a, 0) \mid a \in A\}$ es cerrado para sumas y productos pero no es un subanillo de $A \times B$ (¿por qué?).

6. Dado un número entero m, los conjuntos
$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\} \qquad \text{y} \qquad \mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$$
son subanillos de $\mathbb{C}$. Si además m es positivo, entonces ambos son subanillos de $\mathbb{R}$. Si m es el cuadrado de un número entero entonces esos conjuntos coinciden con $\mathbb{Z}$ y con $\mathbb{Q}$, respectivamente, por lo que el ejemplo carece de interés. Cuando m no es el cuadrado de un entero (por ejemplo $m = 2$ ó $m = -1$) entonces tampoco es el cuadrado de un número racional (¿por qué?), de manera que, en cualquiera de los dos anillos descritos, la igualdad $a + b\sqrt{m} = 0$ implica que $a = 0$ y $b = 0$, y por lo tanto la igualdad $a + b\sqrt{m} = c + d\sqrt{m}$ implica que $a = c$ y $b = d$.

   Un caso particular es el anillo $\mathbb{Z}[i]$, donde $i = \sqrt{-1}$, llamado el *anillo de los enteros de Gauss*. Podemos visualizar $\mathbb{Z}[i]$ dentro del plano complejo como el conjunto de los vértices de un enlosado del plano complejo por losas cuadradas de lado 1, como muestra el siguiente esquema:



Más generalmente, si $m < 0$, entonces podemos visualizar $\mathbb{Z}[\sqrt{m}]$ como el conjunto de vértices de un enlosado del plano complejo por losas rectangulares con una base de longitud 1 y una altura de longitud $\sqrt{-m}$. Por ejemplo, una porción de $\mathbb{Z}[\sqrt{-2}]$ está representada por los siguientes puntos del plano complejo:



7. Todo anillo A puede verse como un subanillo del anillo de polinomios $A[X]$ si identificamos los elementos de A con los *polinomios constantes* (del tipo $P = a_0$).

8. Sea A un anillo y X un conjunto. Entonces la *diagonal*

$$B = \{f \in A^X : f(x) = f(y) \text{ para todo } x, y \in X\}$$

(es decir, el conjunto de las *aplicaciones constantes* de X en A) es un subanillo de A^X.

1.2. Ideales y anillos cociente

Definición 1.8. *Sea A un anillo. Una* combinación lineal *con coeficientes en A (o una* combinación A-lineal*) de los elementos $a_1, \ldots, a_n$ de A es un elemento de A de la forma*

$$r_1 a_1 + \cdots + r_n a_n,$$

donde cada $r_i \in A$. Los enteros r_i son los coeficientes *de la combinación lineal.*

Un subconjunto I de A es un ideal *si no es vacío y si, dados $a, b \in I$, cualquier combinación A-lineal suya $ra + sb$ está en I.*

En la definición podemos sustituir la condición $I \neq \emptyset$ por la condición $0 \in I$. Además cualquier combinación lineal de un numero finito de elementos de un ideal I sigue siendo un elemento de I.

Ejemplos 1.9. *Ideales.*

1. Si A es un anillo, el conjunto

$$bA = (b) = \{ba : a \in A\}$$

es un ideal de A llamado *ideal principal generado por b*. Es fácil demostrar que todos los ideales de $\mathbb{Z}$ son de esta forma. Esto no es cierto en general, como pronto veremos. Obsérvese que bA es el menor ideal de A que contiene a b. Obsérvese también que $1A = A$ y que $0A = \{0\}$, con lo que estos dos son ideales principales de A llamados respectivamente *ideal impropio* (en oposición a *ideales propios*, para los demás) e *ideal cero* o *trivial*. El ideal trivial $\{0\}$ lo representaremos a partir de ahora por 0.

2. Más generalmente, si T es un subconjunto de un anillo, entonces el conjunto

$$(T) = \{\sum_{i=1}^{n} a_i t_i : n \in \mathbb{Z}^+, a_i \in A, t_i \in X\}$$

es un ideal, llamado *ideal generado* por T.

3. Si A y B son dos anillos entonces $A \times 0 = \{(a, 0) : a \in A\}$ es un ideal de $A \times B$.

4. Sea $\mathbb{Z}[X]$ el anillo de los polinomios con coeficientes enteros. Es fácil ver que el ideal generado por el elemento X puede describirse como el de los polinomios sin coeficiente independiente; es decir,

$$I = (X) = \{a_0 + a_1 X + \ldots + a_n X^n \in \mathbb{Z}[X] : a_0 = 0\}.$$

También es sencillo ver que el conjunto

$$J = \{a_0 + a_1 X + \ldots + a_n X^n \in \mathbb{Z}[X] : a_0 \in 2\mathbb{Z}\}$$

de los polinomios con coeficiente independiente par es un ideal de $\mathbb{Z}[X]$.

Definición 1.10. *Sea I un ideal de un anillo A. Decimos que dos elementos $a, b \in A$ son* congruentes módulo *I, y escribimos $a \equiv b \bmod I$, si su diferencia está en I; o sea:*

$$a \equiv b \bmod I \Leftrightarrow b - a \in I.$$

Lema 1.11. *Si A es un anillo, I es un ideal de A y $a, b, c, d \in A$, entonces:*

1. $a \equiv a \bmod I$
2. *Si* $a \equiv b \bmod I$, *entonces* $b \equiv a \bmod I$.
3. *Si* $a \equiv b \bmod I$ *y* $b \equiv c \bmod I$, *entonces* $a \equiv c \bmod I$.
4. $a \equiv b \bmod (0)$ *precisamente si* $a = b$.

Del Lema 1.11 se deduce que la relación "ser congruente módulo I" es una relación de equivalencia en A y, por tanto, las clases de equivalencia por esta relación definen una partición de A. La clase de equivalencia que contiene a un elemento $a \in A$ es

$$a + I = \{a + x : x \in I\}$$

(en particular $0 + I = I$), de modo que

$$a + I = b + I \Leftrightarrow a \equiv b \bmod I$$

(en particular $a + I = 0 + I \Leftrightarrow a \in I$). El conjunto de las clases de equivalencia se denota

$$A/I = \frac{A}{I} = \{a + I : a \in A\}.$$

Proposición 1.12. *Sea A un anillo con un ideal I. Las operaciones suma y producto en A/I dadas por*

$$(a + I) + (b + I) = (a + b) + I, \qquad (a + I) \cdot (b + I) = (ab) + I$$

están bien definidas y dotan a A/I de una estructura de anillo con neutro $0 + I$ y unidad $1 + I$. Este anillo se llama anillo cociente *de A módulo I.*

Al hacer el cociente de un anillo A por un ideal I, elementos que eran distintos en A "pasan a ser iguales" en el cociente (estrictamente hablando, son sus clases de equivalencia las que se hacen iguales); en particular, los elementos de I "se hacen cero". En muchas de las ocasiones en las que se construyen estructuras cociente eso es precisamente lo que se busca, identificar entre sí o anular ciertos elementos.

Ejemplos 1.13. *Anillos cociente.*

1. El anillo cociente del anillo $\mathbb{Z}$ por el ideal (n) es el anillo $\mathbb{Z}_n$ del Ejemplo 1.4.2.
2. Para analizar las soluciones enteras de la ecuación $x^2 - 15y^2 = 2$ podemos considerarla en $\mathbb{Z}_5$, donde toma la forma más sencilla $x^2 = 2$ (¡anulamos ese -15 que complicaba la ecuación!); ahora es elemental ver que esta ecuación no tiene soluciones en $\mathbb{Z}_5$ y deducir que la ecuación inicial no tiene soluciones enteras.
3. $A/0$ es el propio anillo A, mientras que $A/A = 0$.
4. Consideremos el ideal (X) del anillo de polinomios $\mathbb{Z}[X]$ (ver los Ejemplos 1.9). Como todo polinomio es congruente módulo (X) con su coeficiente independiente (visto como polinomio), no es difícil convencerse de que $\mathbb{Z}[X]/(X)$ y $\mathbb{Z}$ son, en esencia, el mismo anillo (más tarde precisaremos este comentario viendo que son *isomorfos*).
5. Sean A y B anillos e $I = A \times 0$. Como $(a, b) \equiv (0, b) \bmod I$, los anillos $(A \times B)/I$ y B son esencialmente iguales (isomorfos).

Lema 1.14. *Un elemento b de un anillo A es invertible si y sólo si $(b) = A$. Por tanto, las siguientes condiciones son equivalentes para un ideal I de A.*

1. *I es impropio; es decir, $I = A$.*
2. *$1 \in I$.*
3. *I contiene una unidad de A; es decir, $I \cap A^* \neq \emptyset$.*

El siguiente resultado describe los ideales de un anillo cociente. Emplearemos la siguiente notación: si A es un anillo e I es un ideal suyo, $\pi : A \to A/I$ denotará la aplicación que lleva cada elemento de A a su clase de equivalencia; es decir, $\pi(a) = a + I$. La imagen por π de un subconjunto J de A es

$$\pi(J) = \{a + I : a \in J\}.$$

Si J contiene a I, denotaremos este conjunto por J/I. La preimagen por π de un subconjunto X de A/I es

$$\pi^{-1}(X) = \{a \in A : a + I \in X\}.$$

Teorema 1.15 (Teorema de la Correspondencia)**.** *Si I es un ideal de un anillo A, las asignaciones $J \mapsto J/I$ y $X \mapsto \pi^{-1}(X)$ son biyecciones (una inversa de la otra) que conservan la inclusión entre el conjunto de los ideales de A que contienen a I y el conjunto de todos los ideales de A/I.*

Demostración. Hay que comprobar los siguientes puntos, cosa que el lector podrá hacer como ejercicio:

- Si J es un ideal de A que contiene a I entonces J/I es un ideal de A/I y $\pi^{-1}(J/I) = J$.
- Si X es un ideal de A/I entonces $\pi^{-1}(X)$ es un ideal de A que contiene a I y $\pi^{-1}(X)/I = X$.
- Si $J \subseteq K$ son ideales de A que contienen a I entonces $J/I \subseteq K/I$.
- Si $X \subseteq Y$ son ideales de A/I entonces $\pi^{-1}(X) \subseteq \pi^{-1}(Y)$.

□

1.3. Homomorfismos de anillos

Definición 1.16. *Sean A y B dos anillos. Un* homomorfismo de anillos *entre A y B es una aplicación $f : A \to B$ que conserva las operaciones y la unidad; es decir, que satisface*

$$f(x+y) = f(x) + f(y), \qquad f(x \cdot y) = f(x) \cdot f(y)$$

para cada par de elementos $x, y \in A$ y

$$f(1) = 1.$$

Un endomorfismo *de A es un homomorfismo de un anillo de A en sí mismo.*

En la definición anterior hemos usado el mismo símbolo para las operaciones y los neutros en los dos anillos que intervienen. Por ejemplo, para calcular $f(x+y)$ primero hay que sumar x con y en A y luego aplicarle f al resultado, mientras que en $f(x)+f(y)$ primero hay que calcular las imágenes de x e y por f y luego hay que sumar éstas en B. Usualmente el contexto hace evidente a qué operación o a qué neutro nos referimos en cada caso, así que mantendremos estos abusos de notación y dejaremos que el lector analice cada caso. Análogamente, las unidades de la ecuación $f(1) = 1$ están en dos anillos probablemente diferentes y por tanto son objetos distintos, que sin embargo denotamos igual.

La condición $f(x+y) = f(x) + f(y)$ suele leerse como *la imagen de la suma es la suma de las imágenes*, o también como *f conserva sumas*. Del mismo modo se habla de aplicaciones que *conservan productos* o que *conservan identidades*.

A continuación establecemos ciertas propiedades elementales de los homomorfismos de anillos. Demostramos algunas y dejamos el resto como ejercicio para el lector.

Proposición 1.17. *Sea $f : A \to B$ un homomorfismo de anillos. Entonces se verifican las siguientes propiedades para $a, b, a_1, \ldots, a_n \in A$:*

1. *(f conserva ceros) $f(0) = 0$.*
2. *(f conserva opuestos) $f(-a) = -f(a)$.*
3. *(f conserva restas) $f(a-b) = f(a) - f(b)$.*
4. *(f conserva sumas finitas) $f(a_1 + \cdots + a_n) = f(a_1) + \cdots + f(a_n)$.*
5. *(f conserva múltiplos enteros) Si $n \in \mathbb{Z}$ entonces $f(na) = nf(a)$.*
6. *(f conserva inversos) Si a es invertible, entonces $f(a)$ es invertible y $f(a)^{-1} = f(a^{-1})$.*
7. *(f conserva productos finitos) $f(a_1 \cdots a_n) = f(a_1) \cdots f(a_n)$.*
8. *Si A_1 es un subanillo de A, entonces $f(A_1)$ es un subanillo de B.*
9. *Si B_1 es un subanillo de B, entonces $f^{-1}(B_1)$ es un subanillo de A.*
10. *Si X es un ideal de B, entonces $f^{-1}(X)$ es un ideal de A.*
11. *Si I es un ideal de A y f es suprayectiva, entonces $f(I)$ es un ideal de B.*

Demostración. Para ver 1 basta con aplicar la propiedad de cancelación a la igualdad $0 + f(0) = f(0+0) = f(0) + f(0)$. 2 se tiene porque $f(a) + f(-a) = f(a + (-a)) = f(0) = 0$, y entonces 3 es claro. 4 se demuestra por inducción; el caso $n = 2$ no es más que la definición de homomorfismo y el caso general se reduce a éste notando que $a_1 + \cdots + a_n = (a_1 + \cdots + a_{n-1}) + a_n$. □

Observación 1.18. En la Proposición 1.17 hemos visto que la conservación de sumas implica la conservación del neutro para la suma, pero no hemos podido adaptar la demostración al caso de productos (¿por qué?); de hecho, en seguida veremos ejemplos de aplicaciones entre anillos que conservan sumas y productos pero no identidades.

Ejemplos 1.19. *Homomorfismos de anillos.*

1. Si A y B son anillos, la aplicación $f : A \to B$ dada por $f(a) = 0$ para cada $a \in A$ *no* es un homomorfismo de anillos salvo que $B = 0$. Si $B = 0$ entonces este homomorfismo se llama *homomorfismo cero* u *homomorfismo trivial*. Obsérvese que no hay ningún homomorfismo $0 \to B$, salvo que B sea 0.

   He aquí otro ejemplo menos trivial de anillos entre los que no hay homomorfismos: la existencia de un homomorfismo de anillos $f : \mathbb{Z}_2 \to \mathbb{Z}_3$ nos llevaría al absurdo

   $$0 + (3) = f(0 + (2) = f(1 + (2) + 1 + (2)) = f(1 + (2)) + f(1 + (2)) = 1 + (3) + 1 + (3) = 2 + (3).$$

2. Sea A un un anillo con un subanillo B. Entonces la aplicación de inclusión $u : B \hookrightarrow A$, dada por $u(b) = b$, es un homomorfismo. En particular, la aplicación identidad $1_A : A \to A$ es un homomorfismo.

3. Sea A un anillo con un ideal I. Entonces la *proyección* (o *proyección canónica*) $\pi : A \to A/I$, dada por $\pi(a) = a + I$, es un homomorfismo. Obsérvese que parte de la demostración del Teorema de la Correspondencia puede verse como un caso particular de los apartados 10 y 11 de la Proposición 1.17 aplicada a la proyección π.

4. Si A es un anillo, la aplicación $\mu : \mathbb{Z} \to A$ dada por $\mu(n) = n1$ (es decir, la aplicación consistente en multiplicar por 1) es un homomorfismo de anillos. De hecho, es el único homomorfismo de anillos $f : \mathbb{Z} \to A$ (¿por qué es el único?).

5. Si A y B son anillos, la aplicación $p_A : A \times B \to A$ dada por $p_A(a, b) = a$ es un homomorfismo llamado *proyección en la primera coordenada*, y de modo análogo se tiene una proyección en la segunda coordenada.

   Dado un producto arbitrario de anillos, debe estar claro cómo se generaliza este ejemplo para definir la proyección en cada coordenada.

6. Dados $a, b \in \mathbb{R}$, el *conjugado* del número complejo $z = a + bi$ es $\bar{z} = a - bi$, y la aplicación *conjugación* $\mathbb{C} \to \mathbb{C}$ dada por $z \mapsto \bar{z}$ es un homomorfismo de anillos.

   Análogamente, si d es un entero que no sea un cuadrado entonces el conjugado $a - b\sqrt{d}$ de $a + b\sqrt{d}$ (elementos de $\mathbb{Q}[\sqrt{d}]$ o de $\mathbb{Z}[\sqrt{d}]$) está bien definido y la conjugación $\mathbb{Q}[\sqrt{d}] \to \mathbb{Q}[\sqrt{d}]$ ó $\mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$ es un homomorfismo de anillos.

7. Sea A un anillo y sea $b \in A$. Entonces la aplicación

   $$\begin{array}{ccc} A[X] & \xrightarrow{S_b} & A \\ P = a_0 + a_1X + \cdots + a_nX^n & \mapsto & P(b) = a_0 + a_1b + \cdots + a_nb^n \end{array}$$

   es un homomorfismo de anillos llamado *homomorfismo de sustitución* en b. En particular, el homomorfismo de sustitución en 0 lleva cada polinomio a su coeficiente independiente.

Hemos visto que, si $f : A \to B$ es un homomorfismo de anillos, entonces $f(A)$ es un subanillo de B, y es evidente que f es suprayectivo precisamente cuando $f(A) = B$. Más generalmente, podemos decir que cuanto mayor es $f(A)$ más cerca está f de ser suprayectivo. En el otro extremo, $f^{-1}(0)$ es un ideal de A que nos va a servir para determinar si f es o no inyectivo.

Definición 1.20. *Sea $f : A \to B$ un homomorfismo de anillos; llamamos* imagen *y* núcleo *de f, respectivamente, a los conjuntos*

$$\text{Im } f = f(A) = \{f(a) : a \in A\} \qquad y \qquad \text{Ker } f = f^{-1}(0) = \{a \in A : f(a) = 0\}$$

(la notación para el núcleo procede de la voz germánica Kernel*). En general* Im f *es un subanillo de B y* Ker f *es un ideal de A.*

Proposición 1.21. *Un homomorfismo de anillos $f : A \to B$ es inyectivo precisamente si* Ker $f = 0$.

Demostración. Si f es inyectivo, entonces $f^{-1}(a)$ tiene a lo sumo un elemento, para todo $a \in A$. En particular Ker $f = f^{-1}(0)$ tiene exactamente un elemento, a saber 0.

Recíprocamente, supongamos que Ker $f = 0$ y sean $a, b \in A$ tales que $a \neq b$. Entonces $f(a) - f(b) = f(a - b) \neq 0$; es decir, $f(a) \neq f(b)$, y por tanto f es inyectiva. □

1.4. Teoremas de isomorfía

Definición 1.22. *Un homomorfismo de anillos $f : A \to B$ que sea biyectivo se llama un* isomorfismo *de anillos. Un* automorfismo *es un endomorfismo biyectivo. Si existe un isomorfismo $f : A \to B$, se dice que los anillos A y B son* isomorfos*, situación que se denota por $A \simeq B$.*

Conforme vayamos estudiando propiedades de los anillos y de sus elementos, veremos que los isomorfismos *conservan esas propiedades* en un sentido que estará claro en cada caso. Como consecuencia, dos anillos isomorfos tendrán las mismas propiedades y deberán ser considerados como *esencialmente iguales.*

Proposición 1.23. *Si $f : A \to B$ es un isomorfismo de anillos, entonces la aplicación inversa $f^{-1} : B \to A$ también lo es. En consecuencia, la relación* ser isomorfos *es una relación de equivalencia en la clase de todos los anillos.*

Demostración. Sean $x, y \in B$; entonces

$$f(f^{-1}(x + y)) = x + y = f(f^{-1}(x)) + f(f^{-1}(y)) = f(f^{-1}(x) + f^{-1}(y)),$$

y como f es inyectiva esto implica que $f^{-1}(x + y) = f^{-1}(x) + f^{-1}(y)$. De igual modo se ve que f^{-1} conserva productos e identidades. Como además f^{-1} es biyectiva, deducimos que es un isomorfismo.

Como las identidades son isomorfismos, la relación de isomorfía es reflexiva, mientras que es simétrica por la primera parte de esta proposición y es transitiva por que la composición de dos isomorfismos es otro isomorfismo. □

Los siguientes resultados establecen la existencia de ciertos isomorfismos de anillos que usaremos con frecuencia.

Teorema 1.24 (Primer Teorema de Isomorfía)**.** *Sea $f : A \to B$ un homomorfismo de anillos. Entonces existe un único isomorfismo de anillos $\bar{f} : A/\text{Ker } f \to \text{Im } f$ que hace conmutativo el diagrama*

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ A/\text{Ker } f & \xrightarrow{\quad \bar{f} \quad} & \text{Im } f \end{array}$$

es decir, $i \circ \bar{f} \circ p = f$, donde i es la inclusión y p es la proyección. En particular

$$\frac{A}{\operatorname{Ker} f} \simeq \operatorname{Im} f.$$

Demostración. Sean $K = \operatorname{Ker} f$ e $I = \operatorname{Im} f$. La aplicación $\bar{f} : A/K \to I$ dada por $\bar{f}(x + K) = f(x)$ está bien definida (no depende de representantes) pues si $x+K = y+K$ entonces $x-y \in K$ y por lo tanto $f(x) - f(y) = f(x - y) = 0$; es decir, $f(x) = f(y)$. Además es elemental ver que es un homomorfismo de anillos y que es suprayectiva. Para ver que es inyectiva usamos la Proposición 1.21: si $x + K$ está en el núcleo de $\bar{f}$ entonces $0 = \bar{f}(x + K) = f(x)$, de modo que $x \in K$ y así $x + K = 0 + K$. Es decir $\operatorname{Ker} \bar{f} = 0$ y por lo tanto $\bar{f}$ es inyectiva. En conclusión, $\bar{f}$ es un isomorfismo, y hace conmutativo el diagrama porque, para cada $x \in K$, se tiene

$$i(\bar{f}(p(x))) = \bar{f}(x + K) = f(x).$$

En cuanto a la unicidad, supongamos que otro homomorfismo $\widehat{f} : A/K \to I$ verifica $i \circ \widehat{f} \circ p = f$; entonces para cada $x \in K$ se tiene $\widehat{f}(x + K) = i(\widehat{f}(p(x))) = f(x) = \bar{f}(x + K)$, y por lo tanto $\widehat{f} = \bar{f}$. □

Teorema 1.25 (Segundo Teorema de Isomorfía)**.** *Sea A un anillo y sean I y J dos ideales tales que $I \subseteq J$. Entonces J/I es un ideal de A/I y existe un isomorfismo de anillos*

$$\frac{A/I}{J/I} \simeq \frac{A}{J}.$$

Demostración. Por el Teorema de la Correspondencia 1.15, J/I es un ideal de A/I. Sea $f : A/I \to A/J$ la aplicación definida por $f(a + I) = a + J$. Es elemental ver que f está bien definida, que es un homomorfismo suprayectivo de anillos y que $\operatorname{Ker} f = J/I$. Entonces el isomorfismo buscado se obtiene aplicando el Primer Teorema de Isomorfía a f. □

Teorema 1.26 (Tercer Teorema de Isomorfía)**.** *Sea A un anillo con un subanillo B y un ideal I. Entonces:*

1. *$B \cap I$ es un ideal de B.*
2. *$B + I$ es un subanillo de A que contiene a I como ideal.*
3. *Se tiene un isomorfismo de anillos $\dfrac{B}{B \cap I} \simeq \dfrac{B + I}{I}$.*

Demostración. Los dos primeros apartados se dejan como ejercicio. En cuanto al último, sea $f : B \to A/I$ la composición de la inclusión $j : B \to A$ con la proyección $p : A \to A/I$. Es claro que $\operatorname{Ker} f = B \cap I$ y que $\operatorname{Im} f = (B + I)/I$, por lo que el resultado se sigue del Primer Teorema de Isomorfía. □

Ejemplos 1.27. *Aplicaciones del Primer Teorema de Isomorfía.*

1. Si A y B son anillos, el homomorfismo $A \times B \to A$ de proyección en la primera componente es suprayectivo y tiene núcleo $I = 0 \times B$, por lo que $\frac{A \times B}{0 \times B} \simeq A$.
2. Si A es un anillo, el homomorfismo $f : A[X] \to A$ de sustitución en 0 (dado por $a_0 + a_1X + \cdots \mapsto a_0$) es suprayectivo y tiene por núcleo el ideal (X) generado por X (consistente en los polinomios con coeficiente independiente nulo), de modo que $A[X]/(X) \simeq A$, como ya habíamos observado en los Ejemplos 1.13.

3. Sean A un anillo e I un ideal de A. Para cada $a \in A$, sea $\overline{a} = a + I$. La aplicación $f : A[X] \to (A/I)[X]$ dada por $f(a_0 + a_1X + \cdots + a_nX^n) = \overline{a}_0 + \overline{a}_1X + \cdots + \overline{a}_nX^n$ es un homomorfismo suprayectivo de anillos cuyo núcleo es $I[X] = \{a_0 + a_1X + \cdots + a_nX^n : a_i \in I\}$. Del Primer Teorema de Isomorfía se deduce que $(A/I)[X] \simeq A[X]/I[X]$.

Definición 1.28. *Sea A un anillo, y recordemos que si $n \in \mathbb{Z}^+$ escribimos $n1 = 1 + \cdots + 1$ (n veces). Si existe $n \in \mathbb{Z}^+$ tal que $n1 = 0$, definimos la* característica *de A como el menor $n \in \mathbb{Z}^+$ que verifica tal igualdad. Si no existe un tal n, decimos que la característica de A es 0.*

Proposición 1.29. *Sea A un anillo A y sea $f : \mathbb{Z} \to A$ el único homomorfismo de anillos (dado por $f(n) = n1$). Para un número natural n las condiciones siguientes son equivalentes:*

1. *n es la característica de A.*
2. *$n\mathbb{Z}$ es el núcleo de f.*
3. *El subanillo primo de A es isomorfo a $\mathbb{Z}_n$ (recuérdese que $\mathbb{Z}_0 = \mathbb{Z}$ y $\mathbb{Z}_1 = 0$).*
4. *A contiene un subanillo isomorfo a $\mathbb{Z}_n$.*

Demostración. La equivalencia entre 1 y 2 se deja como ejercicio para el lector, y es obvio que 3 implica 4.

2 implica 3. Se obtiene aplicando el Primer Teorema de Isomorfía y observando que Im f es el subanillo primo de A.

4 implica 2. Si B es un subanillo de A y $g : \mathbb{Z}_n \to B$ es un isomorfismo, considerando la proyección $\pi : \mathbb{Z} \to \mathbb{Z}_n$ y la inclusión $u : B \hookrightarrow A$ se obtiene un homomorfismo de anillos $u \circ g \circ \pi : \mathbb{Z} \to A$ que debe coincidir con f por su unicidad (Ejemplos 1.19). Como $u \circ g$ es inyectiva, es elemental ver que Ker $f = n\mathbb{Z}$. □

Si I y J son dos ideales de A entonces la suma y producto de A son los conjuntos

$$\begin{aligned} I + J &= \{x + y : x \in I, y \in J\} \\ IJ &= \{x_1y_1 + \ldots + x_ny_n : x_1, \ldots, x_n \in I, y_1, \ldots, y_n \in J\}. \end{aligned}$$

Más generalmente, si $I_1, \ldots, I_n$ son ideales, entonces la suma y estos ideales es

$$I_1 + \cdots + I_n = \{x_1 + \cdots + x_n : x_1 \in I_1, \ldots, x_n \in I_n\}$$

y el producto $I_1 \cdots I_n$ es el ideal formado por las sumas de productos de la forma $x_1 \cdots x_n$ donde $x_1 \in I_1, \ldots, x_n \in I_n$.

Proposición 1.30. *Si $I_1, \ldots, I_n$ son ideales de un anillo A entonces:*

1. *$I_1 \cap \cdots \cap I_n$ es el mayor ideal de A contenido en todos los I_i.*
2. *$I_1 + \cdots + I_n$ es el menor ideal de A que contiene a todos los I_i (es decir, el ideal de A generado por $I_1 \cup \cdots \cup I_n$.*
3. *$I_1 \cdots I_n$ es el ideal de A generado por los productos $x_1 \cdots x_n$ con $x_1 \in I_1, \ldots, x_n \in I_n$.*

Generalizar las definiciones de suma y producto a familias no necesariamente finitas de ideales.

Terminamos esta sección con el Teorema Chino de los Restos.

Teorema 1.31 (Teorema Chino de los Restos)**.** *Sea A un anillo y sean $I_1, \ldots, I_n$ ideales de A tales que $I_i + I_j = A$ para todo $i \neq j$. Entonces $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$. Además*

$$\frac{A}{I_1 \cap \cdots \cap I_n} \simeq \frac{A}{I_1} \times \cdots \times \frac{A}{I_n}.$$

Demostración. Razonamos por inducción sobre n, empezando con el caso $n = 2$. La hipótesis $I_1 + I_2 = A$ nos dice que existen $x_1 \in I_1$ y $x_2 \in I_2$ tales que $x_1 + x_2 = 1$, y entonces para cada $a \in I_1 \cap I_2$ se tiene $a = ax_1 + ax_2 \in I_1 I_2$, de modo que $I_1 \cap I_2 \subseteq I_1 I_2$, y la otra inclusión es clara. Claramente la aplicación $f : A \to A/I_1 \times A/I_2$ dada por $f(a) = (a + I_1, a + I_2)$ es un homomorfismo de anillos con núcleo $I_1 \cap I_2$, y es suprayectiva pues, dado un elemento arbitrario $(a_1 + I_1, a_2 + I_2)$ de $A/I_1 \times A/I_2$, el elemento $a = a_1 x_2 + a_2 x_1$ verifica $f(a) = (a_1 + I_1, a_2 + I_2)$. Ahora el resultado se obtiene aplicando el Primer Teorema de Isomorfía.

En el caso general ($n > 2$) basta ver que las hipótesis implican que $(I_1 \cap \cdots \cap I_{n-1}) + I_n = A$, pues entonces la hipótesis de inducción nos da

$$I_1 \cap \cdots \cap I_{n-1} \cap I_n = (I_1 \cap \cdots \cap I_{n-1}) I_n = I_1 \cdots I_{n-1} I_n$$

y

$$\frac{A}{I_1 \cap \cdots \cap I_n} = \frac{A}{(\cap_{i=1}^{n-1} I_i) \cap I_n} \simeq \frac{A}{\cap_{i=1}^{n-1} I_i} \times \frac{A}{I_n} \simeq \frac{A}{I_1} \times \cdots \times \frac{A}{I_{n-1}} \times \frac{A}{I_n}.$$

Para ver que $(I_1 \cap \cdots \cap I_{n-1}) + I_n = A$ notemos que, para cada $i \leq n-1$, existen $a_i \in I_i$ y $b_i \in I_n$ tales que $1 = a_i + b_i$, y multiplicando todas esas expresiones se obtiene

$$1 = \Pi_{i=1}^{n-1}(a_i + b_i) = a_1 \cdots a_{n-1} + b,$$

donde b engloba a todos los sumandos que se obtendrían desarrollando los productos (excepto $a_1 \cdots a_{n-1}$) y está en I_n porque en cada sumando hay al menos un factor del ideal I_n. Como además $a_1 \cdots a_{n-1} \in I_1 \cap \cdots \cap I_{n-1}$, deducimos que $1 \in (I_1 \cap \cdots \cap I_{n-1}) + I_n$ y así $(I_1 \cap \cdots \cap I_{n-1}) + I_n = A$, como queríamos ver. □

1.5. Cuerpos y dominios; ideales maximales y primos

En esta sección suponemos que, en todos los anillos que aparecen, $1 \neq 0$.

Definición 1.32. *Un elemento a de un anillo A se dice* regular *si la relación $ab = ac$ con $b, c \in A$ implica que $b = c$; es decir, si a es* cancelable*.*

Claramente, el 0 nunca es cancelable[2]*. Un* cuerpo *es un anillo en el que todos los elementos no nulos son invertibles, y un* dominio *(o* dominio de integridad*) es un anillo en el que todos los elementos no nulos son regulares.*

Como todo elemento invertible es regular (Lema 1.2), tenemos:

Proposición 1.33. *Todo cuerpo es un dominio.*

Otras propiedades que se demuestran fácilmente quedan recogidas en el siguiente ejercicio:

Proposición 1.34. *Si A es un anillo, entonces:*

1. Las condiciones siguientes son equivalentes:

[2] Obsérvese la importancia de la hipótesis $1 \neq 0$ en este caso.

a) *A es un cuerpo.*

b) *Los únicos ideales de A son 0 y A.*

c) *Todo homomorfismo de anillos $A \to B$ es inyectivo.*

2. *Un elemento $a \in A$ es regular si y sólo si la relación $ab = 0$ con $b \in A$ implica $b = 0$ (por este motivo, los elementos no regulares se suelen llamar* divisores de cero*).*

3. *A es un dominio si y sólo si, para cualesquiera $a, b \in A$ no nulos, se tiene $ab \neq 0$.*

4. *Todo subanillo de un dominio es un dominio.*

5. *La característica de un dominio es cero o un número primo.*

Ejemplos 1.35. *Dominios y cuerpos.*

1. Los anillos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos y $\mathbb{Z}$ es un dominio que no es un cuerpo (aunque es subanillo de un cuerpo).

2. Para $n \geq 2$, el anillo $\mathbb{Z}_n$ es un dominio si y sólo si es un cuerpo, si y sólo si n es primo (¿por qué?).

3. Si $m \in \mathbb{Z}$ no es un cuadrado entonces $\mathbb{Z}[\sqrt{m}]$ es un dominio (subanillo de $\mathbb{C}$) que no es un cuerpo (el 2 no tiene inverso). Sin embargo, $\mathbb{Q}[\sqrt{m}]$ sí que es un cuerpo; de hecho, si $a + b\sqrt{m} \neq 0$, entonces $q = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - b^2 m$ es un número racional no nulo (¿por qué?) y $aq^{-1} - bq^{-1}\sqrt{m}$ es el inverso de $a + b\sqrt{m}$.

4. Un producto de anillos $A \times B$ nunca es un dominio, pues $(1, 0)(0, 1) = (0, 0)$.

5. Los anillos de polinomios no son cuerpos, pues la indeterminada genera un ideal propio y no nulo.

   Por otra parte, $A[X]$ es un dominio si y sólo si lo es A. Una implicación es clara, pues A es un subanillo de $A[X]$. La otra se sigue del siguiente resultado, interesante en sí mismo, que el lector puede intentar demostrar (véase el Lema 2.1): Si A es un dominio y P, Q son polinomios de $A[X]$ de grados n y m, entonces el grado del producto PQ es $n + m$.

Definición 1.36. *Sean A un anillo e I un ideal propio de A.*
Se dice que I es maximal *si no está contenido en ningún ideal propio (excepto en sí mismo).*
Se dice que I es primo *si, para todo $a, b \in A$, la relación $ab \in I$ implica $a \in I$ ó $b \in I$.*

Proposición 1.37. *Sean A un anillo e I un ideal propio de A. Entonces:*

1. *I es maximal precisamente si A/I es un cuerpo.*

2. *I es primo precisamente si A/I es un dominio.*

3. *Si I es maximal entonces es primo.*

4. *A es un cuerpo precisamente si el ideal 0 es maximal.*

5. *A es un dominio precisamente si el ideal 0 es primo.*

Demostración. El apartado 1 es consecuencia inmediata del primer apartado de la Proposición 1.34 y del Teorema de la Correspondencia 1.15. Para ver 2, supongamos que I es primo y sean $a + I, b + I$ dos elementos no nulos de A/I; entonces $a, b \notin I$ y por lo tanto $ab \notin I$, luego $(a + I)(b + I) = ab + I \neq 0$ y en consecuencia A/I es un dominio. El recíproco se demuestra usando la misma idea, y el resto de apartados se deducen de estos dos y de la Proposición 1.33. □

Proposición 1.38. *Todo ideal propio de un anillo está contenido en un ideal maximal.*

Demostración. Sea I un ideal propio de A y sea Ω el conjunto de los ideales propios de A que contienen a I. Obsérvese que la unión de una cadena $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ de elementos de Ω es un ideal, que además es propio, pues si no lo fuera, contendría a 1 y por tanto algún I_n contendría a 1 en contra de que todos los I_n son ideales propios. Aplicando el Lema de Zorn deducimos que Ω tiene un elemento maximal que obviamente es un ideal maximal de A. □

A continuación estudiamos algunas propiedades de los ideales primos y maximales.

1.6. El cuerpo de fracciones de un dominio

En esta sección vamos a ver que todo dominio D es un subanillo de un cuerpo. De hecho existe un cuerpo que, en cierto sentido, es el menor cuerpo que contiene a D. Dicho cuerpo es único salvo isomorfismos y se llama el *cuerpo de fracciones* de D. Comenzaremos con la construcción de ese cuerpo, que es una traducción literal de la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$, y analizaremos entonces sus propiedades. En realidad, la construcción del cuerpo de fracciones es parte de una construcción más general, que presentaremos al final de la sección en una serie de ejercicios.

En esta sección, D representará un dominio. Un subanillo de un anillo A que sea un cuerpo se llama un *subcuerpo* de A, y un homomorfismo de anillos entre dos cuerpos (que ha de ser inyectivo por la Proposición 1.34) se llama *homomorfismo de cuerpos*.

La idea de la construcción es la de formar un cuerpo $Q(D)$ cuyos elementos sean "fracciones" del tipo a/b con $a, b \in D$ y $b \neq 0$. De este modo, D estará contenido en $Q(D)$ (identificando cada elemento a de D con la fracción $a/1$), y los elementos no nulos de $Q(D)$ serán invertibles, pues si $a, b \in D \setminus \{0,\}$, entonces b/a será el inverso de a/b. Por supuesto, hay que definir con más rigor las fracciones y hay que dotar a $Q(D)$ de una estructura de cuerpo. El primer problema que se presenta, si pensamos en el caso $D = \mathbb{Z}$ y $Q(D) = \mathbb{Q}$, es el hecho de que dos fracciones aparentemente distintas pueden representar el mismo elemento, como en el caso $10/15 = 2/3$. Esto se resuelve identificando ciertas fracciones mediante una relación de equivalencia, y este será el primer paso en nuestra construcción.

Sean $S = D \setminus \{0\}$ y $X = D \times S$. Definimos en X la relación binaria

$$(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow a_1 s_2 = a_2 s_1$$

que, como el lector comprobará fácilmente, es una relación de equivalencia. La clase de equivalencia de (a, s) se denota por a/s o por $\frac{a}{s}$, y el conjunto cociente $X/\sim$ (es decir, el conjunto de las clases de equivalencia para esa relación) por $Q(D)$. Dotamos a $Q(D)$ de una estructura de anillo con las siguientes operaciones:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2} \qquad \frac{a_1}{s_1}\frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}. \tag{1.1}$$

Hay que asegurarse de que esas definiciones no dependen de los representantes elegidos para cada fracción. Es decir, si $a_1/s_1 = b_1/t_1$ y $a_2/s_2 = b_2/t_2$, hay que comprobar que se obtiene la misma suma y el mismo producto si aplicamos las fórmulas a a_1/s_1 y a_2/s_2 que si se las aplicamos a b_1/t_1 y b_2/t_2. Las igualdades anteriores significan que $a_1 t_1 = b_1 s_1$ y $a_2 t_2 = b_2 s_2$, de donde

$$(a_1 s_2 + a_2 s_1)(t_1 t_2) = a_1 s_2 t_1 t_2 + a_2 s_1 t_1 t_2 = b_1 s_2 s_1 t_2 + b_2 s_1 t_1 s_2 = (b_1 t_2 + b_2 t_1)(s_1 s_2)$$

y por tanto $\frac{a_1 s_2 + a_2 s_1}{s_1 s_2} = \frac{b_1 t_2 + b_2 t_1}{t_1 t_2}$. Esto demuestra que la suma está bien definida, y con el producto se procede de modo análogo.

Lema 1.39. *Dados $a, b, s, t \in D$ con $s, t \neq 0$, entonces:*

1. *El neutro para la suma es* $0/1$. *Además, la igualdad* $a/s = 0/1$ *se verifica si y sólo si* $a = 0$.

2. *El neutro para el producto es* $1/1$. *Además, la igualdad* $a/s = 1/1$ *se verifica si y sólo si* $a = s$.

3. *Se tiene* $at/st = a/s$.

4. *La igualdad* $a/s = b/s$ *se verifica si y sólo si* $a = b$.

5. *La definición de suma se simplifica cuando hay "denominador común":* $a/s + b/s = (a + b)/s$.

Usando adecuadamente el Lema 1.39, la comprobación de que $Q(D)$ es un cuerpo es rutinaria. Demostramos como ejemplo la propiedad distributiva, y dejamos el resto para el lector:

$$\frac{a}{s}\left(\frac{b_1}{t_1}+\frac{b_2}{t_2}\right)=\frac{a}{s}\left(\frac{b_1t_2+b_2t_1}{t_1t_2}\right)=\frac{ab_1t_2+ab_2t_1}{st_1t_2}=\frac{ab_1t_2}{st_1t_2}+\frac{ab_2t_1}{st_1t_2}=\frac{ab_1}{st_1}+\frac{ab_2}{st_2}=\frac{a}{s}\frac{b_1}{t_1}+\frac{a}{s}\frac{b_2}{t_2}.$$

Definición 1.40. *El cuerpo* $Q(D)$ *se llama* cuerpo de fracciones *o* cuerpo de cocientes *del dominio* D.

Ejemplos 1.41. *Cuerpos de fracciones.*

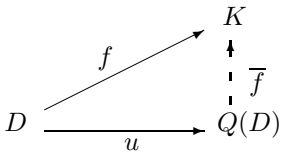
1. Obviamente, $\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$.

2. Supongamos que un anillo de polinomios $A[X]$ es un dominio (lo que ocurre precisamente si A es un dominio por los Ejemplos 1.35). Su cuerpo de fracciones se suele denotar por $A(X)$ y se llama el *cuerpo de las funciones racionales* sobre A. Sus elementos son fracciones del tipo P/Q con $P, Q \in A[X]$, que se suman y se multiplican de forma natural.

Usando el Lema 1.39, es sencillo ver que la aplicación $u : D \to Q(D)$ dada por $u(a) = a/1$ es un homomorfismo inyectivo de anillos, lo que nos permite ver a D como un subanillo de $Q(D)$ si identificamos cada elemento a de D con la fracción $a/1$ de $Q(D)$. El par $(Q(D), u)$ verifica una interesante propiedad:

Proposición 1.42. *Sean* D *un dominio,* $Q(D)$ *su cuerpo de fracciones y* $u : D \to Q(D)$ *la aplicación dada por* $u(a) = a/1$. *Entonces:*

1. **(Propiedad Universal del Cuerpo de Fracciones)** *Para toda pareja* (K, f) *formada por un cuerpo* K *y un homomorfismo inyectivo de anillos* $f : D \to K$, *existe un único homomorfismo de cuerpos* $\bar{f} : Q(D) \to K$ *tal que* $\bar{f} \circ u = f$. *Se dice que* $\bar{f}$ completa de modo único *el diagrama*



2. *Si dos homomorfismos de cuerpos* $g, h : Q(D) \to K$ *coinciden sobre* D *entonces son iguales. Es decir, si* $g \circ u = h \circ u$ *entonces* $g = h$.

3. $Q(D)$ *está determinado salvo isomorfismos por la Propiedad Universal. Explícitamente: supongamos que existen un cuerpo* F *y un homomorfismo inyectivo de anillos* $v : D \to F$ *tales que, para todo cuerpo* K *y todo homomorfismo inyectivo de anillos* $f : D \to K$, *existe un único homomorfismo de cuerpos* $\bar{f} : F \to K$ *tal que* $\bar{f} \circ v = f$. *Entonces existe un isomorfismo* $\phi : F \to Q(D)$ *tal que* $\phi \circ v = u$.

Demostración. 1. Sea $f : D \to K$ como en el enunciado. Si $\bar{f} : Q(D) \to K$ es un homomorfismo de cuerpos tal que $\bar{f} \circ u = f$ entonces, para todo $a/s \in Q(D)$, se verifica

$$\bar{f}(a/s) = \bar{f}(u(a)u(s)^{-1}) = (\bar{f} \circ u)(a)(\bar{f} \circ u)(s)^{-1} = f(a)f(s)^{-1}.$$

Esto prueba que el único homomorfismo de cuerpos $\bar{f} : Q(D) \to K$ que puede satisfacer $\bar{f} \circ u = f$ tiene que venir dada por $\bar{f}(a/s) = f(a)f(s)^{-1}$. Sólo falta comprobar que la aplicación $\bar{f}$ así dada está bien definida y es un homomorfismo. Si $a_1/s_1 = a_2/s_2$ entonces $a_1 s_2 = a_2 s_1$, luego $f(a_1)f(s_2) = f(a_2)f(s_1)$ y, por tanto, $f(a_1)f(s_1)^{-1} = f(a_2)f(s_2)^{-1}$. Esto prueba que $\bar{f}$ está bien definido. Dejaremos que el lector compruebe que es efectivamente un homomorfismo.

2. Si ponemos $f = g \circ u = h \circ u : D \to K$, los homomorfismos g y h completan el diagrama del apartado 1. Por la unicidad se tiene $g = h$.

3. Sea $v : D \to F$ como en el enunciado. Aplicando 1 encontramos un homomorfismo $\bar{v} : Q(D) \to F$ tal que $\bar{v} \circ u = v$, y aplicando la hipótesis de 3 encontramos un homomorfismo $\bar{u} : F \to Q(D)$ tal que $\bar{u} \circ v = u$. Entonces la composición $\bar{u} \circ \bar{v} : Q(D) \to Q(D)$ verifica $(\bar{u} \circ \bar{v}) \circ u = \bar{u} \circ v = u$, y por 2 se obtiene $\bar{u} \circ \bar{v} = 1_{Q(D)}$. En particular $\bar{u}$ es suprayectiva, y como es inyectiva por ser un homomorfismo de cuerpos, $\phi = \bar{u}$ es el isomorfismo que buscamos. □

La Propiedad Universal permite afirmar que $Q(D)$ es "el menor cuerpo que contiene a D" en un sentido que se hace explícito en el siguiente resultado:

Proposición 1.43. *Sea D un dominio. Si K es un cuerpo y $f : D \to K$ es un homomorfismo inyectivo de anillos, entonces K contiene un subcuerpo isomorfo a $Q(D)$.*

Demostración. Por la propiedad universal del cuerpo de fracciones existe un homomorfismo de cuerpos $\bar{f} : Q(D) \to K$, y como $\bar{f}$ es inyectiva, Im $\bar{f}$ es un subcuerpo de K isomorfo a $Q(D)$. □

Ejemplo 1.44. *El cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$.*
Sea m un número entero que no es un cuadrado, y sea $f : \mathbb{Z}[\sqrt{m}] \to \mathbb{C}$ la inclusión. Si $\bar{f}$ es como en la demostración de la Proposición 1.43, entonces Im $\bar{f}$ es el cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$. Un elemento genérico de Im $\bar{f}$ es de la forma $x = \frac{a+b\sqrt{m}}{c+d\sqrt{m}}$, con $a, b, c, d \in \mathbb{Z}$ y $c + d\sqrt{m} \neq 0$. Si ponemos $t = (c + d\sqrt{m})(c - d\sqrt{m}) \neq 0$ entonces $t = c^2 - d^2 m \in \mathbb{Z}$, y así

$$x = \frac{a + b\sqrt{m}}{c + d\sqrt{m}} = \frac{(a + b\sqrt{m})(c - d\sqrt{m})}{t} = \frac{r + s\sqrt{m}}{t} = \frac{r}{t} + \frac{s}{t}\sqrt{m},$$

donde $r, s \in \mathbb{Z}$, y por tanto $x \in \mathbb{Q}[\sqrt{m}]$. Esto demuestra que Im $\bar{f} \subseteq \mathbb{Q}[\sqrt{m}]$, y el otro contenido es claro, pues un elemento genérico $\frac{a}{s} + \frac{b}{t}\sqrt{m}$ de $\mathbb{Q}[\sqrt{m}]$ se reescribe como $\frac{at+bs\sqrt{m}}{st}$.
En conclusión, el cuerpo de fracciones de $\mathbb{Z}[\sqrt{m}]$ es $\mathbb{Q}[\sqrt{m}]$.

Un interesante corolario de la Proposición 1.43 es el siguiente:

Corolario 1.45. *Todo cuerpo K posee un subcuerpo K', llamado el* subcuerpo primo *de K, que está contenido en cualquier otro subcuerpo de K (es decir, K' es "el menor subcuerpo de K"). Si la característica de K es un entero primo p, entonces K' es isomorfo a $\mathbb{Z}_p$; en caso contrario K' es isomorfo a $\mathbb{Q}$.*

Demostración. Si la característica es un primo p entonces el subanillo primo de K (isomorfo a $\mathbb{Z}_p$) es ya un cuerpo, y contiene a cualquier subcuerpo (de hecho, a cualquier subanillo) de K.

En otro caso, al ser K un cuerpo, la característica es cero; es decir, el homomorfismo de anillos $f : \mathbb{Z} \to K$ es inyectivo. El cuerpo de fracciones de $\mathbb{Z}$ es $\mathbb{Q}$, y el homomorfismo de cuerpos $\bar{f} : \mathbb{Q} \to K$ que

nos da la Propiedad Universal viene dada por $\bar{f}(n/m) = f(n)f(m)^{-1}$. Como $\bar{f}$ es inyectivo, $K' = \operatorname{Im} \bar{f}$ es un subcuerpo de K isomorfo a $\mathbb{Q}$, y ahora basta ver que K' está contenido en cualquier subcuerpo F de K. Dado un tal F, se tiene $f(m) \in F$ para cada $m \in \mathbb{Z}$, y si $m \neq 0$ entonces $f(m) \neq 0$ y $f(m)^{-1} \in F$. Por tanto, para cada $n/m \in \mathbb{Q}$ se tiene $\bar{f}(n/m) = f(n)f(m)^{-1} \in F$, lo que demuestra que $K' \subseteq F$. □

1.7. Divisibilidad

Definición 1.46. *Sea A un anillo y sean $a, b \in A$. Se dice que a* divide *a b en A, o que a es* un divisor *de b en A, o que b es* un múltiplo *de a en A, si existe $c \in A$ tal que $b = ac$.*

Para indicar que a divide a b en A escribiremos $a \mid b$ en A. Si el anillo A está claro por el contexto escribiremos simplemente $a \mid b$.

Obsérvese que la noción de divisibilidad depende del anillo. Por ejemplo, si a es un entero diferente de 0, entonces a divide a todos los números enteros en $\mathbb{Q}$, pero no necesariamente en $\mathbb{Z}$.

Lema 1.47. *Si A es un anillo y $a, b, c \in A$ entonces se verifican las siguientes propiedades:*

1. *(Reflexiva) $a \mid a$.*
2. *(Transitiva) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.*
3. *$a \mid 0$ y $1 \mid a$.*
4. *$0 \mid a$ si y sólo si $a = 0$.*
5. *$a \mid 1$ si y sólo si a es una unidad; en este caso $a \mid x$ para todo $x \in A$ (es decir, las unidades dividen a cualquier elemento).*
6. *Si $a \mid b$ y $a \mid c$ entonces $a \mid rb + sc$ para cualesquiera $r, s \in A$ (y en particular $a \mid b + c$, $a \mid b - c$ y $a \mid rb$ para cualquier $r \in A$). Más generalmente, si a divide a ciertos elementos, entonces divide a cualquier combinación lineal suya con coeficientes en A.*
7. *Si A es un dominio, $c \neq 0$ y $ac \mid bc$, entonces $a \mid b$.*

Definición 1.48. *Dos elementos a y b de un anillo A se dice que son* asociados *si se dividen mutuamente; es decir, si $a \mid b$ y $b \mid a$. Cuando no esté claro por el contexto en qué anillo estamos trabajando, hablaremos de elementos* asociados en A.

Por ejemplo, una unidad es lo mismo que un elemento asociado a 1.

Es elemental ver que "ser asociados" es una relación de equivalencia en A, y que dos elementos son asociados si y sólo si tienen los mismos divisores, si y sólo si tienen los mismos múltiplos. Por lo tanto, al estudiar cuestiones de divisibilidad, un elemento tendrá las mismas propiedades que sus asociados.

La siguiente caracterización de la relación "ser asociado" en un dominio será importante (y por motivos como éste pronto empezaremos a suponer sistemáticamente que los anillos que aparecen son dominios):

Lema 1.49. *Si D es un dominio entonces $a, b \in D$ son asociados en D si y sólo si existe una unidad $u \in D^*$ tal que $b = au$.*

Sabemos que cualquier elemento a de un anillo A es divisible por sus asociados y por las unidades de A, y que si a divide a uno de los elementos b ó c entonces divide a su producto bc. A continuación estudiamos los elementos que verifican "los recíprocos" de estas propiedades. A menudo consideraremos elementos a de un anillo A que no son cero ni unidades, lo que sintetizaremos en la forma $0 \neq a \in A \setminus A^*$.

Definición 1.50. *Diremos que un elemento a del anillo A es* irreducible *si $0 \neq a \in A \setminus A^*$ y la relación $a = bc$ en A implica que $b \in A^*$ ó $c \in A^*$ (y por lo tanto que uno de los dos es asociado de a).*

Diremos que a es primo *si $0 \neq a \in A \setminus A^*$ y la relación $a \mid bc$ en A implica que $a \mid b$ ó $a \mid c$.*

Ambas nociones dependen del anillo ambiente, y si éste no está claro por el contexto hablaremos de irreducibles y primos "en A".

Proposición 1.51. *En un dominio A todo elemento primo es irreducible.*

El recíproco no se verifica en general, como muestra el siguiente ejemplo.

Ejemplo 1.52. *Irreducible no implica primo.*

En el anillo $\mathbb{Z}[\sqrt{-5}]$ hay elementos irreducibles que no son primos. Comencemos observando que el cuadrado del módulo de un elemento $a + b\sqrt{-5}$ de $\mathbb{Z}[\sqrt{-5}]$, con $a, b \in \mathbb{Z}$ es $|a + b\sqrt{-5}|^2 = a^2 + 5b^2$. Eso implica que si $x|y$ en $\mathbb{Z}[\sqrt{-5}]$, entonces $|x|^2$ divide a $|y|^2$ en $\mathbb{Z}$. Por otro lado los cuadrados en $\mathbb{Z}_5$ son $0 + (5)$ y $\pm 1 + (5)$, y que por lo tanto la congruencia $a^2 \equiv \pm 2 \bmod 5$ no tiene solución. Esto implica que en $\mathbb{Z}[\sqrt{-5}]$ no hay elementos cuyo módulo al cuadrado valga 2, 3 ó 12 (¿por qué?). Sea ahora $x \in \mathbb{Z}[\sqrt{-5}]$ con $|x|^2 = 4$; si $y \mid x$ entonces $|y|^2$ divide a $|x|^2 = 4$, en $\mathbb{Z}$ y, por lo tanto, $|y|^2$ vale 1, 2 ó 4: En el primer caso $y = \pm 1$ es una unidad, el segundo es imposible y en el tercero y es asociado de x (¿por qué?), y en consecuencia x es irreducible. De igual modo se ve que los elementos con módulo 6 ó 9 son irreducibles, y en particular lo son todos los factores de la igualdad

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Pero ninguno de ellos es primo: por ejemplo de la igualdad se deduce que $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$, y es claro que $2 \nmid (1 + \sqrt{-5})$ y $2 \nmid (1 - \sqrt{-5})$.

Todas las nociones de divisibilidad que hemos presentado pueden reenunciarse en términos de los ideales principales generados por los elementos involucrados.

Lema 1.53. *Si D es un dominio y $a, b \in D$ entonces se verifican las siguientes propiedades:*

1. *$a = 0$ precisamente si $(a) = 0$.*
2. *$a \in D^*$ precisamente si $(a) = D$.*
3. *$a \mid b$ precisamente si $(b) \subseteq (a)$ (o si $b \in (a)$).*
4. *a y b son asociados precisamente si $(a) = (b)$.*
5. *a es primo precisamente si (a) es un ideal primo no nulo de D.*
6. *a es irreducible precisamente si (a) es maximal entre los ideales principales propios no nulos de D; es decir, $a \neq 0$ y $(a) \subseteq (b) \subset D$ implica $(a) = (b)$.*

En vista de estos resultados, las nociones sobre divisibilidad se manejarán fácilmente en dominios en los que todos los ideales son principales.

Definición 1.54. *Un* dominio de ideales principales*, o* DIP *(PID, en la literatura en inglés), es un dominio en el que todos los ideales son principales.*

Proposición 1.55. *Si D es un DIP y $0 \neq a \in D \setminus D^*$, las siguientes condiciones son equivalentes:*

1. *a es irreducible.*
2. *(a) es un ideal maximal.*

3. *$A/(a)$ es un cuerpo.*

4. *a es primo.*

5. *(a) es un ideal primo.*

6. *$A/(a)$ es un dominio.*

Demostración. La equivalencia entre 1, 2 y 3 es consecuencia de la Proposición 1.53 y de la Proposición 1.37, y lo mismo puede decirse de la equivalencia entre 4, 5 y 6. También de la Proposición 1.37 se deduce que 2 implica 5. Finalmente, 4 implica 1 por la Proposición 1.51. □

El Ejemplo prototípico de DIP es el anillo $\mathbb{Z}$ de los números enteros. En el Tema 2 aparecerán otros dominios de ideales principales.

Definición 1.56. *Sea D un dominio. Una* factorización en producto de irreducibles *de un elemento a de D es una expresión del tipo*

$$a = up_1 \cdots p_n$$

donde $n \in \mathbb{N}$, u es una unidad de D y $p_1, \ldots, p_n$ son irreducibles de D (se admite la posibilidad de que sea $n = 0$, en cuyo caso la factorización se reduce a $a = u$). Diremos que D es un dominio de factorización *si todo elemento no nulo de D admite una factorización en producto de irreducibles.*

Dos factorizaciones de $a \in D$ en producto de irreducibles se dice que son equivalentes si sólo se diferencian en el orden y en asociados. Dicho con más rigor, las factorizaciones

$$a = up_1 \cdots p_n = vq_1 \cdots q_m$$

(con $u, v \in D^*$ y el resto de factores irreducibles) son equivalentes *si $n = m$ y existe una* permutación *σ de $\mathbb{N}_n$ (una biyección de $\mathbb{N}_n = \{1, 2, \ldots, n\}$ en sí mismo) tal que p_i y $q_{\sigma(i)}$ son asociados para cada $i = 1, \ldots, n$. Diremos que D es un* dominio de factorización única *ó* DFU *(UFD, en inglés) si es un dominio de factorización en el que, para cada $0 \neq a \in D$, todas las factorizaciones de a son equivalentes.*

Comenzamos observando que, sobre un DFU, los elementos irreducibles coinciden con los primos, por lo que podemos hablar indistintamente de factorizaciones en irreducibles o factorizaciones en primos.

Lema 1.57. *Si D es un DFU, entonces todo elemento irreducible de D es primo.*

Demostración. Sea $p \in D$ irreducible, y sean $a, b, t \in D$ tales que $pt = ab$. Se trata de ver que $p \mid a$ ó $p \mid b$. Si $t = up_1 \cdots p_n$, $a = vq_1 \cdots q_m$ y $b = wr_1 \cdots r_k$ son factorizaciones en irreducibles (con $u, v, w \in D^*$), entonces se tiene

$$upp_1 \cdots p_n = (vw)q_1 \cdots q_m r_1 \cdots r_k,$$

y por la unicidad de la factorización p es asociado de algún q_i (y entonces $p \mid a$) o de algún r_i (y entonces $p \mid b$). □

Proposición 1.58. *Para un dominio D, las condiciones siguientes son equivalentes:*

1. *D es un dominio de factorización única.*

2. *D es un dominio de factorización en el que todo elemento irreducible es primo.*

Demostración. 1 implica 2. Por la definición de DFU y por el Lema 1.57.

2 implica 1. Por hipótesis, todo elemento no nulo de D se factoriza como un producto de primos, y podemos demostrar la unicidad de tales factorizaciones adaptando la demostración del Teorema Fundamental de la Aritmética. En efecto, sean $up_1 \cdots p_n = vq_1 \cdots q_m$, con p_i y q_i irreducibles para todo i, y $u, v \in D^*$. Suponemos que $n \leq m$ y razonamos por inducción sobre n. Si $n = 0$ entonces $m = 0$, ya que los divisores de unidades son unidades, y no hay nada que demostrar. Supongamos que $n > 0$ y, la hipótesis de inducción. Por hipótesis, p_n es primo, luego divide a algún q_i y de hecho son asociados (¿por qué?); además, reordenando si es necesario, podemos suponer que $i = m$. Es decir, existe una unidad w tal que $q_m = wp_n$. Entonces

$$up_1 \cdots p_{n-1} = (vw)q_1 \cdots q_{m-1}.$$

Por hipótesis de inducción se tiene $n-1 = m-1$ (luego $n = m$) y existe una biyección $\tau : \{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ tal que p_i y $q_{\tau(i)}$ son asociados para cada $i = 1, \ldots, n-1$. Ahora es evidente que τ se extiende a una permutación σ de $\mathbb{N}_n$ tal que p_i y $q_{\sigma(i)}$ son asociados para cada $i = 1, \ldots, n$, y por lo tanto las factorizaciones iniciales son equivalentes. □

Teorema 1.59. *Todo dominio de ideales principales D es un dominio de factorización única.*

Demostración. Por las Proposiciones 1.58 y 1.55, basta con demostrar que D es un dominio de factorización. Por reducción al absurdo suponemos que D no lo es, y vamos a construir, por recurrencia, una sucesión $a_1, a_2, \ldots$ de elementos de D que no admiten factorización y tales que $(a_1) \subset (a_2) \subset \cdots$ es una cadena estrictamente creciente de ideales de D. Para el primer paso simplemente elegimos un elemento arbitrario a_1 de D que no admita factorización en irreducibles. Supongamos ahora que hemos elegido $a_1, \ldots, a_n$ satisfaciendo las condiciones requeridas. Entonces a_n no es irreducible, luego existen $x, y \in D \setminus D^*$ tales que $a_n = xy$. Como a_n no es producto de irreducibles, al menos uno de los factores x ó y (digamos que x) no es producto de irreducibles. Entonces, poniendo $a_{n+1} = x$, tenemos $(a_n) \subset (a_{n+1})$ con la inclusión estricta porque y no es una unidad.

Una vez construida la sucesión (a_i), tomamos $I = (a_1, a_2, \ldots) = \cup_{i \in \mathbb{Z}^+}(a_i)$ (dejamos que el lector compruebe la igualdad anterior). Como D es un DIP, existe $x \in D$ tal que $I = (x)$; en particular $x \in I = \cup_{i \in \mathbb{Z}^+}(a_i)$ y por tanto existe un índice i tal que $x \in (a_i)$; como es claro que $a_i \in (x)$, se tiene $(a_i) = (x) = I$ y por lo tanto $(a_i) = (a_{i+1})$, en contra de la construcción realizada. Este absurdo concluye la demostración. □

El recíproco del Teorema 1.59 es falso; en el siguiente capítulo veremos que $\mathbb{Z}[X]$ es un DFU que no es un DIP.

1.8. Problemas

1. Demostrar los lemas 1.2, 1.3, 1.11, 1.14, 1.39, 1.47, 1.49 y 1.53 y las Proposiciones 1.12, 1.14 y 1.34.

2. Sea $m \in \mathbb{Z}$. Demostrar que si m no es un cuadrado en $\mathbb{Z}$, entonces tampoco es un cuadrado en $\mathbb{Q}$.

3. Si n es un entero positivo, demostrar que los ideales de $\mathbb{Z}_n$ son precisamente los de la forma $m\mathbb{Z}_n$, donde m es un divisor positivo de n, y además $m\mathbb{Z}_n$ está contenido en $m'\mathbb{Z}_n$ si y sólo si m' divide a m.

4. Sean a y b dos elementos de un anillo. Demostrar que ab es un divisor de cero precisamente si a ó b es un divisor de cero.

5. Sea A un anillo finito. Demostrar que todo elemento de A es o divisor de cero o unidad. Deducir que todo dominio finito es un cuerpo.

6. Decimos que $d \in \mathbb{Z}$ es *libre de cuadrados* si p^2 no divide a d para ningún número primo p (en particular 1 es libre de cuadrados). Demostrar que para todo $m \in \mathbb{Z}$ existe un $d \in \mathbb{Z}$ libre de cuadrados tal que $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{d}]$. ¿Ocurre lo mismo si cambiamos $\mathbb{Q}$ por $\mathbb{Z}$?

7. Sean A y B dos anillos. Describir los ideales de $A \times B$ en función de los ideales de A y de B. Determinar todos los ideales de $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$.

8. Si I, J y K son ideales de un anillo A, demostrar que:

   a) $I(J \cap K) \subseteq IJ \cap IK$.

   b) $IJ = JI$.

   c) $I(JK) = (IJ)K$.

   d) $I(J + K) = IJ + IK$.

   e) $IA = I$.

9. Comprobar que la hipótesis de suprayectividad en el apartado 11 de la Proposición 1.17 no es superflua; es decir, dar un ejemplo de un homomorfismo de anillos $f : A \to B$ y un ideal I de A, tal que $f(I)$ no es un ideal de B.

10. Demostrar que si $f : A \to B$ es un homomorfismo suprayectivo de anillos y todos los ideales del anillo A son principales entonces todos los ideales de B son principales.

11. Sea $a \in \mathbb{R}$. ¿Qué se deduce al aplicar el Primer Teorema de Isomorfía al homomorfismo $\mathbb{R}[X] \to \mathbb{R}$, dado por $P(X) \mapsto P(a)$? ¿Y qué se deduce al aplicarlo al homomorfismo $\mathbb{R}[X] \to \mathbb{C}$, dado por $P(X) \mapsto P(i)$?

12. Sea $f : A \to B$ un homomorfismo suprayectivo de anillos. Demostrar que existe una correspondencia biunívoca, que conserva la inclusión, entre el conjunto de los ideales de B y los ideales de A que contienen a Ker f.

13. Demostrar el recíproco del Teorema Chino de los Restos para anillos; es decir, probar que si $I_1, \ldots, I_n$ son ideales de un anillo A tales que la aplicación $f : A \to \prod_{i=1}^{n} A/I_i$, dada por $f(a) = (a + I_1, \ldots, a + I_n)$ es suprayectiva, entonces $I_i + I_j = (1)$, para todo $i \neq j$.

14. Si I es un ideal propio del anillo A, las biyecciones del Teorema de la Correspondencia llevan ideales maximales (respectivamente primos) de A que contienen a I a ideales maximales (respectivamente primos) de A/I, y viceversa.

15. Sea $f : A \to B$ un homomorfismo de anillos. Demostrar que:

   a) Si p es un ideal primo de B, entonces $f^{-1}(p)$ es un ideal primo de A.

   b) En general, no se verifica el resultado análogo para ideales maximales. (Indicación: Considerar la inclusión de $\mathbb{Z}$ en $\mathbb{Q}$.)

16. Sea A un anillo cuya característica es un número primo p. Demostrar que la aplicación $x \mapsto x^{p^n}$ es un endomorfismo de A para todo $n \in \mathbb{N}$.

17. Demostrar que, si K es un cuerpo finito con un subcuerpo F, entonces el cardinal de K es una potencia del cardinal de F. (Indicación: Considerar K como espacio vectorial sobre F). Deducir que:

a) El cardinal de cualquier cuerpo finito es una potencia de un número primo. (Indicación: Considerar el subanillo primo de K.)

b) Si K es un cuerpo finito con un subcuerpo F, entonces existen un número primo p y enteros positivos n y m tales que $n \mid m$, $|F| = p^n$ y $|K| = p^m$.

18. Determinar los automorfismos de $\mathbb{C}$ que cumplen $f(x) = x$, para todo $x \in \mathbb{R}$.

19. Demostrar que el único automorfismo de $\mathbb{R}$ es la identidad. (Indicación: Un automorfismo de $\mathbb{R}$ debe fijar los números racionales y conservar el orden.)

20. Sea A un anillo de característica n y sea m un número entero. ¿Cuántos homomorfismos de anillos $\mathbb{Z}_m \to A$ existen? ¿Cuántos homomorfismos de anillos $\mathbb{Z}_n \to \mathbb{Z}_m$ existen?

21. Sea D un dominio y sea Q su cuerpo de fracciones. Demostrar que:

a) Si D' es un subanillo de D con cuerpo de fracciones Q', entonces Q contiene un subcuerpo isomorfo a Q'.

b) Si A es un subanillo de Q que contiene a D, entonces Q es un cuerpo de cocientes de A.

22. Demostrar que si D es un dominio entonces:

a) Un elemento $0 \neq a \in D \setminus D^*$ es irreducible si y sólo si sus únicos divisores son sus asociados y las unidades. Si D no es un dominio se verifica el "sólo si". En $A = \mathbb{Z}_6$ el "si" falla para $a = 4 + (6)$..

b) Si dos elementos son asociados, entonces uno es irreducible (respectivamente primo) si y sólo si lo es el otro.

23. Sean A un anillo, S un subconjunto de A y $a, b, d, m \in A$. Demostrar que:

a) Las condiciones siguientes son equivalentes:

1) m es múltiplo de cada elemento de S, y si un elemento $x \in A$ es múltiplo de cada elemento de S entonces x es múltiplo de m.
2) Un elemento $x \in A$ es múltiplo de cada elemento de S si y sólo si es múltiplo de m.

En este caso se dice que m es un *mínimo común múltiplo* de S, y otro elemento es un mínimo común múltiplo de S si y sólo si es asociado de m. Escribiremos $m = \operatorname{mcm}(S)$, entendiendo que tal elemento (si existe) es único salvo asociados. Asimismo, hablaremos de *el* mínimo común múltiplo de S, con el mismo significado de unicidad salvo asociados.

b) Las condiciones siguientes son equivalentes:

1) d divide a cada elemento de S, y si un elemento $x \in A$ divide a cada elemento de S entonces x divide a d.
2) Un elemento $x \in A$ divide a cada elemento de S si y sólo si divide a d.

En este caso se dice que d es un *máximo común divisor* de S, y otro elemento es un máximo común divisor de S si y sólo si es asociado de d. Escribiremos $d = \operatorname{mcd}(S)$, entendiendo que tal elemento (si existe) es único salvo asociados.

c) Si d es un divisor común de los elementos de S y además es combinación lineal de elementos de S; es decir, existen elementos $s_1, \ldots, s_n \in S$ y $a_1, \ldots, a_n \in A$ tales que

$$d = a_1 s_1 + \cdots + a_n s_n, \tag{1.2}$$

entonces $d = \operatorname{mcd}(S)$, y se dice que esta expresión es una *identidad de Bezout* para S.
Si existe una identidad de Bezout (1.2) con $d = 1$ entonces $\operatorname{mcd}(S) = 1$.

d) Se verifica $1 = \text{mcd}(S)$ si y sólo si los únicos divisores comunes de los elementos de S son las unidades de A. En este caso decimos que los elementos de S son *coprimos*. Si para cada par de elementos distintos $a, b \in S$ se verifica $\text{mcd}(a, b) = 1$, decimos que los elementos de S son *coprimos dos a dos*.

e) $a \mid b$ si y sólo si $a = \text{mcd}(a, b)$, si y sólo si $b = \text{mcm}(a, b)$.

f) En particular, $1 = \text{mcd}(a, 1)$, $\text{mcd}(a, 0) = a = \text{mcm}(a, 1)$ y $0 = \text{mcm}(a, 0)$.

g) Si a es irreducible entonces $\text{mcd}(a, b) = 1$ si y sólo si $a \nmid b$.

24. Demostrar las siguientes propiedades para d y m dos elementos de un dominio D y S un subconjunto de D.

a) $d = \text{mcd}(S)$ precisamente si (d) es mínimo entre los ideales principales que contienen a S (o al ideal generado por S).
En particular, si (S) es un ideal principal entonces cualquier generador suyo es un máximo común divisor de S, y además existe una identidad de Bezout para S.

b) $m = \text{mcm}(S)$ si y sólo si $(m) = \cap_{s \in S}(s)$.
En consecuencia, $\text{mcm}(S)$ existe si y sólo si el ideal $\cap_{s \in S}(s)$ es principal, y entonces cualquier generador de $\cap_{s \in S}(s)$ es un mínimo común múltiplo de S.

25. Sea D un DIP y sean S un subconjunto de D y $a, b, c \in D$. Demostrar

a) S tiene un mínimo común múltiplo.

b) S tiene un máximo común divisor d y además existe una identidad de Bezout para S.

c) El elemento d es un máximo común divisor de $a_1, \ldots, a_n$ si y sólo si $d \mid a_i$ para cada $i = 1, \ldots, n$ y existen $r_1, \ldots, r_n \in D$ tales que

$$r_1 a_1 + \cdots + r_n a_n = d.$$

d) Los elementos $a_1, \ldots, a_n$ son coprimos si y sólo si existen $r_1, \ldots, r_n \in D$ tales que

$$r_1 a_1 + \cdots + r_n a_n = 1.$$

e) Si $d = \text{mcd}(a, b)$, entonces $\text{mcd}(\frac{a}{d}, \frac{b}{d}) = 1$.

f) Si $\text{mcd}(a, b) = \text{mcd}(a, c) = 1$, entonces $\text{mcd}(a, bc) = 1$.

g) Si $\text{mcd}(a, b) = 1$ y $a \mid bc$, entonces $a \mid c$.

h) Si $\text{mcd}(a, b) = 1$, $a \mid c$ y $b \mid c$, entonces $ab \mid c$.

i) ab y $\text{mcd}(a, b)\text{mcm}[a, b]$ son asociados.

26. En este ejercicio todas las propiedades de divisibilidad se refieren al anillo $\mathbb{Z}[\sqrt{-5}]$. Demostrar

a) 2 y $1 + \sqrt{-5}$ son coprimos y sin embargo no hay una identidad de Bezout para $\{2, 1 + \sqrt{-5}\}$.

b) 2 y $1 + \sqrt{-5}$ no tienen mínimo común múltiplo.

c) No existe $\text{mcd}(6, 2(1 + \sqrt{-5}))$.

27. Sean D un DFU y P un conjunto de representantes de los irreducibles de D por la relación de equivalencia "ser asociados", es decir P está formado por irreducibles de D y cada elemento irreducible p de D es asociado de un único elemento de P.

a) Demostrar que cada elemento a de D se puede escribir de forma única como $a = u\prod_{p\in P} p^{\alpha_p}$, donde u es una unidad de D, cada $\alpha_p \geq 0$ y $\alpha_p = 0$ para casi todo $p \in P$. Llamaremos a esto "la" factorización de a en irreducibles de P.

b) Demostrar que si
$$a = u\prod_{p\in P} p^{\alpha_p} \qquad \text{y} \qquad b = v\prod_{p\in P} p^{\beta_p}$$
son las factorizaciones de a y b en irreducibles de P entonces $a \mid b$ precisamente si $\alpha_p \leq \beta_p$, para todo $p \in P$.

c) El número de divisores de un elemento no nulo a de D es finito, salvo asociados. Es decir, existe un conjunto finito F tal que todos los divisores de a son asociados de un elemento de F.

d) Obtener una fórmula para calcular el número de divisores de a, salvo asociados, en términos de una factorización de a.

e) Dar ejemplos de conjuntos P como los del ejercicio para $\mathbb{Z}$ y $K[X]$ donde K es un cuerpo.

28. Demostrar que en un DFU todo conjunto finito tiene un máximo común divisor y un mínimo común múltiplo.

29. Sea D un dominio. Una *función euclídea* en D es una aplicación $\delta : D \setminus \{0\} \to \mathbb{N}$ que cumple las siguientes condiciones:

(DE1) Si $a, b \in D \setminus \{0\}$ verifican $a \mid b$ entonces $\delta(a) \leq \delta(b)$.

(DE2) Dados $a, b \in D$ con $b \neq 0$, existen $q, r \in D$ tales que $a = bq + r$ y o bien $r = 0$ o bien $\delta(r) < \delta(b)$.

Un *dominio euclídeo* es un dominio que admite una función euclídea.

a) Demostrar que las siguientes aplicaciones son funciones euclídeas en los dominios que se indican.
   1) El valor absoluto en $\mathbb{Z}$.
   2) El módulo en el anillo $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.
   3) El grado en el anillo $K[X]$ de los polinomios con coeficientes en un cuerpo K.

b) Demostrar que si δ es una función euclídea en D entonces las siguientes condiciones son equivalentes para $a \in D$:
   1) a es una unidad de D.
   2) $\delta(a) = \delta(1)$.
   3) $\delta(a) \leq \delta(x)$, para todo $x \in D \setminus \{0\}$.

c) Calcular las unidades de $\mathbb{Z}[i]$.

d) Demostrar que todo dominio euclídeo es un DIP.

Capítulo 2

Polinomios

2.1. Anillos de polinomios

Sea A un anillo. En el Ejemplo 1.4.5 definimos el anillo de polinomios $A[X]$ en una indeterminada con coeficientes en A como el conjunto de las expresiones del tipo

$$P = P(X) = p_0 + p_1X + p_2X^2 + \cdots + p_nX^n \tag{2.1}$$

donde n es un número entero no negativo y $a_i \in A$ para todo i. Si P es como en (2.1), entonces $p_0, p_1, p_2, \ldots$ se llaman coeficientes de P. Más precisamente, p_iX^i se llama *monomio* de grado i del polinomio P y p_i se llama *coeficiente* del monomio de grado i de P. Obsérvese que P tiene infinitos coeficientes, aunque todos menos un número finito son iguales a 0. Dos polinomios son iguales si sus coeficientes de los monomios del mismo grado son iguales. El *polinomio cero* o *polinomio nulo* es el polinomio que tiene todos los coeficientes iguales a 0.

La suma y el producto en $A[X]$ se definen

$$(a_0 + a_1X + a_2X^2 + \cdots) + (b_0 + b_1X + b_2X^2 + \cdots) = c_0 + c_1X + c_2X^2 + \cdots,$$

donde cada $c_n = a_n + b_n$, y

$$(a_0 + a_1X + a_2X^2 + \cdots) \cdot (b_0 + b_1X + b_2X^2 + \cdots) = d_0 + d_1X + d_2X^2 + \cdots,$$

donde cada $d_n = a_0b_n + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0 = \sum_{i=0}^{n} a_ib_{n-i}$.

Sea A un anillo y sea $p = \sum_{i\in\mathbb{N}} p_iX^i \in A[X]$ un polinomio no nulo de $A[X]$. Entonces, por definición de polinomio, el conjunto $\{i \in \mathbb{N} : p_i \neq 0\}$ no es vacío y está acotado superiormente. Por tanto ese conjunto tiene un máximo, al que llamamos *grado* del polinomio p y denotamos por $\mathrm{gr}(p)$. Es decir,

$$\mathrm{gr}(p) = \mathrm{máx}\{i \in \mathbb{N} : p_i \neq 0\}.$$

El coeficiente de mayor grado, $p_{\mathrm{gr}(p)}$, se conoce como el *coeficiente principal* de p, y diremos que p es *mónico* si su coeficiente principal es 1. Por convenio, consideramos que el polinomio 0 tiene grado $-\infty$ y coeficiente principal 0. Es claro que los polinomios de grado 0 son precisamente los polinomios constantes no nulos. A veces llamaremos *lineales* a los polinomios de grado 1, *cuadráticos* a los de grado 2, *cúbicos* a los de grado 3, etcétera.

Lema 2.1. *Si $p = a_0 + a_1X + \cdots + a_nX^n$ y $q = b_0 + b_1X + \cdots + b_mX^m$ son polinomios de $A[X]$, con $a_n \neq 0 \neq b_m$ entonces se verifican las siguientes propiedades:*

1. $\mathrm{gr}(p+q) \leq \mathrm{máx}(\mathrm{gr}(p), \mathrm{gr}(q))$*, con la desigualdad estricta si y sólo si $n = m$ y $a_n + b_m = 0$.*

2. $\mathrm{gr}(pq) \leq \mathrm{gr}(p) + \mathrm{gr}(q)$, *con igualdad si y sólo si* $a_n b_m \neq 0$.

3. *Si* a_n *es regular (por ejemplo, si* p *es mónico, o si* A *es un dominio), entonces se tiene*

$$\mathrm{gr}(pq) = \mathrm{gr}(p) + \mathrm{gr}(q).$$

4. *Las desigualdades de los apartados 1 y 2 pueden ser estrictas (buscar un ejemplo cuando* $A = \mathbb{Z}_6$*).*

Demostración. Ejercicio. □

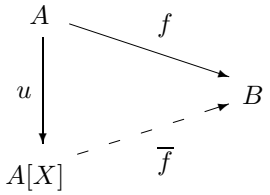
Una consecuencia inmediata del Lema 2.1 es:

Corolario 2.2. *Un anillo de polinomios* $A[X]$ *es un dominio si y sólo si lo es el anillo de coeficientes* A*. En este caso se tiene* $A[X]^* = A^*$*; es decir, los polinomios invertibles de* $A[X]$ *son los polinomios constantes invertibles en* A*. En particular, los polinomios invertibles sobre un cuerpo son exactamente los de grado 0, y* $A[X]$ *nunca es un cuerpo.*

Hemos observado que un anillo A es un subanillo del anillo de polinomios $A[X]$, y por tanto la inclusión $u : A \to A[X]$ es un homomorfismo de anillos. También es claro que el subanillo de $A[X]$ generado por A y X es todo $A[X]$. Es decir, la indeterminada X y las constantes de A (las imágenes de u) generan todos los elementos de $A[X]$. El siguiente resultado nos dice que $A[X]$ puede caracterizarse por una propiedad en la que sólo intervienen X y u.

Proposición 2.3. *Sean* A *un anillo,* $A[X]$ *el anillo de polinomios con coeficientes en* A *en la indeterminada* X *y* $u : A \to A[X]$ *el homomorfismo de inclusión.*

1. **(Propiedad Universal del Anillo de Polinomios, PUAP)** *Para todo homomorfismo de anillos* $f : A \to B$ *y todo elemento* b *de* B *existe un único homomorfismo de anillos* $\overline{f} : A[X] \to B$ *tal que* $\overline{f} \circ u = f$ *y* $\overline{f}(X) = b$*. Se dice que* $\overline{f}$ completa de modo único *el diagrama*



2. *Si dos homomorfismos de anillos* $g, h : A[X] \to B$ *coinciden sobre* A *y en* X *entonces son iguales. Es decir, si* $g \circ u = h \circ u$ *y* $g(X) = h(X)$ *entonces* $g = h$*.*

3. $A[X]$ *y* u *están determinados salvo isomorfismos por la PUAP. Explícitamente: supongamos que existen un homomorfismo de anillos* $v : A \to P$ *y un elemento* $T \in P$ *tales que, para todo homomorfismo de anillos* $f : A \to B$ *y todo elemento* $b \in B$*, existe un único homomorfismo de anillos* $\overline{f} : P \to B$ *tal que* $\overline{f} \circ v = f$ *y* $\overline{f}(T) = b$*. Entonces existe un isomorfismo* $\phi : A[X] \to P$ *tal que* $\phi \circ u = v$ *y* $\phi(X) = T$*.*

Demostración. 1. Sean $f : A \to B$ y $b \in B$ como en el enunciado. Si existe un homomorfismo $\overline{f} : A[X] \to B$ tal que $\overline{f} \circ u = f$ y $\overline{f}(X) = b$, entonces para un polinomio $p = \sum_{n\in\mathbb{N}} p_n X^n$, se tendrá

$$\overline{f}(p) = \overline{f}(\sum_{n\in\mathbb{N}} u(p_n)X^n) = \sum_{n\in\mathbb{N}} f(p_n)b^n.$$

Por tanto, la aplicación dada por $\overline{f}(p) = \sum_{n\in\mathbb{N}} f(p_n)b^n$ es la única que puede cumplir tales condiciones. El lector puede ahora comprobar que esta aplicación $\overline{f}$ es un homomorfismo de anillos, y es elemental ver que satisface $\overline{f} \circ u = f$ y $\overline{f}(X) = b$.

2. Si ponemos $f = g \circ u = h \circ u : A \to B$, los homomorfismos g y h completan el diagrama del apartado 1. Por la unicidad se tiene $g = h$.

3. Sean $v : A \to P$ y $T \in P$ como en 3. Aplicando 1 y la hipótesis de 3 encontramos homomorfismos $\overline{v} : A[X] \to P$ y $\overline{u} : P \to A[X]$ tales que

$$\overline{v} \circ u = v \ \text{ y } \ \overline{v}(X) = T \qquad \overline{u} \circ v = u \ \text{ y } \ \overline{u}(T) = X.$$

Entonces la composición $\overline{u} \circ \overline{v} : A[X] \to A[X]$ verifica

$$(\overline{u} \circ \overline{v}) \circ u = \overline{u} \circ v = u \qquad \text{y} \qquad (\overline{u} \circ \overline{v})(X) = \overline{u}(T) = X,$$

y por 2 se obtiene $\overline{u} \circ \overline{v} = 1_{A[X]}$. De modo análogo, y observando que v y T verifican una condición similar a 2, se demuestra que $\overline{v} \circ \overline{u} = 1_P$, con lo que $\overline{v}$ es el isomorfismo que buscamos. □

La utilidad de la PUAP estriba en que, dado un homomorfismo $f : A \to B$, nos permite crear un homomorfismo $A[X] \to B$ que "respeta" a f y que "se comporta bien" sobre un elemento $b \in B$ que nos interese. Los siguientes ejemplos son aplicaciones de la PUAP a ciertos homomorfismos que aparecen con frecuencia y son importantes tanto en este capítulo como en algunos de los siguientes (y en otras muchas situaciones que no estudiaremos aquí).

Ejemplos 2.4. *Aplicaciones de la PUAP.*

1. Sean A un subanillo de B y $b \in B$. Aplicando la PUAP a la inclusión $A \hookrightarrow B$ obtenemos un homomorfismo $S_b : A[X] \to B$ que es la identidad sobre A (decimos a veces que *fija* los elementos de A) y tal que $S_b(X) = b$. Se le llama el *homomorfismo de sustitución* (o de *evaluación*) en b. Dado $p = p(X) \in A[X]$, escribiremos a menudo $p(b)$ en vez de $S_b(X)$. Podemos describir explícitamente la acción de S_b en un polinomio:

$$S_b : A[X] \to B \qquad p(X) = \sum_{n \in \mathbb{N}} p_n X^n \qquad \rightsquigarrow \qquad S_b(p) = p(b) = \sum_{n \in \mathbb{N}} p_n b^n.$$

2. Sean A un anillo y $a \in A$. Si en el ejemplo anterior tomamos $B = A[X]$ y $b = X + a$, obtenemos un homomorfismo $A[X] \to A[X]$ dado por

$$p(X) \mapsto p(X + a).$$

   Este homomorfismo es un automorfismo cuyo inverso viene dado por $p(X) \mapsto p(X - a)$ (por qué?).

3. Todo homomorfismo de anillos $f : A \to B$ induce un homomorfismo entre los correspondientes anillos de polinomios: Aplicándole la PUAP a la composición de f con la inclusión $B \hookrightarrow B[X]$ obtenemos $\overline{f} : A[X] \to B[X]$ tal que $\overline{f} \mid_A = f$ y $\overline{f}(X) = X$. Explícitamente, dado $p = \sum_{n \in \mathbb{N}} p_n X^n$ en $A[X]$, se tiene

$$\overline{f}(p) = \sum_{n \in \mathbb{N}} f(p_n) X^n.$$

   Es fácil ver que, si f es inyectivo o suprayectivo, entonces lo es $\overline{f}$; como casos particulares de esta afirmación se obtienen los dos ejemplos siguientes:

4. Si A es un subanillo de B entonces $A[X]$ es un subanillo de $B[X]$.

5. Si I es un ideal del anillo A, la proyección $\pi : A \to A/I$ induce un homomorfismo suprayectivo $\overline{\pi} : A[X] \to (A/I)[X]$. Si ponemos $\overline{a} = a + I$, el homomorfismo $\overline{\pi}$ viene dado explícitamente por

$$\overline{\pi}(\sum_{n \in \mathbb{N}} p_n X^n) = \sum_{n \in \mathbb{N}} \overline{p_n} X^n.$$

A $\overline{\pi}$ se le llama el homomorfismo de *reducción de coeficientes módulo* I. Su núcleo, que es un ideal de $A[X]$, consiste en los polinomios con coeficientes en I, y lo denotaremos por $I[X]$. Obsérvese que $(A/I)[X] \simeq \dfrac{A[X]}{I[X]}$.

6. Sea A un subanillo de B y sea $S_b : A[X] \to B$ el homomorfismo de sustitución en cierto elemento b de B. Entonces Im S_b es el subanillo de B generado por $A \cup \{b\}$, y consiste en las "expresiones polinómicas en b con coeficientes en A"; es decir, en los elementos de la forma

$$\sum_{i=0}^{n} a_i b^i,$$

donde $n \in \mathbb{N}$ y $a_i \in A$ para cada i. Este subanillo se suele denotar por $A[b]$.

Por ejemplo, si $A = \mathbb{Z}$, $B = \mathbb{C}$ y $b = \sqrt{m}$ (ó $b = \frac{1+\sqrt{m}}{2}$ con $m \equiv 1 \bmod 4$) para cierto $m \in \mathbb{Z}$, la notación anterior es compatible con la que se usó anteriormente (es decir, $\mathbb{Z}[\sqrt{m}]$ representa el mismo subanillo atendiendo a cualquiera de las dos definiciones). Lo mismo ocurre si se toma $A = \mathbb{Q}$.

2.2. Raíces de polinomios

Empezaremos esta sección con el siguiente lema. Recuérdese que consideramos el polinomio cero como un polinomio de grado $-\infty$.

Lema 2.5. *Sea A un anillo y sean $f, g \in A[X]$. Si el coeficiente principal de g es invertible en A, entonces existen dos únicos polinomios $q, r \in A[X]$ tales que $f = gq + r$ y $\mathrm{gr}(r) < \mathrm{gr}(g)$.*

En esta situación, q y r se llaman cociente *y* resto *de la división de f entre g.*

Demostración. Sea $m = \mathrm{gr}(g)$ y sea b el coeficiente principal de g que es invertible en A, por hipótesis. Dado $f \in A[X]$ vamos a ver, por inducción en $n = \mathrm{gr}(f)$, que existen $q, r \in A[X]$ satisfaciendo las propiedades del Lema. Si $n < m$ podemos tomar $q = 0$ y $r = f$. Supongamos pues que $n \geq m$ y que la propiedad se verifica si f se sustituye por un polinomio de grado menor. Si a es el término principal de f, es claro que el polinomio $f_1 = f - ab^{-1}X^{n-m}g \in A[X]$ tiene grado menor que el de f. Por hipótesis de inducción existen $q_1, r \in A[X]$ tales que $f_1 = gq_1 + r$ y $r = 0$ o $\mathrm{gr}(r) < m$. Entonces $f = g(q_1 + ab^{-1}X^{n-m}) + r$, lo que termina la demostración de la existencia de cociente y resto.

En cuanto a la unicidad, supongamos que $f = gq_1 + r_1 = gq_2 + r_2$ con $\mathrm{gr}(r_i) < \mathrm{gr}(g)$ para cada $i = 1, 2$. Como el término principal de g es regular, del Lema 2.1 se deduce que

$$\mathrm{gr}(g) + \mathrm{gr}(q_1 - q_2) = \mathrm{gr}(g(q_1 - q_2)) = \mathrm{gr}(r_2 - r_1) \leq \mathrm{máx}\{\mathrm{gr}(r_2), \mathrm{gr}(r_1)\} < \mathrm{gr}(g).$$

Luego $\mathrm{gr}(q_1 - q_2) < 0$ y en consecuencia $q_1 = q_2$, de donde $r_1 = r_2$. □

Diremos que $a \in A$ es una *raíz* de $f \in A[X]$ si $f(a) = 0$ (es decir, si $X - a$ divide a f). Por ejemplo, 0 es raíz de f si y sólo si f tiene coeficiente independiente 0, y cualquier elemento de A es raíz del polinomio 0.

Proposición 2.6. *Sean A un anillo, $a \in A$ y $f \in A[X]$. Entonces:*

1. **(Teorema del Resto)** *El resto de la división de f entre $X - a$ es $f(a)$.*
2. **(Teorema de Ruffini)** *f es divisible por $X - a$ precisamente si $f(a) = 0$, es decir si a es una raíz de f.*

Demostración. Dividiendo f entre $X-a$ tenemos $f = q(X-a)+r$ con $\mathrm{gr}(r) < 1$, por lo que r es constante y así $r = r(a) = f(a) - q(a)(a-a) = f(a)$. Esto demuestra 1, y 2 es entonces inmediato. □

Fijemos $a \in A$. Como, para cada $k \in \mathbb{N}$, el polinomio $(X-a)^k$ es mónico de grado k, se tiene $\mathrm{gr}((X-a)^k q) = k + \mathrm{gr}(q)$ para cada $q \in A[X]$. Por tanto, para cada $f \in A[X]$ no nulo, existe un mayor $m \in \mathbb{N}$ tal que $(X-a)^m$ divide a f. Este entero m, que verifica $0 \leq m \leq \mathrm{gr}(f)$, se llama la *multiplicidad de a en f*. Por el Teorema de Ruffini, a es raíz de f precisamente si $m \geq 1$. Cuando $m = 1$ se dice que a es una *raíz simple* de f, y cuando $m > 1$ se dice que a es una *raíz múltiple* de f.

Ejercicio 2.7. *Sean A un anillo y $a \in A$. Demostrar que el polinomio $X-a$ es cancelable en $A[X]$, y deducir que $m \in \mathbb{N}$ es la multiplicidad de a en $f \in A[X]$ si y sólo si existe un polinomio $q \in A[X]$ con $f = (X-a)^m q$ y $q(a) \neq 0$.*

Cuando D es un dominio, del Teorema de Ruffini se deduce que $X-a$ es primo para cualquier $a \in D$. Esto es esencial en la demostración del siguiente resultado.

Proposición 2.8 (Acotación de raíces)**.** *Sean D un dominio y $0 \neq f \in D[X]$. Entonces:*

1. *Si $a_1, \ldots, a_n \in D$ son distintos dos a dos y $\alpha_1, \ldots \alpha_n \geq 1$ son enteros con cada $(X-a_i)^{\alpha_i} \mid f$, entonces $(X-a_1)^{\alpha_1} \cdots (X-a_n)^{\alpha_n} \mid f$. Por tanto $\sum_{i=1}^n \alpha_i \leq \mathrm{gr}(f)$.*

2. *La suma de las multiplicidades de todas las raíces de f es menor o igual que $\mathrm{gr}(f)$. En particular, el número de raíces distintas de f es menor o igual que $\mathrm{gr}(f)$.*

Demostración. Es claro que basta con demostrar la primera afirmación de 1, cosa que hacemos por inducción en $s = \sum_{i=1}^n \alpha_i$ con el caso $s = 1$ evidente. Cuando $s > 1$, usando la hipótesis $(X-a_1)^{\alpha_1} \mid f$ y la hipótesis de inducción, sabemos que existen polinomios g y h tales que

$$g(X-a_1)^{\alpha_1} = f = h(X-a_1)^{\alpha_1 - 1}(X-a_2)^{\alpha_2} \cdots (X-a_n)^{\alpha_n}.$$

Cancelando $(X-a_1)^{\alpha_1 - 1}$ y usando el hecho de que $X-a_1$ es primo y no divide a ningún otro $X-a_i$ (por qué?), deducimos que $X-a_1$ divide a h, y esto nos da el resultado. □

Si D no es un dominio, siempre podemos encontrar un polinomio en $D[X]$ para el que falle la acotación de raíces (es decir, "con más raíces que grado"). En efecto, si $0 \neq a, b \in D$ y $ab = 0$, entonces aX es un polinomio de grado 1 con al menos 2 raíces, 0 y b. Otro ejemplo se obtiene considerando el polinomio $X^2 - 1$, que tiene 4 raíces en $\mathbb{Z}_8$.

El siguiente corolario evidente de la Proposición 2.8 se conoce como el *principio de las identidades polinómicas*. Ya hemos comentado que su segundo apartado falla sobre cualquier anillo finito.

Corolario 2.9. *Sea D un dominio, y sean $f, g \in D[X]$. Entonces:*

1. *Si las funciones polinómicas $f, g : D \to D$ coinciden en m puntos, con $m > \mathrm{gr}(f)$ y $m > \mathrm{gr}(g)$, entonces $f = g$ (como polinomios).*

2. *Si D es infinito entonces dos polinomios distintos definen funciones polinómicas distintas en D.*

La necesidad de la hipótesis de infinitud del dominio D en el Corolario 2.9 resulta obvia si observamos que si K es un cuerpo (recuérdese que todo dominio finito es un cuerpo) entonces hay infinitos polinomios con coeficientes en K pero sólo un número finito de aplicaciones de K en K. Para un ejemplo explícito recordemos el Pequeño Teorema de Fermat que afirma que si p es primo, entonces $a^p \equiv a \bmod p$. Eso implica que todos los elementos del cuerpo $\mathbb{Z}/p\mathbb{Z}$ son raíces del polinomio no nulo $X^p - X$.

El siguiente concepto es útil para calcular multiplicidades: Si A es un anillo, la *derivada* de $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ se define como

$$D(P) = P' = a_1 + 2a_2X + 3a_3X^2 + \cdots + na_nX^{n-1}.$$

Obsérvese que la derivada no se ha definido a partir de ningún concepto topológico, y por ejemplo no es cierto en general que un polinomio con derivada nula sea constante (considérese por ejemplo $X^n \in \mathbb{Z}_n[X]$). Sin embargo, esta *derivada formal* satisface las mismas propiedades algebraicas que la derivada del Análisis.

Lema 2.10. *Dados $a, b \in A$ y $P, Q \in A[X]$, demostrar que:*

1. $(aP + bQ)' = aP' + bQ'$.
2. $(PQ)' = P'Q + PQ'$.
3. $(P^n)' = nP^{n-1}P'$.

Demostración. Ejercicio. □

Proposición 2.11. *Una elemento $a \in A$ es una raíz múltiple de $P \in A[X]$ si y sólo si $P(a) = P'(a) = 0$.*

Demostración. Ya sabemos que a es una raíz de P si y sólo si $P(a) = 0$. Si a es raíz simple se tiene $P = (X - a)Q$ para cierto $Q \in A[X]$ con $Q(a) \neq 0$, por lo que, del Lema 2.10 tenemos que $P' = Q + (X - a)Q'$ y así $P'(a) = Q(a) \neq 0$. Si a es raíz múltiple se tiene $P = (X - a)^2Q$ para cierto $Q \in A[X]$, por lo que $P' = 2(X - a)Q + (X - a)^2Q'$ y así $P'(a) = 0$. □

En dominios de característica cero, la idea de la demostración anterior puede usarse para determinar la multiplicidad de a en P (no sólo para decidir si a es simple o múltiple). Para ello, necesitamos considerar las *derivadas sucesivas* de un polinomio: Para cada $n \in \mathbb{N}$ se define la derivada n-ésima $P^{(n)}$ de $P \in A[X]$, de forma recurrente, por las fórmulas:

$$P^{(0)} = P \quad \text{y} \quad P^{(n+1)} = (P^{(n)})'.$$

Proposición 2.12. *Sea D un dominio de característica 0, y sean $P \in D[X]$ y $a \in D$. Entonces la multiplicidad de a en P es el menor número natural $m \in \mathbb{N}$ tal que $P^{(m)}(a) \neq 0$.*

Demostración. Haremos inducción en la multiplicidad m de a en P, con el caso $m = 0$ claro. Si $m \geq 1$ entonces a es raíz de P y por tanto $P = (X - a)Q$ para cierto $Q \in D[X]$. Entonces la multiplicidad de a en Q es $m - 1$, y por hipótesis de inducción $Q^{(i)}(a) = 0 \neq Q^{(m-1)}(a)$ para todo $i < m - 1$. Además, para cada $t \geq 1$ se tiene

$$P^{(t)} = tQ^{(t-1)} + (X - a)Q^{(t)}.$$

Ahora el lector podrá completar fácilmente la demostración. □

La hipótesis sobre la característica de D en la Proposición 2.12 es necesaria. Por ejemplo, si p es un número primo, $K = \mathbb{Z}_p$ y $P = X^p$, entonces $P' = 0$ y así $P^{(n)}(0) = 0$ para todo n.

No todos los polinomios con coeficientes en un anillo A tienen raíces en A. Por ejemplo, los polinomios de grado 0 no tienen ninguna raíz, y un polinomio lineal $aX + b$ (con $a \neq 0$) tiene una raíz en A si y sólo si a divide a b. En particular, todo polinomio lineal sobre un cuerpo tiene una raíz, pero puede haber polinomios de grado positivo sin raíces: por ejemplo, $X^2 + 1$ no tiene raíces en $\mathbb{R}$, y $X^3 - 2$ no las tiene en $\mathbb{Q}$.

2.3. Divisibilidad en anillos de polinomios

La siguiente proposición caracteriza cuándo un anillo de polinomios es un DIP.

Proposición 2.13. *Para un anillo A, las condiciones siguientes son equivalentes:*

1. *$A[X]$ es un dominio de ideales principales.*
2. *A es un cuerpo.*

En este caso, un polinomio $f \in A[X]$ es irreducible (o primo) si y sólo si $\operatorname{gr}(f) > 0$ y f no es producto de dos polinomios de grado menor; es decir, si una igualdad $f = gh$ en $A[X]$ implica que $\operatorname{gr}(g) = \operatorname{gr}(f)$ (y $\operatorname{gr}(h) = 0$) ó $\operatorname{gr}(h) = \operatorname{gr}(f)$ (y $\operatorname{gr}(g) = 0$).

Demostración. 1 implica 2. Supongamos primero que A es un DIP. Eso implica que A es un dominio. Además el polinomio X es un elemento irreducible de $A[X]$. De la Proposición 1.55 se deduce que (X) es un ideal maximal de $A[X]$ y por tanto $A \simeq A[X]/(X)$ es un cuerpo.

2 implica 1. Supongamos ahora que A es un cuerpo y sea I un ideal de A diferente de 0. De todos los elementos no nulos de I elegimos uno P de grado mínimo y demostramos que $I = (P)$. La inclusión $(P) \subseteq I$ está clara. Para demostrar la otra inclusión razonamos por reducción al absurdo, es decir suponemos que $I \not\subseteq (P)$ y elegimos un elemento de $F \in I \setminus (P)$ de grado mínimo. Del Lema 2.5 deducimos que existen $Q, R \in A[X]$ tales que $F = QP + R$ y $\operatorname{gr}(R) < \operatorname{gr}(P)$, ya que $R \neq 0$, pues por hipótesis $F \notin (P)$. Eso implica que $R = F - QP \in I$, en contra de la minimalidad del grado de P.

Dejamos que el lector demuestre la afirmación sobre los polinomios irreducibles. □

Obsérvese que si $a \in A$ y $f \in A[X]$ entonces $a|f$ si y sólo si a divide a todos los coeficientes de A.

Lema 2.14. *Sea D un dominio y sea $p \in D$.*

1. *p es irreducible en D si y sólo si lo es en $D[X]$.*
2. *Si p es primo en $D[X]$ entonces lo es en D.*
3. *Si además D es un DFU entonces las condiciones siguientes son equivalentes:*
   (a) *p es irreducible en D.*
   (b) *p es irreducible en $D[X]$.*
   (c) *p es primo en D.*
   (d) *p es primo en $D[X]$.*

Demostración. 1 y 2 son consecuencias casi inmediatas del Lema 2.1. Para demostrar 3 basta demostrar (c) implica (d) pues ya sabemos que (d) implica (b) (Proposición 1.51), que (a) y (c) son equivalentes, (Lema 1.57) y (a) y (b) son equivalentes (apartado 1).

Supongamos por tanto que p es primo en D, y veamos que lo es en $D[X]$. Para ello, sean

$$a = a_0 + \cdots + a_n X^n \qquad \text{y} \qquad b = b_0 + \cdots + b_m X^m$$

polinomios de $D[X]$ tales que $p \nmid a$ y $p \nmid b$, y veamos que $p \nmid ab$. Por hipótesis, existen un menor índice i tal que $p \nmid a_i$, y un menor índice j tal que $p \nmid b_j$. El coeficiente de grado $i + j$ de ab es

$$c_{i+j} = a_0 b_{i+j} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0,$$

y las condiciones dadas implican que p divide a todos los sumandos excepto a $a_i b_j$, por lo que $p \nmid c_{i+j}$ y en consecuencia $p \nmid ab$. □

En el resto de la sección D será un DFU y K su cuerpo de fracciones.

Consideramos la función

$$\varphi : D \setminus \{0\} \to \mathbb{N}$$

que a cada $0 \neq a \in D$ le asocia el número $\varphi(a)$ de factores irreducibles en la expresión de a como producto de irreducibles de D, contando repeticiones. Por ejemplo, si $D = \mathbb{Z}$ entonces $\varphi(12) = 3$ y $\varphi(-80) = 5$. Es claro que, si $a, b \in D \setminus \{0\}$, entonces

$$\varphi(ab) = \varphi(a) + \varphi(b) \qquad \text{y} \qquad \varphi(a) = 0 \Leftrightarrow a \in D^*.$$

Lema 2.15. *Si $a \in D$ y $f, g, h \in D[X]$ verifican $af = gh \neq 0$, entonces existen $g_1, h_1 \in D[X]$ tales que*

$$f = g_1 h_1, \qquad \operatorname{gr}(g_1) = \operatorname{gr}(g), \qquad \operatorname{gr}(h_1) = \operatorname{gr}(h).$$

Demostración. Razonamos por inducción en $\varphi(a)$. Si $\varphi(a) = 0$ podemos tomar $g_1 = a^{-1}g$ y $h_1 = h$. Si $\varphi(a) > 0$, existen $p, b \in D$ tales que $a = pb$ y p es primo. Entonces $p \mid af = gh$ en $D[X]$ y, por el Lema 2.14, podemos asumir que $p \mid g$ en $D[X]$. Es decir, existe $\overline{g} \in D[X]$ tal que $g = p\overline{g}$, de donde $\operatorname{gr}(g) = \operatorname{gr}(\overline{g})$. Cancelando p en la igualdad $af = gh$ obtenemos $bf = \overline{g}h$. Como $\varphi(b) = \varphi(a) - 1 < \varphi(a)$, la hipótesis de inducción nos dice que existen $g_1, h_1 \in D[X]$ tales que $f = g_1 h_1$, $\operatorname{gr}(g_1) = \operatorname{gr}(\overline{g})$, y $\operatorname{gr}(h_1) = \operatorname{gr}(h)$, lo que nos da el resultado. □

El siguiente resultado relaciona la irreducibilidad de un polinomio sobre D con su irreducibilidad sobre K. Aunque su recíproco es falso en general (piénsese en $2X$ como polinomio sobre $\mathbb{Z}$), pronto veremos que es válido con una condición extra sobre el polinomio (Proposición 2.19).

Lema 2.16. *Si $f \in D[X]$ es irreducible en $D[X]$, entonces es irreducible (o primo) en $K[X]$.*

Demostración. Supongamos que f no es irreducible en $K[X]$. Por la Proposición 2.13, existen $G, H \in K[X]$ tales que

$$f = GH, \qquad \operatorname{gr}(G) > 0, \qquad \operatorname{gr}(H) > 0.$$

Si $0 \neq b \in D$ es un múltiplo común de los denominadores de los coeficientes de G, se tiene $g = bG \in D[X]$, y análogamente existe $0 \neq c \in D$ tal que $h = cH \in D[X]$. Aplicando el Lema 2.15 a la igualdad $(bc)f = gh$ obtenemos $g_1, h_1 \in D[X]$ tales que $f = g_1 h_1$, $\operatorname{gr}(g_1) = \operatorname{gr}(g) = \operatorname{gr}(G) > 0$, y $\operatorname{gr}(h_1) = \operatorname{gr}(h) = \operatorname{gr}(H) > 0$, lo que nos da una factorización no trivial de f en $D[X]$. □

Podemos ya demostrar el resultado principal de esta sección:

Teorema 2.17. *D es un DFU si y sólo si lo es $D[X]$.*

Demostración. Supongamos primero que $D[X]$ es un DFU. Entonces D es un dominio (Corolario 2.2), y cada $0 \neq a \in D \setminus D^*$ es producto de irreducibles de $D[X]$, que tendrán grado 0 pues lo tiene a. Por el Lema 2.14, ésa será una factorización de a en irreducibles de D. Del mismo lema se deduce que todo irreducible de D es primo en D, por lo que D es un DFU.

Supongamos ahora que D es un DFU y veamos que lo es $D[X]$. Empezaremos demostrando que cada $a = a_0 + \cdots + a_n X^n \in D[X]$ (con $a_n \neq 0$) no invertible es producto de irreducibles, y lo haremos por inducción en $n + \varphi(a_n)$. Obsérvese que a es invertible si y sólo si $n + \varphi(a_n) = 0$. El caso $n + \varphi(a_n) = 1$ se resuelve fácilmente. Supongamos pues que $n + \varphi(a_n) > 1$ y que a no es irreducible. Entonces existen

$$b = b_0 + \cdots + b_m X^m \quad (b_m \neq 0) \qquad \text{y} \qquad c = c_0 + \cdots + c_k X^k \quad (c_k \neq 0)$$

en $D[X]$, no invertibles, con $a = bc$ y b y c elementos de $D[X]$ que no son unidades de $D[X]$. Entonces

$$0 < m + \varphi(b_m), \quad 0 < k + \varphi(c_k) \quad \text{y} \quad n + \varphi(a_n) = m + k + \varphi(b_m) + \varphi(c_k).$$

En consecuencia, podemos aplicar la hipótesis de inducción a b y c, y pegando las factorizaciones así obtenidas conseguimos una factorización en irreducibles de a.

Por la Proposición 1.58, sólo falta demostrar que todo irreducible f de $D[X]$ es primo, y por el Lema 2.14 podemos suponer que $\mathrm{gr}(f) \geq 1$. Sean pues $g, h \in D[X]$ tales que $f \mid gh$ en $D[X]$, y veamos que $f \mid g$ ó $f \mid h$ en $D[X]$. Obviamente, $f \mid gh$ en $K[X]$, y como f es primo en $K[X]$ por el Lema 2.16, podemos asumir que $f \mid g$ en $K[X]$. Es decir, existe $G \in K[X]$ tal que $g = fG$, y si demostramos que $G \in D[X]$ habremos terminado. Para ello, tomando $a \in D$ con $aG \in D[X]$ y $\varphi(a)$ mínimo, basta ver que $\varphi(a) = 0$. Supongamos que $\varphi(a) > 0$ y sean $p, b \in D$ con $a = pb$ y p primo. Entonces, en $D[X]$, se tiene $p \mid ag = f(aG)$. Como p es primo en $D[X]$ (Lemma 2.14) y $p \nmid f$ (pues f es irreducible y $\mathrm{gr}(f) \geq 1$), deducimos que $p \mid aG$ en $D[X]$. Si $g_1 \in D[X]$ verifica $aG = pg_1$ entonces $bG = g_1 \in D[X]$, contra la minimalidad de $\varphi(a)$, y esta contradicción termina la demostración. □

De la Proposición 2.13 y el Teorema 2.17 se deduce que $\mathbb{Z}[X]$ es un DFU pero no un DIP, lo que muestra que el recíproco del Teorema 1.59 no es cierto.

El *contenido de un polinomio* $p = p_0 + \cdots + p_n X^n \in D[X]$ no nulo es el máximo común divisor de sus coeficientes, es decir

$$c(p) = \mathrm{mcd}(p_0, p_1, \ldots, p_n).$$

Obsérvese que el contenido, como un máximo común divisor, no es único en sentido estricto, sino solamente único salvo unidades. Obsérvese que un elemento $d \in D$ divide a p en $D[X]$ si y sólo si divide al contenido de p. Está claro que si $a \in D \setminus \{0\}$, entonces $c(ap) = ac(p)$. Si ahora $p \in K[X]$ y $m \in D \setminus \{0\}$ satisface que $mp \in D[X]$, entonces definimos $c(p) = \frac{c(mp)}{m}$. Está definición no depende de la elección de m pues si $m_1 p, m_2 p \in D[X]$, entonces $\frac{c(m_1 p)}{m_1} = \frac{m_1 m_2 c(p)}{m_1 m_2} = \frac{c(p)}{m_2}$. De nuevo se verifica $c(ap) = ac(p)$, para todo $p \in K[X] \setminus \{0\}$ y $a \in K^*$. Además, si $p \in K[X]$ entonces $p \in D[X]$ si y sólo si $c(p) \in D$. Una implicación está clara. Para demostrar la otra obsérvese que si $p \notin K[X]$ entonces existe un coeficiente $\frac{a}{b}$ de p tal que b es múltiplo de un primo q que no es divisor de a. Podemos elegir el coeficiente de forma que el exponente de q en la factorización de b sea máximo, pongamos n. Si m es el mínimo común múltiplo de los denominadores de p (expresados como fracciones reducidas), entonces $m = q^n k$ con $q \nmid k$ y por tanto q no divide a $\frac{ma}{b}$. Deducimos que q no divide a $c(mp)$ y por tanto $c(p) = \frac{c(mp)}{m}$ no pertenece a D.

Diremos que un polinomio es *primitivo* si tiene contenido 1. Es decir $p \in D[X]$ es primitivo si los únicos divisores de grado 0 son las unidades de $D[X]$. Obsérvese que para todo $0 \neq p \in D[X]$ se tiene que $p/c(p)$ es primitivo y de hecho $c = c(p)$ si y sólo si $p = cp_1$ con $p_1 \in D[X]$, primitivo.

Lema 2.18 (Lema de Gauss)**.** *Si $f, g \in K[X]$, entonces $c(fg) = c(f)c(g)$. En particular, fg es primitivo si y sólo si f y g son primitivos.*

Demostración. Tenemos $f = c(f)f_1$ y $g = c(g)g_1$ con f_1 y g_1 primitivos. Por tanto $fg = c(f)c(g)f_1 g_1$, luego para demostrar que $c(fg) = c(f)c(g)$ basta probar que $f_1 g_1$ es primitivo. En caso contrario $c(f_1 g_1)$ tendría un divisor irreducible p en D. Eso implica que $p | f_1 g_1$. Por el Lema de Gauss, p es primo en $D[X]$ y por tanto $p | f_1$ ó $p | g_1$, lo que implica que $p | c(f_1)$ ó $p | c(g_1)$, en contra de que $c(f_1) = c(g_1) = 1$. □

Proposición 2.19. *Para un polinomio primitivo $f \in D[X] \setminus D$, las condiciones siguientes son equivalentes:*

1. *f es irreducible en $D[X]$.*
2. *f es irreducible en $K[X]$.*
3. *Si $f = GH$ con $G, H \in K[X]$ entonces $\mathrm{gr}(G) = 0$ ó $\mathrm{gr}(H) = 0$.*

4. Si $f = gh$ con $g, h \in D[X]$ entonces $\mathrm{gr}(g) = 0$ ó $\mathrm{gr}(h) = 0$.

Demostración. El Lema 2.16 y la Proposición 2.13 aseguran que 1 implica 2 y que 2 implica 3, respectivamente, y es claro que 3 implica 4. Finalmente, como f es primitivo, sus únicos divisores de grado 0 son unidades, por lo que 4 implica 1. □

Como consecuencia del Lema 2.14 y la Proposición 2.19 se deduce el siguiente corolario.

Corolario 2.20. *Si D es un DFU y K es su cuerpo de fracciones, entonces los irreducibles de $D[X]$ son los irreducibles de D y los polinomios primitivos de $D[X] \setminus D$ que son irreducibles en $K[X]$.*

Nuestro siguiente objetivo es factorizar polinomios en $D[X]$ y en $K[X]$, donde D sigue siendo un DFU y K su cuerpo de fracciones. Para ello es necesario disponer de métodos que nos digan cuándo un polinomio es irreducible. Como se verá, pocos de los resultados prácticos que obtendremos nos dan condiciones necesarias y suficientes para que un polinomio sea irreducible. Asumiremos que disponemos de un método para factorizar los elementos de D, y en particular para decidir si son irreducibles o no. Esto es teóricamente posible si $D = \mathbb{Z}$ ó $D = \mathbb{Z}[i]$ (y también lo es en la práctica en los casos que se nos presentarán), y nos permite además decidir si un polinomio de $D[X]$ es o no primitivo.

En general, dado un polinomio $0 \neq f \in D[X]$, calcularemos $d = c(f)$ y obtendremos $f = df_1$, con $f_1 \in D[X]$ primitivo. El polinomio constante d es una unidad en $K[X]$, mientras que en $D[X]$ tiene la misma factorización en irreducibles que tenga como elemento de D. En cuanto a f_1, para decidir su irreducibilidad, la Proposición 2.19 nos permite considerarlo como polinomio sobre D o sobre K según nos convenga. Por tanto, es importante tener criterios de irreducibilidad como los que siguen para polinomios sobre cuerpos. Para polinomios de grado pequeño esto es fácil.

Lema 2.21. *Sea K un cuerpo y sea $f \in K[X]$. Entonces*

1. *Si $\mathrm{gr}(f) = 1$ entonces f es irreducible en $K[X]$.*
2. *Si $\mathrm{gr}(f) > 1$ y f tiene una raíz en K, entonces f no es irreducible en $K[X]$.*
3. *Si $\mathrm{gr}(f) = 2$ ó 3 entonces f es irreducible en $K[X]$ si y sólo si f no tiene raíces en K.*

Demostración. Ejercicio. □

El Lema 2.21 pone de manifiesto la importancia de encontrar raíces de un polinomio para decidir si es irreducible. Cuando los coeficientes están en un DFU podemos seleccionar los "candidatos a raíces":

Proposición 2.22. *Sea D un DFU con cuerpo de fracciones K, y sea $f = a_0 + a_1X + \cdots + a_nX^n \in D[X]$ con $a_n \neq 0$. Entonces todas las raíces de f en K son de la forma r/s, donde $r \mid a_0$ y $s \mid a_n$.*

Demostración. Sea $t = \frac{r}{s}$ una raíz de f con $r, s \in D$ primos entre sí. Multiplicando la igualdad $f(t) = 0$ por s^n obtenemos

$$a_0s^n + a_1rs^{n-1} + a_2r^2s^{n-2} + \cdots + a_{n-1}r^{n-1}s + a_nr^n = 0,$$

luego $r \mid a_0s^n$ y $s \mid a_nr^n$. Como r y s son coprimos, deducimos que $r \mid a_0$ y $s \mid a_n$. □

Ejemplos 2.23. *Factorizaciones de polinomios.*

1. La no existencia de raíces no garantiza la irreducibilidad de polinomios de grado mayor que 3. Por ejemplo, $X^4 + 2X^2 + 1 = (X^2 + 1)^2$ es reducible en $\mathbb{R}[X]$ pero no tiene raíces reales.

2. Las posibles raíces en $\mathbb{Q}$ del polinomio $f = 3X^3 + X^2 + X - 2$ son ± 2, ± 1, $\pm 2/3$ y $\pm 1/3$, y de hecho $f(2/3) = 0$. Por tanto $(X - 2/3) \mid f$, y así $(3X - 2) \mid f$. Dividiendo se obtiene $f = (3X - 2)(X^2 + X + 1)$. Como ambos factores son primitivos sobre $\mathbb{Z}$ e irreducibles sobre $\mathbb{Q}$ y sobre $\mathbb{R}$, deducimos que la anterior es una factorización en irreducibles de f en cualquiera de los anillos $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ ó $\mathbb{R}[X]$. La factorización en $\mathbb{C}[X]$ es $f = (3X - 2)(X - \omega)(X - \overline{\omega})$, donde $\omega = \frac{-1+\sqrt{-3}}{2}$.

3. El polinomio $f = 6X^4 + 6X^2 + 18X - 30 = 2 \cdot 3 \cdot (X^4 + X^2 + 3X - 5)$ tiene al 1 por raíz, y dividiendo se tiene $X^4 + X^2 + 3X - 5 = (X - 1)(X^3 + X^2 + 2X + 5)$. El factor cúbico es primitivo y no tiene raíces en $\mathbb{Q}$ (al sustituir ± 1 ó ± 5 se obtiene un entero impar), por lo que

$$f = 2 \cdot 3 \cdot (X - 1)(X^3 + X^2 + 2X + 5) \qquad \text{y} \qquad f = 6(X - 1)(X^3 + X^2 + 2X + 5)$$

son las factorizaciones de f en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$, respectivamente (en la segunda el 6 no es un factor irreducible, sino una unidad). El polinomio cúbico no es irreducible en $\mathbb{R}[X]$ ni en $\mathbb{C}[X]$. De hecho, un análisis del crecimiento de la función polinómica $f : \mathbb{R} \to \mathbb{R}$ nos lleva a la conclusión de que f tiene una raíz real y dos complejas conjugadas.

4. El polinomio $f = X^4 + X^3 + 2X^2 + X + 1$ no tiene raíces racionales, pero esto no implica que sea irreducible sobre $\mathbb{Q}$. De hecho, se tiene $f(i) = 0$, y por tanto $(X - i)(X + i) = X^2 + 1$ divide a f; el otro factor es $X^2 + X + 1$, por lo que $f = (X^2 + 1)(X^2 + X + 1)$ es una factorización en irreducibles en $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ ó $\mathbb{R}[X]$, y $f = (X - i)(X + i)(X - \omega)(X - \overline{\omega})$ (con $\omega = \frac{-1+\sqrt{-3}}{2}$) es una factorización en $\mathbb{C}[X]$.

5. Supongamos que el polinomio sin raíces racionales $f = X^4 - 2X^3 + 6X - 3$ no es irreducible en $\mathbb{Z}[X]$. Por la Proposición 2.19, existen $g, h \in \mathbb{Z}[X]$, ambos de grado ≥ 1, tales que $f = gh$. Podemos asumir que g y h son mónicos (por qué?), y por tanto no pueden tener grado 1 (por qué?). En consecuencia, ambos tienen grado 2 y por tanto existen $a, b, c, d \in \mathbb{Z}$ tales que $f = (X^2 + aX + b)(X^2 + cX + d)$. Igualando coeficientes, se obtienen las ecuaciones

$$bd = -3, \quad ad + bc = 6, \quad b + ac + d = 0, \quad a + c = -2.$$

La primera ecuación nos da 4 opciones para los valores de b y d. Una de ellas es $b = 1$ y $d = -3$, que sustituida en la segunda ecuación y combinada con la cuarta nos dice que $a = -2$ y $c = 0$; pero estos valores no satisfacen la tercera ecuación. De modo similar se ve que las otras opciones tampoco funcionan, lo que significa que no existen tales $a, b, c, d \in \mathbb{Z}$ y en consecuencia f es irreducible en $\mathbb{Z}[X]$, y por tanto también en $\mathbb{Q}[X]$.

El último ejemplo muestra lo penoso que puede resultar estudiar la irreducibilidad de un polinomio, incluso de grado bajo, con los métodos que hemos desarrollado hasta ahora. El resto de esta sección lo dedicamos a presentar otros dos criterios de irreducibilidad para polinomios sobre un DFU que son a menudo útiles.

En el primero de ellos usaremos el Ejemplo 3 de 2.4: Un homomorfismo de anillos $\phi : A \to B$ induce otro $A[X] \to B[X]$ dado por

$$f = \sum a_i X^i \mapsto \phi(f) = \sum \phi(a_i) X^i.$$

En general se tiene $\operatorname{gr}(\phi(f)) \leq \operatorname{gr}(f)$, con igualdad si el coeficiente principal de f no está en Ker ϕ.

Proposición 2.24 (Criterio de Reducción)**.** *Sea $\phi : D \to K$ un homomorfismo de anillos, donde D es un DFU y K es un cuerpo, y sea f un polinomio primitivo de $D[X] \setminus D^*$. Si $\phi(f)$ es irreducible en $K[X]$ y $\operatorname{gr}(\phi(f)) = \operatorname{gr}(f)$, entonces f es irreducible en $D[X]$ (o lo que es lo mismo en $K[X]$).*

Demostración. Por la Proposición 2.19 basta ver que, si $f = gh$ con $g, h \in D[X]$, entonces $\mathrm{gr}(g) = 0$ ó $\mathrm{gr}(h) = 0$. Sean a, b y c los coeficientes principales de f, g y h, respectivamente. Entonces $a = bc \notin \mathrm{Ker}\ \phi$ y por tanto $b, c \notin \mathrm{Ker}\ \phi$, por lo que $\mathrm{gr}(\phi(g)) = \mathrm{gr}(g)$ y $\mathrm{gr}(\phi(h)) = \mathrm{gr}(h)$. Como K es un cuerpo y $\phi(f)$ es irreducible en $K[X]$, la igualdad $\phi(f) = \phi(g)\phi(h)$ implica que $\mathrm{gr}(\phi(g)) = 0$ ó $\mathrm{gr}(\phi(h)) = 0$, de donde se sigue el resultado. □

Cuando consideramos la proyección $\mathbb{Z} \to \mathbb{Z}_p$, con p un número primo positivo, el homomorfismo $\mathbb{Z}[X] \to \mathbb{Z}_p[X]$ viene dado por

$$f = \sum a_i X^i \mapsto \overline{f} = \sum \overline{a_i} X^i,$$

donde $\overline{a}$ es la clase de a en $\mathbb{Z}_p$. Aplicando el Criterio de Reducción se obtiene:

Corolario 2.25. *Sea p un entero primo y sea $f = a_0 + \cdots + a_n X^n$ un polinomio primitivo de $\mathbb{Z}[X]$. Si $p \nmid a_n$ y $\overline{f}$ es irreducible en $\mathbb{Z}_p[X]$, entonces f es irreducible en $\mathbb{Z}[X]$.*

Ejemplos 2.26. *Aplicaciones del Criterio de Reducción.*

1. Reduciendo módulo 2 el polinomio $f = 7X^3 + 218X^2 + 121X + 625$ obtenemos el polinomio $\overline{f} = X^3 + X + 1$ de $\mathbb{Z}_2[X]$, que es irreducible porque no tiene raíces. Por tanto f es irreducible en $\mathbb{Z}[X]$ (y en $\mathbb{Q}[X]$).

2. Reduciendo $f = X^4 + 5X + 1 \in \mathbb{Z}[X]$ módulo 2 obtenemos $\overline{f} = X^4 + X + 1 \in \mathbb{Z}_2[X]$. Como $\overline{f}$ no tiene raíces en $\mathbb{Z}_2$, si no fuera irreducible se factorizaría como producto de dos polinomios irreducibles de grado 2 en $\mathbb{Z}_2[X]$. Pero en $\mathbb{Z}_2[X]$ sólo hay 4 polinomios de grado 2, y de ellos sólo $X^2 + X + 1$ es irreducible (por qué?). Como $\overline{f}$ no es el cuadrado de éste, deducimos que $\overline{f}$ es irreducible en $\mathbb{Z}_2[X]$ y por tanto f es irreducible en $\mathbb{Z}[X]$.

3. Consideremos el polinomio $f = X^5 - X - 1$ de $\mathbb{Z}[X]$. Reduciendo módulo 2 obtenemos un polinomio que es divisible por $X^2 + X + 1$, por lo que no podemos aplicar el Criterio de Reducción. Reduciendo módulo 3 obtenemos $\overline{f} = X^5 + 2X + 2 \in \mathbb{Z}_3[X]$, que no tiene raíces. Si no fuera irreducible tendría un factor irreducible de grado 2; es fácil ver que los únicos irreducibles mónicos de grado 2 de $\mathbb{Z}_3[X]$ son

   $$X^2 + 1, \qquad X^2 + X - 1, \qquad X^2 - X - 1.$$

   Comprobando que ninguno de ellos divide a $\overline{f}$ deducimos que $\overline{f}$ es irreducible en $\mathbb{Z}_3[X]$, y por tanto f es irreducible en $\mathbb{Z}[X]$.

4. Dado el polinomio $f = X^4 + 4X + 1$ en $\mathbb{Z}[X]$, se tiene $\overline{f} = (X + 1)^4$ en $\mathbb{Z}_2[X]$ y $\overline{f} = (X + 2)(X^3 + X^2 + X + 2)$ en $\mathbb{Z}_3[X]$, con el factor cúbico irreducible porque no tiene raíces. Por tanto, no podemos aplicar el Criterio de Reducción. Sin embargo, la factorización en $\mathbb{Z}_3[X]$ nos va a permitir demostrar que f es irreducible en $\mathbb{Z}[X]$. En efecto, como f no tiene raíces en $\mathbb{Q}$, si no fuera irreducible en $\mathbb{Z}[X]$ se tendría $f = gh$ con $\mathrm{gr}(g) = \mathrm{gr}(h) = 2$. Esto nos daría, en $\mathbb{Z}_3$, la factorización $\overline{f} = \overline{g}\,\overline{h}$ con $\mathrm{gr}(\overline{g}) = \mathrm{gr}(\overline{h}) = 2$, incompatible con la factorización en irreducibles (única salvo asociados) que acabamos de obtener.

Veamos nuestro último criterio de irreducibilidad:

Proposición 2.27 (Criterio de Eisenstein)**.** *Sea D un DFU y sea $f = a_0 + a_1 X + \cdots + a_n X^n$ (con $a_n \neq 0$) un polinomio primitivo de $D[X]$. Si existe un irreducible $p \in D$ tal que*

$$p \mid a_i \text{ para todo } i < n, \qquad y \qquad p^2 \nmid a_0,$$

entonces f es irreducible en $D[X]$.

Demostración. Veamos que, si $f = gh$ en $D[X]$, entonces $\mathrm{gr}(g) = n$ ó $\mathrm{gr}(h) = n$. Pongamos $g = b_0 + \cdots + b_m X^m$ y $h = c_0 + \cdots + c_k X^k$, con $b_m c_k \neq 0$. Como $p^2 \nmid a_0 = b_0 c_0$, entonces $p \nmid b_0$ ó $p \nmid c_0$. Supongamos que se da la segunda opción. Como f es primitivo se tiene $p \nmid g$, y por tanto existe

$$i = \mathrm{mín}\{j : p \nmid b_j\}.$$

Entonces p no divide a $a_i = (\sum_{j=0}^{i-1} b_j c_{i-j}) + b_i c_0$, y por tanto $i = n$, de modo que $\mathrm{gr}(g) = n$. La opción $p \nmid b_0$ nos llevaría a $\mathrm{gr}(h) = n$, lo que demuestra el resultado. □

Ejemplos 2.28. *Aplicaciones del Criterio de Eisenstein.*

1. Sean a un entero y p un primo cuya multiplicidad en a es 1. Entonces $X^n - a$ es irreducible.

2. Un argumento similar al del apartado 4 de los Ejemplos 4.6.5 nos permitiría ver que el polinomio $f = X^4 - 3X^3 + 6X - 3$ es irreducible en $\mathbb{Z}[X]$. Ahora podemos asegurar lo mismo con menos trabajo aplicando el Criterio de Eisenstein con $p = 3$.

3. A menudo, el Criterio de Eisenstein se combina con un automorfismo de $\mathbb{Z}[X]$ de sustitución en $X+a$ (Ejemplos 2.4). Por ejemplo, el criterio no es aplicable a $f(X) = X^4+4X^3+10X^2+12X+7$, pero sí se puede aplicar (con $p = 2$) a $f(X-1) = X^4+4X^2+2$. Por tanto $f(X-1)$ es irreducible, y en consecuencia lo es $f(X)$.

4. Dado un entero $n \geq 3$, las raíces en $\mathbb{C}$ del polinomio $X^n - 1$ se llaman *raíces n-ésimas* de la unidad (o de 1). Considerando la interpretación geométrica de la multiplicación en $\mathbb{C}$, es fácil ver que estas raíces son exactamente los n vértices del n-ágono regular inscrito en el círculo unidad de $\mathbb{C}$ que tiene un vértice en la posición del 1. Estos números complejos son útiles en muy diversas circunstancias. El polinomio $X^n - 1$ se factoriza como

$$X^n - 1 = (X-1)\Phi_n(X), \qquad \text{donde } \Phi_n(X) = X^{n-1} + X^{n-2} + \cdots + X^2 + X + 1.$$

   El polinomio $\Phi_n(X)$ se conoce como el n-ésimo *polinomio ciclotómico*, y sus raíces son las raíces n-ésimas de 1 distintas de 1. $\Phi_n(X)$ no es en general irreducible sobre $\mathbb{Q}$ (por ejemplo, $\Phi_4(X)$ es divisible por $X + 1$), pero sí lo es cuando $n = p$ es primo. Como en el apartado anterior, esto quedará demostrado si podemos aplicar el Criterio de Eisenstein a $\Phi_p(X + 1)$. Ahora bien, $\Phi_p(X) = (X^n - 1)/(X - 1)$, y por tanto

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{p-1} X^{p-2} + \binom{p}{p-2} X^{p-3} + \cdots + \binom{p}{2} X + p.$$

   Cuando $1 \leq i < p$, el primo p no divide a $i!$ ni a $(p-i)!$, y por tanto sí divide a $\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$, por lo que podemos aplicar el Criterio de Eisenstein, como queríamos.

2.4. Polinomios en varias indeterminadas

Dados un anillo A y un entero $n \geq 2$, definimos el *anillo de polinomios en n indeterminadas con coeficientes en A*, denotado por $A[X_1, \ldots, X_n]$, mediante la fórmula recurrente

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

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*.

Por inducción a partir del Corolario 2.2, de la Proposición 2.13 y del Teorema 2.17, se obtienen fácilmente las siguientes propiedades:

Proposición 2.29. *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 sólo 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 sólo si lo es A.*
5. *$A[X_1, \ldots, X_n]$ es un DIP si y sólo 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 2.30. *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*

$$p = \sum_{i \in \mathbb{N}^n} p_i X_1^{i_1} \cdots X_n^{i_n} \tag{2.2}$$

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

Demostración. Ejercicio. □

Usando la Proposición 2.3 se demuestra fácilmente la siguiente generalización de la Propiedad Universal del Anillo de Polinomios, por inducción en el número de indeterminadas.

Proposición 2.31. *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 $\overline{f} : A[X_1, \ldots, X_n] \to B$ 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 2.32. *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 sólo si $f|A = g|A$ y $f(b_i) = g(b_i)$ para todo i. Para demostrar esto basta aplicar la Proposición 2.31 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 σ 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.

Veamos cómo pueden usarse las identificaciones del apartado 2 de los Ejemplos 2.32.

Ejemplo 2.33. *El Criterio de Eisenstein aplicado a polinomios en dos indeterminadas*
El polinomio $f = X^3Y + X^2Y^2 - X^2 + Y^3 + Y^2 \in \mathbb{Q}[X, Y]$ puede considerarse como un polinomio en $\mathbb{Q}[X][Y]$, poniendo $f = Y^3 + (X^2 + 1)Y^2 + X^3Y - X^2$, o como un polinomio en $\mathbb{Q}[Y][X]$, poniendo $f = YX^3 + (Y^2 - 1)X^2 + (Y^3 + Y^2)$. A esta última expresión le podemos aplicar el Criterio de Eisenstein con el polinomio irreducible $p = Y + 1 \in \mathbb{Q}[Y]$ para deducir que f es irreducible en $\mathbb{Q}[X, Y]$.

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

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

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 2.34. *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 2.30.□

Corolario 2.35. *Si D es un dominio y $n \geq 1$, se tiene* $\mathrm{gr}(pq) = \mathrm{gr}(p) + \mathrm{gr}(q)$ *para cualesquiera* $p, q \in D[X_1, \ldots, X_n]$.

2.5. Polinomios simétricos

Sea A un anillo arbitrario y consideremos n indeterminadas $X_1, \ldots, X_n$. En el Ejemplo 2 de 2.32 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. 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 σ 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

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

Lema 2.36. *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 sólo 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, $\delta(X_1^2 X_2^2 + X_1 X_2 + X_1^3 + X_1^3 X_2 + X_2^6) = (3,1)$, 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 δ satisface propiedades similares a gr. En efecto se verifica el siguiente lema cuya demostración dejamos como ejercicio.

Lema 2.37. *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 sólo 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 sólo si $p = 0$, $q = 0$ ó 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 2.38. *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 $\varphi : A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_n]$, dado por $\varphi(F) = F(S_1, \ldots, S_n)$ 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 2.37 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. 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 $b = (b_1, \ldots, b_n) = A^{-1}\delta(P)$.

φ 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 ψ 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 2.37 se tiene que $\delta(\varphi(p)) = \delta(S_1^{a_1} \cdots S_n^{a_n})$ y, en particular $\varphi(p) \neq 0$.

La imagen de φ es el conjunto de los polinomios simétricos. Está claro que todo elemento de la imagen de φ 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 2.37 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 φ, 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 φ. □

La demostración del Teorema 2.38 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 2.39. 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

$$\begin{aligned} &(T - X_1)(T - X_2) \cdots (T - X_n) = T^n + \textstyle\sum_{i=1}^n (-1)^i S_i T^{n-i} = \\ &T^n - S_1 T^{n-1} + S_2 T^{n-2} - \cdots + (-1)^{n-2} S_{n-2} T^2 + (-1)^{n-1} S_{n-1} T + (-1)^n S_n, \end{aligned} \tag{2.3}$$

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 2.38 permite obtener el resultado de sustituir las raíces de un polinomio en un polinomio simétrico. Veamos un ejemplo.

Ejemplo 2.40. Supongamos que queremos calcular la suma de los cubos de las raíces α_1, α_2 y α_3 del polinomio $T^3 - T + 1$. Aplicando las Fórmulas de Cardano-Vieta obtenemos

$$T^3 - T + 1 = (T - \alpha_1)(T - \alpha_2)(T - \alpha_3) = T^3 - s_1T^2 + s_2T - s_3$$

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 2.41. 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 $\{x_1, x_2, x_3\} = \left\{1, \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right\}$.

2.6. Problemas

1. Demostrar los Lemas 2.1, 2.21, 2.10, 2.30 y 2.37, los apartados 1 y 2 del Lema 2.14, las Proposiciones 2.29 y 2.31, los Corolarios 2.2 y 2.9 y la Fórmula de Cardano-Vieta (2.3).

2. Sea A un anillo y sean $a, u \in A$. Demostrar que el homomorfismo $A[X] \to A[X]$ de sustitución en $uX + a$ es un automorfismo si y sólo si u es invertible en A.

3. Justificar la *regla de Ruffini* para el cálculo del cociente y el resto en la división de $p = p_0 + p_1X + \ldots + p_nX^n$ entre $X - a$. La regla está representada por la tabla

$$\begin{array}{c|cccccc} & p_n & p_{n-1} & p_{n-2} & \cdots & p_1 & p_0 \\ a & 0 & aq_{n-1} & aq_{n-2} & \ldots & aq_1 & aq_0 \\ \hline & q_{n-1} & q_{n-2} & q_{n-3} & \cdots & q_0 & r \end{array}$$

   en la que los q_i se obtienen, de izquierda a derecha, sumando los dos elementos que están encima. Entonces $q = q_0 + q_1X + \cdots + q_{n-1}X^{n-1}$ es el cociente de la división de p entre $X - a$, y r es su resto.

4. ¿Para qué cuerpos es válida la fórmula usual ($\frac{-b \pm \sqrt{b^2-4ac}}{2a}$) para el cálculo de las raíces de un polinomio $aX^2 + bX + c$ de grado 2?

5. Sea p un entero primo. Demostrar que los polinomios $X^p - X$ y $\prod_{i=1}^{p}(X-i)$ de $\mathbb{Z}_p[X]$ son iguales y deducir una nueva demostración del Teorema de Wilson: $(p-1)! \equiv -1 \bmod p$. (Indicación: Para la primera parte, considerar las raíces de ambos polinomios.)

6. Hemos observado que la Proposición 2.8 no se verifica para polinomios sobre un anillo que no sea un dominio. Comprobar que en este caso ni siquiera se verifica la afirmación sobre la finitud del número de raíces; es decir, dar un ejemplo de un polinomio no nulo en una indeterminada con infinitas raíces.

7. Si K es un cuerpo de característica 0, ¿qué polinomios $P \in K[X]$ verifican $P' = 0$? ¿Y si la característica es un primo p?

8. Sea D un dominio y sea $P \in D[X]$ el polinomio

$$P = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$$

($n \in \mathbb{Z}^+$). Demostrar que la multiplicidad de 1 como raíz de P es al menos 3, y que es exactamente 3 si la característica de D es 0. (Advertencia: El caso de característica 2 ha de ser considerado aparte.)

9. Demostrar que si $0 \neq a \in K$, siendo K un cuerpo de característica 0, entonces $X^n - a$ no tiene raíces múltiples en ningún cuerpo que contenga a K como subcuerpo. ¿Qué se puede afirmar si K es un cuerpo de característica p, con p primo.

10. Sean K un cuerpo, $P \in K[X]$ un polinomio no constante y $K_1 = K[X]/(P)$. ¿Cuál es la dimensión de K_1 como espacio vectorial sobre K?

11. Sea K un cuerpo y sean $a_0, a_1, \ldots, a_n \in K$ distintos y $b_0, b_1, \ldots, b_n \in K$. Demostrar que

$$P(X) = \sum_{r=0}^{n} b_r \prod_{i \neq r} \frac{(X - a_i)}{a_r - a_i}$$

es el único polinomio de $K[X]$ de grado $\leq n$ que verifica $P(a_i) = b_i$ para todo i. La fórmula para P se conoce con el nombre de *fórmula de interpolación de Lagrange.*

12. ¿Es cierto que, si D es un DFU y b es un elemento de D, entonces sólo hay una cantidad finita de ideales de D que contienen a b?

13. Dar un ejemplo de un ideal primo no nulo de un DFU que no sea maximal.

14. Demostrar que toda raíz racional de un polinomio mónico con coeficientes enteros es entera.

15. Sea D un DFU y sea $f = a_o + a_1 X + \cdots + a_n X^n$ un polinomio primitivo en $D[X]$. Demostrar que, si existe un irreducible $p \in D$ tal que

$$p \mid a_i \text{ para todo } i > 0, \qquad \text{y} \qquad p^2 \nmid a_n,$$

entonces f es irreducible en $D[X]$ (es decir, el Criterio de Eisenstein se puede aplicar "al revés").

16. Descomponer en factores irreducibles el polinomio $X^4 - 4$ en cada uno de los siguientes anillos: $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{Z}_2[X]$ y $\mathbb{Z}_3[X]$.

17. Descomponer los siguientes anillos cociente como producto de anillos "conocidos":

    a) $\mathbb{R}[X]$ módulo el ideal principal generado por el polinomio $X^3 - X^2 + X - 1$.

b) $\mathbb{Q}[X]$ módulo el ideal principal generado por el polinomio $X^3 - X^2 + X - 1$.

c) $\mathbb{Q}[X]$ módulo el ideal principal generado por el polinomio $3X^2 - 6$.

18. Calcular el máximo común divisor y el mínimo común múltiplo en $\mathbb{Z}[X]$ de las siguientes parejas de polinomios:

a) $X^3 - 6X^2 + X + 4$ y $X^5 - 6X + 1$.

b) $X^2 + 1$ y $X^6 + X^3 + X + 1$.

c) $26X^2 - 104X + 104$ y $195X^2 + 65X - 910$.

19. Demostrar que los siguientes polinomios son irreducibles en los anillos que se indican:

a) $X^4 + X + 1$, $4X^3 - 3X - \frac{1}{2}$, $X^4 + 1$, $X^6 + X^3 + 1$, $X^3 + 6X + 3X + 3$, $X^5 - 5X + 15$ y $X^4 + 5X + 12$ en $\mathbb{Q}[X]$.

b) $X^2 + X + 1$ en $\mathbb{Z}_2[X]$.

c) $X^2 + Y^2 - 1$ y $X^5Y^3 - X^3 + XY^2 - Y^2 + 1$ en $\mathbb{Q}[X, Y]$.

d) $X^4 + X + a$ con a impar, en $\mathbb{Q}[X]$.

e) $X^5 + 3aX^4 - 4X + 4$ con $a \in \mathbb{Z}$, en $\mathbb{Q}[X]$.

f) $Y^3 + X^2Y^2 + X^3Y + X$, en $D[X, Y]$ donde D es un DFU arbitrario.

20. Factorizar los siguientes polinomios en los anillos que se indican:

a) $3X^4 - 3X^2 + 6$, en $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.

b) $X^3 + 3X^2 + 3X + 4$ en $\mathbb{Z}_5[X]$.

21. Decidir cuáles de los siguientes polinomios son irreducibles en los anillos que se indican:

a) $2X^2 + 2X + 2$ en $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ y $\mathbb{Z}_5[X]$.

b) $X^4 + 2$ en $\mathbb{Z}_7[X]$ y $\mathbb{Q}[X]$.

c) $X^3 - 18X^2 + 106X - 203$ en $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$.

d) $X^5 + X + 2$ en $\mathbb{R}[X]$, $\mathbb{Q}[X]$ y $\mathbb{Z}_3[X]$.

e) $X^5 + X - 2$ en $\mathbb{R}[X]$, $\mathbb{Q}[X]$ y $\mathbb{Z}_3[X]$.

f) $2X^5 - 6X^3 + 9X^2 - 15$ en $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$.

g) $X^4 + 15X^3 + 7$ en $\mathbb{Z}[X]$.

h) $X^n - p$, donde $n > 0$ y p es un entero primo con $p \equiv 1 \bmod 3$, en $\mathbb{R}[X]$, $\mathbb{Q}[X]$ y $\mathbb{Z}_3[X]$.

22. Calcular todos los polinomios mónicos irreducibles de grado ≤ 4 en $K[X]$, cuando K es cada uno de los cuerpos $\mathbb{Z}_p$ con p primo menor o igual que 11.

23. 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 es una unidad de A, entonces $A[X_1, \ldots, X_n]/(P) \simeq A[X_1, \ldots, X_{n-1}]$.

24. Sea K un cuerpo y sea $P \in K[X, Y]$. Supongamos que el coeficiente principal de P, considerado como polinomio en $K[X][Y]$, no es divisible por $X - 1$. Demostrar que, si $P(X, 1)$ es irreducible en $K[X]$, entonces $P(X, Y)$ es irreducible en $K[X, Y]$.

25. 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 $K[X]$.)

26. Construir polinomios irreducibles de $\mathbb{Q}[X]$ de grados arbitrariamente grandes.

2.7. Proyectos

1. Hacer un programa que dado un primo p y un número n calcule todos los polinomios mónicos irreducibles de grado $\leq n$ con coeficientes en el cuerpo $\mathbb{Z}_p$. Obsérvese que los polinomios mónicos irreducibles de grado 1 son los de la forma $X - a$ y si P es el conjunto de polinomios mónicos irreducibles de grado menor que k, entonces los polinomios mónicos irreducibles de grado k son los que no sean de la forma $p_1 \cdots p_t$ con $p_1, \ldots, p_k \in P$ y $\mathrm{gr}(p_1) + \ldots + \mathrm{gr}(p_t) = k$.

   Hacer otro programa que decida si un polinomio con coeficientes en $\mathbb{Z}_p$ es irreducible en $\mathbb{Z}_p[X]$ y otro que factorize un polinomio dado.

2. El *método de Kronecker* para factorizar en $\mathbb{Z}[X]$ funciona como sigue: Dado $0 \neq f \in \mathbb{Z}[X]$, podemos limitarnos a buscar divisores g de f con $\mathrm{gr}(g) \leq m$, donde m es la parte entera de $\mathrm{gr}(f)/2$. Dado un tal g, para cada $a \in \mathbb{Z}$ se tiene $g(a) \mid f(a)$ en $\mathbb{Z}$. Si fijamos enteros $a_0, \ldots, a_m$ con $f(a_i) \neq 0$, los posibles valores de cada $g(a_i)$ quedan limitados por la condición $g(a_i) \mid f(a_i)$. Combinando esto con la fórmula de interpolación de Lagrange (Problema 11) obtenemos un número finito de candidatos a divisores de f. Si alguno está en $\mathbb{Z}[X]$ y divide a f, tenemos un primer paso en la factorización y repetimos el método. En caso contrario, f es ya irreducible.

   Un ejemplo: Si $f = X^4 + X + 1$, entonces $m = 2$ y podemos considerar los enteros $a_0 = -1$, $a_1 = 0$ y $a_2 = 1$. Entonces $g(-1) \mid 1$, $g(0) \mid 1$ y $g(1) \mid 3$, por lo que hay 8 posibilidades para g. Se pide: Calcular estos 8 polinomios, comprobar que ninguno divide a f en $\mathbb{Z}[X]$, y deducir que f es irreducible.

   Esto da idea de lo ineficaz que es el método si se emplea "a mano". Sin embargo, el método es fácil de programar, y es eficaz para polinomios "de grado no muy grande y con coeficientes no muy grandes". De hecho, el método funciona si sustituimos $\mathbb{Z}$ por un DFU infinito D (para poder elegir los a_i cuando m es grande) con D^* finito (para que cada $f(a_i)$ tenga un número finito de divisores) en el que haya un método para factorizar elementos.

   Hacer un programa que factorize un polinomio con coeficientes enteros. Modificarlo para que factorize polinomios con coeficientes racionales.

3. Hacer 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.

Capítulo 3

Grupos

3.1. Definiciones y ejemplos

Definición 3.1. *Un* grupo *es una pareja $(G, \cdot)$, formada por un conjunto no vacío G junto una operación interna, es decir una aplicación*

$$\begin{array}{rcl} G \times G & \to & G \\ (g, h) & \mapsto & g \cdot h \end{array}$$

que satisface los siguientes axiomas:

- *(Asociativa) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todo $a, b, c \in G$.*
- *(Neutro) Existe un elemento $e \in G$, llamado* elemento neutro del grupo *tal que $e \cdot a = a = a \cdot e$, para todo $a \in G$.*
- *(Inverso) Para todo $a \in G$ existe otro elemento $a_1 \in G$, llamado* elemento inverso *de a, tal que $a \cdot a_1 = e = a_1 \cdot a$.*

Si además se verifica el siguiente axioma se dice que el grupo es abeliano *o* conmutativo

- *(Conmutativa) $a \cdot b = b \cdot a$, para todo $a, b \in G$.*

Lema 3.2. *Sea $(G, \cdot)$ un grupo.*

1. *(Unicidad del neutro). El neutro de G es único, de hecho, si $e, e' \in G$ satisfacen que $e' \cdot a = a = a \cdot e$ para todo $a \in G$, entonces $e = e'$.*
2. *(Unicidad del inverso). El inverso de un elemento de G es único, de hecho, si $a \cdot a_1 = e = a_2 \cdot a$, entonces $a_1 = a_2$. A partir de ahora el (único) inverso de a lo denotaremos con a^{-1}.*
3. *(Propiedad Cancelativa). Si $a \cdot x = a \cdot y$ ó $x \cdot a = y \cdot a$, con $a, x, y \in G$, entonces $x = y$.*
4. *Para todo $a, b \in G$, las ecuaciones $a \cdot X = b$ y $X \cdot a = b$, tienen una única solución en G.*
5. *$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.*

Demostración. Ejercicio. □

Habitualmente no haremos referencia a la operación del grupo y hablaremos simplemente del grupo G, donde la operación se sobreentiende. Siempre utilizaremos notación multiplicativa, de forma que para un grupo genérico el resultado de operar dos elementos a y b se denota como ab, el neutro lo

denotaremos con 1 y en inverso de a con a^{-1}. Además, si n es un entero positivo definimos a^n como el resultado de operar n veces a consigo mismo. Además ponemos $a^0 = 1$ y $a^{-n} = (a^n)^{-1} = (a^{-1})^n$. De esta forma quedan definidas potencias de elementos de G por exponentes enteros se verifica la siguiente igualdad para cualesquiera $a \in G$ y $n, m \in \mathbb{Z}$:

$$a^{n+m} = a^n a^m, (a^n)^m = a^{nm}.$$

Excepcionalmente utilizaremos notación aditiva para grupos abelianos. En tal caso el neutro lo denotaremos con 0, el inverso de a, lo llamaremos opuesto de a y lo denotamos $-a$ y escribiremos na, en lugar de a^n.

Ejemplos 3.3. 1. Si A es un anillo, entonces $(A, +)$ y $(A^*, \cdot)$ son dos grupos abelianos llamados respectivamente *grupo aditivo* y *grupo de unidades* de A. Por ejemplo, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ y $(\mathbb{Z}_n, +)$ son grupos aditivos y los grupos de unidades de los correspondientes anillos son $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ y

$$\mathbb{Z}_n^* = \{i : 1 \leq i \leq n, \mathrm{mcd}(i, n) = 1\}.$$

Obsérvese que si K es un cuerpo, entonces $K^* = K \setminus \{0\}$.

2. Sea K un anillo y n un entero positivo. Entonces el conjunto $\mathrm{GL}_n(K)$ formado por todas las matrices invertibles cuadradas de tamaño n con entradas en K es un grupo con el producto habitual de matrices. Si $n = 1$, entonces $\mathrm{GL}_1(K) = K^*$ es abeliano. Sin embargo si $n \geq 2$ y $K \neq 0$, entonces $\mathrm{GL}_n(K)$ no es abeliano pues las dos siguientes matrices no conmutan:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Este ejemplo se puede generalizar cambiando el cuerpo K por un anillo arbitrario.

3. Sea X un conjunto y S_X el conjunto de todas las biyecciones de X en si mismo. Entonces $(S_X, \circ)$ es un grupo, llamado *grupo simétrico o* de las permutaciones de X.

4. Si $(G, \star)$ y $(H, *)$ son dos grupos, entonces el producto directo $G \times H$ es un producto directo en el que la operación viene dada componente a componente:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \star g_2, h_1 * h_2).$$

Más generalmente, si $(G_i)_{i \in I}$ es una familia arbitraria de grupos, entonces el producto directo $\prod_{i \in I} G_i$ tiene una estructura de grupo en el que el producto se realiza componente a componente.

5. Para cada número natural positivo n vamos a definir un grupo C_n formado por n elementos

$$C_n = \{1, a, a^2, \ldots, a^{n-1}\},$$

donde a es un símbolo, y en el que la multiplicación viene dada por la siguiente regla:

$$a^i a^j = a^{[i+j]_n}$$

donde $[x]_n$ denota el resto de dividir x entre n. Este *grupo* se llama *cíclico* de orden n.

También definimos el *grupo cíclico infinito* como el conjunto $C_\infty = \{a^n : n \in \mathbb{Z}\}$, donde a es un símbolo y consideramos $a^n = a^m$ si y sólo si $n = m$, y en el que el producto viene dado por $a^n \cdot a^m = a^{n+m}$.

6. Para cada número natural positivo n vamos a definir un grupo formado por $2n$ elementos

$$D_n = \{1, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}$$

en el que la multiplicación viene dada por la siguiente regla:

$$(a^{i_1}b^{j_1})(a^{i_2}b^{j_2}) = a^{[i_1+(-1)^{j_1}i_2]_n}b^{[j_1+j_2]_2}$$

con notación como en el ejemplo anterior. Este grupo se llama *grupo diédrico* de orden $2n$.

El *grupo diédrico infinito* D_∞ está formado por elementos de la forma a^nb^m, con $n \in \mathbb{Z}$ y $m = 0, 1$ con el producto $(a^{i_1}b^{j_1})(a^{i_2}b^{j_2}) = a^{i_1+(-1)^{j_1}i_2}b^{[j_1+j_2]_2}$.

3.2. Subgrupos

Definición 3.4. *Sea G un grupo. Un subconjunto S de G se dice que es un* subgrupo *si la operación que define la estructura de grupo en G induce también una estructura de grupo en S.*

El siguiente lema muestra cuáles son las propiedades que hay que comprobar para demostrar que un subconjunto de un grupo es un subgrupo.

Lema 3.5. *Sea G un grupo y S un subconjunto de G. Las siguientes condiciones son equivalentes:*

1. *S es un subgrupo de G.*
2. *$1 \in S$ y para todo $a, b \in S$, se verifican $ab, a^{-1} \in S$.*
3. *$S \neq \emptyset$ y para todo $a, b \in S$, se verifican $ab, a^{-1} \in S$.*
4. *$1 \in S$ y para todo $a, b \in S$, se verifican $ab^{-1} \in S$.*
5. *$S \neq \emptyset$ y para todo $a, b \in S$, se verifican $ab^{-1} \in S$.*

Demostración. Ejercicio. □

Ejemplos 3.6.

1. Si G es un grupo, entonces $\{1\}$ y G son subgrupos de G. El primero se llama *subgrupo trivial*, denotado 1 y el segundo *subgrupo impropio* de G. Los subgrupos de G diferentes de G se dice que son *subgrupos propios*.

2. Si $(A, +)$ es el grupo aditivo de un anillo, entonces todo subanillo y todo ideal de A son subgrupos de este grupo.

   Si S es un subgrupo de $(\mathbb{Z}, +)$, entonces $nx \in S$, para todo $n \in \mathbb{Z}$ y todo $x \in I$. Eso implica que S es un ideal de $\mathbb{Z}$ y por tanto los subgrupos de $(\mathbb{Z}, +)$ son los de la forma $n\mathbb{Z}$ para n un entero no negativo.

3. Sea $\mathrm{GL}_n(K)$ el grupo de las matrices invertibles de tamaño n con entradas en el cuerpo K. Entonces el $\mathrm{SL}_n(K)$ conjunto formado por las matrices de determinante 1 es un subgrupo de $\mathrm{GL}_n(K)$.

4. Supongamos que A es un anillo y sea S_A el grupo de las permutaciones de A. Entonces el conjunto $\mathrm{Aut}(A)$ formado por los automorfismos de A es un subgrupo de S_A.

   Ejemplos similares se pueden obtener con casi todas las estructuras matemáticas. Por ejemplo, si G es un grupo, entonces decimos que $f : G \to G$ es un automorfismo si f es biyectivo y $f(gh) =$

$f(g)f(h)$ para todo $g, h \in G$. Entonces el conjunto $\mathrm{Aut}(G)$ formado por todos los automorfismos de G es un subgrupo del grupo simétrico S_G de G.

Si X es un espacio topológico entonces el conjunto de todos los homeomorfismos de X (es decir las aplicaciones biyectivas continuas con inversa continua) de X en si mismo es un subgrupo de S_X.

Si X es un espacio métrico con distancia d, entonces el conjunto de las isometrías (es decir, las aplicaciones biyectivas de X en si mismo tales que $d(f(x), f(y)) = d(x, y)$) es un subgrupo de S_X.

5. Si G es un grupo y $g \in G$, entonces

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

es un subgrupo de G, llamado *grupo cíclico* generado por g.

Un *grupo* G se dice que es *cíclico* si tiene un elemento g tal que $G = \langle g \rangle$. En tal caso se dice que g es un generador de G.

Por ejemplo, $(\mathbb{Z}, +)$ es cíclico generado por 1 y $(\mathbb{Z}_n, +)$ es otro grupo cíclico generado por la clase de 1. Otros ejemplos de grupos cíclicos son los grupos C_n y C_∞ del Ejemplo 5 de 3.3.

6. Si X es un subconjunto arbitrario de G, entonces el conjunto formado por todos los elementos de G de la forma $x_1^{n_1} x_2^{n_2} \dots x_m^{n_m}$, con $x_1, \dots x_m \in X$ y $n_1, \dots, n_m \in \mathbb{Z}$, es un subgrupo de G, que resulta ser el menor subgrupo de G que contiene a X y por tanto se llama *subgrupo generado* por X y se denota $\langle X \rangle$.

El subgrupo generado por X se puede construir de otra forma. Es un sencillo ejercicio comprobar que la intersección de subgrupos de G, es un subgrupo. Por tanto la intersección de todos los subgrupos de G que contienen a X es un subgrupo de G y es el menor subgrupo de G que contiene a X, con lo que es el subgrupo generado por X.

7. Si $(G_i)_{i \in I}$ es una familia arbitraria de grupos, entonces el subconjunto $\oplus_{i \in I} G_i$ formado por los elementos $(g_i) \in \prod_{i \in I} G_i$ tales que $g_i = 1$ para todo i, es un subgrupo de $\prod_{i \in I} G_i$.

8. Si G es un grupo arbitrario, entonces

$$Z(G) = \{g \in G : gx = xg, \text{ para todo } x \in G\}$$

es un subgrupo abeliano de G, llamado *centro*.

Más generalmente, si $x \in G$, entonces

$$\mathrm{Cen}_G(x) = \{g \in G : gx = xg\}$$

es un subgrupo de G, llamado *centralizador* de x en G. Obsérvese que $Z(G)$ es la intersección de todos los centralizadores de los elementos de G en G.

Sea G un grupo y H un subgrupo de G. Se define la siguiente relación binaria en G:

$$a \equiv_i b \bmod H \quad \Leftrightarrow \quad a^{-1}b \in H. \qquad\qquad (a, b \in G).$$

Se puede comprobar fácilmente que esta relación es de equivalencia y por tanto define una partición de G en clases de equivalencia. Las clase de equivalencia que contiene a a es

$$aH = \{ah : h \in H\}$$

y se llama *clase lateral de a módulo H por la izquierda*.

Análogamente se puede definir otra relación de equivalencia:

$$a \equiv_d b \bmod H \quad \Leftrightarrow \quad ab^{-1} \in H. \qquad\qquad (a, b \in G)$$

para la que las clase de equivalencia que contiene a a es

$$Ha = \{ah : h \in H\}$$

y se llama *clase lateral de a módulo H por la derecha*.

El conjunto de las clases laterales por la izquierda de G módulo H se denota por G/H y el de clases laterales por la derecha $H\backslash G$.

Como consecuencia del Lema 3.2 las aplicaciones

$$\begin{array}{ccc} H & \to & aH \\ h & \mapsto & ah \end{array} \qquad \begin{array}{ccc} H & \to & Ha \\ h & \mapsto & ha \end{array}$$

son biyectivas, con lo que todas las clases laterales tienen el mismo cardinal. Además la aplicación

$$\begin{array}{ccc} G/H & \to & H\backslash G \\ aH & \mapsto & Ha^{-1} \end{array}$$

es otra biyección.

Denotamos con $|X|$ el cardinal de un conjunto cualquiera. En el caso en que G sea un grupo el cardinal de G se suele llamar *orden* de G. Acabamos de ver que para cada subgrupo H de G se verifica:

$$|aH| = |Ha| = |H| \quad \text{y} \quad |G/H| = |H\backslash G|$$

El cardinal de G/H (y $H\backslash G$) se llama *índice* de H en G y se denota $[G : H]$. Una consecuencia inmediata de estas fórmulas es el siguiente Teorema.

Teorema 3.7 (Teorema de Lagrange)**.** *Si G es un grupo finito y H es un subgrupo de G entonces $|G| = |H|[G : H]$.*

3.3. Subgrupos normales y grupos cociente

Dados subconjuntos A y B de un grupo G, pondremos $AB = \{ab : a \in A, b \in B\}$. Si $X = \{x\}$ pondremos xA en lugar de XA y Ax en lugar de AX, lo que es consistente con la notación usada para las clases laterales. Por otra parte, la asociatividad de G implica que $(AB)C = A(BC)$ para subconjuntos A, B y C arbitrarios, lo que nos permite escribir ABC sin ambigüedad; obviamente $ABC = \{abc : a \in A, b \in B, c \in C\}$.

Proposición 3.8. *Las condiciones siguientes son equivalentes para un subgrupo N de un grupo G:*

1. *$N\backslash G = G/N$.*
2. *Para cada $x \in G$ se tiene $Nx = xN$ (o equivalentemente $x^{-1}Nx = N$).*
3. *Para cada $x \in G$ se tiene $Nx \subseteq xN$ (o equivalentemente $x^{-1}Nx \subseteq N$).*
4. *Para cada $x \in G$ se tiene $xN \subseteq Nx$ (o equivalentemente $xNx^{-1} \subseteq N$).*
5. *Para cualesquiera $a, b \in G$ se tiene $aNbN = abN$.*
6. *Para cualesquiera $a, b \in G$ se tiene $NaNb = Nab$.*

Demostración. Ejercicio □

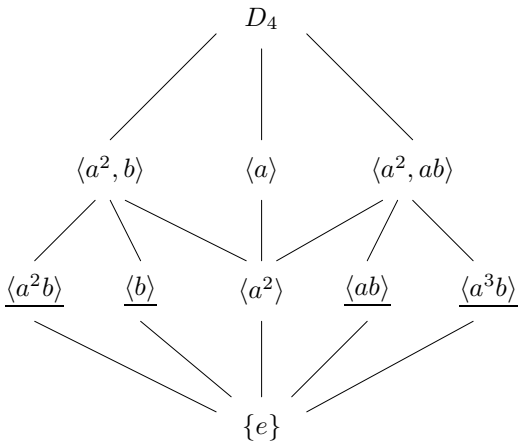
Supongamos que se cumplen las condiciones de la Proposición 3.8. Entonces el producto de dos elementos de G/N (o de $N\backslash G$) es un elemento de G/N, y es elemental comprobar que esta operación dota a G/N de una estructura de grupo. Obsérvese que, para realizar un producto $aN \cdot bN$ en G/N, no necesitamos describir el conjunto resultante, pues éste queda determinado por cualquier representante suyo, por ejemplo ab. El elemento neutro de G/N es la clase $N = 1N$, y el inverso de aN es $a^{-1}N$.

Definición 3.9. *Un subgrupo N de un grupo G es un* subgrupo normal *de G (también se dice que N es* normal en G*) si verifica las condiciones equivalentes de la Proposición 3.8. En ocasiones escribiremos $N \trianglelefteq G$ (respectivamente $N \triangleleft G$) para indicar que N es un subgrupo normal (respectivamente normal y propio) de G.*

Si N es normal en G, el grupo G/N recién descrito se llama grupo cociente *de G módulo N.*

Ejemplos 3.10. *Subgrupos normales.*

1. Es claro que, en un grupo abeliano, todo subgrupo es normal.
2. Si I es un ideal de un anillo A, entonces el grupo cociente A/I es el grupo aditivo del anillo cociente.
3. Si G es un grupo y H es un subgrupo contenido en el centro $Z(G)$, entonces H es normal en G. En particular, el centro es un subgrupo normal.
4. Si H es un subgrupo de G de índice 2, entonces H es normal en G. En efecto, como las clases por la derecha módulo H constituyen una partición de G, sólo hay dos, y una de ellas es H, la otra ha de ser el complementario $\{g \in G : g \notin H\}$. El mismo argumento vale para las clases por la izquierda y en consecuencia $G/N = N\backslash G$.
5. Sea $G = \mathrm{GL}_n(\mathbb{R})$ el grupo lineal general sobre $\mathbb{R}$. Usando el hecho de que, si $a, b \in G$, entonces
$$\det(ba) = \det(b)\det(a) = \det(a)\det(b) = \det(ab),$$
es fácil ver que $\mathrm{SL}_n(\mathbb{R})$ es un subgrupo normal de G.
6. El siguiente es el diagrama de todos los subgrupos de D_4 ordenados por inclusión: una línea entre dos subgrupos significa que el de arriba contiene al de abajo. Los subgrupos de la segunda fila tienen orden 4, y los de la tercera fila tienen orden 2. En el diagrama están subrayados los subgrupos que *no* son normales en D_4:



Los que aparecen son subgrupos y las relaciones de inclusión son claras, pero el lector deberá comprobar esos subgrupos son distintos entre sí y que no hay más, así como la normalidad de los subgrupos no subrayados. Otro ejercicio interesante consiste en demostrar que los subgrupos $\langle a^2, b\rangle$ y $\langle a^2, ab\rangle$ no son cíclicos.

Obsérvese que cualquier subgrupo del diagrama es normal en cualquiera de los subgrupos que lo contengan y estén en el nivel inmediatamente superior. Por ejemplo, $\langle b\rangle \trianglelefteq \langle a^2, b\rangle$ y $\langle a^2, b\rangle \trianglelefteq D_4$; como $\langle b\rangle$ no es normal en D_4, este ejemplo muestra que la relación "ser normal en" no es transitiva.

Acabamos la sección con una versión para grupos del Teorema de la Correspondencia (1.15).

Teorema 3.11 (Teorema de la Correspondencia)**.** *Sea N un subgrupo normal de un grupo G. La asignación $H \mapsto H/N$ establece una biyección entre el conjunto $\mathcal{A}$ de los subgrupos de G que contienen a N y el conjunto $\mathcal{B}$ de los subgrupos de G/N.*

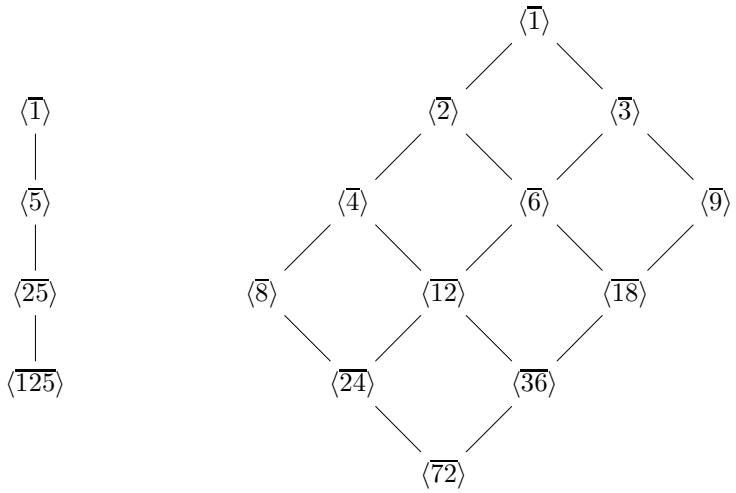
Además, esta biyección conserva las inclusiones, las intersecciones y la normalidad. Es decir, dados $H, K \in \mathcal{A}$, se tiene:

1. *$H \subseteq K$ si y sólo si $(H/N) \subseteq (K/N)$.*
2. *$(H \cap K)/N = (H/N) \cap (K/N)$.*
3. *$H \trianglelefteq G$ si y sólo si $(H/N) \trianglelefteq (G/N)$.*

Demostración. Adaptar la demostración del Teorema 1.15. □

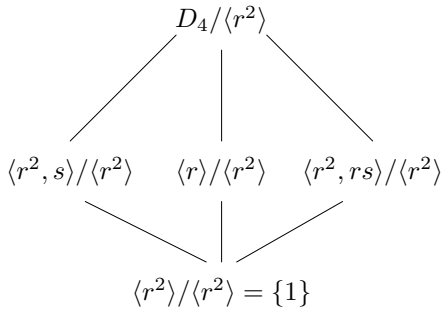
Ejemplos 3.12. *Aplicaciones del Teorema de la Correspondencia.*

1. Dado un entero positivo n, vamos a describir los subgrupos del grupo cociente $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$. Escribiremos $\overline{a} = a + \langle n\rangle$. Sabemos que los subgrupos de $\mathbb{Z}$ son precisamente los de la forma $\langle d\rangle$ con $d \geq 0$, y que $\langle d\rangle \subseteq \langle d'\rangle$ si y sólo si $d' \mid d$. Por tanto, los subgrupos de $\mathbb{Z}_n$ son precisamente los de la forma $\frac{\langle d\rangle}{\langle n\rangle} = \langle \overline{d}\rangle$, donde d es un divisor positivo de n, y además $\langle \overline{d}\rangle \subseteq \langle \overline{d'}\rangle$ si y sólo si $d' \mid d$. Así, el diagrama de los subgrupos de $\mathbb{Z}_n$ puede construirse de modo elemental a partir de los divisores de n como muestran los siguientes diagramas (en el de la izquierda se ha tomado $n = 125$, y en el de la derecha $n = 72$):



En general, si r es el número de divisores primos distintos de n, se necesita un diagrama en r dimensiones; por ejemplo, para $n = 180$ necesitaríamos un diagrama tridimensional.

2. Aplicando el Teorema de la Correspondencia al diagrama de los subgrupos de D_4 (Ejemplo 6 de 3.10), obtenemos el siguiente diagrama de los subgrupos de $D_4/\langle r^2\rangle$.



3.4. Homomorfismos y Teoremas de Isomorfía

Definición 3.13. *Un* homomorfismo *del grupo $(G,\cdot)$ en el grupo $(H,*)$ es una aplicación $f: G \to H$ que conserva la operación; es decir, que verifica*

$$f(a\cdot b) = f(a) * f(b)$$

para cualesquiera $a, b \in G$. Si $G = H$ decimos que f es un endomorfismo *de G.*

Si $f: G \to H$ es un homomorfismo biyectivo, diremos que es un isomorfismo *y que los grupos G y H son* isomorfos*. Un isomorfismo de G en G se dirá un* automorfismo *de G.*

Dado un homomorfismo de grupos $f: G \to H$, se definen su imagen *y su* núcleo *como*

$$\text{Im } f = f(G) = \{f(x) : x \in G\} \quad y \quad \text{Ker } f = f^{-1}(1_H) = \{x \in G : f(x) = 1_H\}.$$

Lema 3.14. *Si $f: G \to H$ es un homomorfismo de grupos entonces se verifican las siguientes propiedades para $a, a_1, \ldots, a_n \in G$:*

1. *(f* conserva el neutro*) $f(1_G) = 1_H$.*
2. *(f* conserva inversos*) $f(a^{-1}) = f(a)^{-1}$.*
3. *(f* conserva productos finitos*) $f(a_1 \cdots a_n) = f(a_1)\cdots f(a_n)$.*
4. *(f* conserva potencias*) Si $n \in \mathbb{Z}$ entonces $f(a^n) = f(a)^n$.*
5. *Si f es un isomorfismo entonces la aplicación inversa $f^{-1}: H \to G$ también lo es.*
6. *Si $g: H \to K$ es otro homomorfismo de grupos entonces $g \circ f: G \to K$ es un homomorfismo de grupos.*
7. *Si H_1 es un subgrupo de H entonces $f^{-1}(H_1) = \{x \in G : f(x) \in H_1\}$ es un subgrupo de G.*

   Si además H_1 es normal en H entonces $f^{-1}(H_1)$ es normal en G; en particular, Ker f *es un subgrupo normal de G.*
8. *f es inyectivo si y sólo si* Ker $f = \{1\}$.
9. *Si G_1 es un subgrupo de G entonces $f(G_1)$ es un subgrupo de H; en particular,* Im f *es un subgrupo de H.*

   Si además G_1 es normal en G y f es suprayectiva entonces $f(G_1)$ es normal en H.

Demostración. Ejercicio. □

Ejemplos 3.15. *Homomorfismos de grupos.*

1. Si H es un subgrupo de G, la inclusión de H en G es un homomorfismo inyectivo.
2. Si N es un subgrupo normal de G, la aplicación $\pi : G \to G/N$ dada por $\pi(x) = xN$ es un homomorfismo suprayectivo que recibe el nombre de *proyección canónica* de G sobre G/N. Su núcleo es $\operatorname{Ker} \pi = N$.
3. Dados dos grupos G y H, la aplicación $f : G \to H$ dada por $f(a) = 1_H$ para cada $a \in G$ es un homomorfismo llamado *homomorfismo trivial* de G en H. Su núcleo es todo G.
4. La aplicación $f : \mathbb{Z} \to \mathbb{Z}$ dada por $f(n) = 2n$ es un homomorfismo inyectivo y no suprayectivo.
5. Si G es cualquier grupo y $x \in G$ es cualquier elemento, la aplicación $\mathbb{Z} \to G$ dada por $n \mapsto x^n$ es un homomorfismo de grupos; como en $\mathbb{Z}$ usamos notación aditiva y en G multiplicativa, la afirmación anterior es equivalente al hecho, que ya conocemos, de que $x^{n+m} = x^n x^m$.
6. Otro ejemplo en el que se mezclan las notaciones aditiva y multiplicativa es el siguiente: Fijado un número real positivo α, la aplicación $\mathbb{R} \to \mathbb{R}^+$ dada por $r \mapsto \alpha^r$ es un isomorfismo de grupos cuya inversa es la aplicación $\mathbb{R}^+ \to \mathbb{R}$ dada por $s \mapsto \log_\alpha s$.

Claramente, si $f : G \to H$ es un homomorfismo inyectivo de grupos entonces $f : G \to \operatorname{Im} f$ es un isomorfismo de grupos que nos permite ver a G como un subgrupo de H.

Los Teoremas de Isomorfía que vimos para anillos tienen una versión para grupos. Las demostraciones son análogas.

Teorema 3.16. *(Teoremas de Isomorfía para grupos)*

1. *Si $f : G \to H$ es un homomorfismo de grupos entonces existe un único isomorfismo de grupos $\bar{f} : G/\operatorname{Ker} f \to \operatorname{Im} f$ que hace conmutativo el diagrama*

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & H \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ G/\operatorname{Ker} f & \overset{\bar{f}}{\dashrightarrow} & \operatorname{Im} f \end{array}$$

   es decir, $i \circ \bar{f} \circ p = f$, donde i es la inclusión y p es la proyección canónica. En particular

$$\frac{G}{\operatorname{Ker} f} \simeq \operatorname{Im} f.$$

2. *Sean N y H subgrupos normales de un grupo G con $N \subseteq H$. Entonces H/N es un subgrupo normal de G/N y se tiene*

$$\frac{G/N}{H/N} \simeq G/H.$$

3. *Sean G un grupo, H un subgrupo de G y N un subgrupo normal de G. Entonces $N \cap H$ es un subgrupo normal de H y se tiene*

$$\frac{H}{N \cap H} \simeq \frac{NH}{N}.$$

Usando el Teorema de la Correspondencia se obtiene el siguiente corolario.

Corolario 3.17. *Si $f : G \to H$ es un homomorfismo de grupos entonces $K \mapsto f(K)$ define una biyección entre el conjunto de los subgrupos de G que contienen a* Ker f *y el de los subgrupos de H contenidos en* Im f.

Ejemplos 3.18. *Aplicaciones de los Teoremas de Isomorfía.*

1. Consideremos los grupos multiplicativos $\mathbb{C}^*$ y $\mathbb{R}^*$, y la aplicación norma $\delta : \mathbb{C}^* \to \mathbb{R}^*$ dada por $\delta(a+bi) = a^2 + b^2$. Entonces δ es un homomorfismo que tiene por núcleo a la circunferencia de radio 1 en $\mathbb{C}$, y por imagen a $\mathbb{R}^+$. Por tanto, el grupo cociente de $\mathbb{C}^*$ por la circunferencia de radio 1 es isomorfo a $\mathbb{R}^+$.

2. La aplicación det : $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ que lleva una matriz a su determinante es un homomorfismo suprayectivo de grupos con núcleo $\mathrm{SL}_n(\mathbb{R})$. Esto nos dice que el cociente de $\mathrm{GL}_n(\mathbb{R})$ por $\mathrm{SL}_n(\mathbb{R})$ es isomorfo a $\mathbb{R}^*$

3. Sea n un entero positivo. Hemos visto (Ejemplos 3.12) que todo subgrupo de $\mathbb{Z}_n = \mathbb{Z}/\langle n\rangle$ es de la forma $\langle \overline{d}\rangle = \langle d\rangle/\langle n\rangle$, para cierto divisor positivo d de n. El Segundo Teorema de Isomorfía nos permite identificar el cociente $\mathbb{Z}_n/\langle \overline{d}\rangle$, pues
$$\frac{\mathbb{Z}_n}{\langle \overline{d}\rangle} = \frac{\mathbb{Z}/\langle n\rangle}{\langle d\rangle/\langle n\rangle} \simeq \frac{\mathbb{Z}}{\langle d\rangle} = \mathbb{Z}_d.$$

3.5. El orden de un elemento de un grupo

Definición 3.19. *Sea G un grupo y $a \in G$. Por definición el orden de a es el orden del subgrupo $\langle a\rangle$ generado por a, y se denota $o(a)$.*

Si consideremos el homomorfismo $f : \mathbb{Z} \to G$ dado por $f(n) = a^n$, entonces la imagen de f es $\langle a\rangle$ y el núcleo de f es un subgrupo de $\mathbb{Z}$. Por tanto Ker $f = n\mathbb{Z}$ para algún entero no negativo n. Si $n = 0$, entonces f es inyectivo y $(\mathbb{Z}, +) \simeq \langle a\rangle$. En caso contrario $\mathbb{Z}_n \simeq \langle a\rangle$, con lo que $n = o(a)$. Luego
$$a^n = 1 \quad \Leftrightarrow \quad o(a)|n. \tag{3.1}$$

Más aún $a^k = a^l$ si y sólo si $k \equiv l \bmod n$ y por tanto $o(a)$ es el menor entero no negativo n tal que $a^n = 1$.

Por el Teorema de Lagrange, si G es finito, entonces $o(a)$ divide a $|G|$. Además, si a tiene orden finito entonces la siguiente fórmula relaciona el orden de un elemento con el de sus potencias:
$$o(a^n) = \frac{o(a)}{\mathrm{mcd}(o(a), n)} \tag{3.2}$$

Demostración. Obsérvese que $m = o(a)$ y $d = \mathrm{mcd}(m, n)$, entonces $\mathrm{mcd}(\frac{m}{d}, \frac{n}{d}) = 1$. Aplicando (3.1) tenemos que $(a^n)^k = 1$ si y sólo si $a^{nk} = 1$ si y sólo si $m|nk$, si y sólo si $\frac{m}{d}$ divide a $\frac{nk}{d} = \frac{n}{d}k$ si y sólo si $\frac{m}{d}$ divide a k. Lo que muestra que $o(a^n) = \frac{m}{d}$. □

Recordando como son los subgrupos de $\mathbb{Z}$ y de $\mathbb{Z}_n$ tenemos que

Proposición 3.20. *Sea G un grupo cíclico generado por a.*

1. *Si G tiene orden infinito entonces $G \simeq (\mathbb{Z}, +)$ y los subgrupos de G son los de la forma $\langle a^n\rangle$ con $n \in \mathbb{N}$. Además, si $n, m \in \mathbb{N}$, entonces $\langle a^n\rangle \subseteq \langle a^m\rangle$ si y sólo si $m|n$.*

   G tiene un subgrupo para cada número entero no negativo n: $\langle a^n\rangle$.

2. *Si G tiene orden n, entonces $G \simeq (\mathbb{Z}_n, +)$ y G tiene exactamente un subgrupo de orden d para cada divisor de n, a saber $\langle a^{n/d} \rangle$.*

En particular todo subgrupo y todo cociente de G son cíclicos.

Teorema 3.21 (Teorema Chino de los Restos para grupos)**.** *Si G y H son dos subgrupos cíclicos de ordenes n y m, entonces $G \times H$ es cíclico si y sólo si* $\mathrm{mcd}(n, m) = 1$.

Más generalmente, si g y h son dos elementos de un grupo G de órdenes coprimos n y m y $gh = hg$, entonces $\langle g, h \rangle$ es cíclico de orden nm.

Demostración. Por la Proposición 3.20, $G \simeq (\mathbb{Z}_n, +)$ y $H \simeq (\mathbb{Z}_m, +)$. Si $\mathrm{mcd}(n, m) = 1$, entonces, por el Teorema Chino de los Restos, $\mathbb{Z}_n \times \mathbb{Z}_m$ y $\mathbb{Z}/nm\mathbb{Z}$ son isomorfos como anillos y por tanto también lo son sus grupos aditivos. Por tanto $G \times H \simeq (\mathbb{Z}_n, +) \times (\mathbb{Z}_m, +) \simeq (\mathbb{Z}/nm\mathbb{Z}, +)$. Sin embargo, si n y m no son coprimos y $d = \mathrm{mcd}(n, m)$, entonces G tiene un subgrupo G_1 de orden d y H tiene otro subgrupo H_1 de orden d. Entonces $G_1 \times 1$ y $1 \times H_1$ son dos subgrupos distintos de $G \times H$ del mismo orden, en contra de la Proposición 3.20.

Supongamos ahora que $g, h \in G$ tienen órdenes coprimos n y m. Entonces la aplicación $f : \mathbb{Z}_n \times \mathbb{Z}_m \to G$ dada por $f(i, j) = g^i h^j$ es un homomorfismo de grupos cuya imagen es $\langle g, h \rangle$. (Observa la importancia de la hipótesis $gh = hg$ aquí.) Por el Teorema de Lagrange, el orden de $\langle g \rangle \cap \langle h \rangle$ divide a n y m. Como n y m son coprimos, este orden es 1. Si $f(i, j) = 1$, entonces $a^{-i} = b^j \in \langle g \rangle \cap \langle h \rangle = 1$. Por tanto $n|i$ y $m|j$, lo que muestra que f es inyectiva. Por tanto f es un isomorfismo, lo que prueba que $\langle g, h \rangle \simeq \mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}/nm\mathbb{Z}$. □

El siguiente teorema que veremos sin demostración describe todos los grupos abelianos finitos salvo isomorfismo.

Teorema 3.22 (Estructura de los grupos abelianos finitos)**.** *Si G es un grupo abeliano finito, entonces existen enteros positivos $d_1|d_2|\ldots|d_n$ tales que*

$$G \simeq C_{d_1} \times C_{d_2} \times \cdots \times C_{d_n}.$$

Además, si $d_1|d_2|\ldots|d_n$ y $e_1|e_2|\ldots|e_m$ son enteros positivos tales que

$$C_{d_1} \times C_{d_2} \times \cdots \times C_{d_n} \simeq C_{e_1} \times C_{e_2} \times \cdots \times C_{e_m}$$

entonces $n = m$ y $d_i = e_i$ para todo i.

3.6. Conjugación y acciones de grupos en conjuntos

Sea G un grupo. Si $a, g \in G$, entonces se define el *conjugado* de g por a como $g^a = a^{-1}ga$. Si X es un subconjunto de G, entonces el conjugado de X por a es $X^a = \{x^a : x \in X\}$. Se dice que dos elementos o subconjuntos x y y de G son *conjugados* en G si $x^a = y$ para algún $a \in G$.

La aplicación $\iota_a : G \to G$ dada por $\iota_a(x) = x^a$ es un automorfismo de G, llamado *automorfismo interno* definido por a, con inverso $\iota_{a^{-1}}$. Eso implica que dos elementos o subconjuntos conjugados de un grupos tienen propiedades similares. Por ejemplo todos dos elementos conjugados de G tiene el mismo orden y el conjugado de un subgrupo de G es otro subgrupo de G del mismo orden.

Es fácil ver que

$$g^{ab} = (g^a)^b \quad \text{para todo } g, a, b \in G,$$

y utilizando esto se demuestra de forma fácil que la relación ser conjugados (tanto de elementos, como de subconjuntos de G) es una relación de equivalencia. Las clases de equivalencia de esta relación de

equivalencia en G se llaman *clases de conjugación* de G. La clase de conjugación de G que contiene a a se denota por a^G. Es decir

$$a^G = \{a^g : g \in G\}.$$

Sean G un grupo y X un conjunto. Una *acción* de G en X es una aplicación

$$\begin{array}{rcl} \cdot : G \times X & \to & X \\ (g, x) & \mapsto & g \cdot x \end{array}$$

que satisface las siguientes propiedades:

1. $(gh) \cdot x = g \cdot (h \cdot x)$, para todo $x \in X$ y todo $g, h \in G$.
2. $1 \cdot x = x$, para todo $x \in X$.

Análogamente se define una acción por la derecha.

Vamos a ver una definición alternativa. Sea $\cdot : G \times X \to X$ una acción por la derecha del grupo G en el conjunto X. Entonces la aplicación $f : G \to S_X$ dada por $f(g)(x) = g \cdot x$ es un homomorfismo de grupos. Recíprocamente, si $f : G \to S_X$ es un homomorfismo de grupos, entonces la aplicación $\cdot : G \times X \to X$, dada por $g \cdot x = f(g)(x)$ es una acción por la derecha de G en X. Por tanto, es lo mismo hablar de una acción de un grupo G en un conjunto X que de un homomorfismo de grupos $G \to S_X$. Análogamente podemos identificar las acciones por la izquierda de G en X con los antihomomorfismos de grupos $f : G \to S_X$, es decir las aplicaciones $f : G \to S_X$ que satisfacen $f(gh) = f(h)f(g)$, para todo $g, h \in G$.

Sea $\cdot : G \times X \to X$ una acción por la izquierda de un grupo G en un conjunto X. Si $x \in X$ entonces $G \cdot x = \{g \cdot x : g \in G\}$ se llama *órbita* de x y $\text{Estab}_G(x) = \{g \in G : g \cdot x = x\}$ se llama *estabilizador* de x en G. Obsérvese que las órbitas forman una partición de G.

Veamos algunos ejemplos de acciones de grupos en conjuntos.

Ejemplos 3.23. Sea G un grupo arbitrario.

1. Consideremos la acción por la derecha de G en si mismo dada por $g \cdot x = gx$. Esta acción se llama *acción por la derecha de* G en si mismo por *translación*. Análogamente se define una acción por la izquierda por traslación. Obsérvese que $\text{Estab}_G(x) = 1$ y $G \cdot x = G$, para todo $x \in G$.

   Más generalmente, si H es un subgrupo de G, entonces G actúa por la derecha en G/H mediante la regla: $g \cdot xH = (gx)H$. Análogamente se define una acción por la izquierda de G en $H\backslash G$. En ambos casos todos los elementos están en la misma órbita y $\text{Estab}_G(xH) = \{g \in G : xgx^{-1} \in H\} = x^{-1}Hx = H^x$.

2. La *acción por conjugación* de G en si mismo viene dada por $g \cdot a = g^a = a^{-1}ga$. La órbita $G \cdot x$ es x^G, la clase de conjugación de x en G y el estabilizador es $\text{Estab}_G(x) = \text{Cen}_G(x)$, el centralizador de x en G.

3. G actúa por la derecha en el conjunto S de sus subgrupos mediante la regla $H \cdot g = H^g$. El estabilizador de H es $\text{Estab}_G(H) = \{g \in H : H^g = H\} = N_G(H)$, el *normalizador* de H en G, es decir, el mayor subgrupo de G que contiene a H como subgrupo normal.

4. Para cada entero positivo n, consideramos S_n actuando por la derecha en en $\{1, 2, \ldots, n\}$ mediante: $\sigma \cdot x = \sigma(x)$. Claramente, todo elemento está en la misma órbita y $\text{Estab}_{S_n}(i) = \{\sigma \in S_n : \sigma(i) = i\} \simeq S_{n-1}$.

5. El grupo simétrico S_n también actúa por la derecha en $A[X_1, \ldots, X_n]$ por la regla $\sigma \cdot p = \overline{\sigma}(p)$ definida en la Sección 2.5. Recuérdese que la órbita de p por esta acción es precisamente lo que habíamos llamado órbita del polinomio p.

Proposición 3.24. *Sea G un grupo actuando en un conjunto X y sean $x \in X$ y $g \in G$. Entonces*

1. $\mathrm{Estab}_G(x)$ *es un subgrupo de* G.
2. $[G : \mathrm{Estab}_G(x)] = |G \cdot x|$. *En particular, si G es finito, entonces el número de elementos de cada órbita es un divisor del orden de G.*
3. $\mathrm{Estab}_G(g \cdot x) = \mathrm{Estab}_G(x)^{g^{-1}}$. *En particular* $\mathrm{Cen}_G(a^g) = \mathrm{Cen}_G(a)^{g^{-1}}$.

Demostración. 1 y 3 se hacen con un simple cálculo.
2. Sea $H = \mathrm{Estab}_G(x)$, entonces la aplicación $gH \mapsto g \cdot x$ induce una biyección entre G/H y $G \cdot x$. □

La primera parte del corolario es un caso particular de la Proposición 3.24 y la segunda es una consecuencia obvia de la primera.

Corolario 3.25. *Sea G un grupo y $a \in G$.*

1. $|a^G| = [G : \mathrm{Cen}_G(a)]$. *En particular, a^G tiene un único elemento si y sólo si a es un elemento del centro $Z(G)$ de G.*
2. *(*Ecuación de Clases*). Si G es finito y X es un subconjunto de G que contiene exactamente un elemento de cada clase de conjugación con al menos dos elementos, entonces*

$$|G| = |Z(G)| + \sum_{x \in X} [G : \mathrm{Cen}_G(x)].$$

Si p es un primo, entonces un *p-grupo finito* es un grupo finito de orden una potencia de p.

Proposición 3.26. *Si G es un p-grupo no trivial para p un primo entonces $Z(G) \neq 1$.*

Demostración. Utilizando la notación del Corolario 3.25 tenemos $|G| = |Z(G)| + \sum_{x \in X} [G : \mathrm{Cen}_G(x)]$. Entonces $|G|$ y $[G : \mathrm{Cen}_G(x)]$ es una potencia de p para todo $x \in X$, con lo que $|Z(G)|$ es múltiplo de p y por tanto $Z(G) \neq 1$. □

3.7. Problemas

1. Construir la tabla de multiplicación de los siguientes grupos.
   a) Los grupos de unidades de $\mathbb{Z}_7$ y $\mathbb{Z}_{16}$.
   b) $\mathrm{GL}_2(\mathbb{Z}_2)$.
   c) El subgrupo de $\mathrm{GL}_2(\mathbb{C})$ generado por las matrices

$$a = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

   Este grupo se llama *grupo de cuaterniones* y se denota Q_8.
   d) El subgrupo de $\mathrm{GL}_2(\mathbb{C})$ generado por las matrices

$$a = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

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

e) El subgrupo de $\mathrm{GL}_2(\mathbb{Q})$ generado por las matrices

$$a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

f) El grupo cociente $G/\langle -I \rangle$, donde G es el grupo del apartado anterior e I es la matriz identidad.

g) El grupo de los automorfismos del grupo $\mathbb{Z}_5$.

h) El subgrupo del grupo de la permutaciones de $A = \mathbb{R} \setminus \{0, 1, 2\}$ generado por f y g, donde

$$f(x) = 2 - x \qquad \text{y} \qquad g(x) = \frac{2}{x}.$$

i) $\mathbb{Z}_{16}$ con la operación $x * y = x + (-1)^x + y$.

Decidir si alguno de estos grupos es isomorfo a algún otro grupo conocido.

2. Construir el diagrama de los subgrupos de los grupos anteriores, indicando cuáles de ellos son normales.

3. Probar que todo grupo G de orden menor o igual a cinco es abeliano.

4. Sea G un grupo. Probar que las siguientes afirmaciones son equivalentes:

   a) G es abeliano.

   b) $(ab)^2 = a^2b^2$ para cualesquiera $a, b \in G$.

   c) $(ab)^{-1} = a^{-1}b^{-1}$ para cualesquiera $a, b \in G$.

   d) $(ab)^n = a^nb^n$ para todo $n \in \mathbb{N}$ y para cualesquiera $a, b \in G$.

5. Demostrar que si G es un grupo tal que $g^2 = 1$, para todo $g \in G$, entonces G es abeliano.

6. Mostrar que la unión de dos subgrupos de un grupo no es necesariamente un subgrupo. Aún más, probar que un grupo nunca puede expresarse como unión de dos subgrupos propios.

7. Para $n = 1, \ldots, 10$, determinar cuáles de los grupos $\mathbb{Z}_n^*$ son cíclicos.

8. La función $\phi : \mathbb{N} \to \mathbb{N}$ que asocia a cada número n el cardinal de $\mathbb{Z}_n^*$ se llama función de Euler. Demostrar que:

   a) Si n y m son coprimos, entonces $\phi(nm) = \phi(n)\phi(m)$.

   b) Si p es primo, entonces $\phi(p^n) = p^{n-1}(p-1)$.

   c) Si $n = p_1^{a_1} \cdots p_k^{a_k}$, con $p_1, \ldots, p_k$ primos distintos entonces $\phi(n) = n\frac{p_1-1}{p_1} \cdots \frac{p_k-1}{p_k}$.

9. Demostrar que si G es cíclico entonces el número de generadores de G es 2, si G tiene orden infinito y $\phi(|G|)$, si G tiene orden finito. Describir los generadores en todos los casos.

10. Encontrar todos los grupos cíclicos G, salvo isomorfismos, que tengan exactamente dos generadores (es decir, tales que existan exactamente dos elementos $x \in G$ con $G = \langle x \rangle$).

11. Demostrar que si p es un primo positivo, entonces todos los subgrupos de orden p son cíclicos isomorfos a C_p.

12. Calcular el orden de cada elemento de los grupos diédricos D_n.

13. ¿Es cíclico el producto directo de dos grupos cíclicos infinitos?

14. Demostrar que la intersección de una familia de subgrupos normales de un grupo también es un subgrupo normal.

15. Demostrar que todo subgrupo de un subgrupo cíclico normal de G es normal en G.

16. Sean N y M subgrupos normales de un grupo G tales que $N \cap M = \{1\}$. Probar que $nm = mn$ para todo $n \in N$ y $m \in M$.

17. Sea N un subgrupo normal de índice n de un grupo G. Demostrar que $g^n \in N$ para todo $g \in G$, y dar un ejemplo que muestre que esta propiedad falla si N no es normal en G.

18. Si N es un subgrupo normal en un grupo G y $a \in G$ tiene orden n, probar que el orden de Na en G/N es un divisor de n.

19. Un subgrupo H del grupo G es *característico* si, para cualquier automorfismo f de G, se verifica $f(H) \subseteq H$. Se pide:

    a) Demostrar que todo subgrupo característico de G es un subgrupo normal de G.

    b) Dar un ejemplo de un grupo con un subgrupo normal que no sea característico.

    c) Demostrar que si H es un subgrupo característico de G y K es un subgrupo característico de H, entonces K es un subgrupo característico de G.

    d) Si H es un subgrupo característico de K y K es un subgrupo normal de G, entonces H es normal en G.

    e) Demostrar que el centro de un grupo es un subgrupo característico.

    f) Supongamos que H es un subgrupo de un grupo G, y que ningún otro subgrupo de G contiene un subgrupo del mismo cardinal que H. Demostrar que H es un subgrupo característico (y por tanto normal) de G.

20. Si G y H son grupos, $\mathrm{Hom}(G, H)$ denota el conjunto de los homomorfismos de G a H.

    a) Demostrar que si H es abeliano, entonces $\mathrm{Hom}(G, H)$ es un grupo con la operación natural:

    $$(\varphi\phi)(g) = \varphi(g)\phi(g), \quad (g \in G).$$

    b) Demostrar que si G es abeliano, entonces $\mathrm{Hom}(\mathbb{Z}, G) \simeq G$ y $\mathrm{Hom}(\mathbb{Z}_n, G) \simeq \{g \in G : g^n = e\}$.

    c) Calcular $\mathrm{Hom}(\mathbb{Z}_3, \mathbb{Z}_8)$ y $\mathrm{Hom}(\mathbb{Z}_3, \mathbb{Z}_{21})$.

    d) Probar que $\mathrm{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^*$.

    e) Mostrar que, aun cuando G sea cíclico, $\mathrm{Aut}(G)$ no tiene por qué ser cíclico.

    f) Describir $\mathrm{Aut}(\mathbb{Z})$.

21. Probar que si $n \mid m$ entonces existen un homomorfismo inyectivo $\mathbb{Z}_n \to \mathbb{Z}_m$ y un homomorfismo suprayectivo $\mathbb{Z}_m \to \mathbb{Z}_n$.

22. Demostrar que, si el grupo G no es abeliano, entonces existe un subgrupo abeliano de G que contiene estrictamente al centro $Z(G)$.

23. Demostrar que, si G el grupo diédrico D_4 o el de cuaterniones Q_8, entonces $Z(G) \simeq \mathbb{Z}_2$ y $G/Z(G) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, y sin embargo $D_4 \not\simeq Q_8$.

24. Probar que, salvo isomorfismos, sólo hay dos grupos no abelianos de orden 8. ¿Cuáles son?

25. Probar que todo grupo no abeliano de orden 6 es isomorfo a S_3.

26. Demostrar que si H es un subgrupo abeliano de un grupo G tal que $HZ(G) = G$, entonces G es abeliano. Deducir que si $G/Z(G)$ es cíclico, entonces G es abeliano.

27. Describir todos los subgrupos normales del grupo diédrico D_n.

28. Calcular los centros de $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{GL}_n(\mathbb{C})$, $\mathrm{SL}_n(\mathbb{R})$ y $\mathrm{SL}_n(\mathbb{C})$.

29. Calcular las clases de conjugación de los grupos del Problema 1 y de los grupos diédricos.

30. Demostrar que p es primo, entonces todos los grupos de orden p^2 son abelianos.

31. Si p es primo, probar que el centro de cualquier grupo no abeliano de orden p^3 tiene orden p.

32. Sea G un grupo abeliano finito en el que, para cada $n \in \mathbb{Z}^+$, la ecuación $x^n = e$ tiene a lo sumo n soluciones. Demostrar que G es cíclico. Deducir que un subgrupo finito del grupo de unidades de un dominio es cíclico. (Indicación: Elegir un elemento de orden máximo y observar que para cada $g \in G$ de orden n, el subgrupo $\langle g \rangle$ contiene n soluciones de la ecuación $x^n = e$.)

33. *a*) Mostrar que las siguientes son acciones del grupo que se indica en el conjunto correspondiente.
    1) De $\mathrm{Aut}(G)$ en un grupo G, dada por $\sigma \cdot x = \sigma(x)$ (por la izquierda).
    2) De un grupo G en G/H, donde H es un subgrupo, dada por $g \cdot xH = (gx)H$ (por la izquierda).
    3) De un grupo G en $H\backslash G$, donde H es un subgrupo, dada por $Hx \cdot g = H(xg)$ (por la derecha).
    4) De un grupo G en el conjunto S de sus subgrupos dada por $H \cdot g = H^g$ (por la derecha).

    b) Sea $\cdot : G \times X \to X$ una acción por la izquierda de un grupo G en un conjunto X. Si $x \in X$ entonces $G \cdot x = \{g \cdot x : g \in G\}$ se llama *órbita* de x y $\mathrm{Estab}_G(x) = \{g \in G : g \cdot x\}$ se llama *estabilizador* de x en G.

    Demostrar las siguientes propiedades para cada $x \in X$ y $g \in G$.
    1) La regla $x \cdot g = g^{-1} \cdot x$ define una acción por la derecha de G en X.
    2) Para cada $g \in G$, la aplicación $\overline{g} : X \to X$ dada por $\overline{g}(x) = g \cdot x$ es biyectiva y la aplicación $G \to S_X$ dada por $g \mapsto \overline{g}$ es un homomorfismo de grupos. Recíprocamente, mostrar como todo homomorfismo de grupos $G \to S_X$ induce una acción por la izquierda de G en X.
    3) $\mathrm{Estab}_G(x)$ es un subgrupo de G y $[G : \mathrm{Estab}_G(x)] = |G \cdot x|$, en particular si G es finito, entonces el cardinal de cada órbita es un divisor del orden de G.
    4) $\mathrm{Estab}_G(g \cdot x) = \mathrm{Estab}_G(x)^{g^{-1}}$. Concluir que $\mathrm{Cen}_G(a^g) = \mathrm{Cen}_G(a)^{g^{-1}}$

    c) Identificar las órbitas y los estabilizadores para las acciones de los Ejemplos 3.23 y del apartado (a).

34. (Teorema de Cauchy) Demostrar que si G es un grupo finito cuyo orden es múltiplo de un primo p, entonces G tiene un elemento de orden p. (Indicación: Considérese $X = \{(x_1, x_2, \ldots, x_p) : x_1 x_2 \cdots x_p = 1\}$ y la siguiente acción del grupo cíclico $C_p = \langle g \rangle$ en X: $g \cdot (x_1, x_2, \ldots, x_p) = (x_p, x_1, x_2, \ldots, x_{p-1})$.)

35. (Primer Teorema de Sylow) Demostrar que si G es un grupo de orden finito n y $n = p^m k$ con $p \nmid k$, entonces G tiene un subgrupo de orden p^m. Estos subgrupos se llaman *subgrupos de Sylow* de G. (Indicación: Razonar por inducción en n, aplicando la Ecuación de Clase en el caso en que p divide a $[G : \mathrm{Cen}_G(g)]$ para todo $g \in G \setminus Z(G)$.

Capítulo 4

Grupos de permutaciones

Este es un capítulo recopilatorio de las principales propiedades del grupo simétrico que suponemos bien conocidas por lo que muchas de las demostraciones las omitiremos.

4.1. Ciclos y trasposiciones

Recordemos que, para cada número natural n, S_n denota el grupo simétrico sobre $\mathbb{N}_n = \{1, 2, \ldots, n\}$; es decir, el grupo de las aplicaciones biyectivas $f : \mathbb{N}_n \to \mathbb{N}_n$ con la composición de aplicaciones como operación. Describiremos a veces un elemento $f \in S_n$ dando la lista de sus imágenes en la forma

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}.$$

Definición 4.1. *Diremos que una permutación $\sigma \in S_n$* fija *un entero $i \in \mathbb{N}_n$ si $\sigma(i) = i$; en caso contrario diremos que σ* cambia *o* mueve *i, y denotaremos por $M(\sigma)$ al conjunto de los enteros cambiados por σ:*

$$M(\sigma) = \{i \in \mathbb{N}_n : \sigma(i) \neq i\}.$$

Es claro que $M(\sigma)$ es vacío si y sólo si $\sigma = 1$, y que $M(\sigma)$ no puede tener exactamente un elemento.

Diremos que dos permutaciones σ y τ de S_n son disjuntas *si lo son los conjuntos $M(\sigma)$ y $M(\tau)$. Es decir, si todos los elementos que cambia una de ellas son fijados por la otra.*

Cuando digamos que ciertas permutaciones $\sigma_1, \ldots, \sigma_r$ son disjuntas entenderemos que lo son dos a dos.

Lema 4.2. *Si σ y τ son permutaciones disjuntas entonces $\sigma\tau = \tau\sigma$ y se tiene $M(\sigma\tau) = M(\sigma) \cup M(\tau)$.*

Definición 4.3. *La permutación $\sigma \in S_n$ es un* ciclo *de longitud s (o un s-ciclo) si $M(\sigma)$ tiene s elementos y éstos pueden ordenarse de manera que se tenga $M(\sigma) = \{i_1, i_2, \ldots, i_s\}$ y*

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \ldots \quad \sigma(i_{s-1}) = i_s, \quad \sigma(i_s) = i_1.$$

Este s-ciclo σ se denota como

$$\sigma = (i_1\ i_2\ i_3\ \ldots\ i_s) \qquad \acute{o} \qquad \sigma = (i_1, i_2, i_3, \ldots, i_s).$$

Los 2-ciclos también se llaman transposiciones.

Por ejemplo, los siguientes elementos de S_4 son ciclos de longitudes 2, 3 y 4, respectivamente:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \qquad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

Lema 4.4. *Sea $\sigma = (i_1 \dots i_s)$ un ciclo de longitud s en S_n.*

1. *Para cada $t \in \{1, 2, \dots, s\}$ se tiene $\sigma = (i_t \dots i_s \; i_1 \dots i_{t-1})$.*
2. *Para cada $t \in \{1, 2, \dots, s\}$ se tiene $i_t = \sigma^{t-1}(i_1)$.*
3. *El orden de σ (como elemento del grupo simétrico) coincide con su longitud s.*

Teorema 4.5. *Toda permutación $\sigma \neq 1$ de S_n se puede expresar de forma única (salvo el orden) como producto de ciclos disjuntos.*

Ejemplo 4.6. *Factorización de una permutación como producto de ciclos disjuntos.*
Consideremos la permutación de S_{11}

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 6 & 5 & 1 & 4 & 2 & 7 & 3 & 8 & 11 & 9 & 10 \end{pmatrix}.$$

Elegimos un elemento arbitrario cambiado por σ, por ejemplo el 1, y calculamos sus imágenes sucesivas por σ:

$$\sigma(1) = 6, \; \sigma^2(1) = \sigma(6) = 7, \; \sigma^3(1) = \sigma(7) = 3, \; \sigma^4(1) = \sigma(3) = 1.$$

Entonces (1 6 7 3) es uno de los factores de σ. Elegimos ahora un elemento de $M(\sigma)$ que no haya aparecido aún, por ejemplo el 2, y le volvemos a seguir la pista, lo que nos da un nuevo factor (2 5). Empezando ahora con el 9 obtenemos un tercer ciclo (9 11 10) que agota el proceso (el 4 y el 8 son fijados por σ) y nos dice que $\sigma = (1\ 6\ 7\ 3)(2\ 5)(9\ 11\ 10)$.

Veamos cómo se puede calcular el orden de una permutación en términos de su factorización como producto de ciclos disjuntos:

Proposición 4.7. *Sea $\sigma = \tau_1 \cdots \tau_k$ la factorización de una permutación σ como producto de ciclos disjuntos, y sea s_i la longitud del ciclo τ_i. Entonces*

$$o(\sigma) = \operatorname{mcm}(s_1, \dots, s_k).$$

Demostración. Sea $m \in \mathbb{N}$. Como los τ_i conmutan entre sí, se tiene $\sigma^m = \tau_1^m \cdots \tau_k^m$. Por otra parte, para cada i se tiene $M(\tau_i^m) \subseteq M(\tau_i)$ y por tanto los τ_i^m son disjuntos. Esto implica, por la unicidad en el Teorema 4.5, que $\sigma^m = 1$ precisamente si cada $\tau_i^m = 1$, y entonces el resultado es claro, pues s_i es el orden de τ_i. □

A continuación vamos a describir las clases de conjugación de S_n.

Definición 4.8. *El* tipo *de una permutación $\sigma \neq 1$ de S_n es la lista $[s_1, \dots, s_k]$ de las longitudes de los ciclos que aparecen en su factorización en ciclos disjuntos, ordenadas en forma decreciente. Por convenio, la permutación identidad tiene tipo* $[1]$.

Por ejemplo, el tipo de un s-ciclo es $[s]$, el de la permutación $(1\ 2)(3\ 4\ 5)(6\ 7) \in S_7$ es $[3, 2, 2]$, y el de la permutación de S_{11} del Ejemplo 4.6 es $[4, 3, 2]$.

Teorema 4.9. *Dos elementos de S_n son conjugados precisamente si tienen el mismo tipo. En consecuencia, cada clase de conjugación de S_n está formada por todos los elementos de un mismo tipo.*

Observación 4.10. *La factorización en ciclos disjuntos de σ^α se obtiene sustituyendo, en la de σ, cada elemento $i \in \mathbb{N}_n$ por $\alpha^{-1}(i)$.*

Por ejemplo, si $\alpha = (1\ 4\ 3)(2\ 5\ 6)$ y $\sigma = (1\ 3)(2\ 4\ 7)$, entonces $\sigma^\alpha = (3\ 4)(6\ 1\ 7)$.

Ejemplo 4.11. *Clases de conjugación de S_n.*

Las 6 permutaciones de S_3 se dividen en una permutación de tipo [1] (la identidad), tres 2-ciclos o permutaciones de tipo [2] (a saber, (1 2), (1 3) y (2 3)), y dos 3-ciclos o permutaciones de tipo [3] (a saber, (1 2 3) y (1 3 2)).

En S_4 hay más variedad, y en particular aparecen permutaciones que no son ciclos. Sus 24 permutaciones se dividen en los siguientes tipos:

Tipo	Permutaciones
[1]	1
[2]	(1 2), (1 3), (1 4), (2 3), (2 4), (3 4)
[3]	(1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3)
[4]	(1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2)
[2,2]	(1 2)(3 4), (1 3)(2 4), (1 4)(2 3)

Por tanto, cada fila de elementos a la derecha de la barra es una clase de conjugación de S_4.

Además de los ciclos, en S_5 hay permutaciones de los tipos $[2,2]$ y $[3,2]$; y en S_6 las hay de los tipos $[2,2]$, $[3,2]$, $[2,2,2]$ y $[3,3]$. En estos casos, por el gran número de elementos en los grupos, es pesado construir tablas como la que acabamos de dar para S_4, pero se puede al menos calcular cuántas permutaciones hay de cada tipo (véase el Problema 7).

Proposición 4.12. *Para $n > 2$, los siguientes son conjuntos generadores de S_n:*

1. *El conjunto de todos los ciclos.*
2. *El conjunto de todas las trasposiciones.*
3. *El conjunto de $n-1$ trasposiciones: $\{(1\ 2), (1\ 3), (1\ 4), \ldots, (1\ n-1), (1\ n)\}$.*
4. *El conjunto de $n-1$ trasposiciones: $\{(1\ 2), (2\ 3), (3\ 4), \ldots, (n-1\ n)\}$.*
5. *El conjunto de una trasposición y un n-ciclo: $\{(1\ 2), (1\ 2\ 3\ \ldots\ n-1\ n)\}$.*

Demostración. 1. Es una consecuencia inmediata del Teorema 4.5.

Para demostrar el resto de apartados bastará con comprobar que los elementos del conjunto dado en cada apartado se expresan como productos de los elementos del conjunto del apartado siguiente.

2. Cada ciclo $\sigma = (i_1\ i_2\ \ldots\ i_s)$ puede escribirse como producto de trasposiciones (no disjuntas):

$$\sigma = (i_1\ i_s)(i_1\ i_{s-1}) \cdots (i_1\ i_3)(i_1\ i_2).$$

3. Es consecuencia de la igualdad $(i\ j) = (1\ i)(1\ j)(1\ i)$.

4. Dado $j \geq 2$, sea $\alpha = (2\ 3)(3\ 4)(4\ 5) \cdots (j-1\ j)$. Usando la Observación 4.10 se obtiene $(1\ 2)^\alpha = (1\ j)$.

5. Sean $\tau = (1\ 2)$ y $\sigma = (1\ 2\ \ldots\ n-1\ n)$. Como σ^{j-1} lleva $1 \mapsto j$ y $2 \mapsto j+1$, la Observación 4.10 nos dice que $\sigma^{j-1}\tau\sigma^{1-j} = (j, j+1)$. □

Corolario 4.13. *Sean p un número primo y H un subgrupo de S_p. Si H contiene una transposición y un p-ciclo, entonces $H = S_p$.*

Demostración. Podemos suponer que H contiene a $(1\ 2)$ y un p-ciclo $\sigma = (a_1\ a_2\ \dots\ a_p)$. Por el Lema 4.4, podemos suponer que $a_1 = 1$. Si $a_i = 2$, entonces $\sigma^{i-1} = (1\ 2\ b_3\ \dots\ b_p)$ y podemos renombrar los b_i de forma que $b_i = i$. Por tanto $(1\ 2), (1\ 2\ \dots\ p) \in H$. Deducimos de la Proposición 4.12 que $H = S_p$. ¿Dónde hemos utilizado que p es primo? □

Aunque toda permutación de S_n se puede expresar como un producto de trasposiciones, estas expresiones no tienen las buenas propiedades que vimos en las descomposiciones en ciclos. Por una parte, no podemos esperar que una permutación arbitraria sea producto de trasposiciones disjuntas (tendría orden 2). Por otra, tampoco se tiene conmutatividad (por ejemplo, $(1\ 3)(1\ 2) \neq (1\ 2)(1\ 3)$) ni unicidad, ni siquiera en el número de factores; por ejemplo

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 3)(1\ 3) = (1\ 3)(2\ 4)(1\ 2)(1\ 4) = (2\ 3)(2\ 3)(1\ 3)(2\ 4)(1\ 2)(1\ 4).$$

Nótese que en todas estas factorizaciones de $(1\ 2\ 3)$ hay un número par de trasposiciones; esto es consecuencia de un hecho general que analizaremos en la sección siguiente (Proposición 4.16).

4.2. El grupo alternado

Fijemos un entero positivo $n \geq 2$ y una permutación $\sigma \in S_n$. Por la Propiedad Universal de los Anillos de Polinomios, existe un homomorfismo de anillos $\bar{\sigma} : \mathbb{Z}[X_1, \dots, X_n] \to \mathbb{Z}[X_1, \dots, X_n]$ tal que $\bar{\sigma}(X_i) = X_{\sigma(i)}$ para cada i (Ejemplos 2.32). Es decir, dado un polinomio Q, su imagen $\bar{\sigma}(Q)$ se obtiene sustituyendo cada X_i por $X_{\sigma(i)}$ en la expresión de Q.

En lo que sigue, P designará al polinomio de $\mathbb{Z}[X_1, \dots, X_n]$ dado por

$$P = \prod_{1 \leq i < j \leq n} (X_j - X_i).$$

La condición $i < j$ implica que cada diferencia entre dos indeterminadas distintas aparece, en cierto orden, exactamente una vez en esa factorización. Como $\bar{\sigma}$ es un homomorfismo de anillos, se tiene

$$\bar{\sigma}(P) = \prod_{i<j} \bar{\sigma}(X_j - X_i) = \prod_{i<j} (X_{\sigma(j)} - X_{\sigma(i)}).$$

Como σ es una biyección, cada diferencia entre dos indeterminadas distintas sigue apareciendo, en cierto orden, exactamente una vez en esta factorización. Fijados $i < j$ pueden ocurrir dos cosas:

- Que sea $\sigma(i) < \sigma(j)$, en cuyo caso el factor $X_{\sigma(j)} - X_{\sigma(i)}$ aparece en $\bar{\sigma}(P)$ igual que en P.
- Que sea $\sigma(i) > \sigma(j)$, en cuyo caso el factor $X_{\sigma(j)} - X_{\sigma(i)}$ aparece en $\bar{\sigma}(P)$ en el orden contrario que en P; en este caso diremos que σ *presenta una inversión* para el par (i, j).

Como cada inversión se traduce en un cambio de signo en $\bar{\sigma}(P)$ con respecto a P, se tiene $\bar{\sigma}(P) = \pm P$, donde el signo es $+$ si y sólo si el número de pares (i, j) (con $i < j$) para los que σ presenta una inversión es par. Esto sugiere las definiciones que siguen:

Definición 4.14. *La permutación $\sigma \in S_n$ es* par *si $\bar{\sigma}(P) = P$; es decir, si σ presenta un número par de inversiones; y es* impar *si $\bar{\sigma}(P) = -P$; es decir, si σ presenta un número impar de inversiones.*

El signo *de σ se define como $\operatorname{sg}(\sigma) = (-1)^k$, donde k es el número de inversiones que presenta σ. Es decir, $\operatorname{sg}(\sigma) = 1$ si σ es par y $\operatorname{sg}(\sigma) = -1$ si σ es impar. Por el comentario previo a esta definición se tiene $\bar{\sigma}(P) = \operatorname{sg}(\sigma)P$.*

Proposición 4.15. *La "aplicación signo" $\operatorname{sg} : S_n \to \mathbb{Z}^* = \{1, -1\}$ es un homomorfismo de grupos.*

Demostración. Sean $\sigma, \tau \in S_n$. Es claro que $\bar{\sigma} \circ \bar{\tau} = \overline{\sigma \circ \tau}$, y por tanto

$$\mathrm{sg}(\sigma \circ \tau)P = \overline{\sigma \circ \tau}(P) = \bar{\sigma}(\bar{\tau}(P)) = \bar{\sigma}(\mathrm{sg}(\tau)P) = \mathrm{sg}(\tau)\bar{\sigma}(P) = \mathrm{sg}(\tau)\mathrm{sg}(\sigma)P,$$

y por tanto $\mathrm{sg}(\sigma \circ \tau) = \mathrm{sg}(\sigma)\mathrm{sg}(\tau)$. □

Proposición 4.16. *En S_n se verifica:*

1. *El signo de una permutación σ es el mismo que el de su inversa σ^{-1} y que el de cualquiera de sus conjugadas σ^{α}.*
2. *Toda trasposición es impar.*
3. *Si $\sigma = \tau_1 \cdots \tau_r$, donde las τ_i son trasposiciones, entonces $\mathrm{sg}(\sigma) = (-1)^r$.*
4. *Una permutación σ es par (respectivamente impar) si y sólo si es producto de un número par (respectivamente impar) de trasposiciones.*
5. *Un ciclo de longitud s tiene signo $(-1)^{s-1}$; es decir, un ciclo de longitud par es impar, y viceversa.*
6. *La paridad de una permutación coincide con la del número de componentes pares de su tipo.*

Ejemplo 4.17. *Calculando la paridad en función del tipo.*
Del Ejemplo 4.11 y del último apartado de la Proposición 4.16 se deduce que, además de la identidad, las permutaciones pares de S_3 son las de tipo [3]; las de S_4 son las de los tipos [3] ó [2, 2]; las de S_5 son las de los tipos [3], [5] ó [2, 2]; y las de S_6 son las de los tipos [3], [5], [2, 2] ó [3, 3].

Definición 4.18. *El* grupo alternado *en n elementos, denotado por A_n, es el núcleo del homomorfismo $\mathrm{sg} : S_n \to \mathbb{Z}^* = \{1, -1\}$. Es decir, es el subgrupo de S_n formado por las permutaciones pares.*

Proposición 4.19. *A_n es un subgrupo normal de S_n, y para $n \geq 2$ se tiene:*

$$[S_n : A_n] = 2, \qquad |A_n| = \frac{n!}{2}, \qquad y \qquad \frac{S_n}{A_n} \simeq \{1, -1\} \simeq \mathbb{Z}_2.$$

Demostración. Al estar definido como el núcleo de un homomorfismo, A_n es normal en S_n. El resto es consecuencia del Primer Teorema de Isomorfía si vemos que, para $n \geq 2$, el homomorfismo sg es suprayectivo, para lo que basta notar que $\mathrm{sg}(1) = 1$ y $\mathrm{sg}(1\ 2) = -1$. □

Es elemental ver que A_2 es el grupo trivial y que A_3 es el subgrupo cíclico de S_3 generado por el 3-ciclo (1 2 3), y por tanto $A_3 \simeq C_3$. En el caso general, tenemos dos maneras sencillas de describir conjuntos de generadores de A_n.

Proposición 4.20. *Los siguientes son sistemas de generadores de A_n:*

1. *El conjunto de todos los productos de dos trasposiciones (disjuntas o no).*
2. *El conjunto de todos los 3-ciclos.*

Demostración. El apartado 1 es una consecuencia inmediata del apartado 4 de la Proposición 4.16. Por la misma proposición, todos los 3-ciclos están en A_n; por tanto, usando 1, para ver 2 sólo hay que probar que cada producto de dos trasposiciones distintas (disjuntas o no) se puede escribir como producto de 3-ciclos, lo que se sigue de las igualdades

$$(i\ j)(i\ k) = (i\ k\ j) \qquad \text{e} \qquad (i\ j)(k\ l) = (j\ l\ k)(i\ k\ j),$$

donde asumimos que i, j, k, l son distintos dos a dos. □

Obsérvese que, como el conjunto vacío genera el subgrupo trivial, la Proposición 4.20 es válida incluso cuando $n = 1$ ó $n = 2$.

A continuación describimos los subgrupos de A_4. Esto nos dará un ejemplo en el que no se verifica el recíproco del Teorema de Lagrange: A_4 tiene orden 12, pero no tiene subgrupos de orden 6.

Ejemplo 4.21. *Subgrupos de A_4.*

En virtud del Ejemplo 4.17, la siguiente es la lista completa de los elementos de A_4:

$$\begin{array}{llll} 1 & \sigma = (1\ 2)(3\ 4) & \tau = (1\ 3)(2\ 4) & \eta = (1\ 4)(2\ 3) \\ \alpha = (1\ 2\ 3) & \beta = (1\ 2\ 4) & \gamma = (1\ 3\ 4) & \delta = (2\ 3\ 4) \\ \alpha^2 = (1\ 3\ 2) & \beta^2 = (1\ 4\ 2) & \gamma^2 = (1\ 4\ 3) & \delta^2 = (2\ 4\ 3) \end{array}$$

Por el Teorema de Lagrange, los subgrupos propios y no triviales de A_4 han de tener orden 2, 3, 4, ó 6. Los de orden 2 han de estar generados por elementos de orden 2, y por tanto son:

$$\langle\sigma\rangle = \{1, \sigma\} \qquad \langle\tau\rangle = \{1, \tau\} \qquad \langle\eta\rangle = \{1, \eta\}.$$

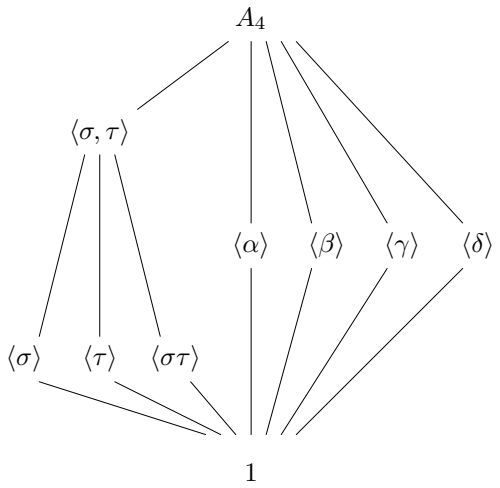
Como $\sigma^\alpha = \tau \notin \langle\sigma\rangle$, deducimos que $\langle\sigma\rangle$ no es normal en A_4, y del mismo modo se ve que no lo son $\langle\tau\rangle$ ni $\langle\eta\rangle$. Los subgrupos de orden 3 han de estar generados por elementos de orden 3, y por tanto son:

$$\begin{array}{ll} \langle\alpha\rangle = \langle\alpha^2\rangle = \{1, \alpha, \alpha^2\} & \langle\beta\rangle = \langle\beta^2\rangle = \{1, \beta, \beta^2\} \\ \langle\gamma\rangle = \langle\gamma^2\rangle = \{1, \gamma, \gamma^2\} & \langle\delta\rangle = \langle\delta^2\rangle = \{1, \delta, \delta^2\}. \end{array}$$

Un subgrupo de orden 4 no puede contener a ninguno de los elementos de orden 3; como el resto de elementos forman un subgrupo

$$N = \{1, \sigma, \tau, \eta\},$$

éste es el único subgrupo de orden 4, que además es normal en S_n por el Teorema 4.9. Por último, veamos que no hay subgrupos de orden 6. Un tal subgrupo H sería normal en A_4 por tener índice 2, por lo que también $N \cap H$ sería normal en A_4. Además se tendría $NH = A_4$ (¿por qué?) y en consecuencia $|N \cap H| = 2$ (Teorema 3.16), en contra del hecho de que ninguno de los subgrupos de orden 2 de A_4 es normal.



4.3. El Teorema de Abel

Definición 4.22. *Un grupo no trivial G es* simple *si sus únicos subgrupos normales son $\{1\}$ y G.*

Como consecuencia inmediata de la Proposición 3.20 se tiene que un grupo abeliano es simple si y sólo si tiene orden primo. Obsérvese que $A_3 \simeq C_3$ es simple, pero A_4 no lo es, como muestra el Ejemplo 4.21.

Lema 4.23. *Si un subgrupo normal H de A_n ($n \geq 5$) contiene un 3-ciclo, entonces $H = A_n$.*

Demostración. Sea σ un 3-ciclo en H. Por la Proposición 4.20, basta ver que cualquier otro 3-ciclo σ' está en H. Sabemos por el Teorema 4.9 que existe $\alpha \in S_n$ tal que $\sigma' = \sigma^\alpha$, de modo que si $\alpha \in A_n$ entonces $\sigma' \in H$, por la normalidad de H en A_n; en consecuencia, podemos suponer que α es una permutación impar. Como σ sólo cambia 3 elementos y $n \geq 5$, existe una trasposición β disjunta con σ, por lo que $\sigma^\beta = \sigma$. Por tanto

$$\sigma^{\beta\alpha} = (\sigma^\beta)^\alpha = \sigma^\alpha = \sigma',$$

y como $\beta\alpha$ está en A_n por ser el producto de dos permutaciones impares, la normalidad de H en A_n implica que $\sigma' \in H$, como queríamos ver. □

Obsérvese que la hipótesis $n \geq 5$ en el Lema anterior es superflua, pues para $n \leq 3$ es obvio que se verifica el Lema y para $n = 4$ es consecuencia del Ejemplo 4.21.

Teorema 4.24 (Abel)**.** *Si $n \geq 5$, entonces A_n es un grupo simple.*

Demostración. Supongamos que $H \neq \{1\}$ es un subgrupo normal de A_n y veamos que $H = A_n$. Por el Lema 4.23, bastará probar que H contiene un 3-ciclo.

Sea $1 \neq \sigma \in H$ tal que $r = |M(\sigma)|$ sea mínimo, es decir, $|M(\nu)| \leq r$ para todo $1 \neq \nu \in H$. Ahora veremos que debe tenerse $r = 3$, por lo que σ será un 3-ciclo en H y habremos terminado.

Desde luego, no puede ser $r = 1$ porque ninguna permutación cambia exactamente un elemento, ni tampoco $r = 2$ porque todas las permutaciones de H son pares. Supongamos pues, en busca de una contradicción, que $r > 3$. Se tienen entonces dos posibilidades:

1. Que, en la factorización de σ en ciclos disjuntos, aparezca alguno de longitud ≥ 3.
2. Que σ sea un producto de (al menos dos) trasposiciones disjuntas.

En el primer caso, σ debe cambiar al menos 5 elementos (si sólo cambiase 4, como en la factorización de σ aparece un ciclo de longitud ≥ 3, σ sería un 4-ciclo, lo que contradice el hecho de que $\sigma \in A_n$). Podemos suponer, sin pérdida de generalidad (¿por qué?), que $1, 2, 3, 4, 5 \in M(\sigma)$ y que alguno de los ciclos disjuntos que componen σ es de la forma (1 2 3 ...) (con longitud al menos 3). Sea $\alpha = (3\ 4\ 5)$. Como $\alpha \in A_n$ y H es normal en A_n, deducimos que $\sigma^\alpha \in H$, y así $\beta = \sigma^{-1}\sigma^\alpha \in H$. Si $\sigma(i) = i$ entonces $i > 5$ y por tanto $\alpha(i) = i$, de donde se sigue que $\beta(i) = i$; por tanto $M(\beta) \subseteq M(\sigma)$, y la inclusión es estricta pues $\sigma(1) = 2$ mientras que $\beta(1) = 1$. En consecuencia, $\beta \in H$ cambia menos de r elementos, así que debe ser $\beta = 1$, por la elección de r. Esto significa que $\sigma^\alpha = \sigma$, y por tanto $\alpha\sigma = \sigma\alpha$. Pero esto es falso, pues $\alpha\sigma(2) = 4$ y $\sigma\alpha(2) = 3$, de manera que la primera de las dos posibilidades consideradas nos lleva a una contradicción.

Pasamos al segundo caso. Reordenando los elementos de $\mathbb{N}_n$ podemos asumir que $\sigma = (1\ 2)(3\ 4)\cdots$ (puede haber más trasposiciones en el producto o no). Sea de nuevo $\alpha = (3\ 4\ 5)$. Como antes, tomamos $\beta = \sigma^{-1}\sigma^\alpha \in H$. Si $i \neq 5$ y $\sigma(i) = i$ entonces $i \neq 3, 4, 5$ y por tanto $\alpha(i) = i$, de donde se sigue que $\beta(i) = i$; por tanto $M(\beta) \subseteq M(\sigma) \cup \{5\}$. Pero el 1 y el 2 son fijados por β y cambiados por σ, de modo que β cambia menos de r elementos y así $\beta = 1$, o sea $\sigma\alpha = \alpha\sigma$. Pero se tiene $\sigma\alpha(3) = 3 \neq 5 = \alpha\sigma(3)$. En cualquier caso, pues, llegamos a la contradicción que buscábamos. □

4.4. Problemas

1. Calcular σ^{1000}, donde $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 5 & 2 & 6 & 1 & 7 & 4 & 0 & 9 & 11 & 8 \end{pmatrix}$.

2. Dada la permutación $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 9 & 8 & 2 & 3 & 4 & 6 & 7 \end{pmatrix}$, calcular el orden de σ^2.

3. Sea $1 \neq \sigma \in S_n$. Demostrar que σ es un ciclo si y sólo si, para cualesquiera $j, k \in M(\sigma)$, existe un entero m tal que $\sigma^m(j) = k$.

4. Probar que para toda permutación $\sigma \in S_n$ se cumple $\sigma(i_1 \cdots i_r)\sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_r))$.

5. Demostrar que una permutación tiene orden primo p si y sólo si se factoriza como un producto de ciclos disjuntos, cada uno de longitud p.

6. Demostrar que para todo $1 \leq k < n$, S_n tiene al menos $\binom{n}{k}$ subgrupos isomorfos a $S_k \times S_{n-k}$ y que todos son conjugados; es decir, para dos de estos grupos H y K existe $\sigma \in G$ tal que $H^\sigma = K$.

7. Dados dos números naturales n y k con $n \geq k \geq 2$, se pide:

   a) Demostrar que, para cada subconjunto A de $\mathbb{N}_n$ de cardinal k, el número de k-ciclos σ de S_n con $M(\sigma) = A$ es $(k-1)!$.

   b) Demostrar que el número de k-ciclos en S_n es $\binom{n}{k}(k-1)!$.

   c) ¿Cuántos elementos de tipo $[2,2]$ hay en S_5? ¿Cuántos de tipo $[2,3]$?

   d) ¿Cuántos elementos de tipo $[2,2]$ hay en S_6? ¿Cuántos de tipo $[2,3]$? ¿Y de tipo $[3,3]$?

   e) [*] Calcular en general el número de elementos de S_n de tipo $[k_1, \ldots, k_r]$.

8. Sea G un grupo finito de orden n, y sea $g \in G$ de orden m. Se define $\phi_g : G \to G$ por $\phi_g(x) = gx$. Viendo a ϕ_g como un elemento de S_n, demostrar que:

   a) ϕ_g es un producto de n/m ciclos de longitud m.

   b) La paridad de ϕ_g coincide con la paridad del entero $(m-1)\frac{n}{m}$.

   c) Si $(m-1)\frac{n}{m}$ es impar, entonces G tiene un subgrupo normal de índice 2.

9. (Teorema de Cayley) Demostrar que todo grupo finito es isomorfo a un subgrupo de S_n para algún n.

10. Demostrar que el centralizador de la permutación $\sigma = (1, 2, \ldots, n)$ en S_n es $\langle \sigma \rangle$.

11. Demostrar que el grupo alternado A_n es un subgrupo característico del grupo simétrico S_n.

12. Sea $n \geq 2$ y sea $f : S_n \to S_{n+2}$ la aplicación dada por $f(\sigma) = \sigma^*$, donde σ^* actúa igual que σ sobre los elementos $1, 2, \ldots, n$, y σ^* fija (respectivamente, intercambia) $n+1$ y $n+2$ cuando σ es par (respectivamente, impar). Demostrar que f es un homomorfismo inyectivo de grupos y que su imagen está contenida en A_{n+2}. Deducir que todo grupo finito es isomorfo a un subgrupo de un grupo alternado.

13. Probar que si P es un subgrupo de orden 4 del grupo alternado A_5, entonces P es isomorfo al grupo de Klein $C_2 \times C_2$.

14. Demostrar que D_n es isomorfo al subgrupo $\langle \rho, \sigma \rangle$ de S_n, donde $\rho = (1, 2, \ldots, n-1, n)$ y σ es el producto de las trasposiciones $(i, n+1-i)$, donde i varía desde 1 hasta la parte entera de $n/2$. ¿Para qué valores de n se tiene $\langle \rho, \sigma \rangle \subseteq A_n$?

15. Dado $f \in \mathrm{Aut}(S_3)$, probar que f induce una permutación del conjunto $X = \{(1\ 2), (1\ 3), (2\ 3)\} \subset S_3$. Deducir que la aplicación $\iota : S_3 \to \mathrm{Aut}(S_3)$ que lleva $\sigma \in S_3$ al automorfismo interno ι_σ es un isomorfismo de grupos.

16. Demostrar que A_n está generado por los 3-ciclos de la forma $(1, 2, i)$ con $i = 3, \ldots, n$.

17. Para $n \geq 5$, demostrar que S_n tiene exactamente tres subgrupos normales.

18. Para $n \geq 2$, demostrar que A_n es el único subgrupo de índice dos de S_n.

19. [*] Sea p un primo impar y sea H un subgrupo propio de S_p que contiene una trasposición. Demostrar que existen $i, j \in \mathbb{N}_p$ tales que $\sigma(i) \neq j$ para todo $\sigma \in H$. (Indicación: Considerar en $\mathbb{N}_p$ la relación de equivalencia en la que $i \sim j$ si $i = j$ ó si $(i, j) \in H$, y comparar el número de elementos de las clases de equivalencia.)

20. [*] Sea $S_\infty = S(\mathbb{N})$ el grupo de permutaciones del conjunto numerable $\mathbb{N}$. El *grupo alternado infinito* es el subgrupo A_∞ de S_∞ generado por todos los 3-ciclos (donde un 3-ciclo se define del modo obvio). Demostrar que A_∞ es un grupo simple infinito.

Capítulo 5

Grupos resolubles

5.1. El subgrupo derivado y la serie derivada

Definición 5.1. *Sea G un grupo. Si $x, y \in G$, entonces 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*

$$G' = \langle (x, y) : x, y \in G \rangle.$$

Por ejemplo, si a, b y c son tres elementos distintos de S_n entonces

$$((a\ b), (a\ c)) = (a\ b)(a\ c)(a\ b)(a\ c) = (b\ c)(a\ c) = (a\ b\ c).$$

Eso implica que todos los tres ciclos de S_n están en A_n y por tanto $A_n \subseteq S_n'$. De hecho se verifica la igualdad pues si $\sigma, \tau \in S_n$ entonces σ^τ tiene la misma paridad que σ y σ^{-1}, lo que implica que $(\sigma, \tau) = \sigma^{-1}\sigma^\tau \in A_n$.

Lema 5.2. *Dados un grupo G y elementos $a, b \in G$, entonces*

1. *$(a, b) = 1$ si y sólo si $ab = ba$.*
2. *G es abeliano si y sólo 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 $x \in G$.*
8. *G' es un subgrupo normal de G.*

Teorema 5.3. *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 5.2, 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 del Lema 5.2.

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 5.3 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 G' se pierde la información sobre G', pues sus elementos representan al neutro en el cociente). Podemos decir que, 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 5.4. *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

$$D_n' = \begin{cases} \langle a \rangle & \text{si } 2 \nmid n \\ \langle a^2 \rangle & \text{si } 2 | n \end{cases}$$

5.2. 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 y propio de G.

Definición 5.5. *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 5.4 y por tanto $D_n'' = 1$. El siguiente ejemplo muestra nuevos 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 5.6. *Resolubilidad de los grupos simétricos*

1. Hemos visto que $S_n' = A_n$. Cuando $n = 3$ tenemos $S_3' = A_3$, que es abeliano. Por tanto S_3 es resoluble con serie derivada $S_3 \rhd A_3 \rhd 1$.

2. Por el Ejemplo 4.21, el único subgrupo normal, propio y no trivial de A_4 es

$$V = \{1,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

   Como A_4 no es abeliano y A_4/V sí lo es (tiene orden 3), del Teorema 5.3 se deduce que $V = A_4' = S_4^{(2)}$. Como V es abeliano, deducimos que $S_4^{(3)}$ es trivial. En consecuencia, S_4 es resoluble con serie derivada $S_4 \rhd A_4 \rhd V \rhd 1$.

3. Si $n \geq 5$ entonces A_n es simple (Teorema de Abel, 4.24) y no abeliano, luego $A_n' = A_n$ por el Teorema 5.3. Es decir, la serie derivada de S_n se estabiliza en A_n y nunca alcanza al grupo trivial. En consecuencia, S_n no es resoluble cuando $n \geq 5$.

Vamos a estudiar las propiedades básicas de los grupos resolubles, y comenzamos con un lema.

Lema 5.7. *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 5.8. *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 5.7 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 5.7 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. Por hipótesis existe $t \geq 1$ tal que $(G/N)^{(t)} = 1$. Aplicando como antes el Lema 5.7 deducimos que $p(G^{(t)})$ es trivial, lo que significa que $G^{(t)} \subseteq \mathrm{Ker}\ p = N$. 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 5.9. *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 3.26 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 5.8 deducimos que G es resoluble. □

La serie derivada de un grupo resoluble sugiere la siguiente definición más general:

Definición 5.10. *Sea G un grupo arbitrario. Una* serie normal[1] *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 $n + 1$).

Una serie abeliana *es una serie normal cuyos factores son abelianos y una* serie cíclica *es una serie normal 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 serie normal (finita) abeliana. De hecho esta propiedad caracteriza los grupos resolubles.

Teorema 5.11. *Un grupo G es resoluble si y sólo si admite una serie normal 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 normal como la de la Definición 5.10 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 5.8 nos dice que G es resoluble, como queríamos ver. □

Teorema 5.12. *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.

[1] En la literatura en inglés se suele utilizar "subnormal series" para lo que nosotros hemos denominado "serie normal", mientras que una "normal series" es una serie en la que cada G_i es normal en G.

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 5.8 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. □

5.3. Problemas

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

2. 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.

3. Probar que si G es resoluble y no trivial entonces $G' \neq G$.

4. Probar que si G es simple y resoluble entonces G es cíclico de orden primo.

5. Formar todas las series con factores de orden primo para un grupo cíclico de orden 20.

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 $H \cap K$.

7. Demostrar que todo grupo de orden menor que 60 es resoluble utilizando los Teoremas de Sylow que dicen lo siguiente:

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. Demostrar que $G \times H$ es resoluble precisamente si G y H lo son.

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 $S_3 \simeq \mathrm{Aut}(S_3)$).

11. Probar que si un grupo G es resoluble y $G/Z(G)$ es simple entonces G es abeliano.

12. Probar que si G es un grupo no abeliano de orden p^3 (con p primo), entonces $G' = Z(G)$ y $G/G' \simeq C_p \times C_p$.

13. Demostrar que un grupo finito abeliano tiene una única serie con factores de orden primo si y sólo si es un p-grupo cíclico, para algún primo p. ¿Es cierto esto si el grupo no es abeliano?

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.

15. Demostrar que si G es un grupo cuyo orden es una potencia de un primo, entonces G es resoluble.

16. Para resolver este ejercicio es necesario utilizar los Teoremas de Sylow que dicen lo siguiente:

    Sea G un grupo finito de orden $n = p^m r$ con p y primo y r coprimo con p. Los subgrupos de orden p^m de G se llaman subgrupos de Sylow.

    - G tiene al menos un subgrupo de orden p^k para cada $k \leq m$.
    - Todos los subgrupos de Sylow de G son conjugados en G.
    - El número n_p de subgrupos de Sylow de G es un divisor de r, congruente con 1 módulo p.

    a) Probar que si p, q, r son primos distintos tales que $pq < r$ entonces todo grupo finito de orden pqr es resoluble.

    b) Probar que todo grupo de orden 56, 63 ó 440 es resoluble.

    c) Demostrar:

    1) Todo grupo de orden 45 es abeliano.
    2) Todo grupo de orden 765 es resoluble.

    d) Dado un grupo G de orden $3^3 \cdot 13$, probar que es resoluble y dar una serie normal con factores cíclicos.

    e) Demostrar que todo grupo de orden $p^2 q$ con p y q primos es resoluble.

    f) Demostrar que todo grupo de orden menor que 60 es resoluble.

    g) Demostrar que si G es un grupo no resoluble de orden $n < 300$, entonces $n = 60, 120, 168, 180$ ó 240.

17. 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:

    a) Todo grupo abeliano es nilpotente.

    b) $Z_n(G) = \{x \in G : (x, y) \in Z_{n-1}(G) \text{ para todo } y \in G\}$.

    c) Todo p-grupo finito (p primo) es nilpotente.

    d) 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 $i = 1, 2, \ldots, n$.

    e) Todo grupo nilpotente es resoluble.

    f) Dar un ejemplo de un grupo resoluble que no sea nilpotente.

    g) Si G es nilpotente y H es un subgrupo de G, entonces H es nilpotente.

h) Si G es nilpotente y N es un subgrupo normal de G, entonces G/N es nilpotente.

i) 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.

j) Demostrar que si G y H son dos grupos nilpotentes, entonces $G \times H$ es un grupo nilpotente.

18. 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.

a) Demostrar que $\mathcal{A}_n = \mathbb{Z}_n^* \times \mathbb{Z}_n$ es un grupo con el siguiente producto.

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1).$$

b) Demostrar que si $n = p$ es primo y $(a, b) \in \mathcal{A}_n$ tiene orden p, entonces $a = 1$.

c) 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 $\mathbb{Z}_n$.

d) 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 $\sigma = \sigma_{b^{-1},\sigma(0)}$.

e) Mostrar que la aplicación $(a, b) \mapsto \sigma_{a,b}$ es un homomorfismo inyectivo $\mathcal{A}_n \to S_n$.

f) 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 $\mathcal{A}_n$.

g) Demostrar que si σ es un n-ciclo, entonces $\langle\sigma\rangle$ es un subgrupo afín de S_n.

h) Demostrar que todo grupo afín es resoluble.

19. Sea G un subgrupo de S_n que seguimos viéndolo como el grupo de las biyecciones de $\mathbb{Z}_n$ y lo consideramos actuando en $\mathbb{N}_n$ de la forma habitual $\sigma \cdot n = \sigma(n)$ (ver Problema 3.3.23). 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:

a) G es transitivo si y sólo si hay una única G-órbita.

b) Si G es transitivo, entonces n es un divisor de $|G|$.

c) Si G es transitivo y N es un subgrupo normal de G, entonces cada N-órbita tiene un cardinal divisor de n.

d) 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 $i < n$.)

e) Demostrar que si p es primo y G es un subgrupo transitivo de S_p, entonces G es resoluble si y sólo si G es afín.

Capítulo 6

Extensiones de cuerpos

6.1. Extensiones de cuerpos

Definición 6.1. *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 se obtiene multiplicando en L ya que tanto los escalares como los vectores pertenecen a 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 $[L : K]$. 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 6.2.

1. Si L/K es una extensión de cuerpos, entonces $[L : K] = 1$ si y sólo 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 sólo 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.

Recuérdese 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 de 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 6.3. *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. Si L/K es una extensión de cuerpos y S es un subconjunto de L, entonces 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. □

Recordemos que si L/K es una extensión y S es un subconjunto de L, entonces $K[S]$ es 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 6.3 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 $a \in L$.

Lema 6.4. *Sea L/K una extensión. Si $\alpha \in L$ es una raíz de un polinomio irreducible p de $K[X]$ entonces*

1. *$K[\alpha] = K(\alpha)$.*
2. *Si $q \in K[X]$, entonces $q(\alpha) = 0$ si y sólo si p divide a q en $K[X]$.*
3. *$[K(\alpha) : K] = \mathrm{gr}(p)$.*
4. *Si $n = \mathrm{gr}(p)$ entonces $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)_K$.*

Demostración. 1 y 2. Consideremos el homomorfismo de sustitución $S = S_\alpha : K[X] \to L$ y sea $I = \mathrm{Ker}\ S = \{q \in K[X] : q(\alpha) = 0\}$. Como obviamente I es un ideal propio de $K[X]$ y α 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 (Proposiciones 1.55 y 2.13). Concluimos que $I = (p)$ y, del Primer Teorema de Isomorfía deducimos que $K[\alpha] = \mathrm{Im}\ S \simeq K[X]/(p)$, 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 sólo si $p|q$ en $K[X]$.

3 y 4. Supongamos que $n = \mathrm{gr}(p)$. Como 3 es una consecuencia inmediata de 4, basta demostrar que $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)_K$. Si $\beta \in K[\alpha]$, entonces $b = f(\alpha)$ para algún $f \in K[X]$.

Dividiendo f entre p (Lema 2.5) obtenemos $q, r \in K[X]$ tales que $f = qp + r$ y $m = \mathrm{gr}(r) < \mathrm{gr}(p) = n$. 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 α es raíz del polinomio $a = \sum_{i=0}^{n-1} a_i X^i$, es decir $a \in KerS = (p)$. Como $n = \mathrm{gr}(p) > \mathrm{gr}(a)$, deducimos que $a = 0$, es decir $a_i = 0$ para todo i. □

6.2. Adjunción de raíces

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

Teorema 6.5 (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 (Proposiciones 1.55 y 2.13). Entonces $L = K[X]/(p)$ es un cuerpo (Proposición 1.37). 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 α de p y $K(\alpha)$ es la menor subextensión de L/K que contiene a α.

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 6.6. *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 α en alguna extensión E de K. Entonces $p = (X - \alpha)q$ para algún $q \in E[X] \setminus E$. Por hipótesis e inducción q es completamente factorizable en alguna extensión L de E, es decir q es producto de polinomios de grado 1 en $L[X]$ y por tanto también p es producto de polinomios de grado 1. □

Como todo dominio es subanillo de su cuerpo de fracciones, los enunciados del Teorema de Kronecker (6.5) y del Corolario 6.6 pueden generalizarse asumiendo que K es un dominio, y sustituyendo las extensiones de cuerpos por extensiones de anillos de K a un cuerpo.

Recordemos que si $\sigma : K \to E$ es un homomorfismo de anillos, entonces σ 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 6.7. *Si $\sigma : E \to L$ es un homomorfismo de cuerpos y $\alpha \in E$ es raíz de $p \in E[X]$, 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 σ es un K-homomorfismo entonces σ 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 σ 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 6.8 (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 α_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 sólo si α_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, σ es un isomorfismo, entonces también $\widehat{\sigma}$ es un isomorfismo.

Demostración. Si existe el homomorfismo $\widehat{\sigma}$ satisfaciendo la propiedad indicada entonces del Lema 6.7 se tiene que $\alpha_2 = \widehat{\sigma}(\alpha_1)$ es una raíz de $\widehat{\sigma}(p) = \sigma(p)$.

Recíprocamente, supongamos que α_2 es una raíz de $\sigma(p)$. Consideremos los homomorfismos de sustitución en α_1 y α_2: $S_\alpha : K_1[X] \to K_1(\alpha_1)$ y $S_{\alpha_2} : K_2[X] \to K_2(\alpha_2)$. Por el Lema 6.4, $K_1[\alpha_1] = K_1(\alpha_1)$, $[K(\alpha_1) : K] = \mathrm{gr}(p)$ y $(p) = \mathrm{Ker}\, S_{\alpha_1}$. Además $\alpha_2 \in \mathrm{Ker}\ (\sigma(p))$. 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 $f_1(\alpha_1) = g(\alpha_1)$, 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 σ es un isomorfismo, entonces $\widehat{\sigma}$ es un isomorfismo pues todo homomorfismo de cuerpos es inyectivo y además K_2 y α_2 están en la imagen de $\widehat{\sigma}$, lo que muestra que $\widehat{\sigma}$ es suprayectivo.

Para la unicidad ver el Ejemplo 1 de 2.32. □

Si aplicamos el Lema anterior al caso en que σ es la aplicación identidad $\sigma : K \to K$ entonces obtenemos que si α 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 isomorfismos.

Proposición 6.9. *Sea $p \in K[X]$ un polinomio irreducible y α y β 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 6.9 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 6.9, 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 α es cualquier raíz de p es una extensión arbitraria de K.

6.3. Extensiones algebraicas

Definición 6.10. *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 α es* transcendente *sobre K. En otras palabras, α es transcendente sobre K si el homomorfismo de sustitución*

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

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

1. *α 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 α 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 α es una raíz de un polinomio irreducible de $K[X]$ y del Lema 6.4 se deduce que $K[\alpha] = K(\alpha)$ y que $K(\alpha)/K$ es finita.

2 implica 3 es obvia.

Para demostrar 3 implica 1 y 4 implica 1 consideramos el homomorfismo de sustitución $S = S_\alpha : K[X] \to K[\alpha]$. Si α 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. □

Sea L/K una extensión y $\alpha \in L$ un elemento 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 α sobre K, denotado $\mathrm{Irr}(\alpha, K)$, al único generador mónico de $I = \mathrm{Ker}\, S_\alpha$. Está claro que $\mathrm{Irr}(\alpha, K)$ es el único polinomio mónico de grado mínimo de I. Del Lema 6.4 se deduce que si $\mathrm{Irr}(\alpha, K)$ tiene grado n, entonces $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)/K$. En resumen:

Lema 6.12. *Si α es algebraico sobre K, entonces $[K(\alpha) : K] = \mathrm{gr}(\mathrm{Irr}(\alpha, K))$ y si este grado es n, entonces $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)_K$.*

Ejemplos 6.13.

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

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 α 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 $\mathrm{Irr}(\alpha, \mathbb{Q}) = X^4 - 10X + 20$.

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 π 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 6.11 es el siguiente corolario que caracteriza las extensiones finitas.

Corolario 6.14. *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 $\alpha \in L$. Del Lema 6.11 se deduce que α 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 α_i es algebraico sobre $K(\alpha_1, \ldots, \alpha_{i-1})$. Por tanto $K(\alpha_1, \ldots, \alpha_i) = K(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i)$ es una extensión finita de $K(\alpha_1, \ldots, \alpha_{i-1})$ por el Lema 6.11. Aplicando que la clase de extensiones finitas es multiplicativa deducimos que $L = K(\alpha_1, \ldots, \alpha_n)/K$ es finita. □

Corolario 6.15. *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 multiplicativas y sea $\alpha \in L$. Entonces α es algebraico sobre E. Sea $p = \mathrm{Irr}(\alpha, E)$ y sean $p_0, p_1, \ldots, p_n$ los coeficientes de p, que son algebraicos sobre K, por hipótesis, lo que implica que $F = K(p_0, p_1, \ldots, p_n)/K$ es finita, por el Corolario 6.14. Además, α 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 6.11 deducimos que α es algebraico sobre K. □

Corolario 6.16. *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.*

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 β 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 6.15. 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 $\alpha\beta^{-1} \in C$. 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 6.17. *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 6.16. Esto prueba que la clase de extensiones algebraicas es cerrada para levantamientos. Como una extensión es finita si y sólo si es algebraica y finitamente generada (Proposición 6.11) 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 6.3). Esta propiedad se verifica de hecho para toda extensión algebraica.

Proposición 6.18. *Si L/K es una extensión algebraica, entonces todo K-endomorfismo de L es un automorfismo.*

Demostración. Sea σ un K-endomorfismo de L. Como todo homomorfismo de cuerpos es inyectivo, sólo hay que probar que σ es suprayectivo. Sea $\alpha \in K$ y sean $p = \mathrm{Irr}(\alpha, K)$, $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ las raíces de p en L y $E = K(\alpha_1, \ldots, \alpha_n)$. Del Lema 6.7 se deduce que σ permuta $\{\alpha_1, \ldots, \alpha_n\}$ y por tanto $\alpha = \sigma(\alpha_i)$ para algún i. □

6.4. Problemas

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

1. Sea α 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. Calcular los grados y una base de las siguientes extensiones.

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

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

4. Hacer el ejercicio anterior cambiando $\mathbb{Q}$ por un cuerpo arbitrario.

5. 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 $K[X]$.

6. Calcular $[K(X)/K(p)]$, donde $p \in K[X]$ es un polinomio irreducible.

7. Demostrar que $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i+\sqrt{2})$. Calcular $\mathrm{Irr}(i+\sqrt{2}, \mathbb{Q})$, $\mathrm{Irr}(i+\sqrt{2}, \mathbb{Q}(i))$ e $\mathrm{Irr}(i+\sqrt{2}, \mathbb{Q}(\sqrt{2}))$.

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

9. 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 8.)

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

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

11. 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 $\mathrm{car}K = 2$.

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

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

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

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

16. 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 $K(\alpha)$.

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

18. 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:

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

    b) Si m es un entero positivo entonces existe un cuerpo de orden m si y sólo si m es una potencia de un primo.

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

    d) 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 $\mathbb{F}_p = \mathbb{Z}_p$.

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

20. 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 sólo si $n|m$.

21. 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 α de $\mathbb{F}_{64}$ verifican que $\mathbb{F}_2[\alpha] = \mathbb{F}_{64}$?

22. 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.

23. 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.

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

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

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

    a) Existe una extensión de K de grado mayor que 1.

    b) Existe una extensión algebraica de K de grado mayor que 1.

    c) Toda extensión simple es algebraica.

    d) Toda extensión es simple.

    e) Todas las extensiones transcendentes simples son isomorfas.

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

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

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

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

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

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

27. Demostrar las siguientes afirmaciones para E/K y F/K dos extensiones admisibles.

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

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

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

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

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

28. Para cada número entero n sea $\xi_n = e^{2\pi i} n = \cos\left(\frac{2\pi}{n}\right) + i \operatorname{sen}\left(\frac{2\pi}{n}\right)$.

    a) Calcular $\operatorname{Irr}(\xi_n, \mathbb{Q})$, para $n \leq 6$.

    b) Demostrar que si p es primo, entonces $\operatorname{Irr}(\xi_p, \mathbb{Q}) = 1 + X + X^2 + \cdots + X^{p-1}$.

    c) Encontrar todos los automorfismos de $\mathbb{Q}(\xi_6)$.

    d) ¿Existe un automorfismo de $\mathbb{Q}(\xi_5)$ que lleve ξ_5 a ξ_5^2?

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

30. Utilizando el Teorema de Lindeman que afirma que π 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 $\mathbb{Q}$.

31. Probar que L/K es algebraica si y sólo si para toda subextensión E de L/K, todo K-endomorfismo de E es un automorfismo.

Capítulo 7

Cuerpos de descomposición

7.1. Cuerpos algebraicamente cerrados

Una consecuencia inmediata del Teorema de Ruffini es la siguiente proposición.

Proposición 7.1. *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 algebraico 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, 3 implica 4 son obvios y 5 implica 6 es consecuencia inmediata de la Proposición 6.14.

4 implica 5. Supongamos que K contiene un subcuerpo K_0 satisfaciendo la propiedad 4. Si L/K es algebraica, entonces L/K_0 es también algebraica. Si $\alpha \in L$, entonces por hipótesis $p = \mathrm{Irr}(\alpha, K_0)$ 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 α de p. Entonces $K(\alpha)/K$ es finita por la Proposición 6.11. Por hipótesis $K(\alpha) = K$ y deducimos que α es una raíz de p en K. □

Se dice que un cuerpo K es *algebraicamente cerrado* cuando verifica las condiciones equivalentes de la Proposición 7.1.

Es fácil encontrar ejemplos de cuerpos que *no* son algebraicamente cerrados. Por ejemplo, considerando el polinomio $X^2 + 1$ vemos que no lo son $\mathbb{Q}$ ni $\mathbb{R}$, y el polinomio $X^2 + X + 1$ nos dice que $\mathbb{Z}_2$ tampoco lo es. 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 1). Sin embargo, se tiene:

Teorema 7.2 (Teorema Fundamental del Álgebra)**.** *El cuerpo $\mathbb{C}$ de los números complejos 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 podemos tomar $r = \dfrac{k + |a_0|}{|a_1|}$. En el caso general, 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 $|z| > r = \text{máx}\{s, 1\}$.

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 sólo 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, claramente, así que se trata de ver que la condición $a_0 \neq 0$ nos lleva a una contradicción.

En este caso, dividir 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

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

para cierto entero m con $1 \leq m \leq n$. Sea ahora ω 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. □

Del Teorema Fundamental del Álgebra se deduce que todo polinomio no constante con coeficientes en $\mathbb{Z}$, $\mathbb{Q}$ ó $\mathbb{R}$ tiene raíces en $\mathbb{C}$. De modo más general, es posible demostrar que todo polinomio sobre un cuerpo tiene raíces "en algún sitio". Recuérdese que una extensión de cuerpos no es más que un homomorfismo de anillos $f : K \to Q$, donde K y Q son cuerpos. Un tal f es necesariamente inyectivo, y esto permite ver a K, identificado con la imagen de f, como un subcuerpo de Q.

7.2. 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 6.6 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 tendría que ser completamente factorizables sobre L. En vista de esto es natural preguntarse si, todo cuerpo K tiene una extensión algebraicamente cerrada. Por otro lado tenemos

Proposición 7.3. *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 $p \in K[X]$, entonces p tiene una raíz α 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 7.4. *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 7.3).

Teorema 7.5. *Todo cuerpo tiene una clausura algebraica.*

Demostración. Por la Proposición 7.3, 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 $g_1p_1(X_{p_1})+\cdots+g_np_n(X_{p_n}) = 1$. Para simplificar la notación vamos a poner X_i en lugar de X_{p_i}, con lo que tenemos

$$g_1p_1(X_1) + \cdots + g_np_n(X_n) = 1 \tag{7.1}$$

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 α_i. Sustituyendo X_i por α_i en la ecuación (7.1) 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 1.38). 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 7.6. *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 σ.*

Demostración. Sea

$$\Omega = \left\{ (E, \tau) : \begin{array}{l} E/K \text{ es una subextensión de } F/K \text{ y} \\ \tau : F_1 \to L \text{ es un homomorfismo que extiende } \sigma \end{array} \right\}$$

y consideremos el siguiente orden en Ω:

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

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

Basta con demostrar que $F \subseteq E$. Sean $\alpha \in F$ y $p = \mathrm{Irr}(\alpha, E)$. Como L es algebraicamente cerrado, el polinomio $\sigma(f)$ tiene una raíz β en L. Del Lema 6.8 deducimos que existe un homomorfismo $\tau' : E(\alpha) \to L$ que extiende τ y tal que $\tau'(\alpha) = \beta$. Entonces $(E(\alpha), \tau') \in \Omega$ y $(E, \tau) \leq (E(\alpha), \tau')$. De la maximalidad de (E, τ) deducimos que $E = E(\alpha)$, es decir $\alpha \in E$. Esto prueba que $F \subseteq E$. □

El siguiente corolario del Teorema 7.6 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 7.7. *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 σ.*

Demostración. Por el Teorema 7.6 hay un homomorfismo $L_1 \to L_2$ que extiende σ. 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. □

7.3. Cuerpos de descomposición y Extensiones normales

Definición 7.8. *Sea 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 7.9. *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 σ.*

Demostración. Sean $\overline{K_1}$ y $\overline{K_2}$ clausuras algebraicas de K_1 y K_2 respectivamente y sean S_1 y S_2 las raíces de los elementos de $\mathcal{P}_1$ y $\mathcal{P}_2$ respectivamente. Del Corolario 7.7 se tiene que existe un isomorfismo $\overline{\sigma} : \overline{K_1} \to \overline{K_2}$, que extiende σ. Si $\alpha \in S_1$, entonces existe $p \in \mathcal{P}_1$ tal que α es raíz de p. Del Lema 6.7 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 7.10.

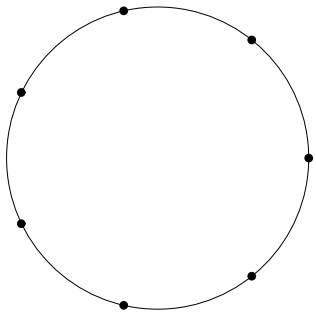
1. El cuerpo de descomposición de $X^2 - 2$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt{2})$ y el de $X^2 + 1$ es $\mathbb{Q}(i)$. Más generalmente, si $q \in \mathbb{Q}$, entonces el cuerpo de descomposición de $X^2 - q$ es $\mathbb{Q}(\sqrt{q})$.
2. El cuerpo de descomposición $X^3 - 1 = (X-1)(X^2+X+1)$ 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 ω^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

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

y están situadas en los vértices de un polígono regular de n lados inscrito en una circunferencia de radio 1.



Denotaremos

$$\xi_n = e^{\frac{2\pi ik}{n}}$$

y observamos que las raíces de $X^n - 1$ son las n potencias de ξ_n. Por tanto el cuerpo de descomposición de $X^n - 1$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\xi_n)$.

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 α, por las n raíces n-ésimas de la unidad. Por tanto el cuerpo de descomposición de $X^n - a$ es $\mathbb{Q}(\alpha, \xi_n)$ donde α es una raíz n-ésima arbitraria de a.

Una *extensión* de cuerpos L/K se dice que es *normal* si L es un cuerpo de descomposición sobre K de una familia de polinomios no constantes de K. El siguiente caracteriza las extensiones normales.

Teorema 7.11. *Las siguientes condiciones son equivalentes para una extensión L/K.*

1. *L/K es normal.*
2. *L es un cuerpo de descomposición sobre K de una familia de polinomios no constantes de K.*
3. *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, $\sigma \in \mathrm{Gal}(L/K)$.*
4. *L/K es algebraica y existe una clausura algebraica F de L que satisface 3.*
5. *L/K es algebraica y para todo $\alpha \in L$, el polinomio $\mathrm{Irr}(\alpha, K)$ factoriza completamente en L.*
6. *L/K es algebraica y todo polinomio irreducible p de $K[X]$ que contenga una raíz en L factoriza completamente en L.*

Demostración. La equivalencia entre 1 y 2 es la definición de extensión normal.

2 implica 3. 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 6.7 se deduce que σ permuta las raíces de cada elemento de $\mathcal{P}$ y por tanto $\sigma(S) = S$. Esto implica que σ es una automorfismo de L.

3 implica 4 es obvio.

4 implica 5. Supongamos que F es una clausura algebraica de L que satisface las condiciones de 4. Si $\alpha \in L$, entonces $p = \mathrm{Irr}(\alpha, K)$ 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 6.9 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 σ como un homomorfismo de $K(\alpha)$ en F y aplicar que la extensión $L/K(\alpha)$ es algebraica para concluir, con el Teorema 7.6, que σ se puede extender a un homomorfismo $L \to F$, que denotaremos también con σ. Por hipótesis $\alpha_i = \sigma(\alpha) \in L$ y concluimos que p factoriza completamente en L.

5 y 6 son equivalentes pues los polinomios irreducibles de $K[X]$ que tienen raíces en L son los de la forma $a\mathrm{Irr}(\alpha, K)$, con $0 \neq a \in K$ y $\alpha \in L$.

6 implica 2. 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 7.12. *Una extensión finitamente generada es normal si y sólo 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 $\prod_{i=1}^{n} \mathrm{Irr}(\alpha_i, K)$. □

Corolario 7.13. *Si L es una clausura algebraica de K entonces L/K es normal.*

Ejemplos 7.14.

1. Todas las extensiones que aparecen en los Ejemplos 7.10 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 $\mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$ 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 ω no lo es, deducimos que el polinomio $\mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q})$ 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 $p = \mathrm{Irr}(\alpha, K)$ 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. Por otro lado, 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 $p = \mathrm{Irr}(\sqrt[4]{2}, \mathbb{Q}) = X^4 - 2$ 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 7.14 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 7.15.

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. Supongamos que todos los E_i son subcuerpos de un cuerpo fijo 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 la 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 7.11, 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 7.11.

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 7.16 (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 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 7.15 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 $\alpha \in B$ sea $p_\alpha = \mathrm{Irr}(\alpha, K)$ y para cada $i = 1, 2$ sea $R_{i,\alpha}$ el conjunto de raíces de p_α 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_α, 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 7.9. Esto prueba 2 y también prueba 3 pues si L/K es finita, entonces B es finita y por tanto $\cup_{\alpha\in B} R_{i,\alpha}$ es finito, con lo que cada N_i/K es una extensión finita. □

7.4. Problemas

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

a) Todo cuerpo algebraicamente cerrado es infinito.

b) 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).

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

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

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

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

5. Sea K un cuerpo arbitrario y α 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.

6. Calcular un cuerpo de escisión L sobre K y $[L : K]$ de cada uno de los siguientes polinomios, para $K = \mathbb{Z}_2$ y $\mathbb{Z}_3$:

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

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 $\mathbb{Q}$.

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

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 sólo si a, b y ab no son cuadrados en K.

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

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.

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 $[N : K]$:

$$\mathbb{Q}(\sqrt[3]{2}), \;\; \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5}), \;\; \mathbb{Q}(\sqrt[8]{2}, \sqrt{3}), \;\; \mathbb{Q}(\xi_5), \;\; \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots).$$

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

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 sólo si $\sigma(L) \subseteq L$ para todo K-automorfismo σ de N.

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 $n!$.

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

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

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

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

18. Demostrar que toda extensión de cuerpos finitos es normal.

19. Sea N/K una extensión normal, $p \in K[X]$ irreducible y 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 8

Extensiones ciclotómicas

8.1. Raíces de la unidad

Como cualquier polinomio, el polinomio $X^n - 1$ es completamente factorizable en algún cuerpo. Las raíces de $X^n - 1$ 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 0 o no es divisor de n, 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 p tiene n raíces distintas. 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 8.1. *Consideremos $X^n - 1$ como un polinomio con coeficientes en un cuerpo K.*

1. *Si la característica de K es 0 o un primo p que no divide a n, 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 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 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 8.2. *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 3.22) 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 sólo si n no es múltiplo de la característica. Como consecuencia inmediata de (3.2) se deduce

Lema 8.3. *Si ξ es una raíz n-ésima primitiva de la unidad, entonces ξ^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 ξ^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 $\phi(n)$ raíces n-ésimas primitivas de la unidad, donde $\phi(n) = |\mathbb{Z}_n^*|$, es decir, ϕ es la Función de Euler (ver el Ejercicio 8 del Capítulo 3.

8.2. Extensiones ciclotómicas

Definición 8.4. *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 7.9).*

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

Sean $\xi_1, \ldots, \xi_r$ las raíces n-ésimas primitivas de la unidad (e implícitamente estamos suponiendo que la característica no divide a n), 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.

Proposición 8.5. *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. $\mathrm{gr}(\Phi_n) = \phi(n) = |\mathbb{Z}_n^*|$.
2. $X^n - 1 = \prod_{d|n} \Phi_d$.
3. $\Phi_n \in P[X]$.
4. *Si ξ es una raíz de la unidad en una extensión de K, entonces* $\mathrm{Irr}(\xi, K) \in P[X]$.

Demostración. 1 es consecuencia del Lema 8.3.

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 G 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 $\Phi_1 = X - 1 \in P[X]$. Si $n > 1$ y suponemos 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 Φ_n es un polinomio mónico de $\mathbb{Q}[X]$. Eso implica que existe un entero a tal que $a\Phi_n$ es primitivo. Eso implica que $a(X^n - 1) = (a\Phi_n)q$ es primitivo, lo que implica que $a = \pm 1$, y por tanto $\Phi_n \in \mathbb{Z}[X]$. □

La Proposición 8.5 proporciona un método recursivo para calcular Φ_n como muestra el siguiente ejemplo.

Ejemplo 8.6. $\Phi_1 = 1$, $\Phi_2 = \frac{X^2-1}{\Phi_1} = \frac{X^2-1}{X-1} = X + 1$, $\Phi_3 = \frac{X^3-1}{\Phi_1} = \frac{X^3-1}{X-1} = X^2 + X + 1$, $\Phi_4 = \frac{X^4-1}{\Phi_1\Phi_2} = \frac{X^4-1}{(X-1)(X+1)} = X^2 + 1$.

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:

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

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

Teorema 8.7. *Los polinomios ciclotómicos en característica* 0 *son irreducibles sobre* $\mathbb{Q}$.

Demostración. Fijemos una raíz n-ésima primitiva de la unidad ξ y sea $f = \mathrm{Irr}(\xi, \mathbb{Q})$. Tenemos que demostrar que $\Phi = \Phi_n$ es irreducible y, como ξ es raíz de Φ y Φ 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 ξ^r con $\mathrm{mcd}(r, n) = 1$) es raíz de p.

Supondremos primero que $r = p$ es primo. Sea $g = \mathrm{Irr}(\xi^p, \mathbb{Q})$. Como ξ^p es raíz de g, ξ es raíz de $g(X^p)$ y por tanto f divide a $g_1 = g(X^p)$ en $\mathbb{Q}[X]$ y como $g_1 \in \mathbb{Z}[X]$, del Lema de Gauss, y de que tanto f como g_1 son mónicos deducimos que f divide a g_1 en $\mathbb{Z}[X]$. Pongamos $g_1 = fg_2$. Considerando el la proyección canónica $\mathbb{Z} \to \mathbb{Z}_p$, que extendemos de forma canónica a $\mathbb{Z}[X] \to \mathbb{Z}_p[X]$. 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 ξ^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 $\mathrm{Irr}(\eta, \mathbb{Q}) = f$. Aplicando ahora el caso visto en el párrafo anterior a η, deducimos que $\xi^r = \eta^{p_k}$ es raíz de f. □

Corolario 8.8. *Si ξ es una raíz n-ésima primitiva de la unidad en característica 0, entonces $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(n)$.*

Ejercicio 8.9. *El Teorema 8.7 no se verifica en característica positiva. Por ejemplo, en característica 2 tenemos $\Phi_7 = 1 + X + X^2 + X^3 + X^4 + X^5 + X^6 = (X^3 + X + 1)(X^3 + X^2 + 1)$.*

8.3. Problemas

Para cada entero positivo, ξ_n denota una raíz n-ésima primitiva de la unidad la clausura algebraica del cuerpo considerado.

1. Calcular Φ_n para todos los números enteros entre 1 y 16.
2. Dar una fórmula general para Φ_{2p} para p un número primo.
3. Demostrar que si n es par, entonces $\mathbb{Q}(\xi_n)$ tiene exactamente n raíces de la unidad y en caso contrario tiene $2n$. ¿Cuáles son las las raíces de la unidad en cada caso?
4. Demostrar que si $n \leq m$, entonces $\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_m)$ si y sólo si $n = m$ ó n es impar y $m = 2n$.
5. Demostrar que si p es un número primo y $\alpha^{p^{n-1}} = \xi_p$ entonces que α es una raíz p^n-ésima primitiva de la unidad.
6. Calcular las raíces de la unidad que pertenecen a $\mathbb{Q}(\sqrt{d})$ donde d es un número entero.
7. Demostrar las siguiente igualdades para $\xi = \xi_n$.
   a) $\prod_{i=0}^{n-1}(X - \xi^i) = X^n - 1$.
   b) $\sum_{i=0}^{n-1} \xi^i = 0$.
   c) $\prod_{i=1}^{n-1}(1 - \xi^i) = n$.
   d) $\prod_{i=1}^{n-1}(1 + \xi^i) = \begin{cases} 0 & \text{si } 2|n \\ 1 & \text{si } 2 \nmid n \end{cases}$.
8. Sean m y n dos números naturales y $d = \mathrm{mcd}(m, n)$. Demostrar que Φ_m es el producto de $\phi(d)$ polinomios irreducibles de $\mathbb{Q}(\xi_n)$ de grado $\phi(m)/\phi(d)$.
9. Demostrar que $F_n = \mathbb{Q}(\xi_n) \cap \mathbb{R} = \mathbb{Q}(\xi_n + \xi_n^{-1}) = \mathbb{Q}(\cos \frac{2\pi}{n})$. Calcular $[\mathbb{Q}(\xi_n) : F_n]$ e $\mathrm{Irr}(\xi_n, F_n)$ en función de n.
10. Demostrar que toda extensión de cuerpos finitos es una extensión ciclotómica.
11. Sea $\mathbb{F} = \mathbb{F}_q$ un cuerpo finito de cardinal q y n un número natural coprimo con q. Demostrar
    a) $[\mathbb{F}(\xi_n) : \mathbb{F}]$ es el menor entero positivo r tal que $q^r \equiv 1 \bmod n$.

b) Demostrar que Φ_n (el n-ésimo polinomio ciclotómico en característica p) es el producto de $\phi(n)/r$ polinomios de grado r, donde r es como en *a*).

c) Si n es primo, entonces $\mathrm{Irr}(\xi_n, \mathbb{F}) = 1 + X + X^2 + \cdots + X^{n-1}$ si y sólo si n no divide a $\prod_{i=1}^{n-2}(q^i - 1)$.

(Indicación: Aplicar propiedades de los grupos cíclicos.)

12. 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 $X^{q^n} - X = \prod_{d|n} \prod_{p \in I_d} p$.

13. 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 $[\mathbb{Q}(\sqrt[n]{p}, e^{2\pi i/n}) : \mathbb{Q}(\sqrt[n]{p})]$.

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

15. Sea $\xi = \xi_p \in \mathbb{Q}$, con p primo y sea λ un generador de $\mathbb{Z}_p^*$. Para cada $i \in \mathbb{Z}_p^*$, sea $\epsilon_i = \xi^{\lambda^i}$. Demostrar

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

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

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

d) 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*.

16. Demostrar las siguientes propiedades de los polinomios ciclotómicos Φ_n.

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

b) $\Phi_n(X) = \Phi_{p_1 \cdots p_s}(X^{p_1^{r_1-1} \cdots p_s^{r_s-1}})$, 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.

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

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

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

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

17. Sea p un número primo impar. Para cada entero n, ponemos

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

Demostrar:

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

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

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

d) Si $\xi = \xi_p$ es una raíz p-ésima primitiva de la unidad en $\mathbb{C}$ y

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

entonces

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

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

f) $\mathbb{Q}(\sqrt{p})$ está contenido en $\mathbb{Q}(\xi_{4p})$.

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

Capítulo 9

Extensiones separables

9.1. Grado de separabilidad

Definición 9.1. *Sea 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_σ^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_σ^E no debe de depender de L ni de σ.

Proposición 9.2. *Si E/K es una extensión algebraica entonces el cardinal S_σ^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_σ^E no se ve afectado si cambiamos L por está clausura algebraica, que también es algebraicamente cerrada por la Proposición 7.3. 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 7.7, existe un isomorfismo $\lambda : L \to L'$ tal que $\lambda(\sigma(k)) = \sigma'(k)$ para todo $k \in K$. La aplicación de S_σ^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_σ^E no depende del cuerpo algebraicamente cerrado L □

Ejemplo 9.3. Supongamos que α es algebraico sobre K y sea L una clausura algebraica de K que contenga a α. Sea $p = \mathrm{Irr}(\alpha, K)$. Por el Lema de Extensión (Lema 6.8) 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 β 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.

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

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

Proposición 9.4 (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_σ^F es una extensión de un elemento de S_σ^E, a saber de su restricción a E, se tiene que $S_\sigma^F = \cup_{\tau \in S_\sigma^E} S_\tau^F$. Claramente los conjuntos S_τ^F son disjuntos y por otro lado de la Proposición 9.2 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 9.5. *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 φ 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. Ejercicio. □

Lema 9.6 (Uniformidad de la Multiplicidad)**.** *Si $f \in K[X]$ es irreducible, entonces todas las raíces de f (en un cuerpo de descomposición de f) tienen la misma multiplicidad. Además*

1. *Si $\mathrm{car}K = 0$ entonces f no tiene raíces múltiples.*
2. *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 sólo 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. Sean $\alpha_1, \ldots, \alpha_n$ las raíces de f y sea m_i la multiplicidad de α_i como raíz de f. Fijemos $\alpha = \alpha_1$ y $m = m_i$. Por el Lema de Extensión, existe un K-isomorfismo $\sigma_j : K(\alpha) \to K(\alpha_j)$ tal que $\sigma_j(\alpha) = \alpha_j$. Por tanto

$$\prod_{i=1}^{n}(X - \alpha_i)^{m_i} = f = \sigma(f) = \prod_{i=1}^{n}(X - \sigma_j(\alpha_i))^{m_j}$$

De la unicidad de la factorización deducimos que m_j = multiplicidad de α_j, en la expresión de la izquierda = Multiplicidad de $\sigma_j(\alpha) = \alpha_j$ es la expresión de la izquierda = m.

Como $\mathrm{gr}(f') < \mathrm{gr}(f)$, se tiene que $f | f'$ si y sólo si $f' = 0$. Si $\mathrm{car}K \neq 0$, entonces $f' \neq 0$ y por tanto f no divide a f' lo que implica que $\mathrm{mcd}(f, f') = 1$ y por tanto f no tiene raíces múltiples. Si $\mathrm{car}K = p > 0$, entonces $f' = 0$ si y sólo si $f_i = 0$ para todo $i \in \mathbb{N}$ que no sea múltiplo de p (recuérdese la notación $f = \sum_i f_i X^i$) si y sólo si $f = g(X^p)$ para algún $g \in K[X]$. Como $\mathrm{gr}(g(X^p)) = p\mathrm{gr}(g) > \mathrm{gr}(g)$, existe un número $n \geq 0$ tal que $f = g(X^{p^n})$ y f no se puede poner en la forma $g(X^{p^{n+1}})$. 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, $\alpha_1^{p^n}, \ldots, \alpha_k^{p^n}$ son raíces de g y todas son distintas,

por el Lema 9.5. 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 γ es una raíz de $(X^{p^n} - \beta_1) \cdots (X^{p^n} - \beta_l)$, entonces γ es una raíz de f y por tanto $\gamma = \alpha_i$ para algún $i = 1, \ldots, k$ y $\gamma^{p^n} = \beta^{p^n}$ algún $j = 1, \ldots, l$. Eso implica que $\alpha_i = \gamma_i = \beta_j$, en contra de que los α y los β 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 9.7. *Si $f \in K[X]$ entonces se llama* grado de separabilidad *de f 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

$$\mathrm{gr}(f) = \mathrm{gr}_s(f)\mathrm{gr}_i(f) \tag{9.1}$$

Del Ejemplo 9.3 se deduce que

Proposición 9.8. *Si α es algebraico sobre K, entonces $[K(\alpha) : K]_s = \mathrm{gr}_s(\mathrm{Irr}(\alpha, K))$.*

Proposición 9.9. *Si E/K es una extensión finita de cuerpos, entonces $[E : K]_s$ es un entero positivo que divide a $[E : K]$.*

Demostración. Que $[L : K]_s$ es positivo quiere decir que todo homomorfismo $K \to L$, con L algebraicamente cerrado se extiende a un homomorfismo $E \to L$, lo cual ya lo vimos en el Teorema 7.6. Para demostrar que $[E : K]_s$ divide a $n = [E : K]$ razonamos por inducción sobre n, con el caso $n = 1$ trivial. Supongamos que $n > 1$ y la hipótesis de inducción. Sea $\alpha \in L \setminus K$. Entonces $[L : K(\alpha)] < n$ y, por la hipótesis inducción, $[L : K(\alpha)]_s$ divide a $[L : K(\alpha)]$. Pongamos $k = [L : K(\alpha)]/[L : K(\alpha)]_s$. Si $p = \mathrm{Irr}(\alpha, K)$, entonces aplicando la Proposición 9.8 y la fórmula (9.1) se deduce que

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

□

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

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

9.2. Extensiones separables

Definición 9.10. *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 α es un elemento *de una extensión L de K entonces se dice que α es* separable *sobre K si es algebraico y* $\mathrm{Irr}(\alpha, K)$ *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 sólo si $\mathrm{gr}_s(f) = \mathrm{gr}(f)$ si y sólo si $\mathrm{gr}_i(f) = 1$. Por otro lado como consecuencia del Lema 9.6 se tiene:

Proposición 9.11. *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 9.8 se deduce que un elemento algebraico α sobre K es separable si y sólo si $[K(\alpha) : K] = [K(\alpha) : K]_s$ si y sólo si $[K(\alpha) : K]_i = 1$.

Teorema 9.12. *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 9.4) 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 α 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 $\mathrm{Irr}(\beta, K(\alpha))$ divide a $\mathrm{Irr}(\beta, K)$, 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 α es separable sobre K se tiene que $[K(\alpha) : K] = [K(\alpha)_s : K]$. 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 9.12 y de las propiedades multiplicativas de los grados es el siguiente

Corolario 9.13. *La clase de extensiones separables es multiplicativa.*

Veamos más consecuencias del Teorema 9.12.

Corolario 9.14. *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 α_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 α. Pero esto está claro pues si α es separable sobre K, entonces $[K(\alpha) : K] = [K(\alpha) : K]_s$, es decir $K(\alpha)/K$ es separable. □

Una consecuencia inmediata del Corolario 9.14 es el siguiente

Corolario 9.15. *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

Un último corolario

Corolario 9.16. *La clase de extensiones separables es cerrada para levantamientos.*

Demostración. Sean E/K y E/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 9.14 deducimos que $EF = F(E)/F$ es separable. □

Finalmente

Proposición 9.17. *Si L/K es una extensión finita y S es la clausura separable de L/K entonces $[L : K]_s = [S : K]$.*

9.3. Elementos primitivos

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

Lema 9.18. *Sean α y β 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 $\alpha \in E$. □

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 9.19 (Artin)**.** *Una extensión finita L/K es simple si y sólo 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 8.2) y si α 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 9.18, deducimos que para todo $\alpha, \beta \in L$ existen dos elementos distintos a y b de K tales que $K(\alpha + a\beta) = K(\alpha + b\beta)$, lo que implica 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 $p_E = \mathrm{Irr}(\alpha, E)$. 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 el producto de algunos de los polinomios $X - \alpha_1, \ldots, X - \alpha_n$. Además $E \mapsto p_K$ 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, si $E \in \mathrm{Sub}(L/K)$ y F es el elemento de $\mathrm{Sub}(L/K)$ generado sobre K por los coeficientes de p_E, $p_E \in F[X]$ 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. □

Corolario 9.20 (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 $L = K(\alpha_1, \ldots, \alpha_n)$. Sea σ la inclusión de K en una clausura algebraica de L y sea $S = S_\sigma^{K(\alpha_1, \alpha_2)} = \{\sigma_1, \ldots, \sigma_m\}$. 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 $n \leq [K(\beta) : K]_s = [K(\beta) : K] \leq [K(\alpha_1, \alpha_2) : K] = [K(\alpha_1, \alpha_2) : K]_s \leq n$. 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. □

9.4. Problemas

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 $\mathbb{Q}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_7$.

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

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

   b) Toda extensión separable en normal.

   c) Toda extensión normal es separable.

d) Toda extensión de cuerpos finitos es separable.

e) Toda extensión finita es separable.

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

g) 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.

h) 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.

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

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

4. Demostrar que las siguientes condiciones son equivalentes para un cuerpo K y un elemento α algebraico sobre K.

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

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

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

   Se dice que α es *puramente inseparable* sobre K si es algebraico sobre K y se verifican las condiciones anteriores.

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

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.

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

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

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).

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 $0^0 = 1$.)

11. Sea L/K una extensión algebraica. Demostrar que existen subextensiones S y P de L/K tales que S/K y L/P son separables y L/S y P/K son puramente inseparables. Demostrar también que si E es una subextensión de L/K, entonces

    a) L/E es puramente inseparable si y sólo si $S \subseteq E$.

    b) L/E es separable si y sólo si $P \subseteq E$.

    c) Si $E \cap S = K$ si y sólo si $E \subseteq P$.

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

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 $L \neq SP$.

14. Demostrar que las siguientes condiciones son equivalentes para un cuerpo K.

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

    b) Toda extensión algebraica de K es separable.

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

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

15. Demostrar:

    a) Todo cuerpo finito es perfecto.

    b) Si K es perfecto y L/K es una extensión algebraica, entonces L es perfecto.

    c) Si L es perfecto y L/K es una extensión separable, entonces K es perfecto.

    d) Si L es perfecto y L/K es una extensión finita, entonces K es perfecto.

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

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

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

    Demostrar que

$$K \subseteq \sqrt[p]{K} \subseteq \sqrt[p]{\sqrt[p]{K}} \subseteq \ldots$$

    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.

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

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

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

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.

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 α y β 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.

23. Sea $p \in K[X]$ de grado n. Demostrar que si la característica de K no divide a $n!$ entonces p es separable sobre K.

Capítulo 10

Extensiones de Galois

10.1. 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 10.1. 1. Claramente $\mathrm{Gal}(K/K) = 1$. De hecho no son estos los únicos ejemplos de 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 ω es una raíz tercera primitiva de la unidad. Como ω no es un número real, la única raíz de p que pertenece a $K(\alpha)$ es α 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 $p = \mathrm{Irr}(\alpha, K)$ 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 $q = \mathrm{Irr}(\beta, K) = X^2 - c$ 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. (¿Estás seguro de que tiene dos?).

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

3. En el Ejercicio 19 del Capítulo 1 se vio que el único automorfismo de $\mathbb{R}$ es la identidad con lo que $\mathrm{Gal}(\mathbb{R}/K) = 1$ para todo subcuerpo K de $\mathbb{R}$.

4. Sea $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 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 12 del Capítulo 6). 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 $\xi = \xi_n$ 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 σ 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 ψ

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 $\mathrm{Irr}(\xi, \mathbb{Q}) = \Psi_n$, el n-ésimo polinomio ciclotómico (Teorema 8.7). 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 τ_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 9.9 deducimos:

Proposición 10.2. *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 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 1.15) 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

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

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

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

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

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

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

Proposición 10.3. *La correspondencia de Galois $(-)'$ de una extensión de cuerpos L/K satisface las siguientes propiedades:*

1. *$L' = 1$ y $K' = G = \mathrm{Gal}(L/K)$.*
2. *$(-)' = \mathrm{Gal}(L/-)$ y $(-)' = L^{(-)}$ son antihomomorfismos.*
3. *$1' = L$ (donde 1 es el subgrupo trivial de $\mathrm{Gal}(L/K)$.*
4. *$X \subseteq X''$ y $X' = X'''$, tanto si $X \in \mathrm{Sub}(L/K)$ como si $X \in \mathrm{Sub}(\mathrm{Gal}(L/K))$.*
5. *Las dos aplicaciones que forman la correspondencia de Galois inducen un anti-isomorfismo de conjuntos ordenados entre sus dos imágenes.*

Demostración. 1, 2, 3 y la inclusión $X \subseteq X''$ son sencillos ejercicios. Por tanto $X \subseteq X''$ y $X' \subseteq X'''$, y de 2 se deduce que $X''' \subseteq X'$. Lo que prueba la igualdad de 4. Finalmente 5 es consecuencia inmediata de 2 y la igualdad de 4. □

Los elementos de las imágenes de las dos aplicaciones de la correspondencia de Galois se dice que son respectivamente *subcuerpos cerrados* en L/K o *subgrupos cerrados* en $\mathrm{Gal}(L/K)$ o en L/K. Obsérvese que de la propiedad 4 de la Proposición 10.3 se tiene que

X es cerrado si y sólo si $X = X''$.

y la propiedad 5 se puede reescribir como

Corolario 10.4. *Las aplicaciones de la correspondencia de Galois de una extensión de cuerpos L/K se restringen a un anti-isomorfismo de conjuntos ordenados entre los subcuerpos 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 10.1) entonces $K'' = 1' = L \neq K$.

Proposición 10.5. *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 $[E_1' : E_2'] \leq [E_2 : E_1]$.*
2. *Si $H_1 \leq H_2$ son subgrupos de $\mathrm{Gal}(L/K)$ con $[H_2 : H_1] < \infty$, entonces $[H_1' : H_2'] \leq [H_2 : H_1]$.*

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 $\alpha \in E_2 \setminus E_1$, $p = \mathrm{Irr}(\alpha, E_1)$ y $s = \mathrm{gr}(p) > 1$. Entonces $[E_2 : E_1(\alpha)] < n$. Si $s < n$, entonces por la hipótesis de inducción tenemos

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

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

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 $[H_1' : H_2'] > n$. Entonces existen $\alpha_1, \ldots, \alpha_n, \alpha_{n+1} \in H_1'$, linealmente independientes sobre H_2'. 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 α_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 α_i son linealmente independientes sobre H_2' existe $1 \leq i \leq r$ tal que $a_i \notin H_2'$. Reordenando $a_1, \ldots, a_r$ podemos suponer que $a_1 \notin H_2'$, 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 10.6. *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 $[E_1' : E_2'] = [E_2 : E_1]$.*

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_2 cerrado en L/K entonces H_1 es cerrado en L/K y $[H_1' : H_2'] = [H_2 : H_1]$.*

Demostración. 1. Aplicando el primer apartado de la Proposición 10.5 a $E_1 \leq E_2$ obtenemos que $[E_1' : E_2'] \leq [E_2 : E_1]$ y aplicando el segundo apartado a $E_2' \subseteq E_1'$ obtenemos $[E_2'' : E_1''] \leq [E_1' : E_2']$. Como E_1 es cerrado tenemos que $[E_2'' : E_1] = [E_2'' : E_1''] \leq [E_2 : E_1]$ y como $E_2 \subseteq E_2''$, concluimos que $E_2 = E_2''$, es decir E_2'' es cerrado.

2. Es completamente análoga. □

10.2. Extensiones de Galois

Definición 10.7. *Una* extensión de Galois *es una extensión de cuerpos que es normal y separable.*

La siguiente proposición es consecuencia inmediata de las Proposiciones 7.15 y 9.16.

Proposición 10.8. *La clase de extensiones de Galois es cerrada para levantamientos.*

El siguiente Teorema caracteriza las extensiones de Galois.

Teorema 10.9. *Las siguientes condiciones son equivalentes para una extensión de cuerpos 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 $\sigma(\alpha) \neq \alpha$. En otras palabras $L^{\mathrm{Gal}(L/K)} = K$.*

Demostración. 1 implica 2 es consecuencia de la Proposición 10.8.

2 implica 3. Supongamos que L/K satisface 2 y sea $E \in \mathrm{Sub}(L/K)$. De la Proposición 10.3 se tiene que $E \subseteq E''$ 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 $p = \mathrm{Irr}(\alpha, E)$ 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 β también es raíz de p. De la Proposición 6.9 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 $L/E(\alpha)$) σ se extiende a un homomorfismo $L \to \overline{L}$, que también denotaremos por σ, 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 y 4 implica 5 son obvios.

5 implica 1. Supongamos que L/K verifica 5. Sea $\alpha \in L$ y sean $p = \mathrm{Irr}(\alpha, K)$ 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 σ 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 α 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 10.10. *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. *$[L : E] = |\mathrm{Gal}(L/E)|$ para todo $E \in \mathrm{Sub}(L/K)$.*

Demostración. 1 implica 3. Supongamos que L/K es de Galois y sea $E \in \mathrm{Sub}(L/K)$. Entonces L/E es de Galois (Teorema 10.10). De que L/E sea normal se deduce que si $\overline{L}$ es una clausura algebraica de E, entonces $\mathrm{Gal}(L/E)$ coincide con el conjunto S_1^L de extensiones de la inclusión $E \to \overline{L}$ a un homomorfismo $L \to \overline{L}$, con lo que $|\mathrm{Gal}(L/E)| = |S_1^L| = [L:E]_s$ y este número coincide con $[L:E]$ por ser L/E separable.

3 implica 2 es obvio.

2 implica 1. Supongamos que $|\mathrm{Gal}(L/K)| = [L:K]$. De la Proposición 10.3 tenemos $[L:K] = |\mathrm{Gal}(L/K)| = |\mathrm{Gal}(L/K'')| \leq [L:K''] \leq [L:K]$ y como $K \subseteq K''$ deducimos que $K = K''$, es decir K es cerrado en L/K y por tanto L/K es de Galois (Teorema 10.10). □

Teorema 10.11 (Teorema Fundamental de la Teoría de Galois)**.** *Si L/K una extensión de Galois finita entonces se verifican las siguientes propiedades:*

1. *Si $E \in \mathrm{Sub}(L/K)$ entonces $[L:E] = |\mathrm{Gal}(L/E)|$ y $[E:K] = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/E)|}$.*
2. *La correspondencia de Galois es un anti-isomorfismo de conjuntos ordenados entre $\mathrm{Sub}(L/K)$ y $\mathrm{Sub}(\mathrm{Gal}(L/K))$.*
3. *Si $E \in \mathrm{Sub}(L/K)$ entonces las siguientes condiciones son equivalentes:*
   a) *E/K es de Galois.*
   b) *E/K es normal.*
   c) *$\sigma(E) \subseteq E$ para todo $\sigma \in \mathrm{Gal}(L/K)$.*
   d) *$\mathrm{Gal}(L/E)$ es normal en $\mathrm{Gal}(L/K)$.*

   Además, si estas condiciones se satisfacen, entonces

$$\mathrm{Gal}(E/K) \simeq \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(E/K)}.$$

Demostración. Sea $G = \mathrm{Gal}(L/K)$.

1. Sea $E \in \mathrm{Sub}(L/K)$, entonces L/E es de Galois y por tanto $[L:E] = \mathrm{Gal}(L/E)$ (Teorema 10.9) de donde se deduce que

$$[E:K] = \frac{[L:K]}{[L:E]} = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/E)|}.$$

2. A la vista de la Proposición 10.3 y el Teorema 10.9 para demostrar 1, sólo falta demostrar que todo subgrupo H de G es cerrado, pero eso es consecuencia inmediata del Corolario 10.6.

3. La equivalencia entre (a) y (b) es consecuencia inmediata de que la clase de extensiones separables es multiplicativa (Proposición 9.13).

(b) implica (c) Supongamos que E/K es normal y sean $\alpha \in E$ y $\sigma \in \mathrm{Gal}(L/K)$. Entonces $p = \mathrm{Irr}(\alpha, K)$ es completamente factorizable en E, pongamos $p = (X-\alpha_1)\cdots(X-\alpha_n) \in K[X]$. 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 $\sigma \in \mathrm{Gal}(L/K)$ y $\tau \in \mathrm{Gal}(L/E)$. Entonces $\sigma(E) \subseteq E$ y por tanto $\tau\sigma(\alpha) = \sigma(\alpha)$, para todo $\alpha \in E$. Esto prueba que $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/E)$.

(d) implica (a) Supongamos que $\mathrm{Gal}(L/E)$ es normal en $\mathrm{Gal}(L/K)$. Queremos demostrar que E/K es de Galois, o lo que es lo mismo que $\mathrm{Gal}(E/K)' \subseteq K$. Sea $\alpha \in \mathrm{Gal}(E/K)'$. Si demostramos que $\sigma(\alpha) = \alpha$ para todo $\sigma \in \mathrm{Gal}(L/K)$, entonces aplicando que L/K es de Galois concluimos que $\alpha \in K$ como deseamos. Por hipótesis, $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/E)$ para todo $\tau \in \mathrm{Gal}(L/E)$, con lo que $\tau\sigma(e) = \sigma(e)$, para todo $e \in E$ y todo $\tau \in \mathrm{Gal}(L/E)$. Esto muestra que $\sigma(e) \in \mathrm{Gal}(L/E)' = E'' = E$, es decir $\sigma \in \mathrm{Gal}(E/K)$ y como $\alpha \in \mathrm{Gal}(E/K)'$, deducimos que $\sigma(\alpha) = \alpha$, como queríamos demostrar.

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 σ a L pertenece a $\mathrm{Gal}(L/K)$ y la aplicación

$$\begin{array}{rcl} Res_L^F : \mathrm{Gal}(F/K) & \to & \mathrm{Gal}(L/K) \\ \sigma & \mapsto & \sigma_L \end{array}$$

es un homomorfismo de grupos. Además, si E es otra subextensión de F/K, entonces Res se restringe a un homomorfismo

$$Res : \mathrm{Gal}(LE/E) \to \mathrm{Gal}(L/L \cap E).$$

Teorema 10.12 (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*

$$Res : \mathrm{Gal}(LE/E) \to \mathrm{Gal}(L/L \cap E)$$

es un isomorfismo de grupos.

Demostración. Como L/K es de Galois, del Teorema 10.9 se deduce que $L/L \cap E$ también es de Galois y de la Proposición 10.8 que lo es LE/E. Que la primera es finita es obvio y que lo sea la segunda es consecuencia de la Proposición 6.17. Que Res sea inyectiva es obvio ya que un elemento del núcleo es un automorfismo σ de LE que verifica $\sigma(x) = x$ para todo $x \in L$ y todo $x \in E$. Finalmente, si $H = \mathrm{Im}\ Res$, entonces $L \cap E = \mathrm{Gal}(L/L \cap E)' \subseteq H'$. Por otro lado, si $\alpha \in H'$, entonces para todo $\sigma \in \mathrm{Gal}(LE/E)$ se verifica $\sigma(\alpha) = \sigma_L(\alpha) = \alpha$, con lo que $\alpha \in \mathrm{Gal}(LE/E)' = E$. Eso prueba que $H' \subseteq L \cap E$. En resumen $L \cap E = H'$ y del Teorema Fundamental de la Teoría de Galois se deduce que $\mathrm{Gal}(L/L \cap E) = (L \cap E)' = H'' = H$, es decir Res es suprayectiva. □

10.3. Problemas

1. Demostrar que toda extensión de grado 2 es de Galois y encontrar una extensión de grado 3 que no sea de Galois.

2. Sea L un cuerpo, G un subgrupo 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 $G = \mathrm{Gal}(L/K)$.

3. 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 2.5. Demostrar

a) 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 $\overline{\sigma}$.

b) $K(X_1, \ldots, X_n)/K(S_1, \ldots, S_n)$ es una extensión de Galois.

c) 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.

4. Sea L/K una extensión finita de Galois y sean E y F subextensiones de L/K. Demostrar que

$$\mathrm{Gal}(L/EF) = \mathrm{Gal}(L/E) \cap \mathrm{Gal}(L/F) \quad \mathrm{Gal}(L/E \cap F) = \langle \mathrm{Gal}(L/E) \cup \mathrm{Gal}(L/F) \rangle.$$

5. Sea $\alpha = \sqrt{5 + 2\sqrt{5}}$.

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

b) Demostrar que $\sqrt{5 - 2\sqrt{5}} \in \mathbb{Q}(\alpha)$ y deducir que $\mathbb{Q}(\alpha)/\mathbb{Q}$ es una extensión de Galois.

c) Calcular $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$.

d) Calcular las subextensiones de $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ y decir cuales de ellas son de Galois sobre $\mathbb{Q}$.

6. Sea n un número entero libre de cuadrados, es decir, n no es divisible por el cuadrado de un entero.

a) Calcular el cuerpo de descomposición L de $X^4 - n$ sobre $\mathbb{Q}$.

b) Demostrar que $\mathrm{Gal}(L/\mathbb{Q})$ es isomorfo al grupo diédrico de orden 8.

c) Calcular todas las subextensiones de $L/\mathbb{Q}$ y decir cuales de ellas son de Galois sobre $\mathbb{Q}$.

d) Calcular $\mathrm{Gal}(L/K)$ y $\mathrm{Gal}(K/\mathbb{Q})$ para cada subextensión K de $L/\mathbb{Q}$.

7. Calcular el grupo de Galois del cuerpo de descomposición de $X^4 - 2$ sobre $\mathbb{F}_3$ y $\mathbb{F}_7$.

8. Sean $\xi = \xi_3 \in \mathbb{C}$ una raíz tercera primitiva de la unidad, p un número primo y $L = \mathbb{Q}(\xi, \sqrt{p})/\mathbb{Q}$.

a) Demostrar que $L/\mathbb{Q}$ es una extensión de Galois.

b) Calcular $\mathrm{Gal}(L/\mathbb{Q})$ y cada uno de sus subgrupos.

c) Calcular las subextensiones de $L/\mathbb{Q}$.

9. Calcular todas las subextensiones de $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$, donde ξ_n es una raíz n-ésima primitiva de la unidad, para $n = 3, 5, 7, 8, 11$ y 16.

10. 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'.
Interpretar los Periodos de Gauss del Problema 15 del Capítulo 8 en términos de estos elementos.

11. Utilizando el Problema 15 del Capítulo 8 describir todos las subextensiones de $\mathbb{Q}(\xi_p)/\mathbb{Q}$, donde p es un número primo y ξ_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 $\mathbb{Q}(\xi_{17})/\mathbb{Q}$ forman una cadena de la forma

$$\mathbb{Q} = L_0 \subset L_1 = L_0(\sqrt{a_0}) \subset L_2 = L_1(\sqrt{a_1}) \subset L_3 = L_2(\sqrt{a_2}) \subset L_4 = L_3(\sqrt{a_3}) = \mathbb{Q}(\xi_{17})$$

con $a_i \in L_i$.

12. Sea K un cuerpo finito de característica p y cardinal $q = p^n$. Demostrar

a) 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.

b) $\mathrm{Gal}(K/\mathbb{F}_p)$ es cíclico de orden n, generado por el automorfismo de Frobenius.

c) Si L/K es una extensión finita, entonces $\mathrm{Gal}(L/K)$ es cíclico generado por el automorfismo de L dado por $\sigma(x) = x^q$.

d) Si α es algebraico sobre K y $[K(\alpha) : K] = m$, entonces

$$\mathrm{Irr}(\alpha, K) = (X - \alpha)(X - \alpha^q) \cdots (X - \alpha^{q^{m-1}}).$$

e) Describir las subextensiones de L/K donde L es una extensión de grado m de K.

f) Demostrar que la aplicación $x \mapsto x^p$ es un endomorfismo no inyectivo de $\mathbb{F}_p(X)$.

13. 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.

a) 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.

b) Demostrar que σ es suprayectiva y que su núcleo es el conjunto de las matrices escalares αI con $\alpha \neq 0$.

c) 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 α es transcendente sobre K).

d) 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.

e) Demostrar que $K(X)/K$ es de Galois si y sólo si K es infinito.

f) Demostrar que si K es infinito, entonces los únicos subgrupos cerrados de $\mathrm{Gal}(K(X)/K)$ son él mismo y sus subgrupos finitos.

g) Calcular H' 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 $(X^2 - X + 1)^3/(X^2 - X)^2 \in H'$.)
- $H = \langle \sigma_A, \sigma_B \rangle$ donde $A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ y $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

14. Sea L una subextensión de una extensión ciclotómica $K(\xi)/K$. Demostrar

a) L/K es una extensión de Galois.

b) $\mathrm{Gal}(L/K)$ es abeliano.

c) Si $\xi^p = 1$, con p primo, entonces $\mathrm{Gal}(L/K)$ es cíclico.

15. 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 sólo 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 $\sigma(i) = j$.)

16. 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.

17. 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 $H_2 = g^{-1}H_1 g$. 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 sólo si F_1' y F_2' son conjugados en G.

18. 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 $\mathrm{Gal}(F_1/K)$.

19. 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

a) Φ es un homomorfismo inyectivo de grupos.

b) Si $L_1 \cap L_2 = K$, entonces Φ es un isomorfismo de grupos.

c) 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.

d) Calcular todas las subextensiones de $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

e) Calcular el grupo de Galois de $L = \mathbb{Q}(i, \sqrt[4]{2}, \sqrt[4]{3})/Q(i) = K$.

f) Calcular las subextensiones de L/K.

g) 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.

20. Dar extensiones de Galois $L/\mathbb{Q}$ para las que $\mathrm{Gal}(L/\mathbb{Q})$ sea isomorfo a cada uno de los siguientes grupos: $C_6, C_{10}, C_{15}, C_2 \times C_{30}$.

21. 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, ξ_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 ϕ es la función de Euler.

Capítulo 11

Construcciones con regla y compás

11.1. Construcciones con regla y compás

Definición 11.1. *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 $\mathcal{A}$.*
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.

Obsérvese que para poder construir con regla y compás un punto, a partir de los elementos de un conjunto $\mathcal{A}$ es necesario que $\mathcal{A}$ tenga al menos dos puntos. Si partimos de 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 $O = (0, 0)$ y $P = (1, 0)$. Diremos que un punto es constructible (con regla y compás) si lo es a partir de dos puntos que identificaremos con $(0, 0)$ y $(1, 0)$.

De forma algo ambigua 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 11.2. *1. Si P y Q son constructibles, entonces la circunferencia con centro P que pasa por Q es constructible.*

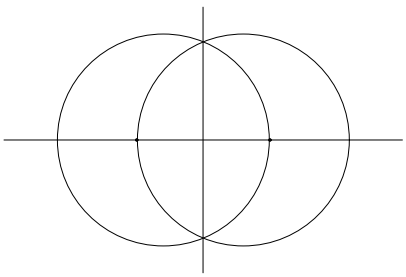
2. El punto medio y la mediatriz entre dos puntos constructibles son constructibles.

3. Si un punto P y una recta L son constructibles a partir de $\mathcal{A}$ entonces también son constructibles las rectas perpendicular y paralela a L que pasan por P.

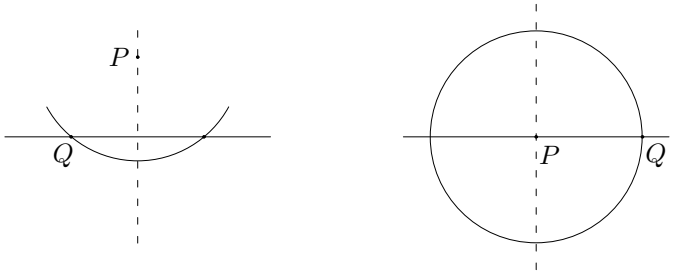
4. Las bisectrices de dos rectas constructibles son constructibles.

Demostración. 1 es obvio.

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.



3. Empecemos construyendo la perpendicular a L que pasa por P. 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 la circunferencia centrada en P que pasa por Q corta a L en uno o dos puntos. Si sólo lo corta en uno, entonces la recta que pasa por P y Q es la perpendicular buscada. En caso contrario los dos puntos de corte 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. □

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 $a + bi$. La clave para caracterizar los puntos constructibles con regla y compás es el siguiente lema. Una consecuencia inmediata de la Proposición 11.2 es el siguiente

Corolario 11.3. *Si $0, 1 \in \mathcal{A} \subseteq \mathbb{C}$ entonces $a + bi$ es constructible con regla y compás a partir de $\mathcal{A}$ si y sólo si lo son a y b.*

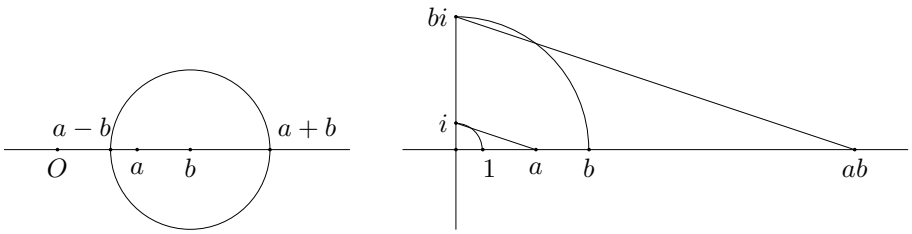
Proposición 11.4. *Sea $\mathcal{A}$ un subconjunto de $\mathbb{C} = \mathbb{R}^2$ que contiene a $(0, 0)$ y $(1, 0)$ y K el conjunto de los puntos constructibles con regla y compás a partir de $\mathcal{A}$. Entonces*

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. 1. Para empezar mostramos que los elementos de $K \cap \mathbb{R}$ forman un subcuerpo de $\mathbb{R}$. Sean $a, b \in K \cap \mathbb{R}$. Entonces $a + b$ y $a - b$ son las intersecciones de la recta real con la circunferencia centrada en b de radio $|a|$, lo que muestra que $a + b$ y $a - b$ pertenecen a $K \cap \mathbb{R}$. pasa por O y a.

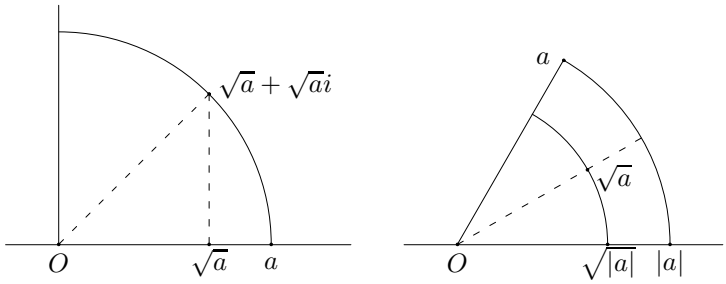
Vamos ahora a demostrar que $ab \in K \cap \mathbb{R}$ es constructible. En vista de que los opuestos de elementos de $K \cap \mathbb{R}$ están en $K \cap \mathbb{R}$, bastará considerar el caso en que a y b son positivos. Como $1 = (1, 0)$ y $b = (b, 0)$ son constructibles, $i = (0, 1)$ y $bi = (0, b)$ son constructibles pues están en las intersecciones de la recta perpendicular a la recta real con las circunferencias centrada en el origen de radios 1 y b respectivamente. Por tanto la recta que pasa por $(0, 1)$ y $(a, 0)$ es constructible y la recta paralela a esta que pasa por $(0, b)$ 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 $a^{-1} \in K \cap \mathbb{R}$.



Para demostrar que K es un cuerpo basta recordar que $a + bi$ es constructible si y sólo si a y b son constructibles (Corolario 11.3) 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. Las raíces del polinomio $aX^2 + bX + c$ coinciden con las raíces del polinomio $X^2 + \frac{b}{a}X + \frac{c}{a}$, con lo que podemos suponer que $a = 1$. Por otro lado $X^2 + bX + c = (X + \frac{b}{2})^2 + c^2 - \frac{b^2}{4}$, con lo que podemos suponer que $b = 0$ y por tanto basta demostrar que si $a \in K$, entonces $\sqrt{a} \in K$. De nuevo consideramos primero el caso en que a es un número real positivo. En tal caso $\sqrt{a} + \sqrt{a}i$ es la intersección de la circunferencia de radio a con la bisectriz del primer cuadrante, con lo que aplicando la Proposición 11.2 y el Corolario 11.3 se deduce que $\sqrt{a} \in K$. Finalmente si $a = x + yi$ es un elemento arbitrario de K, entonces $|a| = \sqrt{x^2 + y^2}$ 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.



□

11.2. 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 $\mathcal{A}$.

Lema 11.5. *Sea $\mathcal{A}$ un subconjunto de $\mathbb{C}$ y $P=(a,b)\in\mathbb{R}^2$. Si P es constructible con regla y compás en un paso a partir de $\mathcal{A}$ entonces $[\mathbb{Q}(\overline{\mathcal{A}}\cup\{a,b\}):\mathbb{Q}(\overline{\mathcal{A}})]\leq 2$.*

Demostración. Pondremos $K=\mathbb{Q}(\overline{\mathcal{A}})$ y tendremos que demostrar que $z=a+bi$ es constructible en un paso a partir de $\mathcal{A}$ si y sólo 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 A.

Pongamos que las rectas son L_1 y L_2 y las parejas de puntos respectivas son $(P_1=(P_{11},P_{12}),Q_1=(Q_{11},Q_{12}))$ y $(P_2=(P_{21},P_{22}),Q_2=(Q_{21},Q_{22}))$ respectivamente, 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

$$\frac{X-P_{11}}{Q_{11}-P_{11}}=\frac{Y-P_{12}}{Q_{12}-P_{12}}\quad\frac{X-P_{21}}{Q_{21}-P_{21}}=\frac{Y-P_{22}}{Q_{22}-P_{22}}$$

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 ≤ 2 de K. Como $p \neq 0$ ó $q \neq 0$, por simetría podemos suponer que $p \neq 0$, con lo que despejando X 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 $\Delta = \sqrt{h^2 - 4k}$. Entonces $a, b = \frac{r - pa}{q} \in E$ y 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 $[K(a, b) : K] \leq 2$. □

Teorema 11.6 (Wantzel)**.** *Sea $\mathcal{A}$ un subconjunto de $\mathbb{C}$ que contiene 0 y 1. Entonces las siguientes condiciones son equivalentes para un $z = a + bi \in \mathbb{C}$.*

1. *z es constructible con regla y compás a partir de $\mathcal{A}$.*
2. *Existe una torre de cuerpos*
$$\mathbb{Q}(\overline{\mathcal{A}}) = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$
tales que $[K_i : K_{i-1}] = 2$ para todo i y $a, b \in K_n$.
3. *Existe una torre de cuerpos*
$$\mathbb{Q}(\mathcal{A}) = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$
tales que $[K_i : K_{i-1}] = 2$ para todo i y $z \in K_n$.

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 11.5 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 las condiciones de 2.

2 implica 3. Supongamos que la sucesión $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ satisface la condición 2 y pongamos $L_j = K_j(i)$. Entonces $[L_j : L_{j-1}] \leq 2$ y $[L_0 : \mathbb{Q}(\mathcal{A})] \leq 2$ (¿por qué?) y de las fórmulas

$$z + \overline{z} = 2a \quad i(\overline{z} - z) = b$$

se deduce que $z \in L_n$. Por tanto eliminando términos repetidos en la torre

$$\mathbb{Q}(\mathcal{A}) \subseteq L_0 \subseteq L_1 \subseteq \cdots \subseteq L_n$$

obtenemos una torre de cuerpos que satisface la condición 3.

3 implica 1. Por inducción sobre n. Si $n = 0$, entonces $z \in \mathbb{Q}(\mathcal{A})$ que es constructible a partir de $\mathcal{A}$ pues el conjunto de puntos constructibles a partir de $\mathcal{A}$ es un subcuerpo de $\mathbb{C}$. Suponemos ahora que $n > 1$ y la hipótesis de inducción. Esta hipótesis implica que todos los elementos de K_{n-1} son constructibles a partir de $\mathcal{A}$. Con lo que si $z \in K_{n-1}$, entonces z es constructible. En caso contrario z es la raíz de $\mathrm{Irr}(z, K_{n-1})$ que tiene grado 2 y coeficientes constructibles a partir de $\mathcal{A}$. De la Proposición 11.4 deducimos que z es constructible a partir de $\mathcal{A}$. □

Una consecuencia del Teorema de Wantzel es el siguiente

Corolario 11.7 (Criterio de Wantzel)**.** *Si $z \in \mathbb{C}$ es constructible con regla y compás a partir de $\mathcal{A}$, entonces $[\mathbb{Q}(\mathcal{A} \cup \{z\}) : \mathbb{Q}(\mathcal{A})]$ es una potencia de 2.*

Si z es constructible con regla y compás, entonces $[\mathbb{Q}(z) : \mathbb{Q}]$ es una potencia de 2.

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 11.8. *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 α, equivale a que el punto $(\cos\alpha, \operatorname{sen}\alpha)$ 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 α con la parte positiva de la recta real. Como $\operatorname{sen}\alpha = \sqrt{1 - \cos(\alpha)}$, se tiene que el ángulo α es constructible si y sólo si $\cos\alpha$ es constructible. Por ejemplo el ángulo π 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

$$\begin{aligned}
\tfrac{1}{2} &= \cos\left(\tfrac{\pi}{3}\right) = \cos\left(\tfrac{\pi}{9} + 2\tfrac{\pi}{9}\right) = \cos\left(\tfrac{\pi}{9}\right)\cos\left(2\tfrac{\pi}{9}\right) - \operatorname{sen}\left(\tfrac{\pi}{9}\right)\operatorname{sen}\left(2\tfrac{\pi}{9}\right) \\
&= \cos\left(\tfrac{\pi}{9}\right)\left(\cos^2\left(\tfrac{\pi}{9}\right) - \operatorname{sen}^2\left(\tfrac{\pi}{9}\right)\right) - 2\operatorname{sen}^2\left(\tfrac{\pi}{9}\right)\cos\left(\tfrac{\pi}{9}\right) = \cos^3\left(\tfrac{\pi}{9}\right) - 3\cos\left(\tfrac{\pi}{9}\right)\operatorname{sen}^2\left(\tfrac{\pi}{9}\right) \\
&= \cos^3\left(\tfrac{\pi}{9}\right) - 3\cos\left(\tfrac{\pi}{9}\right)\left(1 - \cos^2\left(\tfrac{\pi}{9}\right)\right) = 4\cos^3\left(\tfrac{\pi}{9}\right) - 3\cos\left(\tfrac{\pi}{9}\right) = 4\alpha^3 - 3\alpha
\end{aligned}$$

Por tanto α 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 α no es constructible con regla y compás por el Criterio de Wantzel (Corolario 11.7). □

Cuadratura del Círculo: Construir con regla y compás un cuadrado que tenga el mismo área que un círculo dado.

Corolario 11.9. *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 π. Si esto fuera posible, el número π sería constructible con regla y compás, en particular $[\mathbb{Q}(\pi) : \mathbb{Q}]$ sería finito, es decir π sería algebraico. Sin embargo π es transcendente como demostró Lindeman en 1882. □

Duplicación del Cubo: Construir un cubo que tenga el doble del volumen de un cubo dado.

Corolario 11.10. *Es imposible duplicar un cubo arbitrario.*

Demostración. Duplicar el cubo de lado 1, equivaldría a construir el lado α 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. □

11.3. 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

$$\xi_n = e^{2\pi i/n} = \left(\cos\frac{2\pi}{n}, \operatorname{sen}\frac{2\pi}{n}\right),$$

el polígono regular de n lados es constructible con regla y compás si y sólo si ξ_n es constructible con regla y compás, lo que equivale a que $\cos\frac{2\pi}{n}$ sea constructible. Vamos a ver cuándo esto es así. Para ello necesitamos la siguiente proposición.

Por ejemplo, es fácil construir con regla y compás los polígonos regulares de 3, 4 y 5 lados. El de cuatro lados es el más fácil pues $\xi_4 = i$. También podemos utilizar que $\cos\frac{2\pi}{4} = 0$. Para construir el de tres lados observamos que $\xi_3 = \frac{-1+\sqrt{-3}}{2}$ o que $\cos\frac{2\pi}{3} = -\frac{1}{2}$.

Para construir el de 5 lados observamos que ξ_5 no es número real y que $[\mathbb{Q}(\xi_5) : \mathbb{Q}] = 4$. Sea $\alpha = 2\cos\left(\frac{2\pi}{5}\right) = \xi_5 + \xi_5^{-1}$. Utilizando que $1+\xi_5+\xi_5^2+\xi_5^3+\xi_5^4 = 0$ obtenemos que $\alpha^2 = \xi_5^2+2+\xi_5^{-2} = 1-\alpha$, con lo que α es raíz del polinomio $X^2 + X - 1$ y por tanto

$$\alpha = \frac{-1+\sqrt{5}}{2}.$$

Ahora es fácil construir el polígono regular de cinco lados siguiendo las indicaciones de la demostración de la Proposición 11.4

Proposición 11.11. *Si G es un grupo cuyo orden es una potencia de un primo p, entonces existe una sucesión de subgrupos de G*

$$1 = G_0 < G_1 < \ldots < G_n = G$$

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 3.26 deducimos que $Z(G) \neq 1$. Si $1 \neq a \in \mathbb{Z}(G)$, 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.

Teorema 11.12 (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. *$\xi_n = e^{2\pi i/n}$ 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 ξ_n es constructible con regla y compás entonces $[\mathbb{Q}(\xi_n) : \mathbb{Q}]$ es una potencia de 2, por el Criterio de Wantzel, (Corolario 11.7). Aplicando el Corolario 8.8 deducimos que $\phi(n) = [\mathbb{Q}(\xi_n) : \mathbb{Q}]$ es una potencia de 2.

4 implica 2. Supongamos que $\phi(n) = [\mathbb{Q}(\xi_n) : \mathbb{Q}]$ es una potencia de 2. Como $\mathbb{Q}(\xi_n)$ es el cuerpo de descomposición de $X^n - 1$ sobre $\mathbb{Q}$, la extensión $\mathbb{Q}(\xi_n)/\mathbb{Q}$ es normal, y por tanto es de Galois (¿por qué?). Eso implica que $|\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})| = [\mathbb{Q}(\xi_n) : \mathbb{Q}]$ es una potencia de 2. De la Proposición 11.11 deducimos que existe una sucesión

$$1 = G_0 < G_1 < \ldots < G_n = \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$$

de subgrupos de $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ tales que $[G_i : G_{i-1}] = 2$, para todo i. Aplicando el Teorema Fundamental de la Teoría de Galois deducimos que

$$\mathbb{Q} = K_0 = G'_n \subset K_1 = G'_{n-1} \subset \cdots \subset K_{n-1} = G'_1 \subset K_n = G'_0 = \mathbb{Q}(\xi_n)$$

es una torre de cuerpo con $[K_i : K_{i-1}] = 2$, para todo i. Aplicando el Teorema de Wantzel (Teorema 11.6) deducimos que ξ es constructible con regla y compás.

4 y 5 son equivalentes. Sea $n = 2^k p_1^{\alpha_1} \ldots p_m^{\alpha_m}$ con $2, p_1, \ldots, p_m$ primos distintos, $k \geq 0$, y $\alpha_i \geq 1$. Entonces aplicando el Ejercicio 8 del Capítulo 3 deducimos que

$$\phi(n) = 2^{\max\{0,k-1\}} p_1^{\alpha_1 - 1} \cdots p_m^{\alpha_m - 1}(p_1 - 1) \cdots (p_m - 1)$$

con lo que $\phi(n)$ es una potencia de 2 si y sólo 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 mayor que $q > 1$. 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 11.12 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

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$$

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.

11.4. Problemas

1. Dado un triángulo mostrar como 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).

2. Explicar cómo construir con regla y compás los polígonos regulares de 3, 4, 5, 6, 8 y 10 lados.

3. Demostrar 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.

4. ¿Se puede trisecar con regla y compás el ángulo $2\pi/5$?

5. ¿Se puede trisecar con regla y compás un segmento de longitud π?

6. Determinar el conjunto de puntos del plano constructibles con regla y compás a partir de los puntos del eje de abscisas.

7. ¿Son constructibles con regla y compás los ángulos de 1 y 3 grados?

8. Vamos a explicar cómo trisecar con regla y compás un ángulo dado α siguiendo los siguientes pasos:

   a) Supongamos que el ángulo α es el formado por dos semirectas S_1 y S_2 que parten del punto O.

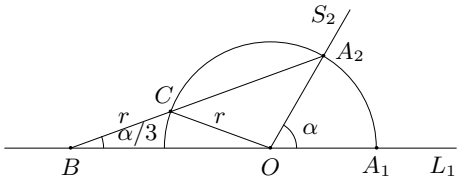
   b) Construimos una circunferencia centrada en O de radio r arbitrario.

   c) 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).

d) 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.

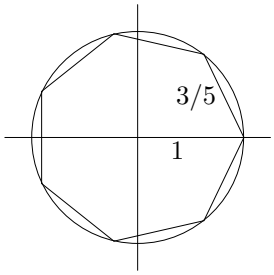
Entonces el ángulo formado por L y L_1 es $\alpha/3$ pues

$$\begin{aligned}\alpha &= \widehat{A_1OA_2} = \pi - \widehat{A_2OB} = \widehat{OBA_2} + \widehat{OA_2B} \\ &= \widehat{OBC} + \widehat{OA_2C} = \widehat{OBC} + \widehat{OCA_2} \\ &= \widehat{OBC} + \pi - \widehat{OCB} = \widehat{OBC} + \widehat{OBC} + \widehat{OCB} \\ &= 3\widehat{OBC}\end{aligned}$$



¿Te imaginas qué pide el problema?

9. Coge una regla y un compás, dibuja un segmento de longitud 1 y construye un heptágono de lado $3/5 = 0{,}6$, como el de la siguiente figura y explica que está pasando aquí.



10. Demostrar que un ángulo α se puede trisecar con regla con regla y compás si y sólo si el polinomio $4X^3 - 3X - \cos(\alpha)$ es reducible sobre $\mathbb{Q}(\cos(\alpha))$.

11. Demostrar que un número complejo $\alpha \neq 0$ se es constructible con regla y compás si y sólo si $\alpha + \alpha^{-1}$ lo es.

12. Demostrar que si α es una raíz del polinomio $8X^3 + 4X^2 - 4X - 1$, entonces α no es constructible con regla y compás.

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.

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.

15. Demostrar que las raíces del polinomio $X^4 + X + 1$ no son constructibles con regla y compás. (Indicación: Calcular $\mathrm{Irr}(\alpha\overline{\alpha} + \beta\overline{\beta}, \mathbb{Q})$, donde α y β son dos raíces no conjugadas del polinomio.)

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 un polígono regular de 17 lados o heptadecágono con regla y compás. 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.

   a) 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											

   b) Sean $\theta = 2\pi/17$, $\xi = \xi_{17} = e^{\theta i}$. Observa que 3 es un generador de $\mathbb{Z}_{17}$ y por tanto $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) = \langle\sigma\rangle$, donde $\sigma(\xi) = \xi^3$. Pongamos $\epsilon_i = \xi^{3^i}$.
   Utilizar la tabla anterior para construir los periodos de Gauss (ver Ejercicio 15 del Capítulo 8)

$$\begin{aligned} x_1 &= \omega_{0,2} = \epsilon_0 + \epsilon_2 + \cdots + \epsilon_{14} \\ x_2 &= \omega_{1,2} = \epsilon_1 + \epsilon_3 + \cdots + \epsilon_{15} \\ y_1 &= \omega_{0,4} = \epsilon_0 + \epsilon_4 + \epsilon_8 + \epsilon_{12} \\ y_2 &= \omega_{1,4} = \epsilon_1 + \epsilon_5 + \epsilon_9 + \epsilon_{13} \\ y_3 &= \omega_{2,4} = \epsilon_2 + \epsilon_6 + \epsilon_{10} + \epsilon_{14} \\ y_4 &= \omega_{3,4} = \epsilon_3 + \epsilon_7 + \epsilon_{11} + \epsilon_{15} \end{aligned}$$

   Demostrar:

$$\begin{aligned} x_1 &= 2(\cos\theta + \cos 8\theta + \cos 4\theta + \cos 2\theta) \\ x_2 &= 2(\cos 3\theta + \cos 7\theta + \cos 5\theta + \cos 6\theta) \\ y_1 &= 2(\cos\theta + \cos 4\theta) \\ y_2 &= 2(\cos 8\theta + \cos 2\theta) \\ y_3 &= 2(\cos 3\theta + \cos 5\theta) \\ y_4 &= 2(\cos 7\theta + \cos 6\theta) \end{aligned}$$

   c) 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 $x_1 > 0 > x_2$

   d) 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 $y_3 > y_4$.

   e) 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.

   f) Construir $\xi = \cos\theta + i\,\mathrm{sen}\,\theta$ con regla y compás.

   g) Demostrar la siguiente fórmula

$$\cos\theta = \frac{1}{16}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{68 + 12\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}}} - 2(1 - \sqrt{17})\sqrt{34 - 2\sqrt{17}}\right)$$

Capítulo 12

Extensiones cíclicas

12.1. Polinomio característico, norma y traza

En esta sección L/K va a ser una extensión finita y vamos a definir tres aplicaciones

$$\begin{array}{rcl} \chi_K^L : L & \to & K[X] \\ N_K^L : L & \to & K \\ T_K^L : L & \to & K \end{array}$$

de la siguiente forma: Para cada $\alpha \in L$ consideramos la aplicación

$$\begin{array}{rcl} \rho_\alpha^L : L & \to & L \\ x & \mapsto & \alpha x \end{array}$$

como un endomorfismo del espacios vectorial L_K. (Obsérvese que también podemos considerar ρ_α^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 $\chi_K^L(\alpha)$, $N_K^L(\alpha)$ y $T_K^L(\alpha)$ son respectivamente el polinomio característico, la norma y la traza de este endomorfismo y se llaman respectivamente *polinomio característico*, *norma* y *traza* de α 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

$$\begin{array}{rcl} N_K^L(\alpha) & = & (-1)^{[L:K]} \text{ Término independiente de } \chi_K^L(\alpha) \\ T_K^L(\alpha) & = & - \text{ Coeficiente de } X^{[L:K]-1} \text{ en } \chi_K^L(\alpha). \end{array} \tag{12.1}$$

La siguiente proposición reúne las propiedades principales del polinomio característico, la norma y la traza.

Proposición 12.1. *Sea L/K una extensión de cuerpos finita y $\alpha \in L$.*

1. *$T_K^L : L \to K$ es una aplicación K lineal y $T_K^L(a) = [L : K]a$, para todo $a \in K$.*
2. *$N_K^L(\alpha\beta) = N_K^L(\alpha)N_K^L(\beta)$ y $T_K^L(a) = a^{[L:K]}$, para todo $a \in K$.*

3. *Si $\alpha \in E \in \mathrm{Sub}(L/K)$, entonces*

$$\chi_K^L(\alpha) = \chi_K^E(\alpha)^{[L:E]}, \quad N_K^L(\alpha) = N_K^E(\alpha)^{[L:E]} \quad y \quad T_K^L(\alpha) = [L:E]T_K^E(\alpha).$$

4. *Si $\sigma_1, \ldots, \sigma_n$ son los K-homomorfismos de L en una clausura algebraica de K, entonces*

$$\chi_K^L(\alpha) = \left(\prod_{i=1}^{n}(X - \sigma_i(\alpha))\right)^{[L:K]_i}, \quad N_K^L(\alpha) = \left(\prod_{i=1}^{n}\sigma_i(\alpha)\right)^{[L:K]_i} \quad y \quad T_N^L(\alpha) = [L:K]_i \sum_{i=1}^{n}\sigma_i(\alpha).$$

En particular, si L/K es separable, entonces

$$\chi_K^L(\alpha) = \prod_{i=1}^{n}(X - \sigma_i(\alpha)), \quad N_K^L(\alpha) = \prod_{i=1}^{n}\sigma_i(\alpha) \quad y \quad T_N^L(\alpha) = \sum_{i=1}^{n}\sigma_i(\alpha).$$

5. *$\chi_K^L(\alpha) = \mathrm{Irr}(\alpha, K)^{[L:K(\alpha)]}$. En particular α es una raíz de $\chi_K^L(\alpha)$ y α es un elemento primitivo de L si y sólo si $\chi_K^L = \mathrm{Irr}(\alpha, K)$.*

6. *Si $\sigma : L \to L'$ es un K-isomorfismo de cuerpos, entonces $\chi_K^L(\alpha) = \chi_K^{L'}(\sigma(\alpha))$, $N_K^L(\alpha) = N_K^{L'}(\sigma(\alpha))$ y $T_K^L(\alpha) = T_K^{L'}(\sigma(\alpha))$.*

7. *(Transitividad de la norma y la traza) Si $E \in \mathrm{Sub}(L/K)$, entonces*

$$N_K^L(\alpha) = N_K^E(N_E^L(\alpha)) \quad y \quad T_K^L(\alpha) = T_K^E(T_E^L(\alpha)).$$

Demostración. 1 y 2 son consecuencias inmediatas de las propiedades del determinante y la traza de una matriz.

En las demostraciones de 3 y 4 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 (12.1).

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

$$\alpha b_i = \rho_\alpha^E(b_i) = \sum_{i_1=1}^{n} a_{i_1 i} b_{i_1}$$

Por tanto

$$\rho_\alpha^L(b_i c_j) = \alpha b_i c_j = \sum_{i_1=1}^{n} a_{i_1 i} b_{i_1} c_j$$

con lo que la matriz asociada a ρ_α^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 se entiende que 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. Si $\alpha_1,\dots,\alpha_r$ son las diferentes raíces de $p=\mathrm{Irr}(\alpha,K)$ en una clausura algebraica $\overline{K}$ de K, entonces $p=\prod_{i=1}^r(X-\alpha_i)^{[K(\alpha):K]_i}$. Además el número de K-homomorfismos de $K(\alpha)$ en $\overline{K}$ es $r=[K(\alpha):K]_s$ y estos r homomorfismos $\tau_1,\dots,\tau_r$ vienen dados por $\tau(\alpha)=\alpha_i$. Cada uno de estos τ_i tiene $s=[L:K(\alpha)]_s$ extensiones a homomorfismos $\rho_{i,j}:L\to\overline{K}$, con lo que $\{\sigma_1,\dots,\sigma_n\}=\{\rho_{i,j}:i=1,\dots,r,j=1,\dots,s\}$ y cada α_i aparece s veces en la lista $\sigma_1(\alpha),\dots,\sigma_n(\alpha)$. Por tanto, aplicando 4 tenemos

$$\begin{aligned}\chi_K^L(\alpha) &= p^{[L:K(\alpha)]}=\left(\textstyle\prod_{i=1}^r(X-\alpha_i)^{[K(\alpha):K]_i}\right)^{[L:K(\alpha)]}\\ &= \left(\textstyle\prod_{i=1}^r(X-\alpha_i)\right)^{[K(\alpha):K]_i[L:K(\alpha)]_i[L:K(\alpha)]_s}\\ &= \left(\textstyle\prod_{i=1}^r(X-\alpha_i)^s\right)^{[L:K]_i}\\ &= \left(\textstyle\prod_{i=1}^n(X-\sigma_i(\alpha))\right)^{[L:K]_i}.\end{aligned}$$

5. En vista del apartado 3, sólo hay que demostrar que $\chi_K^{K(\alpha)}(\alpha)=\mathrm{Irr}(\alpha)$. Pongamos $p=\mathrm{Irr}(\alpha,K)=p_0+p_1X+\cdots+p_{n-1}X^{n-1}+X^n$. Entonces $1,\alpha,\alpha^2,\dots,\alpha_{n-1}$ 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 polinomio característico de $q=p_1+p_2X+\cdots+p_{n-1}X^{n-2}+X^{n-1}$. Aplicando la hipótesis de inducción tenemos que

$$\chi_K^{K(\alpha)}=p_0+Xq=p.$$

6. Es consecuencia inmediata de 4.

7. Sea $\overline{K}$ una clausura algebraica de K y sean

$\tau_1, \ldots, \tau_r : E \to \overline{K}$ los K-homomorfismos definidos en E;
$\overline{\tau}_1, \ldots, \overline{\tau}_r : L \to \overline{K}$ extensiones de los anteriores a L.
$\sigma_1, \ldots, \sigma_s : L \to \overline{K}$, los E-homomorfismos definidos en L.

Entonces 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 $\rho|_E = \tau_i$, para algún i, con lo que $\rho\overline{\tau}_i^{-1}$ es un E-homomorfismo y por tanto $\rho\overline{\tau}_i^{-1} = \sigma_j$, para algún j. Entonces

$$\begin{aligned} N_K^L(\alpha) &= \textstyle\prod_{i,j} \overline{\tau}_i\sigma_j(\alpha)^{[L:K]_i} = \prod_i \overline{\tau}_i \left(\prod_j \sigma_j(\alpha)^{[L:E]_i}\right)^{[E:K]_i} \\ &= \textstyle\prod_i \overline{\tau}_i(N_E^L(\alpha))^{[E:K]_i} = N_K^E(N_E^L(\alpha)) \end{aligned}$$

Esto muestra la transitividad de la norma y la transitividad de la traza se demuestra de forma similar. □

12.2. Teorema 90 de Hilbert

En esta sección veremos un teorema fundamental de Hilbert cuya demostración depende del siguiente lema.

Lema 12.2 (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 σ_i para que los d primeros formen una base de V. Entonces $\sigma = \sigma_n$ es distinto de 0 y de σ_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. □

Corolario 12.3. *Las siguientes condiciones son equivalentes para una extensión finita L/K:*

1. $T_K^L(\alpha) \neq 0$ *para algún* $\alpha \in L$.

2. $T_K^L(\alpha) = 1$ *para algún* $\alpha \in L$.

3. L/K *es separable.*

Demostración. 2 implica 1 es obvio.

1 implica 2. Si $T_K^L(\alpha) \neq 0$, entonces $T_K^L\left(\frac{\alpha}{T_K^L(\alpha)}\right) = 1$.

3 si y sólo si 1. Si elegimos una clausura algebraica $\overline{L}$ de L, y $\sigma_1, \ldots, \sigma_n$ son los K-homomorfismos de L en $\overline{L}$, entonces $\sigma_1, \ldots, \sigma_n$ son linealmente independientes por el Lema 12.2 y $T_K^L = [L:K]_i(\sigma_1 + \cdots + \sigma_n)$, por la propiedad 4 de la Proposición 12.1. Si pensamos $[L:K]_i$ como un elemento t de K, y recordando que si $[L:K]_i \neq 1$, entonces $[L:K]_i$ es una potencia de la característica de K, resulta que L/K es separable si y sólo si $[L:K]_i \neq 1$, si y sólo si $t \neq 0$ si y sólo si $T_K^L \neq 0$ si y sólo si existe $\alpha \in L$ tal que $T_K^L(\alpha) \neq 0$. □

Definición 12.4. *Una* extensión cíclica *es una extensión de Galois cuyo grupo de Galois es cíclico.*

Ejemplos 12.5.

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 ξ_p es una raíz compleja p-ésima primitiva de la unidad, entonces $\mathbb{Q}(\xi_p)/\mathbb{Q}$ 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 8.2 se deduce que $\mathbb{Q}(\xi_p)/\mathbb{Q}$ es cíclico. De hecho si K es cualquier cuerpo y ξ_p es una raíz p-ésima primitiva de la unidad en una extensión de K entonces $K(\xi_p)/K$ 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 σ 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 12.6 (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. $T_K^L(\alpha) = 0$ *si y sólo si* $\alpha = \beta - \sigma(\beta)$ *para algún* $\beta \in L$.

2. $N_K^L(\alpha) = 1$ *si y sólo si* $\alpha = \beta\sigma(\beta)^{-1}$ *para algún* $\beta \in L^*$.

Demostración. Para simplificar la notación pondremos $N = N_K^L$ y $T = T_K^L$. 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 consideremos un elemento $\theta \in L$ tal que $T(\theta) = 1$ cuya existencia está garantizada por el Corolario 12.3. 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 $\alpha = \beta - \sigma(\beta)$) donde los γ_i son la siguientes trazas parciales:

$$\gamma_i = \alpha + \sigma(\alpha) + \cdots + \sigma^{i-1}(\alpha).$$

Obsérvese que la traza total sería $\gamma_n = T(\alpha) = 0$ y la primera es $\gamma_1 = \alpha$. 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

$$\begin{aligned}
\beta - \sigma(\beta) &= \gamma_1\sigma(\theta) + \gamma_2\sigma^2(\theta) + \cdots + \gamma_{n-1}\sigma^{n-1}(\theta) \\
&\quad -\gamma_2\sigma^2(\theta) - \cdots - \gamma_{n-1}\sigma^{n-1}(\theta) - \gamma_n\sigma^n(\theta) \\
&\quad +\alpha(\sigma^2(\theta) + \cdots + \sigma^i(\theta)) \\
&= \alpha(\sigma(\theta) + \cdots + \sigma^{n-1}(\theta) + \sigma^n(\theta)) = \alpha.
\end{aligned}$$

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 (Lema 12.2) 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

$$\alpha\sigma(\beta) = \sigma_1\sigma(\theta) + \gamma_2\sigma^2(\theta) + \cdots + \gamma_{n-1}\sigma^{n-1}(\theta) + \gamma_n\sigma^n(\theta) = \beta$$

pues $\sigma^n = 1$. □

12.3. Caracterización de las extensiones cíclicas

Proposición 12.7. *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 α una raíz de $X^n - a$. Entonces las raíces de $X^n - a$ son $\alpha, \xi\alpha, \ldots, \xi^{n-1}\alpha$, donde $\xi = \xi_n \in K$ es una raíz n-ésima primitiva de la unidad. Por tanto $L = K(\alpha)$ y $\sigma(\alpha) = \xi^{i_\sigma}\alpha$, 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 12.8. *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 el cuerpo de descomposición de $X^n - a$ sobre K para algún $a \in K$.*

Demostración. Fijemos una raíz n-ésima primitiva de la unidad $\xi = \xi_n \in K$.

1 implica 2. Supongamos que L/K es cíclica y σ es un generador de $\mathrm{Gal}(L/K)$. Como $\xi \in K$, se tiene que $N(\xi) = \xi^n = 1$ y del Teorema 90 de Hilbert se deduce que existe $\alpha \in L$ tal que $\sigma(\alpha) = \xi\alpha$. Si $p = \mathrm{Irr}(\alpha, K)$, entonces

$$\alpha, \sigma(\alpha) = \xi\alpha, \sigma^2(\alpha) = \xi^2\alpha, \ldots, \sigma^{n-1}(a) = \xi^{n-1}\alpha$$

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

$$p = (X - \alpha)(X - \xi\alpha)(X - \xi^2\alpha) \cdots (X - \xi^{n-1}\alpha)$$

Aplicando la Fórmula de Cardano-Vieta deducimos que el coeficiente de X^{n-i} $(i = 1, 2, \ldots, n)$ de p es

$$p_{n-i} = (-1)^{n-i} S_i(\alpha, \xi\alpha, \xi^2\alpha, \ldots, \xi^{n-1}\alpha) = \alpha^i S_i(1, \xi, \xi^2, \ldots, \xi^{n-1})$$

donde S_i es el i-ésimo polinomio simétrico elemental en n variables. Como $1, \xi, \xi^2, \xi^{n-1}$ 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 α 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 $\alpha, \xi\alpha, \xi^2\alpha, \ldots, \xi^{n-1}\alpha$ y por tanto L es es cuerpo de descomposición de $X^n - a$ sobre K.

4 implica 1. Es consecuencia de la Proposición 12.7. □

12.4. Problemas

1. Demostrar que la traza de la extensión $K(\sqrt{X})/K = \mathbb{F}_2(X)$ es idénticamente nula.

2. Sea $\xi = \xi_p \in \mathbb{C}$ una raíz p-ésima primitiva de la unidad con p primo. Demostrar que si $a_0, a_1, \ldots, a_{p-2} \in \mathbb{Q}$, entonces
$$T_{\mathbb{Q}}^{\mathbb{Q}(\xi)}\left(\sum_{i=0}^{p-2} a_i \xi^i\right) = (p-1)a_0 + \sum_{i=1}^{p-2} a_i.$$

3. Decir cuáles de las siguientes extensiones son cíclicas.

   a) L/K, donde L es el cuerpo de descomposición de $X^p - 1$ sobre K para un primo p.

   b) Una extensión de grupos finitos.

   c) $\mathbb{Q}(\xi_n)/\mathbb{Q}$, donde ξ_n es una raíz finita de la unidad para cada uno de los números $n \leq 25$.

   d) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

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

   f) El cuerpo de descomposición de $X^3 - 2$ sobre $\mathbb{Q}$, $\mathbb{F}_3$ y $\mathbb{F}_5$.

4. Sea L/K una extensión cíclica de cuerpos de característica $p \neq 0$ y sea σ un generador de L/K. Demostrar que para todo elemento $\beta \in L$ tal que $T_K^L(\beta) = 0$ existe $\alpha \in L$ tal que $\sigma(\alpha) - \alpha = \beta^p - \beta$.

5. Sea K un cuerpo de característica $p \neq 0$ y $f = X^p - X - a$ con $a \in K$. Demostrar:

   a) Si α es una raíz de f, entonces $\alpha + 1$ también es raíz de f.

   b) f es o irreducible o completamente indescomponible sobre K.

   c) Si f es irreducible sobre K y α es una raíz de f es una extensión de K, entonces $K(\alpha)/K$ es una extensión cíclica.

   d) (Teorema de Artin-Schreier) Si L/K es una extensión cíclica de grado p, entonces existen $a \in K$ y una raíz α 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.

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 $\beta_2\beta_1^m \in K$.

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. 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 $\alpha \in L \setminus E$.

9. Sea L/K una extensión cíclica de grado p^n de cuerpos de característica p, sea σ 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:

   a) $\beta^p - \beta = a$

   b) $L = K(\beta)$.

   c) $\sigma^{p^{n-1}}(\beta) = \beta + 1$.

   d) $\alpha^p - \alpha = \sigma(a) - a$, para $\alpha = \sigma(\beta) - \beta$.

10. Sea L/K una extensión finita. Para cada $\alpha, \beta \in L$ sea

$$(\alpha, \beta) = T_K^L(\alpha\beta).$$

Para cada lista $\alpha_1, \ldots, \alpha_n$ de elementos de L ponemos

$$\Delta_K^L(\alpha_1, \ldots, \alpha_n) = \Delta(\alpha_1, \ldots, \alpha_n) = \begin{vmatrix} (\alpha_1, \alpha_1) & (\alpha_1, \alpha_2) & \ldots & (\alpha_1, \alpha_n) \\ (\alpha_2, \alpha_1) & (\alpha_2, \alpha_2) & \ldots & (\alpha_2, \alpha_n) \\ \cdots & \cdots & \cdots & \cdots \\ (\alpha_n, \alpha_1) & (\alpha_n, \alpha_2) & \ldots & (\alpha_n, \alpha_n) \end{vmatrix}.$$

Demostrar

   a) $(-,-)$ es una forma bilineal simétrica del espacio vectorial L_K, es decir, satisface las siguientes condiciones.

      1) Para todo $\alpha \in L$, la aplicación $(\alpha, -) : L \to K$, dada por $(\alpha, -)(\beta) = (\alpha, \beta)$, es K-lineal.
      2) $(\alpha, \beta) = (\beta, \alpha) \in K$, para todo $\alpha, \beta \in L$.

   b) Si $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$ entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base de L_K.

   c) 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 $\Delta(\alpha_1, \ldots, \alpha_n) = \lambda^2\Delta(\beta_1, \ldots, \beta_n)$.

   d) Si $s = [L : K]_s$ y $\{\sigma_1, \ldots, \sigma_s\}$ son los K-homomorfismos de L en una clausura algebraica de K entonces

$$\Delta(\alpha_1, \ldots, \alpha_s) = [L : K]_i^s \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_n) \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{vmatrix}.$$

   e) Sean $p \in K[X]$ un polinomio irreducible separable de grado n, α una raíz de p y $L = K(\alpha)$. Demostrar que $\Delta(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_K^L(\alpha)$.

   f) Las siguientes condiciones son equivalentes, donde $\phi : L \to L^*$ es la aplicación que asocia $\alpha \in L$ con la forma lineal $(\alpha, 0)$.

1) $(-,-)$ es no degenerada, es decir ϕ es inyectiva.
2) ϕ suprayectiva.
3) ϕ biyectiva.
4) $\Delta(\alpha_1,\ldots,\alpha_n)\neq 0$, para alguna base $\{\alpha_1,\ldots,\alpha_n\}$ de L_K.
5) $\Delta(\alpha_1,\ldots,\alpha_n)\neq 0$, para toda base $\{\alpha_1,\ldots,\alpha_n\}$ de L_K.
6) $T_K^L(\alpha)\neq 0$, para algún $\alpha\in L$.
7) L/K es separable.

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 α genera una base normal de L/K.

a) Demostrar que si L/K tiene una base normal, entonces es de Galois.

b) Decir cuáles de los siguientes elementos generan bases normales de las extensiones que se indican.

1) $\sqrt{a}$ de $K(\sqrt{a})/K$ para $a\in K\setminus K^2$.
2) $1+\sqrt{a}$ de $K(\sqrt{a})/K$ para $a\in K\setminus K^2$.
3) Una raíz n-ésima primitiva de la unidad $\xi=\xi_n$ para $\mathbb{Q}(\xi)/\mathbb{Q}$.

c) Sea $\mathrm{Gal}(L/K)=\{\sigma_1,\ldots,\sigma_n\}$ y $\alpha\in L$. Demostrar que α genera una base normal de L/K si y sólo si el determinante de la siguiente matriz es diferente de cero.

$$\begin{pmatrix} \sigma_1^{-1}\sigma_1(\alpha) & \sigma_1^{-1}\sigma_2(\alpha) & \ldots & \sigma_1^{-1}\sigma_n(\alpha)\\ \sigma_2^{-1}\sigma_1(\alpha) & \sigma_2^{-1}\sigma_2(\alpha) & \ldots & \sigma_2^{-1}\sigma_n(\alpha)\\ \ldots & \ldots & \ldots & \ldots\\ \sigma_n^{-1}\sigma_1(\alpha) & \sigma_n^{-1}\sigma_2(\alpha) & \ldots & \sigma_n^{-1}\sigma_n(\alpha)\end{pmatrix}.$$

d) Demostrar que toda extensión de Galois tiene una base normal.

e) Supongamos que $\alpha\in L$ genera una base normal de L/K y sean H un subgrupo de $G=\mathrm{Gal}(L/K)$ y $F=L^H=\{x\in L:\sigma(x)=x,\ \text{para todo } \sigma\in H\}$. Recordemos que $T_H(x)=\sum_{\sigma\in H}\sigma(x)$, 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 σ_i. Para cada $i=1,\ldots,m$ ponemos $H_i=\sigma_i^{-1}H\sigma_i$. Demostrar

1) $T_H(\alpha)$ es un elemento primitivo de E sobre K.
2) $\{\sigma_1(\mathrm{tr}_{H_1}(\alpha)),\ldots,\sigma_m(\mathrm{tr}_{H_m}(\alpha))\}$ es una base de F.
3) Si H es normal en G, entonces $\mathrm{tr}_H(\alpha)$ genera una base normal de F/K.

12. Sea $p\in K[X]$ irreducible de grado primo $p\neq \mathrm{car}K$ y α una raíz de p. Demostrar que si $K(\alpha)$ contiene una raíz de p diferente de α, entonces $K(\alpha)$ es el cuerpo de descomposición de p sobre K y $\mathrm{Gal}(K(\alpha)/K)$ es cíclico.

Capítulo 13

Extensiones radicales

13.1. Extensiones radicales

Definición 13.1. *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* $\alpha_i \in E_i$ *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*

$$K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = L. \tag{13.1}$$

Veamos algunas propiedades elementales de las extensiones radicales.

Lema 13.2. *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. Si

$$K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E$$

y

$$E = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = L$$

son torres radicales, entonces

$$K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = L$$

es una torre radical.

2. Si L/K admite una torre radical como en (13.1) 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 (13.1). Para cada $i = 1, \ldots, n$ sean $\beta_{i1}, \ldots, \beta_{ik_i}$ las raíces de $\mathrm{Irr}(\alpha_i, K)$ 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 $E_{i-1}(\alpha_i) = E_i$ se tiene que $\beta_{ij}^{n_i} \in E_{i-1}$ 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 y por tanto N/K es una extensión radical. □

13.2. Caracterización de extensiones radicales

Lema 13.3. *Si $L = K(\alpha)$, α es separable sobre K y $\alpha^r \in K$, 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 $p \nmid s$ y $\beta = \alpha^s$. Entonces $a = \alpha^r = \beta^{p^t}$, es decir β es raíz del polinomio $f = X^{p^t} - a$. De hecho β es la única raíz de f pues $f = X^{p^t} - \beta^{p^t} = (X - \beta)^{p^t}$. Si $g = \mathrm{Irr}(\beta, K)$, entonces g divide a f, con lo que g sólo tiene una raíz. Sin embargo, como α es separable sobre K, $K(\alpha)/K$ es separable (Corolario 9.14), con lo que β es separable sobre K y por tanto $[K(\beta) : K] = [K(\beta) : K] = 1$, es decir $\alpha^s = \beta \in K$. □

Teorema 13.4. *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 5.8.

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 con $E_n \subseteq L$ y pongamos $E_i = E_{i-1}(\alpha_i)$ con $\alpha^{s_i} \in E_{i-1}$. Por el Lema 13.3, 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 $\xi = \xi_n$ en una extensión de L. Entonces $L(\xi)/K(\xi)$ es una extensión radical de Galois (Lema 13.2) 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. Entonces E_i es el cuerpo de descomposición de $X^{s_i} - \alpha_i^{s_i}$ sobre E_{i-1} y de la Proposición 12.7 deducimos que $E_i(\xi)/E_{i-1}(\xi)$ 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 $\mathrm{Gal}(\overline{L}/\overline{E_i}) \trianglelefteq \mathrm{Gal}(\overline{L}/\overline{E_{i-1}})$ y 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, deducimos que $\overline{L}/K$ es de Galois y $\mathrm{Gal}(\overline{L}/K)$ es resoluble. Por otro lado L/K es de Galois, por hipótesis, y por tanto $\mathrm{Gal}(\overline{L}/L) \trianglelefteq \mathrm{Gal}(\overline{L}/K)$ 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 y radical, por el Lema 13.2. 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 13.2 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 σ a E es un elemento de $\mathrm{Gal}(E/K)$ (Teorema 7.11) 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 ϕ 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 es resoluble.

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 13.4.

Teorema 13.5. *Si L/K es una extensión finita de Galois, $\mathrm{Gal}(L/K)$ es 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 5.12 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 $\xi = \xi_p$. Como $L(\xi)/L$ es de Galois, tenemos que $L(\xi)/K$ es de Galois y, por tanto, también $L(\xi)/K(\xi)$ es de Galois.

Como L/K es de Galois, la restricción $\sigma \mapsto \sigma|_L$ induce un homomorfismo de grupos

$$\Phi : \overline{G} = \mathrm{Gal}(L(\xi)/K(\xi)) \to G = \mathrm{Gal}(L/K).$$

Además Φ es inyectivo, pues si $\sigma, \tau \in \overline{G}$ satisface $\sigma|_L = \tau|_L$, entonces $\sigma(\xi) = \tau(\xi)$ y por tanto $\sigma = \tau$.

Si Φ 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, Φ 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 $L(\xi)/F$ 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 otro lado, 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 12.8). Por tanto $F/K(\xi)$ es radical. Como $K(\xi)/K$ también es radical, deducimos que R/K es radical. □

13.3. Problemas

Salvo que se diga lo contrario, todos los cuerpos tienen característica 0.

1. 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.

2. 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.

3. Sea $p \in \mathbb{Q}[X]$ irreducible de grado 3 y L el cuerpo de descomposición de p sobre $\mathbb{Q}$.

   a) Demostrar que $\mathrm{Gal}(L/K)$ es cíclico de orden 3 o isomorfo a S_3.

   b) Demostrar que L está contenido en una extensión radical R de K.

   c) Demostrar que si $R \subseteq \mathbb{R}$, entonces R/K no es normal.

   d) Demostrar que si $L \subseteq \mathbb{R}$, entonces L/K no es radical.

   e) Dar un ejemplo de una extensión L/K que no sea radical pero que esté contenida en una extensión radical de K.

Capítulo 14

Resolubilidad de ecuaciones por radicales

En este capítulo 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. El lector debería 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.

14.1. El Teorema de Galois

Definición 14.1. *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 f es completamente factorizable en L. En tal caso también se dice que el polinomio p es resoluble por radicales sobre K.*

Si $p \in K$, entonces se llama grupo de Galois *de p sobre K al grupo de Galois* $\mathrm{Gal}(L/K)$*, donde L es un cuerpo de descomposición de p sobre K.*

Obsérvese que el grupo de Galois de $p \in K[X]$ sobre K, en principio depende del cuerpo de descomposición de p elegido, sin embargo, como todos los cuerpos de descomposición de p sobre K son K-isomorfos (Proposición 7.9), el grupo de Galois de p sobre K, está bien definido salvo isomorfismos y lo denotaremos por $\mathrm{Gal}(p/K)$.

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 es 0, nos vamos a restringir a esta hipótesis que simplificará algunos argumentos e hipótesis. El resultado principal es el siguiente.

Teorema 14.2 (Galois)**.** *Sea K un cuerpo de característica 0 y $p \in K[X]$. Entonces p es resoluble por radicales sobre K si y sólo si el grupo* $\mathrm{Gal}(p/K)$ *de Galois de p sobre K 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 $\mathrm{Gal}(p/K) = \mathrm{Gal}(E/K)$ es resoluble por el Teorema 13.4.

Recíprocamente, supongamos que $\mathrm{Gal}(p/K)$ es resoluble y sea E un cuerpo de descomposición de p sobre K. Entonces $\mathrm{Gal}(E/K) = \mathrm{Gal}(p/K)$ es resoluble y, del Teorema 13.5, 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. □

14.2. 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

$$S : K(X_1, \ldots, X_n) \to L.$$

Definición 14.3. *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 $P[C_1, \ldots, C_n]$, donde P 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 14.4. *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, φ es inyectiva y su imagen es claramente $K[S_1, \ldots, S_n]$. Por tanto $K[C_1, \ldots, C_n] \simeq K[S_1, \ldots, S_n]$, con lo que φ 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 7.9 deducimos que φ

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 3 del Capítulo 10, 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 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 14.4 es que esto sólo es posible en pocos casos.

Corolario 14.5. *Si K tiene característica 0, entonces el polinomio general de grado n sobre K es resoluble por radicales si y sólo si $n \leq 4$.*

Demostración. Es una consecuencia inmediata de los Teoremas 14.2 y 14.4 y de que S_n es resoluble si y sólo si $n \leq 4$ (Ejemplos 5.6). □

Corolario 14.6. *Si K tiene característica 0, entonces todo polinomio de $K[X]$ de grado ≤ 4 es resoluble por radicales sobre K. De hecho todo polinomio que sea producto de polinomios de grado ≤ 4 de $K[X]$ es resoluble por radicales sobre K.*

El Teorema 14.5 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 de resolver por radicales las ecuaciones algebraicas con coeficientes racionales 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 $\sigma \in \mathrm{Gal}(p/K)$. Además cada $\sigma \in \mathrm{Gal}(p/K)$ está completamente determinado por la restricción de σ a A. Por tanto $\mathrm{Gal}(p/K)$ es isomorfo a un subgrupo de S_A y a partir de ahora vamos a identificar $\mathrm{Gal}(p/K)$ 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 14.7. *Si p es primo y G es un subgrupo transitivo de S_n que contiene una trasposición, entonces $G = S_p$.*

Demostración. Definimos en $\mathbb{N}_p = \{1, \ldots, n\}$ 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 σ 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, de la Proposición 4.12 deducimos que $G = S_n$. □

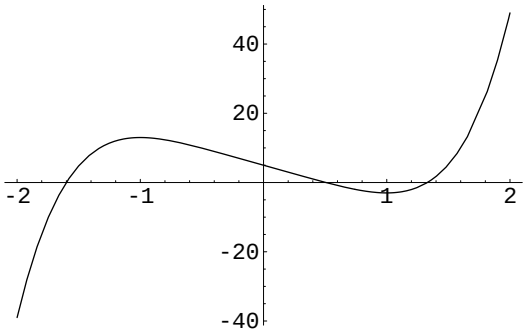
Lema 14.8. *Si $p \in K[X]$ es separable, entonces* $\mathrm{Gal}(p/K)$ *es transitivo si y sólo si p es irreducible sobre K.*

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 α es raíz de f y β es raíz de g, entonces $\sigma(\alpha) \neq \beta$, para todo $\sigma \in \mathrm{Gal}(p/K)$. Esto muestra que $\mathrm{Gal}(p/K)$ no es resoluble.

Por otro lado, si p es irreducible y α y β son dos raíces de p, entonces, por la Proposición 6.9, existe un K-isomorfismo $K(\alpha) \to K(\beta)$ que, como L/K es normal, donde L es el cuerpo de escisión de p sobre K, se puede extender a un elemento σ de $\mathrm{Gal}(L/K) = \mathrm{Gal}(p/K)$. Por tanto $\sigma(\alpha) = \beta$ y esto prueba que $\mathrm{Gal}(L/K)$ es resoluble. □

Proposición 14.9. *Sea K un subcuerpo de los números reales y $f \in K[X]$ un polinomio irreducible de grado primo p. Si f tiene $p-2$ raíces reales y 2 no reales, entonces* $\mathrm{Gal}(f/K) \simeq S_p$.

Demostración. Identificamos $G = \mathrm{Gal}(f/K)$ con un subgrupo del grupo S_A de permutaciones de las p raíces de f 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 14.7. Pero esto está claro pues la conjugación compleja es un elemento σ de $\mathrm{Gal}(p/K)$, ya que $K \subseteq \mathbb{R}$ y este elemento deja invariantes exactamente $p-2$ elementos de A, es decir es una transposición. □



Ejemplo 14.10. La figura anterior representa la curva $y = p(x)$ donde $p = 2X^5 - 10X + 5$, 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 tres puntos, uno en cada uno de los tres intervalos $(-\infty, -1)$, $(-1, 1)$ y $(1, \infty)$. De la Proposición 14.9 se deduce que $\mathrm{Gal}(p/\mathbb{Q}) \simeq S_5$ y por tanto p no es resoluble por radicales sobre $\mathbb{Q}$.

14.3. Resolución efectiva

El Teorema 14.2 transfiere el problema de la resolubilidad de ecuaciones por radicales a un problema de Teoría de Grupos y 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 tiene tantas raíces de la unidad como sea necesario.

1. Calcular $G = \mathrm{Gal}(p/K)$ 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 14.2.

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 12.8).

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 ≤ 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 $\mathrm{Gal}(p/K)$ como un grupo de permutaciones de las raíces de p. Entonces $Gal(p/K)$ es isomorfo a un subgrupo de S_2, con lo que $G = \mathrm{Gal}(p/K)$ 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 que G y S_2. Una 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 α_1 y α_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 α_1 y α_2 también son variables independientes sobre K, de forma que $a = -(\alpha_1 + \alpha_2)$ y $b = \alpha_1\alpha_2$. Por otro lado Δ^2 es un polinomio simétrico en las variables α_1, α_2, con lo que Δ^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 α_1 y α_2 son las soluciones del siguiente sistema lineal de ecuaciones

$$\begin{array}{rcrl} \alpha_1 & + & \alpha_2 & = -a \\ \alpha_1 & - & \alpha_2 & = \Delta. \end{array} \tag{14.1}$$

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 Δ 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. Vamos a considerar $G = \mathrm{Gal}(p/K)$ como un subgrupo de S_n, identificando la restricción de cada σ 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 automorfismo $\overline{\sigma}$ de $K[X_1, \ldots, X_n]$. Obsérvese que si $\sigma \in G$, entonces

$$\sigma(f(\alpha_1, \ldots, \alpha_n)) = \overline{\sigma}(f)(\alpha_1, \ldots, \alpha_n). \tag{14.2}$$

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 (14.2) se tiene que si $\theta = f(\alpha_1, \ldots, \alpha_n)$, entonces

$$\mathrm{Estab}_G(f) = G \cap \mathrm{Estab}_{S_n}(f) \subseteq \{\sigma \in G : \sigma(\theta) = \theta\} = \mathrm{Gal}(L/K(\theta)). \tag{14.3}$$

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 (ver Ejercicio 3.23 del Capítulo 3). 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 14.11. *La resolvente de Galois de $f \in K[X_1, \ldots, X_n]$ y $p \in K[X]$ (un polinomio mónico de grado n) pertenece a $K[X]$.*

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, σ permuta las raíces de $R_{f,p}$, lo que implica que $\sigma(R_{f,p}) = R_{f,p}$ y por tanto $R_{f,p} \in K[X]$. □

Teorema 14.12 (de Factorización de Resolventes)**.** *Sea $p \in K[X]$ un polinomio separable de grado n con raíces $\alpha_1, \ldots, \alpha_n$ y sean $G = \mathrm{Gal}(p/K)$, $f \in K[X_1, \ldots, X_n]$, $E = \mathrm{Estab}_{S_n}(f)$, $\sigma \in S_n$ y $\theta = f(\alpha_1, \ldots, \alpha_n)$. Entonces $\sigma(\theta)$ es una raíz de $R_{f,p}$. Además*

1. *Si $\sigma^{-1}G\sigma \subseteq E$, entonces $\sigma(\theta) \in K$.*
2. *Si $\sigma(\theta) \in K$ y es raíz simple de $R_{f,p}$, entonces $\sigma^{-1}G\sigma \subseteq E$.*

Demostración. Que $\sigma(\theta)$ es una raíz de $R_{f,p}$, es consecuencia de la propia definición de $R_{f,p}$.

1. 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 (14.3) 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 $K = K(\sigma(\theta))$.

2. 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 14.13 (Discriminante)**.** Sea $\Delta = \prod_{1\leq i<j\leq n}(X_i - X_j)$. La Definición 4.14 muestra que $A_n = \mathrm{Estab}_{S_n}(\Delta)$ 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 14.12) deducimos que si $p \in K[X]$ es separable y $G = \mathrm{Gal}(p/K)$, entonces $G \subseteq A_n$ si y sólo si $\sigma^{-1}G\sigma \subseteq A_n$ si y sólo si $G \subseteq A_n$ si y sólo si $R_{\Delta,p}$ tiene una raíz en K si y sólo 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 sólo si p es separable. En tal caso, la extensión $L = K(\alpha_1, \ldots, \alpha_n)/K$ es de Galois y, si $G = \mathrm{Gal}(p/K) = \mathrm{Gal}(L/K)$, 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 14.14 (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 S_1, S_2, S_3, S_4 son los polinomios simétricos elementales en X_1, X_2, X_3, X_4, entonces

$$R = (T - f_1)(T - f_2)(T - f_2) = T^3 - P_1T^2 + P_2X - P_3$$

donde

$$\begin{array}{rclcrcl} P_1 & = & f_1 + f_2 + f_3 & = & \Sigma_4(X_1X_2) & = & S_2 \\ P_2 & = & f_1f_2 + f_1f_3 + f_2f_3 & = & \Sigma_4(X_1^2X_2X_3) & = & S_1S_3 - 4S_4 \\ P_3 & = & f_1f_2f_3 & = & -(\Sigma_4(X_1^2X_2^2X_3^2) + S_4\Sigma_4(X_1^2)) & = & S_3^2 + S_1^2S_4 - 4S_2S_4. \end{array}$$

En resumen

$$R = T^3 - S_2T^2 + (S_1S_3 - 4S_4)T + (4S_2 - S_1^2)S_4 - S_3^2$$

y, por tanto, si $p = X^4 - aX^3 + bX^2 - cX + d$, entonces

$$R_{f,p} = T^3 - bT^2 + (ac - 4d)T + (4b - a^2)d - c^2.$$

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 $L = K(\alpha_1,\alpha_2,\alpha_3,\alpha_4)/F = K(\theta_1,\theta_2,\theta_3)$ es de Galois pues L es el cuerpo de descomposición de p sobre K (y sobre F). Por tanto, si $G = \mathrm{Gal}(p/F)$, entonces $\sigma(\theta_i) \in F$, para todo $\sigma \in S_4$. Aplicando el Teorema de Factorización de Resolventes (Teorema 14.12) 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 F 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 α_1, α_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 (14.1) 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 $\xi = \xi_2 = -1$ 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 α 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

$$V(\lambda_1, \ldots, \lambda_n) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \lambda_1 & \lambda_2 & \ldots & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & \ldots & \lambda_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \ldots & \lambda_n^{n-1} \end{pmatrix}.$$

Recuérdese que el determinante de $V(\lambda_1, \ldots, \lambda_n)$ es invertible si y sólo si los λ_i son diferentes dos a dos, ya que su determinante es $\prod_{i<j}(\lambda_i - \lambda_j)$.

Proposición 14.15. *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*

$$r_0 = (1, \alpha), r_1 = (\xi, \alpha), \ldots, r_{n-1} = (\xi^{n-1}, \alpha)$$

las resolventes de Lagrange de α. 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

$$\begin{aligned} \sigma(r_i) &= \xi^{-i}\alpha + \sigma(\alpha) + \xi^i\sigma^2(\alpha) + \cdots + \xi^{(n-2)i}\sigma^{n-1}(\alpha) \\ &= \xi^{-i}(\alpha + \xi^i\sigma(\alpha) + \xi^{2i}\sigma^2(\alpha) + \cdots + \xi^{(n-1)i}\sigma^{n-1}(\alpha)) = \xi^{-i}r_i \end{aligned}$$

Por tanto,

$$\sigma(r_i^n) = \sigma(r_i)^n = (\xi^{-i}r_i)^n = \xi^{-in}r_i^n = r_i^n.$$

□

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) y sus raíces T_1, T_2, T_3, $L = K(T_1, T_2, T_3)$, el cuerpo de descomposición de p 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 $S_4 \rhd A_4 \rhd 1$ 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:

$$\begin{aligned} D &= (T_1 - T_2)^2(T_1 - T_3)^2(T_2 - T_3)^2 \\ &= T_1^4T_2^2 + T_1^2T_2^4 + T_1^4T_3^2 + T_2^4T_3^2 + T_1^2T_3^4 + T_2^2T_3^4 \\ &\quad -2(T_1^3T_2^3 + T_1^3T_3^3 + T_2^3T_3^3) \\ &\quad -2(T_1^4T_2T_3 + T_1T_2^4T_3 + T_1T_2T_3^4) \\ &\quad +2(T_1^3T_2^2T_3 + T_1^2T_2^3T_3 + T_1^3T_2T_3^2 + T_1T_2^3T_3^2 + T_1^2T_2T_3^3 + T_1T_2^2T_3^3) \\ &\quad -6T_1^2T_2^2T_3^2 \\ &= \Sigma_3(T_1^4T_2^2) - 2\Sigma_3(T_1^3T_2^3) - 2C_3\Sigma_3(T_1^3) + 2C_3\Sigma_3(T_1^2T_2) - 6C_3^2. \end{aligned}$$

Aplicando el algoritmo explicado en la Sección 2.5 tenemos

$$\begin{aligned} \Sigma_3(T_1^4T_2^2) &= C_1^2C_2^2 - 2C_2^3 - 2C_1^3C_3 + 4C_1C_2C_3 - 3C_3^2, \\ \Sigma_3(T_1^3T_2^3) &= C_2^3 - 3C_1C_2C_3 + 3C_3^2, \\ \Sigma_3(T_1^3) &= C_1^3 - 3C_1C_2 + 3C_3, \\ \Sigma_3(T_1^2T_2) &= C_1C_2 - 3C_3. \end{aligned}$$

con lo que

$$\begin{aligned} D &= C_1^2C_2^2 - 2C_2^3 - 2C_1^3C_3 + 4C_1C_2C_3 - 3C_3^2 \\ &\quad -2(C_2^3 - 3C_1C_2C_3 + 3C_3^2) - 2C_3(C_1^3 - 3C_1C_2 + 3C_3) \\ &\quad +2C_3(C_1C_2 - 3C_3) - 6C_3^2 \\ &= C_1^2C_2^2 - 4C_2^3 - 4C_1^3C_3 + 18C_1C_2C_3 - 27C_3^2. \end{aligned}$$

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 14.16. *Si Δ 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

$$\mathrm{Gal}(p/K) \simeq \begin{cases} A_3 \simeq C_3, & \text{si } a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2 \text{ es un cuadrado en } K; \\ S_3, & \text{en caso contrario} \end{cases}$$

y $\mathrm{Gal}(p/K(\Delta))$ 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

$$\begin{aligned} r_0 &= (1, T) &&= T_1 + T_2 + T_3 = -a \\ r_1 &= (\xi, T) &&= T_1 + \xi T_2 + \xi^2 T_3 \\ r_2 &= (\xi^2, T) &&= T_1 + \xi^2 T_2 + \xi T_3 \end{aligned} \tag{14.4}$$

Resolviendo el sistema de ecuaciones tenemos

$$T_1 = \frac{\begin{vmatrix} r_0 & 1 & 1 \\ r_1 & \xi & \xi^2 \\ r_2 & \xi^2\xi & \end{vmatrix}}{\begin{vmatrix} 1 & 1 & 1 \\ 1 & \xi & \xi^2 \\ 1 & \xi^2\xi & \end{vmatrix}} = \frac{r_0 + r_1 + r_2}{3}. \tag{14.5}$$

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

$$(T_1 + \xi T_2 + \xi^2 T_3)^3 + (T_1 + \xi^2 T_2 + \xi T_3)^3 = 2C_1^3 - 6C_1C_2 + 18C_3 + 3(\xi + \xi^2)\Sigma_3(T_1^2T_2)$$

Teniendo en cuenta que $\xi + \xi^2 = -1$ y $\Sigma_3(T_1^2T_2) = C_1C_2 - 3C_3$ 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

$$(T_1 + \xi T_2 + \xi^2 T_3)^3 - (T_1 + \xi^2 T_2 + \xi T_3)^3 = 3(\xi - \xi^2)(T_1 - T_2)(T_1 - T_3)(T_2 - T_3) = 3\sqrt{-3}\Delta.$$

Por tanto

$$\begin{array}{rcl} r_1^3 + r_2^3 & = & 2C_1^3 - 9C_1C_2 + 27C_3, \\ r_1^3 - r_2^3 & = & 3\sqrt{-3}\Delta \end{array}$$

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 (CubicaT1) 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:

$$\begin{array}{rcl} r_1r_2 & = & (T_1 + \xi T_2 + \xi^2 T_3)(T_1 + \xi^2 T_2 + \xi T_3) \\ & = & (T_1^2 + T_2 + T_3^2) + (\xi + \xi^2)(T_1T_2 + T_1T_3 + T_2T_3) \\ & = & (T_1 + T_2 + T_3)^2 - 3(T_1T_2 + T_1T_3 + T_2T_3) \\ & = & C_1^2 - 3C_2. \end{array}$$

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 α por $\xi\alpha$ y $\xi^2\alpha$ obtenemos los valores de T_2 y T_3 tal como aparecen en (14.4).

En resumen, cambiando de nuevo C_1, C_2 y C_3 por $-a, b$ y $-c$ obtenemos:

Teorema 14.17. *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 $a^2 - 3b$.

La cuártica

Consideremos ahora el polinomio general de grado 4,

$$G_4 = X^4 - C_1X^3 + C_2X^2 - C_3X + C_4 = (X - T_1)(X - T_2)(X - T_3)(X - T_4) \in K[X].$$

con $K = F(C_1, C_2, C_3, C_4)$ y $L = K(T_1, T_2, T_3, T_4)$. 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 14.14 tenemos que $F^V = K(C_1, C_2, C_3, f_1, f_2, f_3)$ 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 14.17 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

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} T_1 \\ T_2 \\ T_3 \\ T_4 \end{pmatrix} = \begin{pmatrix} C_1 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}$$

que nos proporciona

$$\begin{array}{rcl} T_1 & = & \frac{1}{4}(\beta_1 + \beta_2 + \beta_3 + C_1) \\ T_2 & = & \frac{1}{4}(\beta_1 - \beta_2 - \beta_3 + C_1) \\ T_3 & = & \frac{1}{4}(-\beta_1 + \beta_2 - \beta_3 + C_1) \\ T_4 & = & \frac{1}{4}(\beta_1 - \beta_2 + \beta_3 + C_1) \end{array}$$

y sólo falta calcular los β_i. Para ello observamos que $\sigma(\beta_i) = \pm\beta_i$ para todo $\sigma \in V$, con lo que los cuadrados de los β_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 β_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 β_i determina el del tercero. La elección de dos de los signos de los β_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 14.18. *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 β_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 14.18 tenemos dos elecciones posibles para los signos de cada uno de los β_i. Combinando estas tres parejas de elecciones tenemos ocho elecciones posibles de los signos de los β_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.

14.4. 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 $\sigma_{a,b}(x) = ax + b$. Obsérvese que $\sigma_{a,b} = \sigma_{1,b}\sigma_{a,0} \in S_n$ y de hecho el conjunto

$$\mathcal{A}f_n = \{\sigma_{a,b} : a \in \mathbb{Z}_n^*, b \in \mathbb{Z}_n\}$$

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 14.19. Todo subgrupo de S_n generado por un n-ciclo es afín. En efecto, si σ es un n-ciclo, entonces σ es conjugado en S_n de $\sigma_{1,1} = (0, 1, 2, \ldots, n-1)$ (Teorema 4.9). Por tanto $\langle\sigma\rangle$ es conjugado de $\langle\sigma_{1,1}\rangle$ en S_n.

Proposición 14.20. *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 cuyo núcleo es precisamente N. Por tanto $\mathcal{A}f_n/N$ es isomorfo a un subgrupo de H, lo que implica que $\mathcal{A}f_n/N$ es abeliano. Como N también es abeliano, de la Proposición 5.8 deducimos que $\mathcal{A}f_n$ es resoluble. □

Recordemos que el grupo de Galois de un polinomio irreducible separable es transitivo (Lema 14.8). El siguiente Teorema caracteriza los subgrupos transitivos resolubles de S_p para p primo. Pero antes necesitamos alguna notación y un lema.

Si G es un subgrupo de S_n y $x \in \mathbb{Z}_n$ entonces ponemos

$$G(x) = \{\sigma(x) : \sigma \in G\} \quad \text{Estab}_G(x) = \{\sigma \in G : \sigma(x) = x\}.$$

Obsérvese que G es transitivo si y sólo si $G(x) = \mathbb{Z}_n$, para todo $x \in \mathbb{Z}_x$ si y sólo si $G(x) = \mathbb{Z}_n$, para algún $x \in \mathbb{Z}_x$.

Recordemos que si $\sigma \in S_n$ entonces $M(\sigma)$ denota el conjunto de los elementos de $\mathbb{Z}_n$ movidos por σ (Definición 4.1). Vamos a denotar por $F(\sigma)$ al complemento de $M(\sigma)$ en $\mathbb{Z}_n$.

Lema 14.21. *Sea G un subgrupo de S_n.*

1. *Los conjuntos de la forma $G(x)$, con $x \in \mathbb{Z}_n$, forman una partición de $\mathbb{Z}_n$.*
2. *Si $x \in \mathbb{Z}_n$, entonces $|G(x)| = [G : \text{Estab}_G(x)]$.*
3. *Si $\sigma \in S_n$, satisface $\sigma^{-1}G\sigma = G$ y $x \in \mathbb{Z}_n$, entonces $\text{Estab}_G(\sigma(x)) = \sigma^{-1}\text{Estab}_G(x)\sigma$ y en particular $|G(x)| = |G(\sigma(x))|$.*
4. *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.*
5. *Si G es un subgrupo afín de S_p, con p primo y $1 \neq \sigma \in G$, entonces $|F(\sigma)| \leq 1$.*
6. *Si $\sigma^{-1}\sigma_{11}\sigma \in \mathcal{A}f_p$, con p primo, entonces $\sigma \in \mathcal{A}f_p$.*
7. *Si $\sigma \in S_p$, con p primo y $F_\sigma = \emptyset$, entonces σ es un p-ciclo.*

Demostración. 1, 2, 3 y 7 se dejan como ejercicio.

4. 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 $|N(x)| = |N(\sigma(x))| = |N(y)|$, por 3.

5. 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, $\rho = \tau^{-1}\sigma\tau \in \mathcal{A}f_p$ para algún $\tau \in S_p$. Luego σ y ρ son del mismo tipo (Teorema 4.9) y por tanto $|F(\rho)| = |F(\sigma)|$. Si $\rho = \sigma_{a,b}$, con $(a, b) \in \mathbb{Z}_p^* \times \mathbb{Z}_p$. Si x, y son dos elementos distintos de $F(\sigma)$, 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 $\rho = \sigma_{1,0} = 1$ y concluimos que $\sigma = 1$.

6. 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 $a^p \equiv a \bmod p$ 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, si $k = xb^{-1}$. Entonces

$$\sigma(x) = \sigma(kb) = \sigma((k-1)b+b) = \sigma((k-1)b)+1 = \sigma((k-2)b)+2 = \cdots = \sigma(0)+k = b^{-1}x+\sigma(0)\sigma_{b^{-1},\sigma(0)}(x)$$

es decir $\sigma = \sigma_{b^{-1},\sigma(0)} \in \mathcal{A}f_p$. □

Teorema 14.22. *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 14.20.

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 14.21 a $N = G_{i-1}$, un subgrupo normal de G_{i-1}, se deduce que los conjuntos de la forma $N(x)$, 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 $N \neq 1$, $|N(x)| > 1$ para algún x (y por tanto para todos), de donde se deduce que $N(x) = \mathbb{Z}_p$, es decir N es transitivo.

Luego $G_{n-1} = \langle\sigma\rangle$ es cíclico y transitivo y por tanto σ es un p-ciclo (¿por qué?). Como $\sigma_{1,1}$ es otro p-ciclo, Del Teorema 4.9 deducimos que $\tau^{-1}\sigma\tau = \sigma_{1,1}$. 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 14.21 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 14.21.

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, $p = |G(x)| = [G : \mathrm{Estab}_G(x)]$, es decir $|\mathrm{Estab}_G(x)| = |G|/p$ para todo $x \in \mathbb{Z}_p$. Por tanto, si $n = |G|$,

$$\Omega = \bigcup_{x\in\mathbb{Z}_p} (\mathrm{Estab}_G(x) \setminus \{1\})$$

es la unión de p subconjuntos disjuntos de G, cada uno de cardinal $\frac{n}{p} - 1$. Luego

$$N = G \setminus \Omega = n - p\left(\frac{n}{p} - 1\right) = p.$$

Por tanto existe $1 \neq \sigma \in N$, es decir G tiene un elemento σ tal que $F_\sigma = \emptyset$. Del Lema 14.21 se deduce que σ es un p-ciclo. Por tanto $N = \langle\sigma\rangle$ tiene orden p y del Lema 14.21 deducimos que 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 14.21 se deduce que σ 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 14.21 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 14.21 y que G es transitivo deducimos que $p = |G(x)| = [G : \mathrm{Estab}_G(x)]$ un divisor de $|G|$.

6 implica 4. Esta parte de la demostración utiliza los Teoremas de Sylow (Teorema 14.24).

Supongamos que $n = pm < p^2$. Entonces $p \nmid m$ y, por los Teoremas de Sylow, 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 14.23. *(Galois) Si $f \in K[X]$ es irreducible de grado primo entonces f es resoluble por radicales sobre K si y sólo si $K(\alpha, \beta)$ es un cuerpo de descomposición de f para cada dos raíces distintas de α, β 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 14.2 y 14.22 se deduce que f es resoluble por radicales sobre K si y sólo si G es resoluble por radicales si y sólo $|F(\sigma)| \leq 1$, para todo $1 \neq \sigma \in G$, si y sólo si $\mathrm{Gal}(L/K(\alpha, \beta)) = 1$, para cada elementos diferentes $\alpha, \beta \in A$ si y sólo si $L = K(\alpha, \beta)$. □

Cerramos el capítulo con el enunciado de los Teoremas de Sylow, que hemos utilizado en la demostración del Teorema 14.22. La demostración de estos teoremas excede el ámbito de estos apuntes.

Teorema 14.24 (Teoremas de Sylow)**.** *Sea G un grupo finito de orden $n = p^k m$, con p primo y $p \nmid m$. Un* p-subgrupo *de G es un subgrupo cuyo orden es una potencia de p y un* p-subgrupo de Sylow *de G es un subgrupo de orden p^k.*

1. *G tiene al menos un p-subgrupo de Sylow.*
2. *Si H es un p-subgrupo de G y S es un p-subgrupo de Sylow de G entonces $g^{-1}Hg \subseteq S$ para algún $g \in G$. En particular todos los subgrupos de Sylow de G son conjugados en G.*
3. *Si n_p es el número de p-subgrupos de Sylow de G, entonces n_p divide a m y $n_p \equiv 1 \bmod p$.*

14.5. 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 14.2 no termina de ser satisfactoria pues necesitamos calcular $\mathrm{Gal}(p/K) = \mathrm{Gal}(L/K)$, 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 $p = X^n - S_1X^{n-1} + S_2X^{n-2} + \cdots + (-1)^{n-1}S_1 + (-1)^n S_n \in K[X]$, un polinomio irreducible y separable sobre K. Supongamos que $\alpha_1, \ldots, \alpha_n$ son las raíces de p. 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 $\sigma_T(\beta) = \sigma_\alpha^{-1}(\beta)$ 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 y por tanto es un polinomio en los coeficientes de p. En otras palabras

$$Q = \sum_{j=0}^{n!} \left(\sum_{(i)} f_j(S_1, \ldots, S_n) T_1^{i_1} \cdots T_n^{i_n} \right) X^j,$$

donde cada $f_i(S_1, \ldots, S_n)$ 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. 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 $\overline{\sigma}(Q) = Q$ 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 14.25. *Si $p \in K[X]$ es irreducible y separable sobre K, entonces* $\mathrm{Gal}(p/K) \simeq \mathrm{Estab}_{S_n}(Q_1)$, *donde Q_1 es como antes.*

Demostración. Obsérvese que

$$\begin{aligned} A_1 &= \{\sigma \in S_n : X - \sigma_T(\beta) \text{ divide a } Q_1\} \\ &= \{\sigma \in S_n : X - \beta \text{ divide a } \sigma_T^{-1}(Q_1)\} \\ &= \{\sigma \in S_n : Q_1 = \sigma_T^{-1}(Q_1)\} \\ &= \mathrm{Estab}_{S_n}(Q_1). \end{aligned}$$

Sean $G = \mathrm{Gal}(p/K)$ y

$$P = \prod_{\sigma \in G} (X - \sigma_\alpha(\beta)) = \prod_{\sigma \in G} (X - \sigma_T(\beta)).$$

Entonces P divide a Q, con lo que P es el producto de algunos de los Q_i. Además β es una raíz de P, con lo que uno de los divisores irreducibles de P es Q_1. Por tanto Q_1 divide a P. Esto prueba que $A_1 \subseteq G$.

Recíprocamente, si $\tau \in G$, entonces

$$\begin{aligned} \overline{\tau}(Q_1) &= \textstyle\prod_{\sigma \in A_1}(X - \tau_T \sigma_T(\beta)) \\ &= \textstyle\prod_{\sigma \in A_1}(X - \tau_\alpha^{-1} \sigma_T(\beta)) \\ &= \tau_\alpha^{-1}\left(\textstyle\prod_{\sigma \in A_1}(X - \sigma_T(\beta))\right) \\ &= \tau_\alpha^{-1}(Q_1) = Q_1. \end{aligned}$$

La última igualdad es consecuencia de que los coeficientes de Q_1 pertenecen a K. Luego $\tau \in \mathrm{Estab}_{S_n}(Q_1)$. □

Está claro que el método proporcionado a pesar de ser algorítmico es poco satisfactorio ya que requiere unos cálculos enormes. Para el caso en que p sea un polinomio irreducible separable de grado primo q, el Teorema 14.22, junto con el Teorema de Factorización de Resolvente proporciona un método alternativo para estudiar si p es resoluble.

Proposición 14.26. *Sean p sea un polinomio irreducible de grado primo q sobre un cuerpo K de característica* 0, *$f \in K[X_1, \ldots, X_n]$ un polinomio tal que* $\mathrm{Estab}_{S_q}(f) = \mathcal{A}f_q$ *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 $\alpha_1, \ldots, \alpha_n$ las raíces de p en un cuerpo de descomposición de p sobre K y sea $\theta = f(\alpha_1, \ldots, \alpha_n)$.

1. Si p es resoluble por radicales sobre K, entonces $G = \mathrm{Gal}(p/K)$ es resoluble (Teorema 14.2) y por tanto G es afín (Teorema 14.22), es decir existe $\sigma \in G$ tal que $\sigma^{-1} G \sigma \subseteq \mathcal{A}f_q = \mathrm{Estab}_{S_n}(f)$. Aplicando el Teorema de Factorización de Resolventes deducimos que $\sigma(\theta)$ es una raíz de p que pertenece a K.

2. Si $\beta \in K$ es una raíz simple de R entonces $\beta = \sigma(\theta)$ para algún $\sigma \in S_n$. Del Teorema de Factorización de Resolventes deducimos que $\sigma^{-1} G \sigma \subseteq \mathcal{A}f_q$, con lo que G es un subgrupo afín de S_q. Del Teorema 14.22 deducimos que G es resoluble y, del Teorema 14.2, 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 al polinomio con el que cerramos esta sección. 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 14.27. Si $p=X^5+X^2-1$, entonces $R_{f,p}=1+6T+15T^2+20T^3+15T^4+6T^5+T^6$, que no tiene ninguna raíz en $\mathbb{Q}$. Deducimos que p no es resoluble por radicales sobre $\mathbb{Q}$ de la De la Proposición 14.26.

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 14.26 deducimos que p es resoluble por radicales sobre $\mathbb{Q}$.

La resolvente séxtica de la ecuación de quinto grado

$$
\begin{aligned}
&T^6\\
+&T^5 \quad (-2a_1a_2a_3+6a_3^2+6a_1^2a_4-8a_2a_4-14a_1a_5)\\
+&T^4 \quad (a_1^2a_2^2a_3^2+2a_2^3a_3^2+2a_1^3a_3^3-16a_1a_2a_3^3+15a_3^4+2a_1^2a_2^3a_4-6a_2^4a_4-17a_1^3a_2a_3a_4+34a_1a_2^2a_3a_4+\\
&\quad 31a_1^2a_3^2a_4-40a_2a_3^2a_4+24a_1^4a_4^2-72a_1^2a_2a_4^2+40a_2^2a_4^2+a_1^3a_2^2a_5-8a_1^4a_3a_5+55a_1^2a_2a_3a_5-\\
&\quad 50a_2^2a_3a_5-70a_1a_2^2a_5-80a_1^3a_4a_5+160a_1a_2a_4a_5+40a_1^2a_5^2)\\
+&T^3 \quad (-2a_1a_2^4a_3^3-2a_1^4a_2a_3^4+8a_1^2a_2^2a_3^4+10a_2^3a_3^4+10a_1^3a_3^5-44a_1a_2a_3^5+20a_3^6-2a_1^3a_2^4a_3a_4+\\
&\quad 5a_1a_2^5a_3a_4+10a_1^4a_2^2a_3^2a_4+3a_1^2a_2^3a_3^2a_4-45a_2^4a_3^2a_4+8a_1^5a_3^3a_4-114a_1^3a_2a_3^3a_4+167a_1a_2^2a_3^3a_4+\\
&\quad 64a_1^2a_3^4a_4-80a_2a_3^4a_4+8a_1^4a_2^3a_4^2-37a_1^2a_2^4a_4^2+40a_2^5a_4^2-54a_1^5a_2a_3a_4^2+187a_1^3a_2^2a_3a_4^2-\\
&\quad 152a_1a_2^3a_3a_4^2+116a_1^4a_3^2a_4^2-284a_1^2a_2a_3^2a_4^2+160a_2^2a_3^2a_4^2+56a_1^6a_4^3-268a_1^4a_2a_4^3+384a_1^2a_2^2a_4^3-\\
&\quad 160a_2^3a_4^3-32a_1^3a_3a_4^3-2a_1^3a_2^5a_5+9a_1a_2^6a_5+10a_1^4a_2^3a_3a_5-61a_1^2a_2^4a_3a_5+15a_2^5a_3a_5+\\
&\quad 30a_1^3a_2^2a_3^2a_5+63a_1a_2^3a_3^2a_5-72a_1^4a_3^3a_5+236a_1^2a_2a_3^3a_5-200a_2^2a_3^3a_5-140a_1a_3^4a_5-12a_1^5a_2^2a_4a_5+\\
&\quad 76a_1^3a_3^2a_4a_5-54a_1a_2^4a_4a_5-32a_1^6a_3a_4a_5+316a_1^4a_2a_3a_4a_5-914a_1^2a_2^2a_3a_4a_5+400a_2^3a_3a_4a_5-\\
&\quad 236a_1^3a_2^3a_4a_5+640a_1a_2a_3^2a_4a_5-240a_1^5a_4^2a_5+952a_1^3a_2a_4^2a_5-640a_1a_2^2a_4^2a_5+32a_1^6a_2a_5^2-\\
&\quad 236a_1^4a_2^2a_5^2+400a_1^2a_2^3a_5^2-125a_2^4a_5^2+128a_1^5a_3a_5^2-310a_1^3a_2a_3a_5^2+175a_1a_2^2a_3a_5^2+160a_1^2a_3^2a_5^2+\\
&\quad 120a_1^4a_4a_5^2-780a_1^2a_2a_4a_5^2+320a_1^3a_5^3)\\
+&T^2 \quad (a_2^6a_3^4+4a_1^3a_2^3a_3^5-14a_1a_2^4a_3^5+a_1^6a_3^6-14a_1^4a_2a_3^6+27a_1^2a_2^2a_3^6+18a_2^3a_3^6+18a_1^3a_3^7-56a_1a_2a_3^7+\\
&\quad 15a_3^8+3a_1^2a_2^6a_3^2a_4-6a_2^7a_3^2a_4+3a_1^5a_2^2a_3^3a_4-44a_1^3a_2^4a_3^3a_4+72a_1a_2^5a_3^3a_4-13a_1^6a_2a_3^4a_4+\\
&\quad 102a_1^4a_2^2a_3^4a_4-73a_1^2a_2^3a_3^4a_4-107a_2^4a_3^4a_4+31a_1^5a_3^5a_4-251a_1^3a_2a_3^5a_4+297a_1a_2^2a_3^5a_4+\\
&\quad 66a_1^2a_3^6a_4-80a_2a_3^6a_4+a_1^4a_2^6a_4^2-6a_1^2a_2^7a_4^2+9a_2^8a_4^2-13a_1^5a_2^4a_3a_4^2+67a_1^3a_2^5a_3a_4^2-90a_1a_2^6a_3a_4^2+\\
&\quad 33a_1^6a_2^2a_3^2a_4^2-70a_1^4a_2^3a_3^2a_4^2-68a_1^2a_2^4a_3^2a_4^2+196a_2^5a_3^2a_4^2+22a_1^7a_3^3a_4^2-347a_1^5a_2a_3^3a_4^2+831a_1^3a_2^2a_3^3a_4^2-\\
&\quad 556a_1a_2^3a_3^3a_4^2+211a_1^4a_3^4a_4^2-420a_1^2a_2a_3^4a_4^2+240a_2^2a_3^4a_4^2+22a_1^6a_2^3a_4^3-138a_1^4a_2^4a_4^3+260a_1^2a_2^5a_4^3-\\
&\quad 136a_2^6a_4^3-116a_1^7a_2a_3a_4^3+618a_1^5a_2^2a_3a_4^3-1016a_1^3a_2^3a_3a_4^3+472a_1a_2^4a_3a_4^3+228a_1^6a_2^3a_4^4-\\
&\quad 876a_1^4a_2a_3^2a_4^3+1132a_1^2a_2^2a_3^2a_4^3-480a_2^3a_3^2a_4^3-96a_1^3a_3^3a_4^3+96a_1^8a_4^4-632a_1^6a_2a_4^4+1404a_1^4a_2^2a_4^4-\\
&\quad 1248a_1^2a_2^3a_4^4+400a_2^4a_4^4-48a_1^5a_3a_4^4+128a_1^3a_2a_3a_4^4-64a_1^4a_4^5+2a_1^4a_2^6a_3a_5-9a_1^2a_2^7a_3a_5-\\
&\quad 11a_1^5a_2^4a_3^2a_5+56a_1^3a_2^5a_3^2a_5+12a_1a_2^6a_3^2a_5+10a_1^6a_2^2a_3^3a_5-52a_1^4a_2^3a_3^3a_5-169a_1^2a_2^4a_3^3a_5-5a_2^5a_3^3a_5-\\
&\quad 12a_1^7a_3^4a_5+109a_1^5a_2a_3^4a_5-49a_1^3a_2^2a_3^4a_5+325a_1a_2^3a_3^4a_5-209a_1^4a_3^5a_5+378a_1^2a_2a_3^5a_5-\\
&\quad 300a_2^2a_3^5a_5-140a_1a_3^6a_5-5a_1^5a_2^5a_4a_5+32a_1^3a_2^6a_4a_5-36a_1a_2^7a_4a_5+30a_1^6a_2^3a_3a_4a_5-\\
&\quad 225a_1^4a_2^4a_3a_4a_5+219a_1^2a_2^5a_3a_4a_5+90a_2^6a_3a_4a_5+48a_1^7a_2a_3^2a_4a_5-260a_1^5a_2^2a_3^2a_4a_5+\\
&\quad 1020a_1^3a_2^3a_3^2a_4a_5-925a_1a_2^4a_3^2a_4a_5-236a_1^6a_3^3a_4a_5+1412a_1^4a_2a_3^3a_4a_5-3024a_1^2a_2^2a_3^3a_4a_5+\\
&\quad 1200a_2^3a_3^3a_4a_5-228a_1^3a_3^4a_4a_5+960a_1a_2a_3^4a_4a_5-36a_1^7a_2^2a_4^2a_5+260a_1^5a_2^3a_4^2a_5-357a_1^3a_2^4a_4^2a_5-\\
&\quad 40a_1a_2^5a_4^2a_5-120a_1^8a_3a_4^2a_5+1128a_1^6a_2a_3a_4^2a_5-4058a_1^4a_2^2a_3a_4^2a_5+5124a_1^2a_2^3a_3a_4^2a_5-\\
&\quad 1400a_2^4a_3a_4^2a_5-840a_1^5a_3^2a_4^2a_5+2488a_1^3a_2a_3^2a_4^2a_5-1920a_1a_2^2a_3^2a_4^2a_5-416a_1^7a_4^3a_5+\\
&\quad 2640a_1^5a_2a_4^3a_5-4568a_1^3a_2^2a_4^3a_5+1920a_1a_2^3a_4^3a_5+624a_1^4a_3a_4^3a_5+7a_1^6a_2^4a_5^2-13a_1^4a_2^5a_5^2-\\
&\quad 63a_1^2a_2^6a_5^2-72a_1^7a_2^2a_3a_5^2+330a_1^5a_2^3a_3a_5^2+2a_1^3a_2^4a_3a_5^2+20a_1a_2^5a_3a_5^2+48a_1^8a_3^2a_5^2-224a_1^6a_2a_3^2a_5^2-\\
&\quad 731a_1^4a_2^2a_3^2a_5^2+152a_1^2a_2^3a_3^2a_5^2+250a_2^4a_3^2a_5^2+782a_1^5a_3^3a_5^2-721a_1^3a_2a_3^3a_5^2+525a_1a_2^2a_3^3a_5^2+\\
&\quad 240a_1^2a_3^4a_5^2+144a_1^8a_2a_4a_5^2-984a_1^6a_2^2a_4a_5^2+1726a_1^4a_2^3a_4a_5^2-1276a_1^2a_2^4a_4a_5^2+500a_2^5a_4a_5^2+\\
&\quad 384a_1^7a_3a_4a_5^2-1220a_1^5a_2a_3a_4a_5^2+4854a_1^3a_2^2a_3a_4a_5^2-3300a_1a_2^3a_3a_4a_5^2-844a_1^4a_3^2a_4a_5^2-\\
&\quad 2340a_1^2a_2a_3^2a_4a_5^2+96a_1^6a_4^2a_5^2-3112a_1^4a_2a_4^2a_5^2+3340a_1^2a_2^2a_4^2a_5^2-64a_1^9a_5^3+176a_1^7a_2a_5^3+\\
&\quad 1036a_1^5a_2^2a_5^3-2800a_1^3a_2^3a_5^3+875a_1a_2^4a_5^3-968a_1^6a_3a_5^3+720a_1^4a_2a_3a_5^3+1450a_1^2a_2^2a_3a_5^3+\\
&\quad 960a_1^3a_3^2a_5^3+2400a_1^5a_4a_5^3-880a_1^3a_2a_4a_5^3-2560a_1^4a_5^4)+\cdots
\end{aligned}
$$

$$
\begin{aligned}
+T\quad & (-2a_1^2a_2^5a_3^6+4a_2^6a_3^6-2a_1^5a_2^2a_3^7+18a_1^3a_2^3a_3^7-28a_1a_2^4a_3^7+4a_1^6a_3^8-28a_1^4a_2a_3^8+34a_1^2a_2^2a_3^8+14a_2^3a_3^8+\\
& 14a_1^3a_3^9-34a_1a_2a_3^9+6a_3^{10}-a_1a_2^8a_3^3a_4-4a_1^4a_2^5a_3^4a_4+32a_1^2a_2^6a_3^4a_4-31a_2^7a_3^4a_4-a_1^7a_2^2a_3^5a_4+\\
& 39a_1^5a_2^3a_3^5a_4-202a_1^3a_2^4a_3^5a_4+201a_1a_2^5a_3^5a_4+2a_1^8a_3^6a_4-62a_1^6a_2a_3^6a_4+263a_1^4a_2^2a_3^6a_4-\\
& 167a_1^2a_2^3a_3^6a_4-103a_2^4a_3^6a_4+39a_1^5a_3^7a_4-228a_1^3a_2a_3^7a_4+229a_1a_2^2a_3^7a_4+34a_1^2a_3^8a_4-40a_2a_3^8a_4-\\
& a_1^3a_2^8a_3a_4^2+3a_1a_2^9a_3a_4^2-a_1^6a_2^5a_3^2a_4^2+27a_1^4a_2^6a_3^2a_4^2-91a_1^2a_2^7a_3^2a_4^2+69a_2^8a_3^2a_4^2+10a_1^7a_2^3a_3^3a_4^2-\\
& 170a_1^5a_2^4a_3^3a_4^2+519a_1^3a_2^5a_3^3a_4^2-424a_1a_2^6a_3^3a_4^2-19a_1^8a_2a_3^4a_4^2+227a_1^6a_2^2a_3^4a_4^2-446a_1^4a_2^3a_3^4a_4^2+\\
& 81a_1^2a_2^4a_3^4a_4^2+269a_2^5a_3^4a_4^2+77a_1^7a_3^5a_4^2-646a_1^5a_2a_3^5a_4^2+1118a_1^3a_2^2a_3^5a_4^2-656a_1a_2^3a_3^5a_4^2+\\
& 170a_1^4a_3^6a_4^2-276a_1^2a_2a_3^6a_4^2+160a_2^2a_3^6a_4^2+2a_1^6a_2^6a_4^3-15a_1^4a_2^7a_4^3+37a_1^2a_2^8a_4^3-32a_2^9a_4^3-\\
& 19a_1^7a_2^4a_3a_4^3+115a_1^5a_2^5a_3a_4^3-232a_1^3a_2^6a_3a_4^3+188a_1a_2^7a_3a_4^3+34a_1^8a_2^2a_3^2a_4^3-9a_1^6a_2^3a_3^2a_4^3-\\
& 462a_1^4a_2^4a_3^2a_4^3+726a_1^2a_2^5a_3^2a_4^3-348a_2^6a_3^2a_4^3+28a_1^9a_3^3a_4^3-628a_1^7a_2a_3^3a_4^3+2341a_1^5a_2^2a_3^3a_4^3-\\
& 2864a_1^3a_2^3a_3^3a_4^3+1220a_1a_2^4a_3^3a_4^3+278a_1^6a_3^4a_4^3-848a_1^4a_2a_3^4a_4^3+1112a_1^2a_2^2a_3^4a_4^3-480a_2^3a_3^4a_4^3-\\
& 96a_1^3a_3^5a_4^3+28a_1^8a_2^3a_4^4-222a_1^6a_2^4a_4^4+621a_1^4a_2^5a_4^4-732a_1^2a_2^6a_4^4+256a_2^7a_4^4-128a_1^9a_2a_3a_4^4+\\
& 892a_1^7a_2^2a_3a_4^4-2320a_1^5a_2^3a_3a_4^4+2948a_1^3a_2^4a_3a_4^4-1312a_1a_2^5a_3a_4^4+328a_1^8a_2^3a_4^4-1636a_1^6a_2a_3^2a_4^4+\\
& 2560a_1^4a_2^2a_3^2a_4^4-2432a_1^2a_2^3a_3^2a_4^4+800a_2^4a_3^2a_4^4-112a_1^5a_3^3a_4^4+256a_1^3a_2a_3^3a_4^4+96a_1^{10}a_5^4-816a_1^8a_2a_5^4+\\
& 2632a_1^6a_2^2a_5^4-4128a_1^4a_2^3a_5^4+2848a_1^2a_2^4a_5^4-512a_2^5a_5^4-144a_1^7a_3a_5^4+896a_1^5a_2a_3a_5^4-512a_1^3a_2^2a_3a_5^4-\\
& 128a_1^4a_3^2a_5^4-128a_1^6a_4^4-2a_1^3a_2^8a_3^2a_5+9a_1a_2^9a_3^2a_5-2a_1^6a_2^5a_3^3a_5+32a_1^4a_2^6a_3^3a_5-118a_1^2a_2^7a_3^3a_5+\\
& 31a_2^8a_3^3a_5+9a_1^7a_2^3a_3^4a_5-123a_1^5a_2^4a_3^4a_5+428a_1^3a_2^5a_3^4a_5-93a_1a_2^6a_3^4a_5+76a_1^6a_2^2a_3^5a_5-\\
& 347a_1^4a_2^3a_3^5a_5-225a_1^2a_2^4a_3^5a_5+3a_2^5a_3^5a_5-58a_1^7a_3^6a_5+365a_1^5a_2a_3^6a_5-210a_1^3a_2^2a_3^6a_5+\\
& 461a_1a_2^3a_3^6a_5-234a_1^4a_3^7a_5+268a_1^2a_2a_3^7a_5-200a_2^2a_3^7a_5-70a_1a_3^8a_5-2a_1^5a_2^8a_4a_5+15a_1^3a_2^9a_4a_5-\\
& 27a_1a_2^{10}a_4a_5+22a_1^6a_2^6a_3a_4a_5-179a_1^4a_2^7a_3a_4a_5+369a_1^2a_2^8a_3a_4a_5-117a_2^9a_3a_4a_5-\\
& 60a_1^7a_2^4a_3^2a_4a_5+550a_1^5a_2^5a_3^2a_4a_5-1136a_1^3a_2^6a_3^2a_4a_5+327a_1a_2^7a_3^2a_4a_5-4a_1^8a_2^2a_3^3a_4a_5-\\
& 182a_1^6a_2^3a_3^3a_4a_5+160a_1^4a_2^4a_3^3a_4a_5+546a_1^2a_2^5a_3^3a_4a_5+75a_2^6a_3^3a_4a_5-24a_1^9a_3^4a_4a_5+\\
& 470a_1^7a_2a_3^4a_4a_5-1854a_1^5a_2^2a_3^4a_4a_5+3512a_1^3a_2^3a_3^4a_4a_5-2359a_1a_2^4a_3^4a_4a_5-390a_1^6a_3^5a_4a_5+\\
& 1694a_1^4a_2a_3^5a_4a_5-3306a_1^2a_2^2a_3^5a_4a_5+1200a_2^3a_3^5a_4a_5-68a_1^3a_3^6a_4a_5+640a_1a_2a_3^6a_4a_5-\\
& 29a_1^7a_2^5a_4^2a_5+252a_1^5a_2^6a_4^2a_5-628a_1^3a_2^7a_4^2a_5+420a_1a_2^8a_4^2a_5+134a_1^8a_2^3a_3a_4^2a_5-1291a_1^6a_2^4a_3a_4^2a_5+\\
& 3179a_1^4a_2^5a_3a_4^2a_5-1673a_1^2a_2^6a_3a_4^2a_5-260a_2^7a_3a_4^2a_5+120a_1^9a_2a_3^2a_4^2a_5-526a_1^7a_2^2a_3^2a_4^2a_5+\\
& 2365a_1^5a_2^3a_3^2a_4^2a_5-6589a_1^3a_2^4a_3^2a_4^2a_5+3732a_1a_2^5a_3^2a_4^2a_5-588a_1^8a_3^3a_4^2a_5+4074a_1^6a_2a_3^3a_4^2a_5-\\
& 9182a_1^4a_2^2a_3^3a_4^2a_5+10368a_1^2a_2^3a_3^3a_4^2a_5-2800a_2^4a_3^3a_4^2a_5-982a_1^5a_3^4a_4^2a_5+2120a_1^3a_2a_3^4a_4^2a_5-\\
& 1920a_1a_2^2a_3^4a_4^2a_5-104a_1^9a_2^2a_3^4a_5+952a_1^7a_2^3a_3^4a_5-2510a_1^5a_2^4a_3^4a_5+1896a_1^3a_2^5a_3^4a_5+8a_1a_2^6a_3^4a_5-\\
& 176a_1^{10}a_3a_4^3a_5+1648a_1^8a_2a_3a_4^3a_5-7764a_1^6a_2^2a_3a_4^3a_5+17448a_1^4a_2^3a_3a_4^3a_5-14056a_1^2a_2^4a_3a_4^3a_5+\\
& 2400a_2^5a_3a_4^3a_5-880a_1^7a_2^2a_3^2a_4^3a_5+2808a_1^5a_2a_2^3a_3^2a_4^3a_5-6056a_1^3a_2^2a_2^3a_3^2a_4^3a_5+3840a_1a_2^3a_2^3a_3^2a_4^3a_5+\\
& 1248a_1^4a_3^3a_4^3a_5-416a_1^9a_4^4a_5+3712a_1^7a_2a_4^4a_5-10248a_1^5a_2^2a_4^4a_5+10624a_1^3a_2^3a_4^4a_5-4000a_1a_2^4a_4^4a_5+\\
& 928a_1^6a_3a_4^4a_5-1664a_1^4a_2a_3a_4^4a_5+640a_1^5a_4^5a_5-a_1^6a_2^7a_5^2+18a_1^4a_2^8a_5^2-81a_1^2a_2^9a_5^2+108a_2^{10}a_5^2-\\
& 112a_1^5a_2^6a_3a_5^2+647a_1^3a_2^7a_3a_5^2-855a_1a_2^8a_3a_5^2+24a_1^8a_2^3a_3^2a_5^2+226a_1^6a_2^4a_3^2a_5^2-1920a_1^4a_2^5a_3^2a_5^2+\\
& 2254a_1^2a_2^6a_3^2a_5^2+325a_2^7a_3^2a_5^2-580a_1^7a_2^2a_3^3a_5^2+3444a_1^5a_2^3a_3^3a_5^2-2437a_1^3a_2^4a_3^3a_5^2-1335a_1a_2^5a_3^3a_5^2+\\
& 312a_1^8a_3^4a_5^2-1851a_1^6a_2a_3^4a_5^2-257a_1^4a_2^2a_3^4a_5^2+270a_1^2a_2^3a_3^4a_5^2+875a_2^4a_3^4a_5^2+1441a_1^5a_3^5a_5^2-\\
& 512a_1^3a_2a_3^5a_5^2+525a_1a_2^2a_3^5a_5^2+160a_1^2a_3^6a_5^2+38a_1^8a_2^4a_4a_5^2-198a_1^6a_2^5a_4a_5^2+62a_1^4a_2^6a_4a_5^2+\\
& 613a_1^2a_2^7a_4a_5^2-525a_2^8a_4a_5^2-288a_1^9a_2^2a_3a_4a_5^2+1844a_1^7a_2^3a_3a_4a_5^2-2385a_1^5a_2^4a_3a_4a_5^2-\\
& 227a_1^3a_2^5a_3a_4a_5^2+30a_1a_2^6a_3a_4a_5^2+96a_1^{10}a_3^2a_4a_5^2-688a_1^8a_2a_3^2a_4a_5^2-838a_1^6a_2^2a_3^2a_4a_5^2-\\
& 379a_1^4a_2^3a_3^2a_4a_5^2+7310a_1^2a_2^4a_3^2a_4a_5^2-1750a_2^5a_3^2a_4a_5^2+1316a_1^7a_3^3a_4a_5^2-1544a_1^5a_2a_3^3a_4a_5^2+\\
& 5101a_1^3a_2^2a_3^3a_4a_5^2-6600a_1a_2^3a_3^3a_4a_5^2-2048a_1^4a_3^4a_4a_5^2-2340a_1^2a_2a_3^4a_4a_5^2+336a_1^{10}a_2a_4^2a_5^2-\\
& 2736a_1^8a_2^2a_4^2a_5^2+6772a_1^6a_2^3a_4^2a_5^2-6258a_1^4a_2^4a_4^2a_5^2+1950a_1^2a_2^5a_4^2a_5^2+500a_2^6a_4^2a_5^2+1056a_1^9a_3a_4^2a_5^2-\\
& 4480a_1^7a_2a_3a_4^2a_5^2+13828a_1^5a_2^2a_3a_4^2a_5^2-23296a_1^3a_2^3a_3a_4^2a_5^2+9700a_1a_2^4a_3a_4^2a_5^2-248a_1^6a_3^2a_4^2a_5^2-\\
& 1572a_1^4a_2a_3^2a_4^2a_5^2+6680a_1^2a_2^2a_3^2a_4^2a_5^2-608a_1^8a_4^3a_5^2-2096a_1^6a_2a_4^3a_5^2+9112a_1^4a_2^2a_4^3a_5^2-\\
& 3680a_1^2a_2^3a_4^3a_5^2-3856a_1^5a_3a_4^3a_5^2+16a_1^9a_2^3a_5^3-310a_1^7a_2^4a_5^3+1535a_1^5a_2^5a_5^3-2828a_1^3a_2^6a_5^3+\\
& 2250a_1a_2^7a_5^3+1040a_1^8a_2^2a_3a_5^3-6810a_1^6a_2^3a_3a_5^3+12487a_1^4a_2^4a_3a_5^3-8755a_1^2a_2^5a_3a_5^3-625a_2^6a_3a_5^3-\\
& 736a_1^9a_2^2a_5^3+4392a_1^7a_2a_2^3a_5^3-798a_1^5a_2^2a_3^2a_5^3-6377a_1^3a_2^3a_3^2a_5^3+6125a_1a_2^4a_3^2a_5^3-3812a_1^6a_3^3a_5^3+\\
& 786a_1^4a_2a_3^3a_5^3+2900a_1^2a_2^2a_3^3a_5^3+960a_1^3a_3^4a_5^3-128a_1^{11}a_4a_5^3-288a_1^9a_2a_4a_5^3+7448a_1^7a_2^2a_4a_5^3-\\
& 21968a_1^5a_2^3a_4a_5^3+24086a_1^3a_2^4a_4a_5^3-9000a_1a_2^5a_4a_5^3-1456a_1^8a_3a_4a_5^3-3856a_1^6a_2a_3a_4a_5^3+\\
& 8836a_1^4a_2^2a_3a_4a_5^3-7800a_1^2a_2^3a_3a_4a_5^3+10144a_1^5a_3^2a_4a_5^3-1760a_1^3a_2a_3^2a_4a_5^3+5408a_1^7a_4^2a_5^3-\\
& 6368a_1^5a_2a_4^2a_5^3-1240a_1^3a_2^2a_4^2a_5^3+640a_1^{10}a_5^4-4144a_1^8a_2a_5^4+6784a_1^6a_2^2a_5^4-1800a_1^4a_2^3a_5^4-\\
& 1000a_1^2a_2^4a_5^4+3125a_2^5a_5^4+3648a_1^7a_3a_5^4-2400a_1^5a_2a_3a_5^4-7200a_1^3a_2^2a_3a_5^4-5120a_1^4a_3^2a_5^4-\\
& 12160a_1^6a_4a_5^4+13760a_1^4a_2a_4a_5^4+6656a_1^5a_5^5)+\cdots
\end{aligned}
$$

$$
\begin{aligned}
+\ & (a_1^4a_2^4a_3^8 - 4a_1^2a_2^5a_3^8 + 4a_2^6a_3^8 - 4a_1^5a_2^2a_3^9 + 16a_1^3a_2^3a_3^9 - 16a_1a_2^4a_3^9 + 4a_1^6a_3^{10} - 16a_1^4a_2a_3^{10} + 14a_1^2a_2^2a_3^{10} + \\
& 4a_2^3a_3^{10}4a_1^3a_3^{11} - 8a_1a_2a_3^{11} + a_3^{12} + a_1^3a_2^7a_3^5a_4 - 2a_1a_2^8a_3^5a_4 + a_1^6a_2^4a_3^6a_4 - 21a_1^4a_2^5a_3^6a_4 + 57a_1^2a_2^6a_3^6a_4 - \\
& 38a_2^7a_3^6a_4 - 4a_1^7a_2^2a_3^7a_4 + 72a_1^5a_2^3a_3^7a_4 - 199a_1^3a_2^4a_3^7a_4 + 141a_1a_2^5a_3^7a_4 + 4a_1^8a_3^8a_4 - 68a_1^6a_2a_3^8a_4 + \\
& 178a_1^4a_2^2a_3^8a_4 - 93a_1^2a_2^3a_3^8a_4 - 35a_2^4a_3^8a_4 + 16a_1^5a_3^9a_4 - 74a_1^3a_2a_3^9a_4 + 65a_1a_2^2a_3^9a_4 + 7a_1^2a_3^{10}a_4 - \\
& 8a_2a_3^{10}a_4 + a_2^{11}a_3^2a_4^2 + a_1^5a_2^7a_3^3a_4^2 - 9a_1^3a_2^8a_3^3a_4^2 + 3a_1a_2^9a_3^3a_4^2 - 13a_1^6a_2^5a_3^4a_4^2 + 119a_1^4a_2^6a_3^4a_4^2 - \\
& 199a_1^2a_2^7a_3^4a_4^2 + 125a_2^8a_3^4a_4^2 + 41a_1^7a_2^3a_3^5a_4^2 - 358a_1^5a_2^4a_3^5a_4^2 + 649a_1^3a_2^5a_3^5a_4^2 - 417a_1a_2^6a_3^5a_4^2 \\
& + a_1^{10}a_3^6a_4^2 - 48a_1^8a_2a_3^6a_4^2 + 316a_1^6a_2^2a_3^6a_4^2 - 436a_1^4a_2^3a_3^6a_4^2 + 166a_1^2a_2^4a_3^6a_4^2 + 113a_2^5a_3^6a_4^2 + 72a_1^7a_3^7a_4^2 - \\
& 372a_1^5a_2a_3^7a_4^2 + 474a_1^3a_2^2a_3^7a_4^2 - 252a_1a_2^3a_3^7a_4^2 + 51a_1^4a_3^8a_4^2 - 68a_1^2a_2a_3^8a_4^2 + 40a_2^2a_3^8a_4^2 + a_1^2a_2^{11}a_4^3 - \\
& 4a_2^{12}a_4^3 - 3a_1^5a_2^8a_3a_4^3 + 7a_1^3a_2^9a_3a_4^3 + 20a_1a_2^{10}a_3a_4^3 + 31a_1^6a_2^6a_3^2a_4^3 - 151a_1^4a_2^7a_3^2a_4^3 + 163a_1^2a_2^8a_3^2a_4^3 \\
& - 160a_2^9a_3^2a_4^3 + 2a_1^9a_2^3a_3^3a_4^3 - 99a_1^7a_2^4a_3^3a_4^3 + 418a_1^5a_2^5a_3^3a_4^3 - 480a_1^3a_2^6a_3^3a_4^3 + 418a_1a_2^7a_3^3a_4^3 - \\
& 12a_1^{10}a_2a_3^4a_4^3 + 148a_1^8a_2^2a_3^4a_4^3 - 227a_1^6a_2^3a_3^4a_4^3 - 223a_1^4a_2^4a_3^4a_4^3 + 226a_1^2a_2^5a_3^4a_4^3 - 195a_2^6a_3^4a_4^3 + \\
& 60a_1^9a_3^5a_4^3 - 794a_1^7a_2a_3^5a_4^3 + 2097a_1^5a_2^2a_3^5a_4^3 - 2024a_1^3a_2^3a_3^5a_4^3 + 748a_1a_2^4a_3^5a_4^3 + 101a_1^6a_3^6a_4^3 - \\
& 240a_1^4a_2a_3^6a_4^3 + 364a_1^2a_2^2a_3^6a_4^3 - 160a_2^3a_3^6a_4^3 - 32a_1^3a_3^7a_4^3 + a_1^8a_2^6a_4^4 - 5a_1^6a_2^7a_4^4 + 13a_1^4a_2^8a_4^4 - 48a_1^2a_2^9a_4^4 + \\
& 48a_2^{10}a_4^4 - 12a_1^9a_2^4a_3a_4^4 + 42a_1^7a_2^5a_3a_4^4 + 45a_1^5a_2^6a_3a_4^4 - 94a_1^3a_2^7a_3a_4^4 + 64a_1a_2^8a_3a_4^4 + 36a_1^{10}a_2^2a_3^2a_4^4 - \\
& 84a_1^8a_2^3a_3^2a_4^4 - 456a_1^6a_2^4a_3^2a_4^4 + 1117a_1^4a_2^5a_3^2a_4^4 - 1126a_1^2a_2^6a_3^2a_4^4 + 240a_2^7a_3^2a_4^4 + 16a_1^{11}a_3^3a_4^4 - \\
& 440a_1^9a_2a_3^3a_4^4 + 2392a_1^7a_2^2a_3^3a_4^4 - 4756a_1^5a_2^3a_3^3a_4^4 + 4904a_1^3a_2^4a_3^3a_4^4 - 1536a_1a_2^5a_3^3a_4^4 + 312a_1^8a_3^4a_4^4 - \\
& 1076a_1^6a_2a_3^4a_4^4 + 1168a_1^4a_2^2a_3^4a_4^4 - 1184a_1^2a_2^3a_3^4a_4^4 + 400a_2^4a_3^4a_4^4 - 64a_1^5a_3^5a_4^4 + 128a_1^3a_2a_3^5a_4^4 + \\
& 16a_1^{10}a_2^3a_4^5 - 120a_1^8a_2^4a_4^5 + 316a_1^6a_2^5a_4^5 - 451a_1^4a_2^6a_4^5 + 368a_1^2a_2^7a_4^5 - 192a_2^8a_4^5 - 96a_1^{11}a_2a_3a_4^5 + \\
& 768a_1^9a_2^2a_3a_4^5 - 2264a_1^7a_2^3a_3a_4^5 + 3788a_1^5a_2^4a_3a_4^5 - 3392a_1^3a_2^5a_3a_4^5 + 1472a_1a_2^6a_3a_4^5 + 224a_1^{10}a_3^2a_4^5 - \\
& 1856a_1^8a_2a_3^2a_4^5 + 4460a_1^6a_2^2a_3^2a_4^5 - 5280a_1^4a_2^3a_3^2a_4^5 + 2272a_1^2a_2^4a_3^2a_4^5 - 512a_2^5a_3^2a_4^5 - 224a_1^7a_3^3a_4^5 \\
& + 1024a_1^5a_2a_3^3a_4^5 - 512a_1^3a_2^2a_3^3a_4^5 - 64a_1^4a_3^4a_4^5 + 64a_1^{12}a_4^6 - 640a_1^{10}a_2a_4^6 + 2528a_1^8a_2^2a_4^6 - 5280a_1^6a_2^3a_4^6 + \\
& 5776a_1^4a_2^4a_4^6 - 2816a_1^2a_2^5a_4^6 + 256a_2^6a_4^6 + 64a_1^9a_3a_4^6 + 640a_1^7a_2a_3a_4^6 - 2048a_1^5a_2^2a_3a_4^6 + 2048a_1^3a_2^3a_3a_4^6 - \\
& 128a_1^6a_3^2a_4^6 - 320a_1^8a_4^7 + 1024a_1^6a_2a_4^7 - 1024a_1^4a_2^2a_4^7 + a_1^2a_2^{10}a_3^3a_5 - 4a_2^{11}a_3^3a_5 - 11a_1^3a_2^8a_3^4a_5 + \\
& 44a_1a_2^9a_3^4a_5 + a_1^8a_2^4a_3^5a_5 - 9a_1^6a_2^5a_3^5a_5 + 80a_1^4a_2^6a_3^5a_5 - 241a_1^2a_2^7a_3^5a_5 + 19a_2^8a_3^5a_5 - 4a_1^9a_2^2a_3^6a_5 + \\
& 34a_1^7a_2^3a_3^6a_5 - 216a_1^5a_2^4a_3^6a_5 + 569a_1^3a_2^5a_3^6a_5 - 15a_1a_2^6a_3^6a_5 + 8a_1^8a_2a_3^7a_5 + 60a_1^6a_2^2a_3^7a_5 - \\
& 312a_1^4a_2^3a_3^7a_5 - 278a_1^2a_2^4a_3^7a_5 + 23a_2^5a_3^7a_5 - 72a_1^7a_3^8a_5 + 338a_1^5a_2a_3^8a_5 - 132a_1^3a_2^2a_3^8a_5 + 199a_1a_2^3a_3^8a_5 - \\
& 89a_1^4a_3^9a_5 + 71a_1^2a_2a_3^9a_5 - 50a_2^2a_3^9a_5 - 14a_1a_3^{10}a_5 + a_1^4a_2^{10}a_3a_4a_5 - 9a_1^2a_2^{11}a_3a_4a_5 + 18a_2^{12}a_3a_4a_5 + \\
& a_1^7a_2^7a_3^2a_4a_5 - 18a_1^5a_2^8a_3^2a_4a_5 + 119a_1^3a_2^9a_3^2a_4a_5 - 218a_1a_2^{10}a_3^2a_4a_5 - 12a_1^8a_2^5a_3^3a_4a_5 + 142a_1^6a_2^6a_3^3a_4a_5 - \\
& 730a_1^4a_2^7a_3^3a_4a_5 + 1234a_1^2a_2^8a_3^3a_4a_5 - 105a_2^9a_3^3a_4a_5 + 29a_1^9a_2^3a_3^4a_4a_5 - 321a_1^7a_2^4a_3^4a_4a_5 + \\
& 1595a_1^5a_2^5a_3^4a_4a_5 - 2574a_1^3a_2^6a_3^4a_4a_5 + 45a_1a_2^7a_3^4a_4a_5 + 16a_1^{10}a_2a_3^5a_4a_5 - 101a_1^8a_2^2a_3^5a_4a_5 - \\
& 190a_1^6a_2^3a_3^5a_4a_5 + 436a_1^4a_2^4a_3^5a_4a_5 + 1296a_1^2a_2^5a_3^5a_4a_5 - 139a_2^6a_3^5a_4a_5 - 74a_1^9a_3^6a_4a_5 + 947a_1^7a_2a_3^6a_4a_5 - \\
& 2863a_1^5a_2^2a_3^6a_4a_5 + 3200a_1^3a_2^3a_3^6a_4a_5 - 1488a_1a_2^4a_3^6a_4a_5 - 203a_1^6a_3^7a_4a_5 + 598a_1^4a_2a_3^7a_4a_5 - \\
& 1196a_1^2a_2^2a_3^7a_4a_5 + 400a_2^3a_3^7a_4a_5 + 4a_1^3a_3^8a_4a_5 + 160a_1a_2a_3^8a_4a_5 - 2a_1^7a_2^8a_4^2a_5 + 20a_1^5a_2^9a_4^2a_5 - \\
& 64a_1^3a_2^{10}a_4^2a_5 + 66a_1a_2^{11}a_4^2a_5 + 17a_1^8a_2^6a_3a_4^2a_5 - 188a_1^6a_2^7a_3a_4^2a_5 + 645a_1^4a_2^8a_3a_4^2a_5 - 774a_1^2a_2^9a_3a_4^2a_5 + \\
& 196a_2^{10}a_3a_4^2a_5 - 6a_1^9a_2^4a_3^2a_4^2a_5 + 216a_1^7a_2^5a_3^2a_4^2a_5 - 836a_1^5a_2^6a_3^2a_4^2a_5 + 802a_1^3a_2^7a_3^2a_4^2a_5 - \\
& 87a_1a_2^8a_3^2a_4^2a_5 - 134a_1^{10}a_2^2a_3^3a_4^2a_5 + 899a_1^8a_2^3a_3^3a_4^2a_5 - 2687a_1^6a_2^4a_3^3a_4^2a_5 + 4087a_1^4a_2^5a_3^3a_4^2a_5 - \\
& 1614a_1^2a_2^6a_3^3a_4^2a_5 + 330a_2^7a_3^3a_4^2a_5 - 28a_1^{11}a_3^4a_4^2a_5 + 688a_1^9a_2a_3^4a_4^2a_5 - 3747a_1^7a_2^2a_3^4a_4^2a_5 + \\
& 9141a_1^5a_2^3a_3^4a_4^2a_5 - 12571a_1^3a_2^4a_3^4a_4^2a_5 + 4254a_1a_2^5a_3^4a_4^2a_5 - 778a_1^8a_2^5a_3^2a_4^2a_5 + 4139a_1^6a_2a_3^5a_4^2a_5 - \\
& 5654a_1^4a_2^2a_3^5a_4^2a_5 + 5244a_1^2a_2^3a_3^5a_4^2a_5 - 1400a_2^4a_3^5a_4^2a_5 - 382a_1^5a_3^6a_4^2a_5 + 584a_1^3a_2a_3^6a_4^2a_5 - \\
& 640a_1a_2^2a_3^6a_4^2a_5 - 22a_1^9a_2^2a_3^4a_5 + 251a_1^7a_2^6a_3^4a_5 - 1011a_1^5a_2^7a_3^4a_5 + 1735a_1^3a_2^8a_3^4a_5 - 1072a_1a_2^9a_3^4a_5 + \\
& 48a_1^{10}a_2^3a_3a_3^4a_5 - 758a_1^8a_2^4a_3a_3^4a_5 + 3537a_1^6a_2^5a_3a_3^4a_5 - 6671a_1^4a_2^6a_3a_3^4a_5 + 4498a_1^2a_2^7a_3a_3^4a_5 - \\
& 160a_2^8a_3a_3^4a_5 + 296a_1^{11}a_2a_3^2a_3^4a_5 - 2264a_1^9a_2^2a_3^2a_3^4a_5 + 6448a_1^7a_2^3a_3^2a_3^4a_5 - 9011a_1^5a_2^4a_3^2a_3^4a_5 + \\
& 8588a_1^3a_2^5a_3^2a_3^4a_5 - 5888a_1a_2^6a_3^2a_3^4a_5 - 600a_1^{10}a_3^3a_3^4a_5 + 6156a_1^8a_2a_3^3a_3^4a_5 - 19956a_1^6a_2^2a_3^3a_3^4a_5 + \\
& 25472a_1^4a_2^3a_3^3a_3^4a_5 - 10620a_1^2a_2^4a_3^3a_3^4a_5 + 2400a_2^5a_3^3a_3^4a_5 - 416a_1^7a_3^4a_3^4a_5 - 544a_1^5a_2a_3^4a_3^4a_5 - \\
& 1488a_1^3a_2^2a_3^4a_3^4a_5 + 1920a_1a_2^3a_3^4a_3^4a_5 + 624a_1^4a_3^5a_3^4a_5 - 48a_1^{11}a_2^2a_4^4a_5 + 544a_1^9a_2^3a_4^4a_5 - 2208a_1^7a_2^4a_4^4a_5 + \\
& 4170a_1^5a_2^5a_4^4a_5 - 3648a_1^3a_2^6a_4^4a_5 + 1376a_1a_2^7a_4^4a_5 - 224a_1^{12}a_3a_4^4a_5 + 2256a_1^{10}a_2a_3a_4^4a_5 - \\
& 9256a_1^8a_2^2a_3a_4^4a_5 + 19748a_1^6a_2^3a_3a_4^4a_5 - 24916a_1^4a_2^4a_3a_4^4a_5 + 15168a_1^2a_2^5a_3a_4^4a_5 - 1600a_2^6a_3a_4^4a_5 - \\
& 1232a_1^9a_3^2a_4^4a_5 + 4520a_1^7a_2a_3^2a_4^4a_5 - 512a_1^5a_2^2a_3^2a_4^4a_5 - 2112a_1^3a_2^3a_3^2a_4^4a_5 - 4000a_1a_2^4a_3^2a_4^4a_5 + \cdots
\end{aligned}
$$

$$
\begin{aligned}
+\ & 1072a_1^6a_3^3a_4^4a_5 - 1664a_1^4a_2a_3^3a_4^4a_5 - 192a_1^{11}a_4^5a_5 + 1920a_1^9a_2a_4^5a_5 - 7056a_1^7a_2^2a_4^5a_5 + 13504a_1^5a_2^3a_4^5a_5 - \\
& 12192a_1^3a_2^4a_4^5a_5 + 3328a_1a_2^5a_4^5a_5 + 1472a_1^8a_3a_4^5a_5 - 9472a_1^6a_2a_3a_4^5a_5 + 9728a_1^4a_2^2a_3a_4^5a_5 + \\
& 640a_1^5a_2^3a_4^5a_5 + 1152a_1^7a_4^6a_5 - 1024a_1^5a_2a_4^6a_5 + a_1^6a_2^{10}a_5^2 - 9a_1^4a_2^{11}a_5^2 + 27a_1^2a_2^{12}a_5^2 - 27a_2^{13}a_5^2 - \\
& 11a_1^7a_2^8a_3a_5^2 + 97a_1^5a_2^9a_3a_5^2 - 285a_1^3a_2^{10}a_3a_5^2 + 279a_1a_2^{11}a_3a_5^2 + 45a_1^8a_2^6a_3^2a_5^2 - 381a_1^6a_2^7a_3^2a_5^2 + \\
& 1074a_1^4a_2^8a_3^2a_5^2 - 1007a_1^2a_2^9a_3^2a_5^2 - 42a_2^{10}a_3^2a_5^2 - 76a_1^9a_2^4a_3^3a_5^2 + 585a_1^7a_2^5a_3^3a_5^2 - 1509a_1^5a_2^6a_3^3a_5^2 + \\
& 1417a_1^3a_2^7a_3^3a_5^2 + 81a_1a_2^8a_3^3a_5^2 + 32a_1^{10}a_2^2a_3^4a_5^2 - 129a_1^8a_2^3a_3^4a_5^2 + 238a_1^6a_2^4a_3^4a_5^2 - 1232a_1^4a_2^5a_3^4a_5^2 + \\
& 916a_1^2a_2^6a_3^4a_5^2 + 200a_2^7a_3^4a_5^2 - 80a_1^9a_2a_3^5a_5^2 - 351a_1^7a_2^2a_3^5a_5^2 + 3851a_1^5a_2^3a_3^5a_5^2 - 3321a_1^3a_2^4a_3^5a_5^2 - \\
& 882a_1a_2^5a_3^5a_5^2 + 505a_1^8a_3^6a_5^2 - 2783a_1^6a_2a_3^6a_5^2 + 1258a_1^4a_2^2a_3^6a_5^2 + 518a_1^2a_2^3a_3^6a_5^2 + 500a_2^4a_3^6a_5^2 + \\
& 787a_1^5a_3^7a_5^2 - 101a_1^3a_2a_3^7a_5^2 + 175a_1a_2^2a_3^7a_5^2 + 40a_1^2a_3^8a_5^2 + 15a_1^8a_2^7a_4a_5^2 - 121a_1^6a_2^8a_4a_5^2 + 297a_1^4a_2^9a_4a_5^2 - \\
& 174a_1^2a_2^{10}a_4a_5^2 - 99a_2^{11}a_4a_5^2 - 133a_1^9a_2^5a_3a_4a_5^2 + 1037a_1^7a_2^6a_3a_4a_5^2 - 2278a_1^5a_2^7a_3a_4a_5^2 + \\
& 544a_1^3a_2^8a_3a_4a_5^2 + 1763a_1a_2^9a_3a_4a_5^2 + 344a_1^{10}a_2^3a_3^2a_4a_5^2 - 2473a_1^8a_2^4a_3^2a_4a_5^2 + 3701a_1^6a_2^5a_3^2a_4a_5^2 + \\
& 4528a_1^4a_2^6a_3^2a_4a_5^2 - 8732a_1^2a_2^7a_3^2a_4a_5^2 - 1250a_2^8a_3^2a_4a_5^2 - 128a_1^{11}a_2a_3^3a_4a_5^2 + 196a_1^9a_2^2a_3^3a_4a_5^2 + \\
& 6290a_1^7a_2^3a_3^3a_4a_5^2 - 22646a_1^5a_2^4a_3^3a_4a_5^2 + 18944a_1^3a_2^5a_3^3a_4a_5^2 + 3475a_1a_2^6a_3^3a_4a_5^2 + 472a_1^{10}a_3^4a_4a_5^2 - \\
& 4676a_1^8a_2a_3^4a_4a_5^2 + 10872a_1^6a_2^2a_3^4a_4a_5^2 - 8585a_1^4a_2^3a_3^4a_4a_5^2 + 2473a_1^2a_2^4a_3^4a_4a_5^2 - 2250a_2^5a_3^4a_4a_5^2 + \\
& 1016a_1^7a_3^5a_4a_5^2 + 223a_1^5a_2a_3^5a_4a_5^2 + 247a_1^3a_2^2a_3^5a_4a_5^2 - 3300a_1a_2^3a_3^5a_4a_5^2 - 1084a_1^4a_3^6a_4a_5^2 - \\
& 780a_1^2a_2a_3^6a_4a_5^2 + 128a_1^{10}a_2^4a_4^2a_5^2 - 1116a_1^8a_2^5a_4^2a_5^2 + 3125a_1^6a_2^6a_4^2a_5^2 - 2763a_1^4a_2^7a_4^2a_5^2 - 564a_1^2a_2^8a_4^2a_5^2 + \\
& 1200a_2^9a_4^2a_5^2 - 648a_1^{11}a_2^2a_3a_4^2a_5^2 + 5772a_1^9a_2^3a_3a_4^2a_5^2 - 15950a_1^7a_2^4a_3a_4^2a_5^2 + 14455a_1^5a_2^5a_3a_4^2a_5^2 - \\
& 2253a_1^3a_2^6a_3a_4^2a_5^2 + 590a_1a_2^7a_3a_4^2a_5^2 + 176a_1^{12}a_3^2a_4^2a_5^2 - 1640a_1^{10}a_2a_3^2a_4^2a_5^2 - 552a_1^8a_2^2a_3^2a_4^2a_5^2 + \\
& 14982a_1^6a_2^3a_3^2a_4^2a_5^2 - 7956a_1^4a_2^4a_3^2a_4^2a_5^2 - 15414a_1^2a_2^5a_3^2a_4^2a_5^2 + 3750a_2^6a_3^2a_4^2a_5^2 + 2560a_1^9a_3^3a_4^2a_5^2 - \\
& 9928a_1^7a_2a_3^3a_4^2a_5^2 + 7032a_1^5a_2^2a_3^3a_4^2a_5^2 - 5476a_1^3a_2^3a_3^3a_4^2a_5^2 + 9700a_1a_2^4a_3^3a_4^2a_5^2 - 328a_1^6a_3^4a_4^2a_5^2 + \\
& 1540a_1^4a_2a_3^4a_4^2a_5^2 + 3340a_1^2a_2^2a_3^4a_4^2a_5^2 + 416a_1^{12}a_2a_4^3a_5^2 - 4160a_1^{10}a_2^2a_4^3a_5^2 + 14888a_1^8a_2^3a_4^3a_5^2 - \\
& 25092a_1^6a_2^4a_4^3a_5^2 + 22636a_1^4a_2^5a_4^3a_5^2 - 9206a_1^2a_2^6a_4^3a_5^2 - 2000a_2^7a_4^3a_5^2 + 928a_1^{11}a_3a_4^3a_5^2 - 4464a_1^9a_2a_3a_4^3a_5^2 + \\
& 15112a_1^7a_2^2a_3a_4^3a_5^2 - 44116a_1^5a_2^3a_3a_4^3a_5^2 + 50372a_1^3a_2^4a_3a_4^3a_5^2 - 9600a_1a_2^5a_3a_4^3a_5^2 - 1856a_1^8a_3^2a_4^3a_5^2 + \\
& 14784a_1^6a_2a_3^2a_4^3a_5^2 - 15188a_1^4a_2^2a_3^2a_4^3a_5^2 - 3680a_1^2a_3^3a_3^2a_4^3a_5^2 - 3856a_1^5a_3^3a_4^3a_5^2 - 448a_1^{10}a_4^4a_5^2 - \\
& 1152a_1^8a_2a_4^4a_5^2 + 10528a_1^6a_2^2a_4^4a_5^2 - 13728a_1^4a_2^3a_4^4a_5^2 + 3600a_1^2a_2^4a_4^4a_5^2 - 3904a_1^7a_3a_4^4a_5^2 + \\
& 7808a_1^5a_2a_3a_4^4a_5^2 - 1856a_1^6a_4^5a_5^2 - 5a_1^9a_2^6a_5^3 + 49a_1^7a_2^7a_5^3 - 212a_1^5a_2^8a_5^3 + 489a_1^3a_2^9a_5^3 - 477a_1a_2^{10}a_5^3 + \\
& 32a_1^{10}a_2^4a_3a_5^3 - 249a_1^8a_2^5a_3a_5^3 + 986a_1^6a_2^6a_3a_5^3 - 2594a_1^4a_2^7a_3a_5^3 + 2870a_1^2a_2^8a_3a_5^3 - 64a_1^{11}a_2^2a_3^2a_5^3 + \\
& 296a_1^9a_2^3a_3^2a_5^3 - 1132a_1^7a_2^4a_3^2a_5^3 + 5939a_1^5a_2^5a_3^2a_5^3 - 9633a_1^3a_2^6a_3^2a_5^3 + 2325a_1a_2^7a_3^2a_5^3 + 256a_1^{10}a_2a_3^3a_5^3 + \\
& 674a_1^8a_2^2a_3^3a_5^3 - 12779a_1^6a_2^3a_3^3a_5^3 + 23780a_1^4a_2^4a_3^3a_5^3 - 10205a_1^2a_2^5a_3^3a_5^3 - 625a_2^6a_3^3a_5^3 - 1724a_1^9a_3^4a_5^3 + \\
& 11168a_1^7a_2a_3^4a_5^3 - 11700a_1^5a_2^2a_3^4a_5^3 - 1045a_1^3a_2^3a_3^4a_5^3 + 5250a_1a_2^4a_3^4a_5^3 - 3370a_1^6a_3^5a_5^3 + 66a_1^4a_2a_3^5a_5^3 + \\
& 1450a_1^2a_2^2a_3^5a_5^3 + 320a_1^3a_3^6a_5^3 - 48a_1^{11}a_2^3a_4a_5^3 + 160a_1^9a_2^4a_4a_5^3 + 874a_1^7a_2^5a_4a_5^3 - 4855a_1^5a_2^6a_4a_5^3 + \\
& 8399a_1^3a_2^7a_4a_5^3 - 5525a_1a_2^8a_4a_5^3 + 256a_1^{12}a_2a_3a_4a_5^3 - 640a_1^{10}a_2^2a_3a_4a_5^3 - 6568a_1^8a_2^3a_3a_4a_5^3 + \\
& 29878a_1^6a_2^4a_3a_4a_5^3 - 48041a_1^4a_2^5a_3a_4a_5^3 + 32815a_1^2a_2^6a_3a_4a_5^3 - 1250a_2^7a_3a_4a_5^3 - 1248a_1^{11}a_2^3a_4a_5^3 + \\
& 10760a_1^9a_2a_3^2a_4a_5^3 - 22888a_1^7a_2^2a_3^2a_4a_5^3 + 19404a_1^5a_2^3a_3^2a_4a_5^3 - 6935a_1^3a_2^4a_3^2a_4a_5^3 - 13000a_1a_2^5a_3^2a_4a_5^3 - \\
& 2600a_1^8a_3^3a_4a_5^3 - 8020a_1^6a_2a_3^3a_4a_5^3 + 24292a_1^4a_2^2a_3^3a_4a_5^3 - 7800a_1^2a_2^3a_3^3a_4a_5^3 + 7744a_1^5a_3^4a_4a_5^3 - \\
& 880a_1^3a_2a_3^4a_4a_5^3 - 320a_1^{13}a_4^2a_5^3 + 1824a_1^{11}a_2a_4^2a_5^3 + 944a_1^9a_2^2a_4^2a_5^3 - 22480a_1^7a_2^3a_4^2a_5^3 + 53412a_1^5a_2^4a_4^2a_5^3 - \\
& 55720a_1^3a_2^5a_4^2a_5^3 + 23000a_1a_2^6a_4^2a_5^3 - 3104a_1^{10}a_3a_4^2a_5^3 + 7408a_1^8a_2a_3a_4^2a_5^3 - 5352a_1^6a_2^2a_3a_4^2a_5^3 + \\
& 10428a_1^4a_2^3a_3a_4^2a_5^3 - 3900a_1^2a_2^4a_3a_4^2a_5^3 + 7408a_1^7a_3^2a_4^2a_5^3 - 18344a_1^5a_2a_3^2a_4^2a_5^3 - 1240a_1^3a_2^2a_3^2a_4^2a_5^3 + \\
& 5824a_1^9a_3^3a_4^2a_5^3 - 18304a_1^7a_2a_3^3a_4^2a_5^3 + 14064a_1^5a_2^2a_3^3a_4^2a_5^3 - 5760a_1^3a_2^3a_3^3a_4^2a_5^3 + 7488a_1^6a_3a_3^3a_4^2a_5^3 - 16a_1^{10}a_3^2a_4^2a_5^3 + \\
& 688a_1^8a_2^4a_4^2a_5^3 - 4504a_1^6a_2^5a_4^2a_5^3 + 10994a_1^4a_2^6a_4^2a_5^3 - 11500a_1^2a_2^7a_4^2a_5^3 + 3125a_2^8a_4^2a_5^3 - 256a_1^{11}a_2a_3a_4^2a_5^3 - 568a_1^9a_2^2a_3a_4^2a_5^3 + \\
& 13420a_1^7a_2^3a_3a_4^2a_5^3 - 38326a_1^5a_2^4a_3a_4^2a_5^3 + 40615a_1^3a_2^5a_3a_4^2a_5^3 - 10000a_1a_2^6a_3a_4^2a_5^3 + 2864a_1^{10}a_3^2a_4^2a_5^3 - 21384a_1^8a_2a_3^2a_4^2a_5^3 + \\
& 42212a_1^6a_2^2a_3^2a_4^2a_5^3 - 32718a_1^4a_2^3a_3^2a_4^2a_5^3 + 2750a_1^2a_2^4a_3^2a_4^2a_5^3 + 3125a_2^5a_3^2a_4^2a_5^3 + 6832a_1^7a_3^3a_4^2a_5^3 - 2616a_1^5a_2a_3^3a_4^2a_5^3 - \\
& 7200a_1^3a_2^2a_3^3a_4^2a_5^3 - 2560a_1^4a_3^4a_4^2a_5^3 + 1152a_1^{12}a_4a_4^2a_5^3 - 8736a_1^{10}a_2a_4a_4^2a_5^3 + 21920a_1^8a_2^2a_4a_4^2a_5^3 - 24120a_1^6a_2^3a_4a_4^2a_5^3 + \\
& 11564a_1^4a_2^4a_4a_4^2a_5^3 + 3000a_1^2a_2^5a_4a_4^2a_5^3 - 9375a_2^6a_4a_4^2a_5^3 + 2528a_1^9a_3a_4a_4^2a_5^3 + 13072a_1^7a_2a_3a_4a_4^2a_5^3 - 48216a_1^5a_2^2a_3a_4a_4^2a_5^3 + \\
& 45900a_1^3a_2^3a_3a_4a_4^2a_5^3 - 19904a_1^6a_3^2a_4a_4^2a_5^3 + 13760a_1^4a_2a_3^2a_4a_4^2a_5^3 - 13952a_1^8a_4^2a_4^2a_5^3 + 32768a_1^6a_2a_4^2a_4^2a_5^3 - \\
& 17760a_1^4a_2^2a_4^2a_4^2a_5^3 - 1856a_1^{11}a_5^5 + 15712a_1^9a_2a_5^5 - 48864a_1^7a_2^2a_5^5 + 76400a_1^5a_2^3a_5^5 - 64500a_1^3a_2^4a_5^5 + \\
& 18750a_1a_2^5a_5^5 - 5248a_1^8a_3a_5^5 + 5888a_1^6a_2a_3a_5^5 + 7200a_1^4a_2^2a_3a_5^5 + 6656a_1^5a_3^2a_5^5 + 16896a_1^7a_4a_5^5 - \\
& 23808a_1^5a_2a_4a_5^5 - 6144a_1^6a_5^6)
\end{aligned}
$$

14.6. Problemas

1. Demostrar el Teorema 14.2 cambiando la hipótesis de que K tenga característica 0 por la de que la característica de K no divide a $n!$; el Corolario 14.6 y los Teoremas 14.17 y 14.18, cambiando la hipótesis de que K tenga característica 0 por la de que K tenga característica diferente de 2 y 3; y el Corolario 14.23, cambiando la hipótesis de que K tenga característica 0 por la de que la característica de K sea mayor que el grado de f.

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 sólo si p tiene una única raíz real y que en caso contrario p tiene 3 raíces reales.

3. Demostrar que para todo cuerpo K el polinomio $X^3 - 3X + 1$ es irreducible o se descompone completamente en K.

4. Sean K un cuerpo de característica diferente de 2 y $p \in K[X]$ un polinomio separable irreducible con discriminante D tal que $\mathrm{Gal}(f/K)$ es cíclico. Demostrar que $\sqrt{D} \in K$ si y sólo si $|\mathrm{Gal}(p, K)|$ es impar.

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.

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 grado 2.

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

   a) $m = 1, 2, 3$ ó 6.

   b) Si $m = 6$, entonces $G \simeq S_4$.

   c) Si $m = 3$, entonces $G \simeq A_4$.

   d) Si $m = 1$, entonces $G \simeq C_2 \times C_2$ (el producto directo de dos grupos cíclicos de orden 2).

   e) Si $m = 2$ y f es irreducible sobre F, entonces $G \simeq D_4$, el grupo diédrico de orden 8.

   f) Si $m = 2$ y f es reducible sobre F, entonces G es cíclico de orden 4.

8. Sea K un cuerpo irreducible de grado 4 sobre un cuerpo de característica 0 y α una raíz de K. Demostrar que K y $K(\alpha)$ son las únicas subextensiones de L/K si y sólo si $\mathrm{Gal}(p/K)$ is isomorfo a A_4 ó S_4.

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.

10. Sean K un cuerpo de característica cero, $p = X^4 + aX^2 + b \in K[X]$ irreducible y $G = \mathrm{Gal}(p/K)$. Demostrar

    a) Si b es un cuadrado en K, entonces $G \simeq C_2 \times C_2$.

    b) 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.

    c) Si ninguna de las dos condiciones anteriores se verifica entonces $G \simeq D_4$.

11. Sean K un cuerpo de característica cero, $p = X^4 + bX^3 + cX^2 + bX + 1 \in K[X]$ irreducible, $G = \mathrm{Gal}(p/K)$, $\alpha = c^2 + 4c + 4 - 4b$ y $\beta = b^2 - 4c + 8$. Demostrar

    a) Si α es un cuadrado en K, entonces $G \simeq C_2 \times C_2$.

    b) Si α no es un cuadrado en K pero $\alpha\beta$ es un cuadrado en K, entonces G es cíclico de orden 4.

    c) Si ninguna de las dos condiciones anteriores se verifica, entonces $G \simeq D_4$.

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 $\mathbb{Q}(i\sqrt{5})$.

13. Determinar el grupo de Galois sobre los cuerpos indicados de cada uno de los siguientes polinomios:

    $X^3 + 2X + 2$ sobre $\mathbb{Z}_3$.
    $X^5 + 4X^3 + X$ sobre $\mathbb{Q}$.
    $X^4 - X^2 - 2$ sobre $\mathbb{Q}$.
    $X^5 - 3x^3 - 2X^2 + 6$ sobre $\mathbb{Q}$.
    $X^4 - 2$ sobre $\mathbb{Q}(i)$.
    $X^4 + 6X^2 + 9$ sobre $\mathbb{Q}$.
    $X^4 + X^2 - 6$ sobre $\mathbb{Q}$.
    $X^6 - 9$ sobre $\mathbb{Q}$.
    $X^3 - 10$ sobre $\mathbb{Q}(\sqrt{-3})$.
    $X^4 - 4X^2 + 2$ sobre $\mathbb{Q}$.
    $X^4 - 4X^2 + 16$ sobre $\mathbb{Q}$.
    $4X^4 - 8X^2 + 1$ sobre $\mathbb{Q}$.
    $X^4 - 5$ sobre $\mathbb{Q}(\sqrt{5})$.

14. Demostrar que si $p \in K[X]$ es irreducible, K tiene característica 0 y p es resoluble por radicales, entonces $|\mathrm{Gal}(p/K)|$ divide a $p(p-1)$.

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.

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 $\mathrm{Gal}(p/K)$ es isomorfo a A_4 ó $C_2 \times C_2$ si y sólo si D es un cuadrado en K.

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 sólo si n es múltiplo de 4. (Indicación: Obsérvese que si α y β son dos raíces de f que no son iguales ni conjugadas, entonces $(\alpha - \beta)(\overline{\alpha} - \overline{\beta}) \in \mathbb{R}$ y que $(\alpha - \overline{\alpha})^2 < 0$.)

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 $p \geq 5$.

    a) 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 14.23.)

    b) Si $f = X^p - aX + b \in \mathbb{Q}[X]$ con $a > 0$ entonces f no es resoluble por radicales sobre $\mathbb{Q}$.

    c) 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 17).

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 sólo si lo es q.

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.

    $X^5 - 2X^4 + 2$, $X^5 - 4X^2 + 2$, $X^5 - 4X + 2$, $X^5 - 4X + 10$, $x^6 - 10x^2 + 5, X^7 - 10X^5 + 15X + 5$.

Índice alfabético