Departamento de Álgebra

UCM

Estructuras Algebraicas

Miguel González

3 de octubre de 2016

Índice

Capítulo 1

Anillos

1.1. Definición y propiedades

Definición 1.1.1. (1) Un anillo $(R, +, \cdot)$ es un conjunto no vacío R, junto con dos operaciones binarias, suma y producto, $+, \cdot : R \times R \to R$, sujetas a los siguientes axiomas.

a) Asociativa suma: $(r + s) + t = r + (s + t)$ para todos $r, s, t \in R$

b) Elemento neutro de la suma: Existe $0 \in R$ tal que $r + 0 = 0 + r$ para todo $r \in R$,

c) Elemento opuesto: para todo $r \in R$ existe $-r \in R$ tal que $r + (-r) = (-r) + r = 0$,

d) Conmutativa suma: $r + s = s + r$ para todos $r, s \in R$.
Los cuatro primeros axiomas dicen que $(R, +)$ es un grupo conmutativo (o abeliano).

e) Asociativa producto: $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ para todos $r, s, t \in R$

f) Distributiva del producto respecto de la suma.

$$r \cdot (s + t) = r \cdot s + r \cdot t,$$
$$(r + s) \cdot t = r \cdot t + s \cdot t,$$

para todos $r, s, t \in R$

(2) El anillo se dice conmutativo (o abeliano) si la multiplicación es conmutativa: $r \cdot s = s \cdot r$ para todos $r, s \in R$.

(3) El anillo es unitario (o con elemento unidad), si existe $1 \in R$ $(1 \neq 0)$ tal que $1 \cdot r = r \cdot 1 = r$ para todo $r \in R$.

(4) Denotaremos, a partir de ahora, $r \cdot s = rs$.

Observación 1.1.2. (1) 0 es único: si 0 y 0′ verifican el axioma *b*), entonces $0 = 0 + 0'$, por *b*) para 0′, y $0 + 0' = 0'$ por *b*) para 0.

(2) Para cada $r \in R$ el opuesto $-r$ es único: $-r = -r+0 = -r+(r+(-r')) = (-r+r)+(-r') = 0 + (-r') = -r'$.

Denotaremos $r + (-s) = r - s$.

(3) $-(-r) = r$.

(4) Para todo $r \in R$, es $r0 = 0 = 0r$. En efecto, $0r = (0 + 0)r = 0r + 0r$. Por tanto $0 = 0r + (-0r) = (0r + 0r) + (-0r) = 0r + (0r + (-0r)) = 0r + 0 = 0r$.

(5) $R = \{0\}$ si, y sólo si, $1 = 0$. En efecto, si $1 = 0$, entonces para todo $r \in R$ se tiene $r = r1 = r0 = 0$.

Supondremos, por tanto, que $1 \neq 0$.

(6) Si existe elemento unidad es único. En efecto, si $1, 1' \in R$ verifican la condición de elemento unidad, entonces $1 = 1 \cdot 1'$, por ser $1'$ elemento unidad, y $1 \cdot 1' = 1'$ por ser 1 elemento unidad.

(7) La ley distributiva impone que la suma sea conmutativa.

$$(1 + 1)(r + s) = 1(r + s) + 1(r + s) = 1r + 1s + 1r + 1s = r + s + r + s,$$
$$(1 + 1)(r + s) = (1 + 1)r + (1 + 1)s = 1r + 1r + 1s + 1s = r + r + s + s.$$

De $r + s + r + s = r + r + s + s$, sumando a izquierda el opuesto de r y a derecha el opuesto de s, se obtiene $s + r = r + s$.

(8) Un anillo unitario se dice anillo de *división* si para todo elemento $0 \neq r \in R$ existe $s \in R$ tal que $rs = 1 = sr$. Un anillo de división conmutativo es un *cuerpo*.

(9) Si $sr = 1 = rt$ entonces $s = s1 = s(rt) = (sr)t = 1t = t$. Por tanto, si para $r \in R$ existe $s \in R$ tal que $sr = 1 = rs$, entonces s es único. Escribiremos $s = r^{-1}$. Diremos que el elemento $r \in R$ es una unidad y $r^{-1} \in R$ su inverso. Es claro que $(r^{-1})^{-1} = r$. Además, si $r, s \in R$ son unidades entonces rs es unidad y $(rs)^{-1} = s^{-1}r^{-1}$.

(10) El conjunto R^* de unidades de un anillo unitario es un *grupo multiplicativo*.

Proposición 1.1.3. *Sean R un anillo y $r, s \in R$.*

(1) $0r = r0 = 0$.

(2) $(-r)s = r(-s) = -(rs)$.

(3) $(-r)(-s) = rs$.

(4) Si R tiene 1, éste es único y $-r = (-1)r$.

Demostración. (1)

(2) $(-r)s + rs = ((-r) + r)s = 0s = 0$, por tanto, $(-r)s = -(rs)$.

(3) $(-r)(-s) = -(r(-s)) = -(-rs) = rs$.

(4) $(-1)r + r = (-1)r + 1r = (-1 + 1)r = 0r = 0$.

□

Definición 1.1.4. *Dados $r \in R$ y $0 \neq n \in \mathbb{N}$ definimos $nr = r + \overset{n}{\cdots} + r, 0r = 0$, $(-n)r = (-r) + \overset{n}{\cdots} + (-r)$ y $r^n = r \overset{n}{\cdots} r, r^0 = 1$.*

Proposición 1.1.5. *$r, s \in R, m, n \in \mathbb{N}$*

(1) $n(r + s) = nr + ns$.

(2) $(m + n)r = mr + nr$.

(3) $(mn)r = m(nr)$.

(4) $r^m r^n = r^{m+n}$.

(5) $(r^m)^n = r^{mn}$.

(6) Si $rs = sr$, entonces

$$(r + s)^n = \sum_{k=0}^{n} \binom{n}{k} r^{n-k} s^k$$

y, más general, si $r_i r_j = r_j r_i$ para todos i, j, entonces

$$(r_1 + \cdots + r_p)^n = \sum_{\substack{0 \leq k_1, \ldots, k_p \leq n \\ k_1 + \cdots + k_p = n}} \frac{n!}{k_1! \cdots k_p!} r_1^{k_1} \cdots r_p^{k_p}.$$

Ejemplos 1.1.6. (1) Anillo trivial $(R, +)$ con $rs = 0$ para todo $r, s \in R$. No es nada más que un grupo abeliano.

(2) El anillo conmutativo y unitario de los enteros $\mathbb{Z}$. Los cuerpos de los números racionales, reales, complejos: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(3) $n\mathbb{Z}$ anillo conmutativo no unitario.

(4) El anillo conmutativo y unitario $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ de los enteros módulo n. (En ocasiones, denotaremos $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$).

(5) El anillo conmutativo y unitario de los enteros de Gauss, $\mathbb{Z}[i] \subset \mathbb{C}$ definido por $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$, donde $i = \sqrt{-1}$.

(6) El anillo de polinomios $\mathbb{K}[X]$, donde $\mathbb{K}$ es un cuerpo.

(7) Si R es un anillo (unitario), el conjunto $\mathscr{M}_n(R)$ de matrices cuadradas de orden n con entradas en R, es un anillo (unitario) con la suma y producto habituales.

(8) El producto $R \times S$ de dos anillos (unitarios) R, S tinen una estructura de anillo con la suma y producto definidas componente a componente. El cero es $(0_R, 0_S)$ (y el uno es $(1_R, 1_S)$).

(9) Un interesante anillo *no conmutativo* (Hamilton 1843) es el anillo de los cuaternios reales

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k,$$

con la suma de $\mathbb{R}^4$ componente a componente y el producto definido por la ley distributiva de forma que

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j,$$

(donde los coeficientes reales conmutan con i, j, k). De forma similar podemos definir los anillos de los cuaternios racionales (o enteros) con $a, b, c, d \in \mathbb{Q}$ ($\mathbb{Z}$).

En todos los casos podemos definir la conjugación: si $\alpha = a+bi+cj+dk$ el conjugado es $\bar{\alpha} = a - bi - cj - dk$, y la norma $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2$. Es claro que $\alpha = 0$ si, y sólo si, $N(\alpha) = 0$. Los cuaternios reales o racionales son *anillos de división*, el inverso de $0 \neq \alpha$ es $\alpha^{-1} = N(\alpha)^{-1}\bar{\alpha}$.

(10) Sean $X \neq \emptyset$ un conjunto y A un anillo. El conjunto

$$R = \{f : X \to A \mid f \text{ aplicación}\}$$

es un anillo con las operaciones

$$(f + g)(x) = f(x) + g(x),\ \ (fg)(x) = f(x)g(x).$$

El anillo R es conmutativo si, y sólo si, A es conmutativo, y R tiene 1 si, y sólo si, A tiene 1, en este caso $1_R(x) = 1_A$ para todo $x \in X$.

(11) Una función $f : \mathbb{R} \to \mathbb{R}$ se dice de soporte compacto si existen $a \leq b \in \mathbb{R}$ tales que $f(x) = 0$ si $x \notin [a, b]$. El conjunto de las funciones de soporte compacto con las suma y el producto del ejemplo anterior es un anillo sin unidad.

(12) Todo anillo R se puede sumergir en un anillo con unidad: $R \times \mathbb{Z}$ con la suma obvia y producto definido por $(r, m)(s, n) = (rs + nr + ms, mn)$. Es $R \subset R \times \mathbb{Z}$ vía $r \mapsto (r, 0)$ y $(r, m)(0, 1) = (r, m)$. Esto es $1_{R\times\mathbb{Z}} = (0, 1)$.

1.2. Divisores de cero. Unidades

Definición 1.2.1. Sea R un anillo.

(1) Un elemento $0 \neq r \in R$ se dice divisor de cero por la izquierda si existe $0 \neq s \in R$ tal que $rs = 0$, divisor de cero por la derecha si existe $0 \neq t \in R$ tal que $tr = 0$, divisor de cero si es divisor de cero a izquierda y derecha.

(2) Un anillo con $1 \neq 0$ se dice dominio de integridad (DI) si no tiene divisores de cero a izquierda ni a derecha. Es claro que no tiene divisores de cero a izquierda si, y sólo si, no los tiene a derecha.

(3) Un elemento $r \in R$ se dice nilpotente si $r^n = 0$ para cierto $n \in \mathbb{N}$. En $\mathbb{Z}/12\mathbb{Z}$ se verifica $\overline{6}^2 = \overline{0}$.

(4) Supongamos que R tiene $1 \neq 0$. Un elemento $r \in R$ tiene inverso a izquierda (derecha) si existe $s \in R, (t \in R)$ tal que $sr = 1, (rt = 1)$, tiene inverso si existe $r^{-1} \in R$ tal que $r^{-1}r = rr^{-1} = 1$. Si $r \in R$ tiene inverso a izquierda s e inverso a derecha t entonces $s = t$ ($s = s1 = s(rt) = (sr)t = 1t = t$) y, por tanto, r tiene inverso $r^{-1} = s = t$ y el inverso es único. Diremos que r es una unidad. El conjunto de las unidades R^* es un grupo multiplicativo.

Observación 1.2.2. (1) Un divisor de cero a la izquierda (derecha) no admite inverso a la izquierda (derecha): si $rs = 0$ y $ur = 1$ entonces $urs = 0$, esto es $s = 0$. En consecuencia un anillo de división es dominio de integridad.

(2) Propiedad cancelativa. Sean $r, s, t \in R$ si r no es divisor de cero (a izquierda) y $rs = rt$ entonces $r(s - t) = 0$. Por tanto $s - t = 0$, esto es $s = t$.

(3) Un dominio de integridad finito es un anillo de división. Un elemento $0 \neq r \in R$ es no divisor de cero por la izquierda si, y sólo si, la aplicación de multiplicación $R \to R, s \mapsto rs$ es inyectiva -análogo enunciado por la derecha- (ejercicio). Sean, ahora, R un dominio de integridad finito y $0 \neq r \in R$, se trata de hallar inverso a la derecha (e inverso a la izquierda) para r. La aplicación $R \to R, s \mapsto rs$ es inyectiva y R es un conjunto finito, por tanto, esta aplicación es sobreyectiva. En particular, $1 \in R$ está en la imagen de esta aplicación, esto es existe $s \in R$ tal que $rs = 1$.

(4) Un teorema (difícil) de Wedderburn afirma que todo anillo de división finito es conmutativo, en consecuencia, es un cuerpo.

(5) Más adelante veremos que todo elemento que no es divisor de cero tiene inverso en un anillo más grande.

(6) El anillo $\mathbb{Z}$ es un dominio de integridad con grupo de unidades $\mathbb{Z}^* = \{-1, 1\}$.

(7) En el anillo de matrices $\mathscr{M}_n(R)$, donde R es un anillo conmutativo unitario, una matriz es unidad si, y sólo si, su determinante es una unidad en R.

(8) Sea $n \geq 2$. Un elemento $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ es unidad si, y sólo si, $\text{mcd}(a, n) = 1$ si, y sólo si, $\bar{a}$ es un generador del grupo cíclico aditivo $(\mathbb{Z}/n\mathbb{Z}, +)$. Si $\bar{0} \neq \bar{a}$ no es unidad entonces es divisor de cero.

(9) $\mathbb{Z}/n\mathbb{Z}$ es un cuerpo si, y sólo si, para todo $1 \leq a < n$ es $\text{mcd}(a, n) = 1$ si, y sólo si, n es primo.

(10) $\mathbb{Z}/n\mathbb{Z}$ contiene nilpotentes no nulos si, y sólo si, n tiene algún divisor primo múltiple.

(11) Sea R el anillo de funciones reales definidas en $[0, 1]$. Las unidades de R son las $f \in R$ tales que $f(x) \neq 0$ para todo $x \in [0, 1]$. Si $0 \neq f$ no es unidad entonces $fg = 0$ donde $g(x) = 0$ si $f(x) \neq 0$ y $g(x) = 1$ si $f(x) = 0$, esto es f es divisor de cero.

(12) Sea R el anillo de funciones reales continuas en $[0, 1]$. Las unidades son las funciones continuas tales $f(x) \neq 0$ para todo $x \in [0, 1]$. Ahora hay funciones que no son unidad ni divisor de cero. Por ejemplo $f(x) = x - 1/2$. Si $fg = 0$ entonces $g(x) \neq 0$ para todo $x \neq 1/2$. de aquí $g = 0$ puesto que g es continua. De forma similar ninguna función con una cantidad numerable de ceros es un divisor de cero. Sin embargo hay divisores de cero $fg = 0$ para $f(x) = \begin{cases} 0 & \text{si } 0 \leq x \leq 1/2 \\ x - 1/2 & \text{si } 1/2 \leq x \leq 1 \end{cases}$ y $g(x) = f(1 - x)$.

(13) Sean $D \in \mathbb{Z}$ libre de cuadrados y $\mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$. Es $(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D}$. Además $a + b\sqrt{D} = 0$ si, y sólo si, $a = b = 0$ si, y sólo si, $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2 = 0$. Por tanto, si $0 \neq a + b\sqrt{D}$ entonces $(a + b\sqrt{D})^{-1} = a/(a^2 - Db^2) - b/(a^2 - Db^2)\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$. Diremos que $\mathbb{Q}[\sqrt{D}]$ es un cuerpo cuadrático.

1.3. Subanillos

Definición 1.3.1. Un subanillo de R es un subgrupo aditivo S que es cerrado para el producto. Por tanto $\emptyset \neq S \subset R$ es subanillo si, y sólo si, para todo $x, y \in S$ se tiene $x - y \in S$ y $xy \in S$. El subanillo S es subanillo unitario si $1_R \in S$.

Ejemplos 1.3.2. (1) La cadena $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ son subanillos unitarios.

(2) Los enteros pares $2\mathbb{Z} \subset \mathbb{Z}$ es subanillo no unitario.

(3) Anillo de enteros de un cuerpo cuadrático $\mathbb{Q}[\sqrt{D}]$. El conjunto

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$$

es un subanillo de $\mathbb{Q}[\sqrt{D}]$. Es el anillo de enteros de $\mathbb{Q}[\sqrt{D}]$ si $D \equiv 2, 3 \pmod 4$. Si $D \equiv 1 \pmod 4$ el algo más grande subconjunto $(a + b\sqrt{D} = (a-b) + (2b)(1 + \sqrt{D})/2)$,

$$\mathbb{Z}[\frac{1+\sqrt{D}}{2}] = \{a + b\frac{1+\sqrt{D}}{2} \mid a, b \in \mathbb{Z}\}$$

es un subanillo, puesto que $(a + b(1 + \sqrt{D})/2)(c + d(1 + \sqrt{D})/2 = (ac + bd(D-1)/4) + (ad + bc + bd)(1 + \sqrt{D})/2)$. Definimos $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$, donde

$$\omega = \begin{cases} \sqrt{D} & \text{si } D \equiv 2, 3 \pmod 4 \\ \dfrac{1+\sqrt{D}}{2} & \text{si } D \equiv 1 \pmod 4. \end{cases}$$

El anillo $\mathbb{Z}[\omega]$ es el anillo de enteros de $\mathbb{Q}[\sqrt{D}]$, es decir es la clausura íntegra de $\mathbb{Z}$ en $\mathbb{Q}[\sqrt{D}]$ (esto significa que $\mathbb{Z}[\omega] = \{\alpha \in \mathbb{Q}[\sqrt{D}] \mid \alpha$ es raíz de un polinomio mónico con coeficientes enteros $\}$) y, por tanto, tiene muchas propiedades análogas a aquéllas de $\mathbb{Z}$ como subanillo de $\mathbb{Q}$. Si $D = -1$ obtenemos $\mathbb{Z}[i]$ el anillo de los enteros de Gauss.

Definimos la norma $N : \mathbb{Q}[\sqrt{D}] \to \mathbb{Q}$ por

$$N(\alpha = a + b\sqrt{D}) = \alpha\bar{\alpha} = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2.$$

La norma es multiplicativa: $N(\alpha\beta) = N(\alpha)N(\beta)$, y $N(\alpha) = 0$ si, y sólo si, $\alpha = 0$.

En $\mathbb{Z}[\omega]$ la norma

$$N(a + b\omega) = (a + b\omega)(a + b\bar{\omega}) = \begin{cases} a^2 - Db^2 & \text{si } D \equiv 2, 3 \pmod 4 \\ a^2 + ab + \dfrac{1-D}{4}b^2 & \text{si } D \equiv 1 (\text{mod } 4), \end{cases}$$

donde

$$\bar{\omega} = \begin{cases} -\sqrt{D} & \text{si } D \equiv 2,3 \pmod 4 \\ \dfrac{1-\sqrt{D}}{2} & \text{si } D \equiv 1 \pmod 4 \end{cases}$$

Podemos usar la norma para caracterizar las unidades de $\mathbb{Z}[\omega]$.

Lema 1.3.3. *El elemento $\alpha \in \mathbb{Z}[\omega]$ es unidad en $\mathbb{Z}[\omega]$ si, y sólo si, $N(\alpha) = \pm 1$. En este caso $\alpha^{-1} = \pm\bar{\alpha}$.*

Demostración. Por definición, $\alpha \in \mathbb{Z}[\omega]$ es unidad si existe $\beta \in \mathbb{Z}[\omega]$ tal que $\alpha\beta = 1$.

Supongamos que $\alpha\beta = 1$ entonces $N(\alpha)N(\beta) = 1$ y, por tanto, $N(\alpha) = \pm 1$. Recíprocamente, si $N(\alpha) = \pm 1$, entonces $\alpha\bar{\alpha} = N(\alpha) = \pm 1$. De aquí $\alpha^{-1} = \pm\bar{\alpha} \in \mathbb{Z}[\omega]$. □

En particular, la solución de la ecuación de Pell $x^2 - Dy^2 = 1$ en $\mathbb{Z}$ equivale a determinar las unidades de $\mathbb{Z}[\omega]$.

a) Si $D = -1$ las unidades $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$

b) Si $D = -3$ las unidades $\mathbb{Z}[(1+\sqrt{-3})/2)]^* = \{a+b(1+\sqrt{-3})/2) \mid a^2+ab+b^2 = \pm 1\}$. La ecuación $a^2 + ab + b^2 = \pm 1$ equivale a $(2a + b)^2 + 3b^2 = \pm 4$, cuyas soluciones son $2a + b = \pm 2, b = 0$; $2a + b = \pm 1, b = \pm 1$, esto es $a = \pm 1, b = 0$; $a = 0, b = \pm 1$; $a = -1, b = 1$; $a = 1, b = -1$. De donde $\mathbb{Z}[(1 + \sqrt{-3})/2)]^* = \{\pm 1, \pm\rho, \pm\rho^2\}$ con $\rho = (1 + \sqrt{-3})/2$ una raíz primitiva sexta de la unidad. Es decir, el grupo de unidades es el grupo cíclico de las raíces sextas de la unidad.

c) Si $D < 0$ y $D \neq -3, -1$ es sencillo mostrar que $\mathbb{Z}[\omega]^* = \{\pm 1\}$.

d) Si $D > 0$ se puede probar que $\mathbb{Z}[\omega]^*$ es siempre infinito. Por ejemplo, $1 + \sqrt{2}$ es unidad en $\mathbb{Z}[\sqrt{2}]$ y $\{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$ son unidades todas distintas (de hecho, estas son todas, pero es difícil probar este hecho).

(4) Anillo de series formales y anillo de polinomios.

Sea $\mathbb{N} = \{0, 1, 2, \ldots\}$. El conjunto $R[[X]] = \{f : \mathbb{N} \to R\}$, de las sucesiones de elementos de un anillo R admite una estructura de anillo, con la suma definida componente a componente, y el producto dado por la ley distributiva, i.e.:

$$(f + g)(n) = f(n) + g(n), \qquad (fg)(n) = \sum_{k=0}^{n} f(k)g(n-k).$$

Diremos que $(R[[X]], +, \cdot)$ es el *anillo de series formales* en la indeterminada X con coeficientes en R.

a) Si R es unitario $R[[X]]$ es unitario y $X = (0, 1, 0, \cdots)$, $X^2 = (0, 0, 1, 0, \cdots), \cdots, X^n = (0, 0, \cdots, 1, 0, \cdots)$, con 1 en la posición n. En este caso, identificamos R con su imagen en $R[[X]]$ por el homomorfismo $r \mapsto (r, 0, \cdots)$ y escribimos un elemento $f \in R[[X]]$ en la forma

$$f = \sum_{n=0}^{\infty} f(n)X^n.$$

b) Si R es conmutativo $R[[X]]$ es conmutativo.

c) El subanillo $R[X]$ formado por aquellas sucesiones que tienen a lo más una cantidad finita de términos no nulos, es el *anillo de polinomios* en la indeterminada X con coeficientes en R. Cada polinomio se escribe, en este caso como una auténtica suma finita, en la forma habitual

$$f = \sum_{k=0}^{n} f(k)X^k.$$

para algún $n \in \mathbb{N}$.

1.4. Homomorfismos de anillos

Definición 1.4.1. Sean R, S anillos una aplicación $f : R \to S$ es un homomorfismo si para todo $r, s \in R$

(1) $f(r + s) = f(r) + f(s)$.

(2) $f(rs) = f(r)f(s)$.

Si R, S son unitarios, el homomorfismo se dice unitario si $f(1_R) = 1_S$.

Observación 1.4.2. Sean R, S unitarios y $f : R \to S$ una aplicación multiplicativa.
Si $f(1_R) = 0_S$ entonces $f(r) = f(r1_R) = f(r)f(1_R) = 0_S$ para todo $r \in R$.
Sea f tal que $f(1_R) \neq 0_S$.
De $f(1_R) = f(1_R1_R) = f(1_R)f(1_R)$ se obtiene $f(1_R)(1_S - f(1_R)) = (1_S - f(1_R))f(1_R) = 0_S$. Por tanto, o $0_S \neq f(1_R)$ es un divisor de cero en S (cuando $f(1_R) \neq 1_S$, y, en este caso, para cada $r \in R$ es $f(r)(1_S - f(1_R)) = f(r)f(1_R)(1_S - f(1_R)) = 0_S$, i.e. $f(r)$ es divisor de cero para cada r tal que $f(r) \neq 0_S$) o $f(1_R) = 1_S$.
En particular, sea f no idénticamente nula y multiplicativa:

(1) si f es sobreyectiva, ha de ser $f(1_R) = 1_S$, o

(2) si S es DI, ha de ser $f(1_R) = 1_S$.

Un ejemplo de homomorfismo que no lleva 1_R a 1_S es $R \to R \times R$ definido por $r \mapsto (r, 0)$, donde R es un anillo unitario.

Proposición 1.4.3. *Sean $f : R \to S$ un homomorfismo de anillos, $r \in R$.*

(1) $f(0_R) = 0_S$.

(2) $f(-r) = -f(r)$.

(3) $f(nr) = nf(r), n \in \mathbb{Z}$.

(4) $f(r^n) = f(r)^n, n \in \mathbb{N}$.

(5) La composición de homomorfismos es homomorfismo.

(6) El conjunto $\mathrm{Hom}(R, S)$ *de los homomorfismos de R en S es un anillo con la suma y el producto* $(f + g)(r) = f(r) + g(r), (f \cdot g)(r) = f(r) \cdot g(r)$.

(7) Si $f : R \to S$ es un homomorfismo biyectivo (isomorfismo), entonces la aplicación inversa f^{-1} es homomorfismo. Diremos que f es un isomorfismo.

(8) El conjunto $\mathrm{Hom}(R, R) = \mathrm{End}(R)$ *(endomorfismos de R) es un anillo con la suma y la composición como producto. El conjunto* $\mathrm{Aut}(R)$ *de los isomorfismos $R \to R$ es el grupo de las unidades del anillo de los endomorfismos.*

Definición 1.4.4. Sea $f : R \to S$ un homomorfismo de anillos unitarios.

(1) El núcleo, $\ker f = \{r \in R | f(r) = 0\}$ es un subanillo (no unitario) de R.

(2) La imagen, $\mathrm{im} f = \{f(r) \in S | r \in R\}$ es un subanillo unitario de S.

Observación 1.4.5. Un homomorfismo $f : R \to S$ es inyectivo si, y sólo si, $\ker f = \{0_R\}$.

Ejemplos 1.4.6. (1) La inclusión $S \subset R$ de un subanillo S de R es un homomorfismo. Es inyectivo.

(2) $\mathbb{Z} \xrightarrow{f} \mathbb{Z}/2\mathbb{Z}$ definido por $n \mapsto \begin{cases} 0 & \text{si } n \text{ par,} \\ 1 & \text{si } n \text{ impar.} \end{cases}$

(3) $\mathbb{Z} \xrightarrow{f} \mathbb{Z}/n\mathbb{Z}$ definido por $x \mapsto \bar{x}$. Su núcleo $\ker f = n\mathbb{Z}$ y f es sobreyectivo.

(4) El homomorfismo de sustitución $\mathbb{Q}[X] \xrightarrow{\varphi} \mathbb{Q}$ definido por $f(X) \mapsto f(q)$ para $q \in \mathbb{Q}$ fijado.

Ejercicios 1.4.7. (1) Para cada anillo unitario R existe un único homomorfismo de anillos unitarios $\mathbb{Z} \to R$.

(2) El único homomorfismo de anillos $2\mathbb{Z} \to 3\mathbb{Z}$ es el homomorfismo constante cero.

(3) $\mathbb{Z}[X]$ y $\mathbb{Q}[X]$ no son isomorfos como anillos. Indicación: 2 es unidad en $\mathbb{Q}$, no lo es en $\mathbb{Z}$.

1.5. Ideales. Anillo cociente

Sean R un anillo e I un subgrupo aditivo de R ($0 \in I$ y para todo $x, y \in I$ se verifica $y - x \in I$). El conjunto cociente R/I, por la relación de equivalencia $x \sim y$ si, y sólo si, $y - x \in I$ es un grupo aditivo, con la operación $\overline{x} + \overline{y} = \overline{x+y}$. En este grupo $0_{R/I} = \overline{0_R}$ y $-\overline{x} = \overline{-x}$. Basta comprobar que la operación está bien definida. En efecto, si $\overline{x} = \overline{p}, \overline{y} = \overline{q}$, entonces $p - x, q - y \in I$. Por tanto $(p+q) - (x+y) = (p-x) + (q-y) \in I$ y se verifica que $\overline{x+y} = \overline{p+q}$.
La aplicación canónica $R \to R/I, x \mapsto \overline{x}$ es un homomorfismo sobreyectivo de grupos aditivos cuyo núcleo es I.
Buscamos las condiciones que debe verificar I para que el grupo aditivo cociente R/I admita una estructura de anillo de modo que la aplicación canónica $R \to R/I$ sea un homomorfismo de anillos. Esto significa que el producto en R/I está definido por $\overline{r}\overline{s} = \overline{rs}$. Se trata, por tanto, de buscar condiciones que debe cumplir I para que este producto esté bien definido. Esto ocurre si para cada $x, y \in R$, $\overline{(r+x)(s+y)} = \overline{rs}$. De forma equivalente, $ry + xs + xy \in I$. Haciendo $s = 0 = x, r = 0 = y$, esta última condición es equivalente a las condiciones: $ry \in I$ para todo $r \in R, y \in I$, $xs \in I$ para todo $s \in R, x \in I$.

Definición 1.5.1. Un ideal (bilátero) es un subgrupo aditivo I en R que verifica las condiciones:

(1) $ry \in I$ para todo $r \in R, y \in I$ (ideal por la izquierda),

(2) $xs \in I$ para todo $s \in R, x \in I$ (ideal por la derecha).

En este caso R/I es un anillo y el homomorfismo canónico es un homomorfismo sobreyectivo de anillos cuyo núcleo es I.

1.5.1. Teorema de isomorfismo

El bien conocido teorema de isomorfismo para grupos aditivos es válido para las estructuras de anillo.

Teorema 1.5.2 (1º teorema de isomorfismo)**.** *Sea $f : R \to S$ un homomorfismo de anillos. Entonces el núcleo* $\ker f$ *es un ideal de R, la imagen* $\mathrm{im} f$ *es un subanillo de S y existe un único homomorfismo de anillos $\bar{f} : R/\ker f \to \mathrm{im} f$ que hace conmutativo el diagrama*

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ R/\ker f & \xrightarrow{\bar{f}} & \mathrm{im} f. \end{array}$$

El homomorfismo $\bar{f} : R/\ker f \to \mathrm{im} f$ es un isomorfismo.

Ejemplos 1.5.3. (1) $\{0\}, R$ son ideales. Un ideal es propio si $I \subsetneq R$.

(2) Sea $f : R \to S$ un homomorfismo. El núcleo $\ker f$ es un ideal (bilátero) de R.

(3) Los ideales de $\mathbb{Z}$ son los $n\mathbb{Z}$. El anillo cociente $\mathbb{Z}/n\mathbb{Z}$ es el anillo de restos módulo n.

(4) En $\mathbb{Z}[X]$ el conjunto $I = \{0\} \cup \{$ polinomios con primer coeficiente no nulo en grado $\geq 2\} = X^2\mathbb{Z}[X]$ es un ideal. El cociente es $\mathbb{Z}[X]/I = \mathbb{Z}[x]$, con $x = X + I$ que verifica $x^2 = 0$. Si $J = (2, X^2)\mathbb{Z}[X]$ ¿qué es $\mathbb{Z}[X]/J$?

(5) Sean A un anillo, X un conjunto no vacío y $R = \{f : X \to A\}$ el anillo de las funciones de X en A. Para cada $x \in X$ tenemos un homomorfismo sobreyectivo de anillos, el homomorfismo de evaluación en x, definido por

$$\begin{aligned} ev_x : R &\to A \\ f &\mapsto f(x). \end{aligned}$$

El núcleo es $\ker ev_x = \{f \mid f(x) = 0\}$. Así $R/\ker ev_x \simeq A$.

(6) Sean R un anillo conmutativo y $r \in R$. El homomorfismo de evaluación

$$\begin{aligned} R[X] &\xrightarrow{\varphi_r} R \\ f(X) &\mapsto f(r), \end{aligned}$$

es sobreyectivo. Puesto que la división $f(X) = (X - r)g(X) + f(r)$, su núcleo es $\ker \varphi_r = (X - r)R[X]$. Así

$$R[X]/(X - r)R[X] \xrightarrow{\sim} R.$$

(7) Sean $a, 0 \neq b \in \mathbb{R}$ y $X^2 - 2aX + (a^2 + b^2) \in \mathbb{R}[X]$. La división $f(X) = (X^2 - 2aX + (a^2 + b^2))g(X) + (mX + n)$ muestra que el núcleo del epimorfismo (si $b \neq 0$, entonces $\frac{n}{b}X + m - \frac{an}{b} \mapsto m + ni$) de evaluación

$$\begin{aligned} \mathbb{R}[X] &\xrightarrow{\varphi} \mathbb{C} \\ f(X) &\mapsto f(a + bi), \end{aligned}$$

es $\ker \varphi = (X^2 - 2aX + (a^2 + b^2))\mathbb{R}[X]$. Así

$$\mathbb{R}[X]/(X^2 - 2aX + (a^2 + b^2))\mathbb{R}[X] \xrightarrow{\sim} \mathbb{C}.$$

En particular,

$$\mathbb{R}[X]/(X^2 + 1)\mathbb{R}[X] \xrightarrow{\sim} \mathbb{C}.$$

(8) Sean R un anillo, $J \subset R$ un ideal, $n \geq 2$ y $\mathscr{M}_n(R)$ el anillo de matrices. El subconjunto $\mathscr{M}_n(J)$ de matrices con coeficientes en J es el núcleo del epimorfismo $\mathscr{M}_n(R) \to \mathscr{M}_n(R/J)$. Por tanto, $\mathscr{M}_n(J)$ es un ideal de $\mathscr{M}_n(R)$ y

$$\mathscr{M}_n(R)/\mathscr{M}_n(J) \xrightarrow{\sim} \mathscr{M}_n(R/J).$$

Si R tiene $1 \in R$, entonces todo ideal de $\mathscr{M}_n(R)$ es de la forma $\mathscr{M}_n(J)$ para cierto ideal $J \subset R$.

(9) Sea R conmutativo con $0 \neq 1 \in R$. Sean $1 \leq j \leq n$ y $\mathscr{L}_j \subset \mathscr{M}_n(R)$ el conjunto de las matrices con entradas arbitrarias en la columna j y ceros en las otras columnas. Es claro que $\mathscr{L}_j$ es un subgrupo aditivo. Para cada $T \in \mathscr{M}_n(R)$ y $A \in \mathscr{L}_j$ es $TA \in \mathscr{L}_j$. Esto muestra que $\mathscr{L}_j$ es un ideal por la izquierda. Sin embargo, $\mathscr{L}_j$ no es ideal por la derecha. En efecto, si E_{pq} es la matriz con entrada 1 en la posición pq y ceros en las otras entradas, entonces $E_{1j} \in \mathscr{L}_j$ pero $E_{1j}E_{ji} = E_{1i} \notin \mathscr{L}_j$ si $i \neq j$.

Teorema 1.5.4. *Sea R un anillo.*

(1) (Teorema de la correspondencia para anillos) Sea I un ideal de R. La correspondencia $A \mapsto A/I$ es una biyección que conserva la inclusión entre el conjunto de subanillos de R que contienen a I y el conjunto de subanillos de R/I. Además, A (subanillo que contiene a I) es un ideal de R si, y sólo si, A/I es un ideal de R/I.

(2) (2^o teorema de isomorfismo) Sean I, J ideales de R tales que $I \subset J$. Entonces $J/I = \{\bar{a} \mid a \in J\}$ es un ideal de R/I y existe un isomorfismo natural $\frac{R/I}{J/I} \simeq R/J$.

(3) (3^o teorema de isomorfismo) Sean A un subanillo de R e I un ideal de R. Entonces $A + I$ es un subanillo de R, la intersección $A \cap I$ es un ideal de A y existe un isomorfismo natural $A + I/I \simeq A/A \cap I$.

1.5.2. Operaciones con ideales

Definición 1.5.5. Sean I, J ideales en un anillo R con $1 \neq 0$.

(1) El ideal suma es $I + J = \{a + b \mid a \in I, b \in J\}$. Es el menor ideal que contiene a ambos I, J.

(2) El ideal producto es $IJ = \{\sum_{i=1}^{n} a_i b_j \mid a_i \in I, b_i \in J, n \geq 1\}$.

(3) El ideal potencia n–ésima es $I^n = \{\sum_{i=1}^{k} a_{i1} \cdots a_{in} \mid a_{ij} \in I, k \in \mathbb{N}\}$.

(4) La intersección de una familia cualquiera de ideales es un ideal. Es claro que $IJ \subset I \cap J$.

(5) Si R es conmutativo, el radical de un ideal I es el ideal $\sqrt{I} = \{r \in R \mid r^n \in I$ para algún $n \in \mathbb{N}\}$.

(6) Si R es conmutativo, el ideal cociente es $I : J = \{r \in R \mid rJ \subset I\}$.

(7) El ideal (A) generado por un subconjunto $A \subset R$ es el menor ideal ($(A)_i$ a izquierda, $(A)_d$ a derecha) de R que contiene a A (si $A = \emptyset$ ponemos $(A) = \{0\}$). El ideal (A) ($(A)_i$, $(A)_d$) es la intersección de la familia de ideales (a izquierda, a derecha) de R que contienen a A.

(8) El conjunto $RA = \{\sum_{i=1}^{n} r_i a_i \mid r_i \in R, a_i \in A, n \geq 1\}$ (con $RAR = \{0\}$ si $A = \emptyset$) es un ideal a izquierda que contiene a A. Recíprocamente, todo ideal a izquierda que contiene a A contiene a RA. Por tanto $(A)_i = RA$. Análogo para AR.

(9) El conjunto $RAR = \{\sum_{i=1}^{n} r_i a_i s_i \mid r_i, s_i \in R, a_i \in A, n \geq 1\}$ (con $RAR = \{0\}$ si $A = \emptyset$) es un ideal que contiene a A. Recíprocamente, todo ideal que contiene a A contiene a RAR. Por tanto $(A) = RAR$.

(10) Si R conmutativo $RA = AR = RAR = (A)$.

(11) El ideal, llamado principal, (a) generado por un elemento es $(a) = RaR = \{\sum_{i=1}^{n} r_i a s_i \mid r_i, s_i \in R, n \geq 1\}$.

(12) Si R conmutativo $(a) = RaR = aR = Ra = \{ra \mid r \in R\}$.

(13) Un ideal I se dice finitamente generado si I es el ideal generado por un subconjunto finito de R.

(14) Un anillo conmuattivo, unitario en el que todos sus ideales son finitamente generados se llama anillo noetheriano. Ejemplo: $\mathbb{C}[X, Y]$.

Proposición 1.5.6. *Sea I un ideal en un anillo R.*

(1) Un ideal a izquierda (derecha) I es $I = R$ si, y sólo si, I contiene una unidad.

(2) Los únicos ideales a izquierda (derecha) de un anillo de división D son $\{0\}, D$.

(3) Supongamos R conmutativo. Si los únicos ideales de R son $\{0\}, R$, entonces R es un cuerpo.

(4) Sea F un cuerpo. Los únicos ideales del anillo $\mathscr{M}_n(F)$, son $\{0\}, \mathscr{M}_n(F)$. Sin embargo, si $n \geq 2$ el anillo $\mathscr{M}_n(F)$ no es de división (tiene ideales propios sólo a izquierda e ideales propios sólo a derecha).

Definición 1.5.7. Un anillo R cuyos únicos ideales (biláteros) son $\{0\}, R$ se denomina simple.

Ejemplos 1.5.8. (1) En $R = \mathbb{Z}$ o $R = F[X]$, con F cuerpo, todo ideal es principal (en ambos hay una división). Si $r, s \in R = \mathbb{Z}, F[X]$ el ideal $(r, s)R = rR + sR = \text{mcd}(r, s)R$.

(2) El ideal $(2, X)\mathbb{Z}[X] = \{2p(X) + Xq(X) \mid p(X), q(X) \in \mathbb{Z}[X]\}$ = { polinomios cuyo término constante es par } no es principal. En efecto, supongamos $(2, X)\mathbb{Z}[X] = a(X)\mathbb{Z}[X]$. Entonces $2 = p(X)a(X)$, para algún $p(X) \in \mathbb{Z}[X]$. Puesto que el grado del producto $p(X)a(X)$ es la suma de los grados de $p(X), a(X)$, se deduce $p(X), a(X) \in \mathbb{Z}$. Así $p(X), a(X) \in \{\pm 1, \pm 2\}$. Si $a(X) = \pm 1$ entonces $1 \in (2, X)\mathbb{Z}[X]$, y es claro que $1 = 2q(X) + Xr(X)$ no tiene solución. Si $a(X) = \pm 2$, entonces $X = 2q(X)$, imposible.

Observemos, sin embargo, que $(2, X)\mathbb{Q}[X] = \mathbb{Q}[X]$.

Teorema 1.5.9 (Teorema de división entera)**.** *Sea $0 \neq d \in \mathbb{Z}$ un entero no nulo. Para cada entero $m \in \mathbb{Z}$ existen únicos enteros $q, r \in \mathbb{Z}$ tales que $m = dq + r$ y $0 \leq r <| d |$.*

Demostración. Si $d < 0$ y $m = (-d)q + r$ es la división de m por $-d$, entonces $m = d(-q) + r$ es la división de m por d. Por tanto, podemos suponer $d > 0$. Si $m < 0$ y $(-m) = dq + r$, con $0 \leq r < d$ es la división de $-m$ por d, entonces si $r = 0$ la división de m por d es $m = d(-q)$ y, si $r > 0$ la división de m por d es $m = d(-q-1) + (d-r)$. Por tanto, podemos suponer $d > 0$ y $m \geq 0$. Si $0 \leq m < d$, la división de m por d es $m = d0 + m$. Supongamos que $m \geq d$ y que, por hipótesis de inducción hay división de todo $0 \leq n < m$ por d. Entonces para $0 \leq m - d < m$ hay división $m - d = dq_1 + r$, con $0 \leq r < d$. Así $m = d(q_1 + 1) + r$ es la división de m por d.
Respecto de la unicidad, si $m = dq + r$ y $m = dq' + r'$ son divisiones, entonces $|d||q - q'| = |r' - r|$. Puesto que de $0 \leq r, r' < |d|$ se deduce $|r' - r| < d$, de la igualdad $|d||q - q'| = |r' - r|$ se obtiene $|r' - r| = 0 = |q - q'|$. □

Corolario 1.5.10. *Todo ideal de $\mathbb{Z}$ es principal.*

Demostración. Sea $I \subset \mathbb{Z}$ un ideal. Si $I = \{0\}$, entonces $I = 0\mathbb{Z}$. Supongamos que $I \neq \{0\}$. Entonces $I^+ = \{s \in I \,|\, s > 0\} \neq \emptyset$. Sea d el mínimo del conjunto I^+. Demostremos que $I = d\mathbb{Z}$. Puesto que $d \in I$ es $d\mathbb{Z} \subset I$. Recíprocamente, si $m \in I$, consideramos la división $m = dq + r$, con $0 \leq r < d$. Entonces $r = m - dq \in I$ y, por tanto ha de ser $r = 0$. Así $m = dq \in d\mathbb{Z}$. □

1.5.3. Función de Euler

Consideramos el grupo de las unidades $\mathbb{Z}_n^*$ del anillo $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}, n \geq 2$.

Lema 1.5.11. *Un elemento $\bar{a} \in \mathbb{Z}_n$ es unidad si, y sólo si,* $\mathrm{mcd}(a, n) = 1$ *si, y sólo si, $\bar{a}$ es un generador del grupo cíclico aditivo $(\mathbb{Z}_n, +)$. Si $\bar{0} \neq \bar{a}$ no es unidad entonces es divisor de cero en $\mathbb{Z}_n$.*

Demostración. $\bar{a} \in \mathbb{Z}_n$ es unidad $\Leftrightarrow$ existen $u, v \in \mathbb{Z}$ tales que $au - 1 = nv \Leftrightarrow \mathrm{mcd}(a, n) = 1$ $\Leftrightarrow$ para todo $1 \leq r < n$ existen $k, l \in \mathbb{Z}$ tales que $ak - r = nl \Leftrightarrow$ para todo $\bar{r} \in \mathbb{Z}_n$ existe $k \in \mathbb{Z}$ tal que $k\bar{a} = \bar{r}$. Si $1 < d = \mathrm{mcd}(a, n)$, entonces $n = dq, a = db$, Así $\bar{a}\bar{q} = \bar{d}\bar{b}\bar{q} = \bar{n}\bar{b} = \bar{0}$ y $\bar{q} \neq \bar{0}$. □

Proposición–Definición 1.5.12. El orden del grupo $\mathbb{Z}_n^*$ es el número

$$\varphi(n) = |\{a \mid 1 \leq a < n \ \ \& \ \ \mathrm{mcd}\,(a, n) = 1\}|$$

Diremos que $\varphi(n)$ es la función de Euler.

Demostración. Lemma 1.5.11 □

Corolario 1.5.13 (Teorema de Euler)**.** *Sean $a, n \in \mathbb{N}$ tales que* $\mathrm{mcd}(a, n) = 1$*, entonces $a^{\varphi(n)} \equiv 1 \,(\mathrm{mod}\, n)$.*

Demostración. Proposición 1.5.12 y Teorema 2.1.19. □

Lema 1.5.14. *Sean $m, n \in \mathbb{Z}$. Entonces la aplicación $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ dada por $f(\bar{k}) = (\bar{k}, \bar{k})$ está bien definida y es el único homomorfismo de anillos unitarios de $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$. Además f es un isomorfismo si, y sólo si,* $\mathrm{mcd}(m, n) = 1$.

Demostración. $\mathrm{mcd}(m, n) = 1 \Rightarrow mu + nv = 1$, para ciertos $u, v \in \mathbb{Z}$. Veamos que f es inyectiva, en efecto, si $m \mid k$ y $n \mid k$, entonces $mn = \mathrm{mcm}(m, n) \mid k$. Puesto que f es inyectiva y se trata de dos conjuntos finitos con el mismo número de elementos se deduce que es sobreyectiva. También podemos ver que f es sobreyectiva de forma directa.Sean a, b y $k = mub + nva$, entonces $k \equiv b \pmod{n}$ y $k \equiv a \pmod{m}$. Recíprocamente, si f es inyectiva, entonces para todo k de $m \mid k, n \mid k$ se deduce que $mn \mid k$. En particular, para $k = \mathrm{mcm}(m, n)$ se verifica $mn \mid \mathrm{mcm}(m, n)$. De aquí $\mathrm{mcd}(m, n) = 1$. □

Proposición 1.5.15. *Sean $m, n \in \mathbb{N}$ tales que* $\mathrm{mcd}(m, n) = 1$, *entonces*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Demostración. El isomorfismo de anillos

$$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$$

induce un isomorfismo entre los grupos de unidades

$$(\mathbb{Z}_{mn})^* \simeq (\mathbb{Z}_m)^* \times (\mathbb{Z}_n)^*.$$

Por tanto,

$$\varphi(mn) = \varphi(m)\varphi(n).$$

□

Proposición 1.5.16. *Sea $n = p_1^{a_1} \cdots p_s^{a_s}$, donde p_i primos distintos y $a_i \geq 1$. Entonces*

$$\varphi(n) = \prod_{i=1}^{s} p_i^{a_i - 1}(p_i - 1) = n \prod_{i=1}^{s} (1 - \frac{1}{p_i}).$$

Demostración. El isomorfismo de anillos

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{a_s}\mathbb{Z}$$

induce un isomorfismo entre los grupos de unidades

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_s^{a_s}\mathbb{Z})^*.$$

Por tanto,

$$\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_s^{a_s}).$$

Para calcular $\varphi(p^s)$, restamos de $p^s - 1$ el número de múltiplos de p entre 1 y $p^s - 1$, que es $p^{s-1} - 1$. Obtenemos, por tanto,

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

□

Definición 1.5.17. Denominaremos función de Mobius a la función en los enteros positivos definida por

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n \text{ es producto de } k \text{ primos distintos,} \\ 0 & \text{si } n \text{ es divisible por el cuadrado de un primo.} \end{cases} .$$

Proposición 1.5.18. *Si* $mcd(m,n) = 1$, *entonces* $\mu(mn) = \mu(m)\mu(n)$.

Demostración. Si $\text{mcd}(m,n) = 1$, entonces $m = p_1^{a_1} \cdots p_r^{a_r}, n = q_1^{b_1} \cdots q_s^{b_s}$, donde p_i, q_j primos distintos y $a_i, b_j \geq 1$. Si alguno de los a_i o de los b_j es ≥ 2, entonces $\mu(m) = 0$ o $\mu(n) = 0$ y $\mu(mn) = 0$. Si todos los a_i, b_j son 1, entonces $\mu(m) = (-1)^r, \mu(n) = (-1)^s, \mu(mn) = (-1)^{r+s}$. □

Definición 1.5.19. Una función $f(n)$ definida en los enteros positivos de dice multiplicativa si $f(mn) = f(m)f(n)$ siempre que $\text{mcd}(m,n) = 1$.

Lema 1.5.20. *Sea* $f(n)$ *multiplicativa y* $g(n) = \sum_{d|n} f(n)$, *entonces*

(1) $g(n)$ *es multiplicativa, y*

(2) $f(n) = \sum_{d|n} \mu(d)g(\frac{n}{d})$ *(fórmula de inversión).*

Demostración. Para $\text{mcd}(m,n) = 1$, cada divisor de mn es de la forma d_1d_2 con $d_1 \mid m, d_2 \mid n$ de modo único, por tanto, $g(mn) = \sum_{d|mn} f(mn) = \sum_{d_1|m, d_2|n} f(d_1d_2) = (\sum_{d_1|m} f(d_1))(\sum_{d_2|n} f(d_2)) = g(m)g(n)$.

$$\sum_{d|n} \mu(d)g\left(\frac{n}{d}\right) = \sum_{d|n}\left(\sum_{c|\frac{n}{d}} \mu(d)f(c)\right) =$$

$$= \sum_{c|n}\left(f(c)\sum_{d|\frac{n}{c}} \mu(d)\right) = \sum_{c|n} f(c)\left(\begin{cases} 1 & \text{si } \frac{n}{c} = 1, \\ 0 & \text{si } \frac{n}{c} > 1. \end{cases}\right) =$$

$$= f(n).$$

□

Lema 1.5.21.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & si\ n = 1, \\ 0 & si\ n > 1. \end{cases}$$

Demostración. Puesto que μ es multiplicativa , la función $g(n) = \sum_{d|n} \mu(d)$ también es multiplicativa, por tanto, si $1 < n = \prod_{p|n} p^{b_p}$, entonces $g(n) = \prod_{p|n} g(p^{b_p})$. Ahora bien, para p primo $g(p^b) = \sum_{d|p^b} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^b) = 1 - 1 + 0 + \cdots + 0 = 0$. □

Proposición 1.5.22.

$$\sum_{d|n} \varphi(d) = n.$$

Demostración. En Lema 1.5.11 hemos visto que $\varphi(n)$ es el número de generadores del grupo cíclico $\mathbb{Z}_n$. Por otra parte, sabemos que $\mathbb{Z}_n$ tiene exactamente un subgrupo de orden d para cada divisor $d \mid n$ y todos los subgrupos son cíclicos. De aquí se sigue la fórmula. □

Corolario 1.5.23.

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Demostración. Se deduce de Proposicion 1.5.22 y Lema 1.5.20 para $g(n) = n, f(n) = \varphi(n)$. □

1.5.4. Ideales maximales. Ideales primos

Definición 1.5.24. Un ideal (ideal a la izquierda, derecha) M en un anillo R se dice maximal si $M \neq R$ y los únicos ideales (ideales a izquierda, derecha) que contienen a M son M, R.

Un anillo arbitrario no necesariamente tiene ideales maximales. Por ejemplo, un grupo abeliano como $\mathbb{Q}$ (sin subgrupos maximales) visto como anillo trivial ($xy = 0$, para todo $x, y \in \mathbb{Q}$). Afortunadamente todo anillo con $1 \neq 0$ tiene ideales maximales.

Teorema 1.5.25. *Sea R un anillo con $1 \neq 0$. Cada ideal (ideal a izquierda, derecha) propio está contenido en un ideal (ideal a izquierda, derecha) maximal.*

Demostración. Sean $I \subsetneq R$ y $\mathscr{S} = \{\text{ideales propios de } R \text{ que contienen a } I\}$. Puesto que $I \in \mathscr{S} \neq \emptyset$ ordenamos $\mathscr{S}$ por inclusión para probar la existencia de elementos maximales en $(\mathscr{S}, \subset)$ aplicando el lema de Zorn. Sea $\mathscr{C} \subset \mathscr{S}$ una cadena, i.e., un subconjunto totalmente ordenado. Hemos de probar que $\mathscr{C}$ tiene una cota superior en $\mathscr{S}$. Bastará para ello probar que la unión de todos los elementos de $\mathscr{C}$ es un ideal J. En efecto, sean $a, b \in J$ existen $A, B \in \mathscr{C}$ tal que $a \in A, b \in B$. Puesto que $A \subset B$ o $B \subset A$, si e.g., $A \subset B$, entonces $a - b \in B \subset J$. La condición multiplicativa es similar. Además $1 \notin J$ puesto que $1 \notin A$ para cada $A \in \mathscr{C}$. Así $J \in \mathscr{S}$. Por lema de Zorn, $\mathscr{S}$ tiene algún elemento maximal, que resulta ser un ideal maximal que contiene a I. □

Teorema 1.5.26. *Sea M un ideal en un anillo R con $1 \neq 0$.*

(1) Si R/M es un anillo de división, entonces M es maximal.

(2) Si R es conmutativo y M es maximal, entonces R/M es un cuerpo.

Demostración. Supongamos que R/M es un anillo de división. Entonces $1_{R/M} \neq 0$. Esto es $1 \notin M$. Sea $M \subsetneq I \subset R$ y $a \in I - M$. Entonces $a + M$ tiene inverso (inverso a izquierda, derecha) en R/M. Esto es $1 - ra \in M$ para algún $r \in R$. Así $1 - ra \in I$. Puesto que $ra \in I$ es $1 \in I$, esto es $I = R$.
Sean R conmutativo y M maximal. La condición $M \subsetneq R$ significa $1_{R/M} \neq 0$. Sea $a + M \neq 0$. Entonces $M \subsetneq M + (a)$. Puesto que R es conmutativo $(a) = Ra$, y podemos escribir $1 = m + ra$ con $m \in M, r \in R$. Así $1 + M = (a + M)(r + M)$. □

Ejemplos 1.5.27. (1) En el anillo $2\mathbb{Z}$, que no tiene 1, el ideal $4\mathbb{Z}$ es maximal. Es claro que $2\mathbb{Z}/4\mathbb{Z}$ no es cuerpo.

(2) El anillo $R = \mathscr{M}_n(D)$, con D anillo de división y $n \geq 2$ es simple, esto es $\{0\}$ es maximal. Sin embargo $R = R/\{0\}$ no es anillo de división puesto que tiene divisores de cero.

(3) $n\mathbb{Z}$ es maximal si, y sólo si, n primo si, y sólo si, $\mathbb{Z}/n\mathbb{Z}$ es un cuerpo. En efecto, sean $p \in \mathbb{Z}$ primo y $\overline{0} \neq \overline{a} \in \mathbb{Z}/p\mathbb{Z}, 1 \leq a < p$, hay que probar que $\overline{a}$ tiene inverso en $\mathbb{Z}/p\mathbb{Z}$. La condición $\overline{0} \neq \overline{a}$ significa que $a \notin p\mathbb{Z}$. El ideal $a\mathbb{Z} + p\mathbb{Z}$ es principal $a\mathbb{Z}+p\mathbb{Z} = d\mathbb{Z}$ con $d > 0$. En particular $d \mid p$. Puesto que p es primo, ha de ser $d = 1, p$. Si $d = p$, entonces $a \in p\mathbb{Z}$. Por tanto, $d = 1$. Así, existen $u, v \in \mathbb{Z}$ tales que $au+pv = 1$. Entonces $\overline{a}\,\overline{u} = \overline{1}$. Recíprocamente, si $\mathbb{Z}/n\mathbb{Z}$ es un cuerpo y $1 \leq a < n$, el elemento $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ tiene inverso. Esto significa que existem $u, v \in \mathbb{Z}$ tales que $au + nv = 1$. Si suponemos que $a|n$, existe $w \in \mathbb{Z}$ tal que $n = aw$. Entonces $a(u + wv) = 1$. De esta igualdad se deduce $a = 1$. Por tanto, n es primo.

(4) $(2, X)\mathbb{Z}[X]$ es maximal puesto que $\mathbb{Z}[X]/(2, X)\mathbb{Z}[X] \simeq \mathbb{Z}/2\mathbb{Z}$.

(5) $X\mathbb{Z}[X]$ no es maximal puesto que $X\mathbb{Z}[X] \subsetneq (2, X)\mathbb{Z}[X]$.

Definición 1.5.28. Sea R un anillo conmutativo. Un ideal P se dice primo si $P \neq R$ y siempre que $xy \in P$, con $x, y \in R$, entonces $x \in P$ ó $y \in P$.

Ejemplo 1.5.29. (1) $0 \neq p \in \mathbb{Z}$ es primo si, y sólo si, $\{0\} \neq p\mathbb{Z}$ ideal primo. En efecto, sean $0 \neq p \in \mathbb{Z}$ primo, $xy \in p\mathbb{Z}$ y $x \notin p\mathbb{Z}$. Entonces, (razonando como en (1.5.27) $xu + pv = 1$ para ciertos $u, v \in \mathbb{Z}$. Así $y = y1 = yxu + ypv \in p\mathbb{Z}$. Recíprocamente si $\{0\} \neq n\mathbb{Z}$ es ideal primo y $1 \leq a < n$ verifica $n = au$, ha de ser $u \in n\mathbb{Z}$, esto es $u = nw$. Entonces $n = anw$ y, puesto que, $0 \neq n$ es $1 = aw$. Así $a = 1$.

(2) $I = (X^2+Y^2-1)\mathbb{C}[X, Y]$, $J = (X)\mathbb{C}[X, Y]$ son primos. La suma $I+J = (Y^2-1, X)\mathbb{C}[X, Y]$ no es primo, puesto que $Y^2 - 1 = (Y + 1)(Y - 1) \in I + J$, pero $Y \pm 1 \notin I + J$

Proposición 1.5.30. *Un ideal $P \subset R$ es primo si, y sólo si, R/P es un dominio de integridad.*

Demostración. En primer lugar, $P \neq R$ si, y sólo si, $1_{R/P} \neq 0$. Por otra parte, $xy \in P$ si, y sólo si, $(x + P)(y + P) = 0$, y, $x \in P$ ó $y \in P$ si, y sólo si, $x + P = 0$ ó $y + P = 0$. □

Corolario 1.5.31. *En un anillo conmutativo todo ideal maximal es primo.*

Ejemplos 1.5.32. (1) En el teorema de la correspondencia (1.5.4), el ideal J/I, $I \subset J$, es primo (maximal) si, y sólo si, J es primo (maximal).

(2) $0 \neq n\mathbb{Z}$ primo si, y sólo si, $\{0\} \neq n\mathbb{Z}$ maximal si, y sólo si, $0 \neq n$ primo.

(3) $X\mathbb{Z}[X]$ es primo, no maximal: $\mathbb{Z}[X]/X\mathbb{Z}[X] = \mathbb{Z}$.

1.6. Anillos de fracciones

Sea R un anillo conmutativo con unidad. Un no divisor de cero $r \in R$ es cancelable. Así un no divisor de cero comparte esta propiedad con las unidades. El objeto de esta sección es probar que R se puede sumergir en un anillo mayor F de forma que todo no divisor de cero en R es unidad en F. En el caso de un dominio de integridad R este anillo F es un cuerpo denominado cuerpo de fracciones de F.
Un subconjunto $\emptyset \neq D \subset R$ es multiplicativamente cerrado si $1 \in D$ y $dd' \in D$ siempre que $d, d' \in D$. El anillo de fracciones $R[D^{-1}]$ es el conjunto cociente de $R \times D$ por la relación de equivalencia $(r, d) \sim (r', d')$ si, y sólo si, existe $d'' \in D$ tal que $d''(rd' - dr') = 0$. Si D no contiene divisores de cero la relación de equivalencia es $(r, d) \sim (r', d')$ si, y sólo si, $rd' - dr' = 0$, como en el caso de los números racionales o las fracciones algebraicas.
La clase de equivalencia de (r, d) se denota

$$\frac{r}{d}.$$

Las operaciones

$$\frac{r}{d} + \frac{r'}{d'} = \frac{rd' + dr'}{dd'},$$
$$\frac{r}{d} \cdot \frac{r'}{d'} = \frac{rr'}{dd'}$$

están bien definidas y hacen de $R[D^{-1}]$ un anillo conmutativo con $0_{R[D^{-1}]} = \frac{0}{1}$, $-\frac{r}{d} = \frac{-r}{d}$, y unidad $1_{R[D^{-1}]} = \frac{1}{1}$. Es claro que $1_{R[D^{-1}]} = 0_{R[D^{-1}]}$ si, y sólo si, $0 \in D$. Por tanto, supondremos que $0 \notin D$.
El homomorfismo natural $R \xrightarrow{\varphi} R[D^{-1}]$ definido por $r \mapsto \frac{r}{1}$ es inyectivo si, y sólo si, D no contiene divisores de cero, puesto que $\ker \varphi = \{r \in R \mid \text{existe } d \in D \text{ con } dr = 0\}$.

Ejemplos 1.6.1. (1) El conjunto D de todos los no divisores de cero en R es multiplicativamente cerrado. En este caso, la relación de equivalencia es la bien conocida

$$\frac{r}{d} = \frac{r'}{d'} \Leftrightarrow rd' = dr'.$$

Además, el anillo R se sumerge como subanillo del anillo de fracciones $F = R[D^{-1}]$ donde todo no divisor de cero de R tiene inverso. Si R es un DI, entonces $D = R - \{0\}$ y F es un cuerpo que denominaremos cuerpo de fracciones de R.

(2) El complementario de un ideal primo P es multiplicativamente cerrado. Denotaremos R_P el anillo de fracciones. Este anillo es un anillo local, i.e., un anillo con un único ideal maximal.

(3) El conjunto $D = \{d^n \mid n \geq 0\}$ de las potencias de un elemento $d \in R$ es multiplicativamente cerrado. El anillo de fracciones R_d es no nulo si, y sólo si, d no es nilpotente.

(4) $\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$

(5) El cuerpo de fracciones de $\mathbb{Q}[X]$ es $\mathbb{Q}(X) = \{p(X)/q(X) | 0 \neq q(X), p(X) \in \mathbb{Q}[X]\}$.

Teorema 1.6.2. *Sean T un anillo conmutativo con unidad y $R \xrightarrow{f} T$ un homomorfismo tal que $f(d)$ es unidad en T para cada $d \in D$, con D multiplicativamente cerrado en R. Entonces existe un único homomorfismo de anillos $\Phi : R[D^{-1}] \to T$, definido por $\Phi(r/d) = f(r)f(d)^{-1}$, que hace conmutativo el diagrama*

$$\begin{array}{ccc} R & \xrightarrow{f} & T \\ {\scriptstyle\varphi}\downarrow & \nearrow_{\Phi} & \\ R[D^{-1}] & & \end{array} .$$

1.7. Anillos de polinomios

Definición 1.7.1. Sea R un anillo conmutativo y unitario. El anillo $R[X]$ de polinomios en una indeterminada con coeficientes en R es el conjunto

$R[X] = \{p : \mathbb{N}\cup\{0\} \to R \mid p(n) = 0$ salvo, a lo mas para una cantidad finita de $n \in \mathbb{N}\cup\{0\}\}$.

Esto es, un polinomio p es una sucesión de elementos de R

$$p = (r_0, r_1, \ldots, r_k, 0, \ldots),$$

donde, a partir de cierto índice, todos los elementos son cero.
Denotamos

$$X = (0, 1, 0, \ldots).$$

Definimos las operaciones

$$(r_0, r_1, \ldots, r_k, 0, \ldots) + (s_0, s_1, \ldots, s_l, 0, \ldots) = (r_0 + s_0, r_1 + s_1, \ldots),$$

$$(r_0, r_1, \ldots, r_k, 0, \ldots) \cdot (s_0, s_1, \ldots, s_l, 0, \ldots) = (t_0, t_1, \ldots),$$

$$t_m = \sum_{i=0}^{m} r_i s_{m-i}.$$

Con estas operaciones $R[X]$ es un anillo conmutativo con $0_{R[X]} = (0, 0, \ldots)$, $-p = (-r_0, -r_1, \ldots)$ y con unidad $1_{R[X]} = (1, 0, \ldots)$.
La aplicación $R \to R[X]$, $r \mapsto (r, 0, \ldots)$ es un homomorfismo inyectivo de anillos. Identificamos

$$r = (r, 0, \ldots)$$

Se verifica que

$$X^n = (0, 0, \ldots, \overset{n}{1}, 0, \ldots).$$

Con estas notaciones

$$p = (r_0, r_1, \ldots, r_k, 0, \ldots) = \sum_{i=0}^{k} r_i X^i.$$

Denotaremos

$$p(X) = \sum_{i=0}^{k} r_i X^i = r_0 + r_1 X + \cdots + r_k X^k.$$

$$r_0 + r_1 X + \cdots + r_k X^k = s_0 + s_1 X + \cdots + s_l X^l \Leftrightarrow r_0 = s_0, r_1 = s_1, \ldots.$$

El coeficiente r_0 es el término independiente de $p(X)$. Si

$$0 \neq p(X) = r_0 + r_1 X + \cdots + r_k X^k, r_k \neq 0, k \geq 0,$$

diremos que el polinomio $0 \neq p(X)$ tiene grado $\deg p(X) = k$, y que r_k es su coeficiente principal. El polinomio 0 se puede considerar con grado $-\infty$, donde $-\infty < k, -\infty + k = -\infty, (-\infty) + (-\infty) = (-\infty)$.

Proposición 1.7.2. *Sean* $p(X) = r_0 + r_1X + \cdots + r_kX^k, q(X) = s_0 + s_1X + \cdots + s_lX^l \in R[X]$.

(1) $\deg(p(X) + q(X)) \leq \max\{\deg p(X), \deg q(X)\}$

(2) $\deg(p(X)q(X)) \leq \deg p(X) + \deg q(X)$*, con igualdad si, y sólo si,* $r_ks_l \neq 0$.

Proposición 1.7.3. *Sea R un dominio de integridad.*

(1) $R[X]$ *es dominio de integridad.*

(2) $R[X]^* = R^*$.

Demostración. (1) Si $p(X)q(X) = 0$, entonces $-\infty = \deg(p(X)q(X)) = \deg p(X) + \deg q(X)$. Por tanto, $\deg p(X) = -\infty$ o $\deg q(X) = -\infty$ y, en consecuencia, $p(X) = 0$ o $q(X) = 0$.
(2) Si $p(X)q(X) = 1$, entonces $0 = \deg(p(X)q(X)) = \deg p(X) + \deg q(X)$. Por tanto, $\deg p(X) = \deg q(X) = 0$. Así, $p(X) = r_0 \in R$, $q(X) = s_= \in R$ y $r_0s_0 = 1$. En consecuencia, $p(X) = r_0 \in R^*, q(X) = s_0 \in R^*$. □

Ejemplo 1.7.4. En $(\mathbb{Z}/12\mathbb{Z})[X]$ se verifica $(\overline{6}X + \overline{5})(\overline{6}X + \overline{5}) = \overline{1}$.

Proposición 1.7.5. *Sea* $I \subset R$ *un ideal. El ideal* $IR[X]$ *generado por I en* $R[X]$ *coincide con el conjunto* $I[X]$ *de polinomios con coeficientes en I. Esto es,* $IR[X]$ *es el núcleo del homomorfismo natural* $R[X] \to (R/I)[X]$*. En consecuencia,* $R[X]/IR[X] \simeq (R/I)[X]$*. En particular,* $IR[X]$ *es primo si, y sólo si, I es primo.*

1.7.6. El anillo de polinomios en n variables es $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$. Un elemento típico se escribe en la forma

$$\sum_{i_1+\cdots+i_n\leq k} r_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n},$$

para algún $k \geq 0$ y $a_{i_1,\ldots,i_n} \in R$. Este elemento es cero si, y sólo si, todo $r_{i_1,\ldots,i_n} = 0$.

Teorema 1.7.7. *Sean S un anillo conmutativo unitario,* $s_1, \ldots, s_n \in S$ *y* $R \xrightarrow{\varphi} S$ *un homomorfismo de anillos. Existe un único homomorfismo de anillos (homomorfismo de sustitución)* $R[X_1, \ldots, X_n] \xrightarrow{\Phi} S$ *tal que* $\Phi_{|R} = \varphi$ *y* $\Phi(X_i) = s_i$ *para cada* $i = 1, \ldots, n$*. El homomorfismo* Φ *está definido por*

$$\sum_{i_1+\cdots+i_n\leq k} r_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n} \mapsto \sum_{i_1+\cdots+i_n\leq k} \varphi(r_{i_1,\ldots,i_n}) s_1^{i_1} \cdots s_n^{i_n}.$$

Ejemplo 1.7.8. El homomorfismo aditivo de sustitución no es multiplicativo si R no es conmutativo. Sean $R = \mathbb{H}$ y $p(X) = X^2 + 1 = (X + i)(X - i) \in \mathbb{H}[X]$. La sustitución $X = j$ no es multiplicativa, puesto que $j^2 + 1 = 0$ y, sin embargo, $(j+i)(j-i) = j^2 - ji + ij - i^2 = 2k \neq 0$.

Teorema 1.7.9 (Teorema de la base de Hilbert)**.** *Sea R un anillo conmutativo unitario, tal que todos sus ideales son finitamente generados (anillo noetheriano). Entonces el anillo* $R[X_1, \ldots, X_n]$ *es noetheriano.*

Demostración. Enunciamos este teorema por su importancia. Se puede encontrar una prueba en la bibliografía. □

Teorema 1.7.10 (Teorema de división)**.** *Sean R un anillo conmutativo con unidad, $f(X) \in R[X]$ y $0 \neq d(X) = aX^n + \cdots \in R[X]$, con $0 \neq a \in R$ y $n = \deg d \geq 0$. Sean m el grado de $f(X)$ y $k = \max\{m - n + 1, 0\}$. Existen $q(X), r(X) \in R[X]$ tales que*

$$a^k f(X) = d(X)q(X) + r(X),$$

con $\deg r(X) < \deg d(X)$. Si a es no divisor de cero en R, entonces $q(X), r(X)$ son únicos con estas condiciones. Si a es unidad en R (en particular, si R es un cuerpo) la división se puede escribir en la forma

$$f(X) = d(X)q(X) + r(X),$$

para únicos $q(X), r(X)$ con la condición $\deg r(X) < \deg d(X)$.

Demostración. Si $n = 0$, entonces $d(X) = a$, $k = m + 1, q(X) = a^m f(X)$ y $r(X) = 0$. Sea $n > 0$ fijado. Hacemos inducción en $m = \deg f$. Si $f(X) = 0$ o $m < n$, entonces $k = 0$, $q(X) = 0$ y $r(X) = f(X)$. Supongamos $m \geq n$ y el enunciado cierto para $\deg f(X) < m$. Sea $f(X) = bX^m + \cdots$, con $0 \neq b \in R$. Entonces $\deg(af(X) - bX^{m-n}d(X)) \leq m - 1$. Así $a^{(m-1)-n+1}(af(X) - bX^{m-n}d(X)) = d(X)q_1(X) + r(X)$, con $\deg r(X) < \deg d(X)$. De donde $a^{m-n+1}f(X) = (a^{m-n}bX^{m-n} + q_1(X))d(X) + r(X)$.
Supongamos que a es no divisor de cero en R. Si $dq + r = dq_1 + r_1$ con $\deg r_1 < \deg d$, entonces $d(q - q_1) = r_1 - r$. En esta igualdad $\deg(r_1 - r) < \deg d$ y $\deg d(q - q_1) = \deg d + \deg(q - q_1)$. Por tanto $\deg(q - q_1) = -\infty$. Así $q = q_1, r = r_1$. □

Ejemplo 1.7.11.

$$2^2(X^3 + 2X^2 + X + 1) = (2X^2 + X + 1)(2X + 3) + (-X + 1).$$

Ejemplo 1.7.12. Sean R un DI y $a_1, \ldots, a_r \in R$.

(1) El ideal $I = (X_1 - a_1, \ldots, X_r - a_r)R[X_1, \ldots, X_n]$, con $r \leq n$, es primo. En efecto, usando el teorema de división es sencillo comprobar que I es el núcleo del homomorfismo sobreyectivo $R[X_1, \ldots, X_n] \to R[X_{r+1}, \ldots, X_n]$ definido por $f(X_1, \ldots, X_n) \mapsto f(a_1, \ldots, a_r, X_{r+1}, \ldots, X_n)$. Así $R[X_1, \ldots, X_n]/I \simeq R[X_{r+1}, \ldots, X_n]$ que es un DI.

(2) Si $R = F$ es un cuerpo, entonces $(X_1 - a_1, \ldots, X_n - a_n)F[X_1, \ldots, X_n]$ es maximal.

Proposición 1.7.13. *Sea F un cuerpo. Todo ideal del anillo $F[X]$ es principal.*

Demostración. Sea $I \subset F[X]$ un ideal. Si $I = \{0\}$, entonces $I = (0)F[X]$. Si $I \neq 0$ contiene un elemento $0 \neq a \in I \cap F$, entonces $I = F[X] = (1)F[X]$, Si $I \neq 0$ e I no contiene polinomios no nulos de grado cero, elegimos un polinomio $0 \neq d(X) \in I$ con $1 \leq \deg d(X)$ mínimo entre los grados de los elementos de $I - \{0\}$. Entonces $(d(x))F[X] \subset I$. recíprocamente, sea $p(X) \in I$. Dividimos $p(X) = d(X)q(X) + r(X)$ con $\deg r < \deg d$. Entonces $r(X) = p(X) - d(X)q(X) \in I$. La minimalidad del grado de $d(X)$ implica que $\deg r(X) = -\infty$. Así, $r(X)0$. En consecuencia, $I = (d(X))F[X]$. □

Observación 1.7.14. La unicidad de la división implica que el resto y cociente son independientes del cuerpo extensión donde situemos los coeficientes. Sean $F \subset E$ cuerpos y $f(X), 0 \neq d(X) \in F[X]$. Dividimos $f(X) = d(X)q(X) + r(X)$ en $F[X]$ y $f(X) = d(X)q_1(X) + r_1(X)$ en $E[X]$. Entonces la unicidad de la división en $E[X]$ implica que $q_1(X) = q(X) \in F[X]$ y $r_1(X) = r(X) \in F[X]$. En particular $d(X) \mid f(X)$ en $E[X]$ si, y sólo si, $d(X) \mid f(X)$ en $F[X]$.

Corolario 1.7.15 (Teorema del resto)**.** *Sean $f(X) \in R[X]$ y $a \in R$.*

(1) Existe un único $q(X) \in R[X]$ tal que $f(X) = (X - a)q(X) + f(a)$.

(2) $f(a) = 0$ si, y sólo si, $X - a \mid f(X)$ en $R[X]$.

Corolario 1.7.16. *Sean $f(X) \in R[X]$ y $a \in R$ tales que $f(a) = 0$. Entonces, para un $s \leq \deg f$ y $q(X) \in R[X]$ bien definidos, $f(X) = (X - a)^s q(X)$, con $q(a) \neq 0$. Diremos que s es el orden de anulación (o la multiplicidad) de $f(X)$ en a.*

Demostración. Si $f(a) = 0$ entonces $f(X) = (X - a)g(X)$, con $g(X) \in R[X]$ único y de grado $\deg g = (\deg f) - 1$, puesto que el coeficiente principal de $X - a$ es 1. Si $g(a) = 0$ entonces $f(X) = (X - a)^2 h(X)$ con $h(X) \in R[X]$. Así $f(X) = (X - a)^s q(X)$, con $q(X) \in R[X]$ y $q(a) \neq 0$. Supongamos $(X - a)^s q_1(X) = (X - a)^t q_2(X)$, con $q_1(a) \neq 0, q_2(a) \neq 0$. Si $s \geq t$ es $(X - a)^t((X - a)^{s-t} q_1 - q_2) = 0$. Puesto que $(X - a)^t$ no es divisor de cero en $R[X]$, ya que su coeficiente principal es 1, ha de ser $(X - a)^{s-t} q_1 - q_2 = 0$. De aquí $q_2(a) = 0$ si $s > t$. Por tanto $s = t$ y $q_1 = q_2$. □

Proposición 1.7.17. *Sean $f(X) \in R[X]$ y $a \in R$ tales que $f(a) = 0$. El orden de anulación de $f(X)$ en a es ≥ 2 si, y sólo si, $f'(a) = 0$.*

Demostración. Si $f(X) = (X - a)q(X)$, entonces $f'(X) = q(X) + (X - a)q'(X)$. El orden $s \geq 2$ si, y sólo si, $q(a) = 0$, y esto es equivalente a $f'(a) = 0$. □

Proposición 1.7.18. *Sean R un DI, $f(X) \in R[X]$ y $a_1, \ldots, a_r \in R$, distintos dos a dos, tales $f(a_i) = 0$ para cada $i = 1, \ldots, r$ con órdenes de anulación s_i. Entonces $(X - a_1)^{s_1} \cdots (X - a_r)^{s_r} \mid f(X)$ en $R[X]$. En particular, $s_1 + \cdots + s_r \leq n$.*

Demostración. Inducción en r. El caso $r = 1$ es obvio. Sea $r > 1$ y cierto para menos de r raíces distintas. Entonces, $f(X) = (X - a_1)^{s_1} q(X)$ con $q(a_1) \neq 0$. Puesto que R es DI se deduce que $q(a_i) = 0$ para $i = 2, \ldots, r$. Si probamos que el orden de anulación de a_i con $i = 2, \ldots, r$ en $f(X)$ y en $q(X)$ coincide, aplicando la hipótesis de inducción a $q(X)$, es claro que se obtiene el enunciado. Sea $2 \leq i \leq r$ y $(X - a_i)^{s_i} p(X) = f(X), (X - a_i)^t r(X) = q(X)$ con $p(a_i) \neq 0, r(a_i) \neq 0$. Supongamos $s_i < t$, entonces $0 = (X - a_i)^{s_i}((X - a_1)^{s_1}(X - a_i)^{t-s_i} r(X) - p(X))$. Puesto que $R[X]$ es DI; se deduce que $0 = (X - a_1)^{s_1}(X - a_i)^{t-s_i} r(X) - p(X)$. Sustituyendo $X = a_i$ se obtiene $p(a_i) = 0$, contradicción. Supongamos $t < s_i$, entonces $0 = (X - a_i)^t((X - a_i)^{s_i - t} p(X) - (X - a_1)^{s_1} r(X))$. Como antes, obtenemos $r(a_i) = 0$, contradicción. Por tanto, $s_i = t$. □

Ejemplo 1.7.19. En $(\mathbb{Z}/12\mathbb{Z})[X]$, $X^2 - \overline{6}X + \overline{5} = (X - \overline{1})(X - \overline{5}) = (X - \overline{7})(X - \overline{11})$.

Teorema 1.7.20 (Teorema Fundamental del Álgebra)**.** *Sea $p(X) \in \mathbb{C}[X]$ un polinomio de grado positivo con coeficientes complejos. Entonces existe $z \in \mathbb{C}$ tal que $p(z) = 0$.*

Demostración. Ver Teorema 3.9.1. □

Corolario 1.7.21. *Sea $p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdot + a_1 X + a_0 \in \mathbb{C}[X]$, donde $n \geq 1, a_n \neq 0$. Entonces existen $z_1, \ldots, z_n \in \mathbb{C}$ tales que $p(X) = a_n(X - z_1) \cdots (X - z_n)$.*

1.8. Divisibilidad

1.8.1. Definición y propiedades

Definición 1.8.1. Sean R un anillo conmutativo unitario (supondremos R dominio de integridad) y $a, b \in R$ con $b \neq 0$.

(1) Diremos que b divide a a, o que a es múltiplo de b, o que a es divisible por b, si existe $x \in R$ tal que $a = bx$. De forma equivalente, b divide a a si, y sólo si, $a \in bR$ si, y sólo si, $aR \subset bR$. Escribiremos $b \mid a$ (en R).

(2) Un máximo común divisor de $a \neq 0, b \neq 0$ es un elemento $0 \neq d \in R$ tal que

   a) $d \mid a$ y $d \mid b$, y

   b) si $d' \mid a$ y $d' \mid b$ entonces $d' \mid d$.

   En términos de ideales las condiciones anteriores se enuncian

   a) $(a, b)R \subset dR$, y

   b) si $(a, b)R \subset d'R$ entonces $dR \subset d'R$.

   Es decir, d es un máximo común divisor si dR es el menor ideal principal que contiene a $(a, b)R$, suponiendo que tal ideal exista. Denotaremos $d = \text{mcd}(a, b)$.

(3) Un mínimo común múltiplo de $a \neq 0, b \neq 0$ es un elemento $0 \neq m \in R$ tal que

   a) $a \mid m$ y $b \mid m$, y

   b) si $a \mid m'$ y $b \mid m'$ entonces $m \mid m'$.

   En términos de ideales las condiciones anteriores se enuncian

   a) $mR \subset aR \cap bR$, y

   b) si $m'R \subset aR \cap bR$ entonces $m'R \subset mR$.

   La simetría con la definición de máximo común divisor es aparente, puesto que las condiciones:

   a) $mR \subset aR \cap bR$, y

   b) si $m'R \subset aR \cap bR$ entonces $m'R \subset mR$,

   son obviamente equivalentes a la igualdad

   a) $aR \cap bR = mR$.

   Es decir, existe mínimo común múltiplo de $a, b \in R$ si, y sólo si, el ideal $aR \cap bR$ es principal. Denotaremos $m = \text{mcm}(a, b)$.

Observación 1.8.2. Supongamos que R es un DI. Sean $0 \neq x, 0 \neq y \in R$. Entonces $xR = yR$ si, y sólo si, existe una unidad $u \in R$ tal que $y = xu$. En efecto, $xR = yR$ significa $y = xu, x = yv$ para ciertos $u, v \in R$. Así, $y = yvu$. Esto es $y(1-vu) = 0$. De donde $1-vu = 0$ puesto que R es DI y $0 \neq y$.
Por tanto, en un DI, mcd y mcm están bien definidos, salvo producto por unidades.

Observación 1.8.3. Sea R un DI.

(1) Si a es unidad, entonces $\text{mcm}(a, b) = b$ y $\text{mcd}(a, b) = a$.

(2) Si existe $\text{mcm}(a, b) = m$, es decir, si $aR \cap bR = mR$ y $ab = m \cdot d$, entonces $d = \text{mcd}(a, b)$. En efecto, si $m = ar, m = bs$, entonces $b = rd, a = ds$ y, por tanto, $(a, b)R \subset dR$. Por otra parte, si $a = d's, b = d'r$, entonces $d'sr = ar = bs \in ar \cap bR = mR$. Así $d'sr = m\alpha$ y $md = ab = d'sd'r = d'm\alpha$. De aquí $d = \alpha d'$.

(3) Si existe $d = \text{mcd}(a, b)$ y $a = da'$, $b = db'$, entonces $1 = \text{mcd}(a', b')$. En efecto, se trata de ver que si $a'R + b'R \subset tR$ entonces t es unidad. Escribimos $a' = ta''$, $b' = tb''$. Entonces $a = dta''$, $b = dtb''$. Por tanto, $aR + bR \subset dtR$. De aquí, por la definición de máximo común divisor, obtenemos $dR \subset dtR$. Así, $d = dtu$ para cierto $u \in R$. Puesto que R es DI, se deduce $1 = tu$.

(4) Si el ideal $(a, b)R$ es principal $(a, b)R = dR$, entonces $d = \text{mcd}(a, b)$ y, además se tiene una identidad de Bezout $d = au + bv$, para ciertos $u, v \in R$.

(5) Si $d = au + bv$ es una identidad de Bezout entonces $d = a(u + rb') + b(v - ra')$, donde $a = da'$, $b = db'$ y $r \in R$ es un elemento cualquiera, es otra identidad de Bezout. Además, toda identidad de Bezout $d = au_1 + bv_1$ se obtiene de esta forma a partir de $d = au + bv$. En efecto, de $da'(u_1 - u) = db'(v - v_1)$, teniendo en cuenta que $1 = a'u + b'v$, se deduce, primero, $v - v_1 = a'r$ para cierto $r \in R$, y luego, $u_1 - u = b'r$.

(6) Si el ideal $(a, b)R$ es principal, entonces $1 = \text{mcd}(a, b)$ si, y sólo si, existen $u, v \in R$ tales que $1 = au + bv$. Por ejemplo: $29 \cdot (-31) + 75 \cdot (12) = -899 + 900 = 1$.

(7) En $F[X, Y]$, con F cuerpo, el ideal $(X, Y)F[X, Y] \subsetneq F[X, Y]$ y $\text{mcd}(X, Y) = 1$.

(8) En $\mathbb{Z}$, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ es equivalente a $d = \text{mcd}(a, b)$.

(9) En $\mathbb{Z}[\sqrt{-5}]$ los elementos $2(1 + \sqrt{-5})$ y 6 no tienen máximo común divisor. En efecto: $6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$. Por tanto, 2 y $1 + \sqrt{-5}$ son divisores comunes de $2(1 + \sqrt{-5})$ y 6, pero 2 no divide a $1 + \sqrt{-5}$ y $1 + \sqrt{-5}$ no divide a 2.

1.9. Elemento irreducible. Elemento primo

A partir de ahora R denotará un dominio de integridad.

Definición 1.9.1. Sean R un DI y $r, p \in R$ no nulos ni unidades.

(1) Diremos que r es *irreducible* en R si siempre que $r = xy$ con $x, y \in R$ entonces x es unidad o y es unidad en R.

(2) Diremos que p es *primo* si el ideal pR es primo. De forma equivalente, si siempre que $p \mid xy$ con $x, y \in R$ entonces $p \mid x$ ó $p \mid y$.

(3) Diremos que dos elementos $0 \neq x, 0 \neq y \in R$ son *asociados* si existe una unidad $u \in R$ tal que $y = xu$.

(4) Un elemento es irreducible o primo si, y sólo si, cualquiera de sus asociados es irreducible o primo.

Ejemplo 1.9.2. (1) En $\mathbb{Z}$ los conceptos de elemento primo o irreducible coinciden con la clásica noción de número primo. Dos enteros $x, y \in \mathbb{Z}$ son asociados si, y sólo si, $x = \pm y$.

(2) Sea $\mathbb{Z}[\omega]$ un anillo de enteros cuadrático. Si $N(\alpha) = \pm p$, donde p es un entero primo, entonces α es irreducible en $\mathbb{Z}[\omega]$.

En efecto, usando Lema 1.3.3, vemos que α no es unidad. Si $\alpha = \beta\delta$ entonces $N(\alpha) = N(\beta)N(\delta)$. Puesto que $N(\alpha)$ es primo (de hecho irreducible) $N(\beta) = \pm 1$ o $N(\delta) = \pm 1$. Por tanto β es unidad o δ es unidad.

Por ejemplo, $1 + i$ es irreducible en $\mathbb{Z}[i]$, puesto que $N(1 + i) = (1 + i)(1 - i) = 2$.

Proposición 1.9.3. *Sea R un DI. Todo elemento primo en R es irreducible en R.*

Demostración. Sea p un elemento primo. Por definición p no es nulo ni unidad. Escribamos $p = xy$. Entonces $p \mid xy$. Puesto que, por hipótesis, p es primo $p \mid x$ ó $p \mid y$. Si $x = pr$ entonces $p = pry$. Esto es $p(1 - ry) = 0$. Puesto que $0 \neq p$ y R es DI, $1 = ry$. Esto es y es unidad. Por tanto p es irreducible. □

Ejemplos 1.9.4. (1) En $\mathbb{Z}[\sqrt{-5}]$, el elemento 3 es irreducible: no es unidad puesto que su norma no es ± 1 (de hecho $\mathbb{Z}[\sqrt{-5}]^* = \{\pm 1\}$) y, si $3 = \alpha\beta$, es $9 = N(\alpha)N(\beta)$, por tanto $N(\alpha) = 1, 3, 9; N(\beta) = 9, 3, 1$. La igualdad $a^2 + 5b^2 = 3$ no tiene soluciones enteras. Así $N(\alpha) = 1$ o $N(\beta) = 1$. Esto es α es unidad o β es unidad. Sin embargo, 3 no es primo: $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$, pero 3 no divide a $(1 + \sqrt{-5})$ ni a $(1 - \sqrt{-5})$, esto es $3 = (1 \pm \sqrt{-5})(a + b\sqrt{-5})$ no tiene solución con $a, b \in \mathbb{Z}$.

(2) De forma análoga, $2 \in \mathbb{Z}[\sqrt{-3}]$ es irreducible no primo: $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$.

(3) El ideal $I = (3, 2 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$ no es principal. En efecto, supongamos $I = (a + b\sqrt{-5})\mathbb{Z}[\sqrt{-5}]$. Así $3 = \alpha(a + b\sqrt{-5})$ y $2 + \sqrt{-5} = \beta(a + b\sqrt{-5})$ con $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Tomando normas $9 = N(\alpha)(a^2 + 5b^2)$. Así $a^2 + 5b^2 = 1, 3, 9$. Como $a^2 + 5b^2 = 3$ no tiene soluciones enteras, será $a^2 + 5b^2 = 1, 9$. Si $a^2 + 5b^2 = 9$ entonces $3(a - b\sqrt{-5}) = \alpha(a^2 + 5b^2) = 9\alpha$ y, por tanto, $a + b\sqrt{-5} = 3\bar{\alpha}$. Sustituyendo en $2 + \sqrt{-5} = \beta(a + b\sqrt{-5})$, obtenemos $2 + \sqrt{-5} = 3\bar{\alpha}\beta$, igualdad que no es posible, puesto que 3 no divide a 2. Por tanto $a^2 + 5b^2 = 1$. Entonces $\pm 1 = a + b\sqrt{-5} \in I$. Esto es $1 = 3\gamma + (2 + \sqrt{-5})\delta$, para ciertos $\gamma, \delta \in \mathbb{Z}[\sqrt{-5}]$. Esto tampoco es posible, puesto que se tiene entonces $2 - \sqrt{-5} = 3(2 - \sqrt{-5})\gamma + (2 - \sqrt{-5})(2 + \sqrt{-5})\delta = 3\omega$.

(4) Existen DI donde hay elementos que no admiten factorización finita. Sea $R = \mathbb{Q}[X^{\frac{1}{n}}, n \in \mathbb{N}]$ (expresiones polinómicas en $X, X^{\frac{1}{2}}, X^{\frac{1}{3}}, \ldots$), entonces $X = X^{\frac{1}{2}}X^{\frac{1}{2}} = X^{\frac{1}{2}}X^{\frac{1}{4}}X^{\frac{1}{4}} = X^{\frac{1}{2}}X^{\frac{1}{4}}X^{\frac{1}{8}}X^{\frac{1}{8}} = \cdots$, no admite factorización finita en producto de irreducibles.

1.10. Dominios de ideales principales

Definición 1.10.1. Sea R un DI. Diremos que R es un *dominio de ideales principales*, DIP, si todo ideal en R es principal, es decir cada ideal es de la forma xR para cierto $x \in R$.

Ejemplo 1.10.2. La existencia de división en $\mathbb{Z}$ o en el anillo $F[X]$ de polinomios con coeficientes en un cuerpo F, tiene como consecuencia que todo ideal es principal en estos anillos. Sea $I \subset F[X]$ un ideal. Si $I = \{0\}$ entonces $I = 0R$. Supongamos $I \neq 0$. Elegimos $0 \neq d$ con grado mínimo entre los elementos no nulos de I. Es claro que $dR \subset I$. Sea $f \in I$. Dividimos $f = dq + r$ con $r = 0$ o $\deg r < \deg d$. Entonces $r = f - dq \in I$. Por tanto $r = 0$, por la elección de d. Esto es $I \subset dR$. Así $I = dR$ es principal.

Proposición 1.10.3. *Sean R un DIP y $0 \neq a, 0 \neq b \in R$. Si $aR + bR = dR$ y $aR \cap bR = mR$, entonces $d = \text{mcd}(a, b)$ y $m = \text{mcm}(a, b)$.*

Demostración. Se sigue directamente de las definiciones. □

Proposición 1.10.4. *Sea R un DIP. Todo elemento irreducible en R genera un ideal maximal. En particular, todo elemento irreducible es primo y todo ideal primo no nulo es maximal. Recíprocamente, si $0 \neq rR$ es maximal, entonces r es irreducible.*

Demostración. Sea $p \in R$ irreducible. Puesto que, por definición, $0 \neq p$ no es unidad $pR \neq R$. Sea I ideal tal que $pR \subset I$. Por hipótesis, $I = xR$ para cierto $x \in R$. Puesto que $p \in I$, existe $r \in R$ con $p = xr$. Por hipótesis, p es irreducible, en consecuencia, r es unidad o x es unidad. Si r es unidad $I = pR$, si x es unidad $I = R$. Por tanto, pR es maximal.
Si $0 \neq rR$ es maximal, entonces $0 \neq r$ no es unidad y, si $r = xy$, entonces $rR \subset xR$. Si $xR = R$, entonces x es unidad. Si $xR = rR$, entonces y es unidad. Por otra parte, si $P = xR$ es un ideal primo no nulo, entonces x es un elemento primo que, según Proposición 1.9.3 resulta ser irreducible. Por tanto, xR es maximal. □

Damos otra demostración directa de la última afirmación.

Proposición 1.10.5. *Sea R un DIP. Todo ideal primo no nulo es maximal.*

Demostración. Sean $0 \neq P = pR$ un ideal primo, e I un ideal tal que $P \subset I \subset R$. Hay que probar que $I = P$ o $I = R$. Puesto que R es DIP, $I = xR$. Así, podemos escribir $0 \neq p = mx$ para cierto $m \in R$. Entonces $mx \in P$. Por definición de ideal primo deducimos $m \in P$ o $x \in P$. Si $x \in P$, entonces $I = P$. Si $m \in P$, entonces $m = pr$. Así $p = prx$. De aquí $p(1-rx) = 0$. Puesto que R es DI y $p \neq 0$ deducimos $1 - rx = 0$. Esto es $1 = rx \in I$. De aquí $I = R$. □

Ejemplo 1.10.6. Sea $\mathbb{F}_p$ el cuerpo finito de p elementos. Si $p(X) = X^n - a_{n-1}X^{n-1} - \cdots - a_1X - a_0 \in \mathbb{F}_p[X]$ es irreducible, entonces el cociente $\mathbb{F}_p[X]/p(X)\mathbb{F}_p[X]$ es un cuerpo finito con p^n elementos.

Lema 1.10.7. *Sea R un DIP. Si $a_1R \subset a_2R \subset \cdots$ es una cadena de ideales en R, entonces para cierto entero positivo n, $a_jR = a_nR$ para todo $j \geq n$.*

Demostración. El conjunto $I = \cup_{i\geq 1} a_i R$ es un ideal en R. Si $b, c \in I$, entonces $b \in a_i R$ y $c \in a_j R$. Si, por ejemplo, $i \geq j$ entonces $b, c \in a_i R$ y, por tanto, $c - b \in a_i R \subset I$. Por hipótesis $I = rR$, para cierto $r \in R$. Por definición de I, para cierto n, $r \in a_n R$. De aquí $a_j R = a_n R$ para todo $j \geq n$. □

Proposición 1.10.8. *Sea R un DIP. Entonces todo elemento $r \in R$ no nulo ni unidad se escribe como producto de elementos irreducibles en R.*

Demostración. Sea S el conjunto de los elementos no nulos, no unidad de R que no se pueden escribir como producto de un número finito de elementos irreducibles de R. Supongamos que $S \neq \emptyset$ y $a \in S$. Entonces $aR \subset cR$, donde cR es maximal. El elemento c es irreducible, según Proposición 1.10.4, y $c|a$. Por tanto, podemos elegir para cada $a \in S$ un divisor irreducible c_a de a (axioma de elección). Puesto que R es DI, c_a determina unívocamente un elemento no nulo $x_a \in R$ tal que $c_a x_a = a$. Afirmamos que $x_a \in S$. En efecto, si x_a es unidad, entonces $a = c_a x_a$ es irreducible. Por tanto, x_a es no unidad y si $x_a \notin S$, entonces x_a es producto de un número finito de irreducibles y, por tanto, a es producto finito de irreducibles. Esto prueba que $x_a \in S$. Además, afirmamos que $aR \subsetneq x_a R$. En efecto, si $x_a = ay$, entonces $a = x_a c_a = ayc_a$ y $1 = yc_a$, en contra de $c_a R \subsetneq R$. Por tanto, $aR \subsetneq x_a R$. Entonces la función $f : S \to S$ dada por $f(a) = x_a$ está bien definida. Por el teorema de recursión (ver [Hun74, Theorem 6.2, Introduction]) existe una función $\varphi : \mathbb{N} \to S$ tal que $\varphi(0) = a$ y $\varphi(n+1) = f(\varphi(n)) = x_{\varphi(n)}$ para $n \geq 0$. Si denotamos $\varphi(n) = a_n$, tenemos una sucesión de elementos de S: $a, a_1, a_2, \ldots$, tal que

$$a_1 = x_a; a_2 = x_{a_1}; \cdots; a_{n+1} = x_{a_n}; \cdots .$$

En consecuencia, habremos construido una sucesión estrictamente creciente de ideales

$$aR \subsetneq a_1 R \subsetneq a_2 R \subsetneq a_3 R \subsetneq \cdots ,$$

en contradicción con Lema 1.10.7. Esto prueba que $S = \emptyset$. □

1.11. Dominios de factorización única

1.11.1. Definición y propiedades

La factorización de un entero como producto de números primos o de un polinomio como producto de polinomios irreducibles, conduce al concepto de dominio de factorización única, la clase de anillos en los que cada elemento se puede escribir, con unicidad, como producto de elementos irreducibles. Esta factorización proporciona un método para hallar el máximo común divisor de dos elementos cualesquiera del anillo. Hemos visto que en un DIP

(1) todo elemento no nulo ni unidad se escribe como producto de irreducibles y,

(2) el concepto de elemento irreducible equivale al de elemento primo.

Vamos a probar que en un DI cualquiera que verifique la primera condición, la segunda es equivalente a la unicidad de la factorización de cada elemento. Esto definirá la clase de los *dominios de factorización única*, en siglas DFU.

Teorema–Definición 1.11.1. *Sea R un DI. Supongamos que se verifica la condición:*

FU1 *todo elemento no nulo ni unidad $r \in R$ puede ser escrito como producto $r = p_1 \cdots p_n$ de elementos $p_1, \ldots, p_n$ irreducibles en R.*

Entonces son equivalentes las condiciones:

FU2 *la factorización es única, en el sentido siguiente: si $r = q_1 \cdots q_m$ es otra factorización en producto de irreducibles, entonces $m = n$ y, tras una permutación p_i y q_i son asociados para $i = 1, \ldots, n$, y*

FU2' *todo elemento irreducible es primo.*

Si se verifican las condiciones **FU1**, **FU2** *diremos que R es un dominio de factorización única.*

Demostración. **FU2** $\Rightarrow$ **FU2'** Si p es irreducible y $p \mid ab$, entonces $ab = pc$ para cierto $c \in R$. Así, por *FU2*, p es un irreducible de la factorización de a ó b. Sea, e.g., $a = (up)p_2 \cdots p_n$, con u unidad, de donde $p \mid a$.

FU2' $\Rightarrow$ **FU2** Inducción sobre el número de elemento de alguna factorización de cada elemento en producto de irreducibles.

Si r es irreducible, veamos que la factorización $r = r$ es única salvo producto por unidades. En efecto, si $r = p_1 \cdots p_n$, $n \geq 1$, entonces $r = p_1(p_2 \cdots p_n)$, con r irreducible y p_1 no unidad, así $(p_2 \cdots p_n)$ es unidad, i.e., $n = 1$ y r y p_1 son asociados.

Supongamos que $n > 1$ y que todos los elementos que admiten una factorización con menos de n factores se factorizan con unicidad. Sean $r = p_1 \cdots p_n = q_1 \cdots q_m$, dos factorizaciones en producto de irreducibles. Entonces $p_1 \mid q_1 \cdots q_m$. La hipótesis *FU2'* implica que p_1 divide a algún q_i. Reordenando, podemos suponer $p_1 \mid q_1$. Puesto que q_1 es irreducible

y p_1 no unidad, ambos p_1, q_1 son asociados. Podemos, por tanto, cancelar p_1 en la igualdad inicial para obtener $p_2 \cdots p_n = uq_2 \cdots q_m$, con u unidad. Por hipótesis de inducción $n-1 = m-1$ y, tras una permutación, cada par p_i, q_i son asociados para $i = 2, \ldots, n$. □

Ejemplos 1.11.2. (1) Un cuerpo F es, de modo trivial, DFU.

(2) Todo DIP es DFU. Por ejemplo, $\mathbb{Z}$ y el anillo de polinomios $F[X]$ donde F es un cuerpo.

(3) Demostraremos que si R es DFU entonces el anillo de polinomios $R[X]$ es DFU.

(4) Si F es un cuerpo, $F[X, Y]$ es un DFU que no es DIP.

(5) El conjunto $R = \mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\}$ es subanillo de $\mathbb{Z}[i]$. El anillo R es un DI que no es DFU. Los elementos 2 y $2i$ son irreducibles en R y, puesto que $i \notin R$, son no asociados en R. Así, $4 = 2 \cdot 2 = (-2i)(2i)$, son factorizaciones distintas en R. Observemos que $2i$ no es primo en R, puesto que $R/(2i) \simeq \mathbb{Z}/4\mathbb{Z}$.

(6) El anillo $R = \mathbb{Z}[\sqrt{-5}]$ en otro ejemplo de DI que no es DFU. El elemento $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ admite dos factorizaciones distintas. El ideal $(6) = P_2^2 P_3 P_3'$ es producto de cuatro ideales primos, donde $P_2^2 = (2), P_3 P_3' = (3)$ o $P_2 P_3 = (1 + \sqrt{-5}), P_2 P_3' = (1 - \sqrt{-5})$. Aunque los elementos de un anillo de enteros cuadráticos R no necesariamente tienen factorización única, es un teorema que cada ideal en R se puede escribir como producto de ideales primos, de modo único. La factorización única de ideales en producto de ideales primos ocurre, en general, en anillos de enteros de cuerpos de números algebraicos. Este hecho conduce al concepto de dominio de Dedekind. Fue el fallo en tener factorización única en producto en irreducibles para elementos, la situación que condujo a definir la noción de ideal. La unicidad resultante, confiere a los "ideales" un comportamiento ideal, que es la razón de la elección del nombre.

1.11.2. Máximo común divisor y mínimo común múltiplo

Proposición 1.11.3. *Sean R un DFU y $a, b \in R - \{0\}$, no unidades. Escribamos $a = up_1^{r_1} \cdots p_n^{r_n}$, $b = vp_1^{s_1} \cdots p_n^{s_n}$, donde u, v son unidades, p_i irreducibles no asociados dos a dos, $r_i, s_i \geq 0$ enteros tales que $r_i > 0$ o $s_i > 0$ para cada i. Sean $\epsilon_i = \min\{r_i, s_i\}$, $\delta_i = \max\{r_i, s_i\}$. Entonces $d = p_1^{\epsilon_i} \cdots p_n^{\epsilon_n}$ es un* $\mathrm{mcd}(a, b)$ *y $m = p_1^{\delta_1} \cdots p_n^{\delta_n}$ es un* $\mathrm{mcm}(a, b)$*. Además ab y dm son asociados.*

Proposición 1.11.4. *Sean R un DFU y $a, b \in R - \{0\}$ tales que* $\mathrm{mcd}(a, b) = 1$*. Si $a \mid bc$, con $c \in R$, entonces $a \mid c$.*

Demostración. Factorizamos $a = up_1^{r_1} \cdots p_n^{r_n}$, $b = vp_1^{s_1} \cdots p_n^{s_n}, c = wp_1^{t_1} \cdots p_n^{t_n}$, con $r_i \geq 0, s_i \geq 0, t_i \geq 0$. Por la unicidad de la factorización, $a \mid c$ si, y sólo si, $t_i \geq r_i$ para todo i. Por otra parte, $\mathrm{mcd}(a, b) = 1$ si, y sólo si, $r_i s_i = 0$, para cada i. Para cada i tal que $r_i > 0$ (y, por tanto, $s_i = 0$) $p_i^{r_i} \mid bc = vwp_1^{s_1+t_1} \cdots p_n^{s_n+t_n}$. Por tanto $s_i + t_i \geq r_i$. Así, $t_i \geq r_i$. □

La proposición anterior admite una demostración distinta en el caso DIP.

Proposición 1.11.5. *Sea R un DI. Supongamos que $a, b \in R - \{0\}$ son tales que $(a, b)R = R$ (e.g., R es DIP y $\mathrm{mcd}(a, b) = 1$). Si $a \mid bc$, con $c \in R$, entonces $a \mid c$.*

Demostración. Puesto que $(a, b)R = R$, existe una identidad de Bezout $au + bv = 1$. Escribamos $bc = ax$. Entonces $c = cau + cbv = cau + axv = a(cu + xv)$. □

Hemos visto que el anillo de polinomios con coeficientes en un cuerpo es DIP. Esta es la única situación posible.

Proposición 1.11.6. *Sea R un anillo. Si $R[X]$ es DIP entonces R es un cuerpo.*

Demostración. Puesto que, por definición de DIP, $R[X]$ es DI, el subanillo $R \subset R[X]$ es DI. Por otra parte, $R \simeq R[X]/XR[X]$, de forma que $XR[X]$ es ideal primo. Pero todo ideal primo no nulo en un DIP es maximal. Así R es un cuerpo. □

1.12. Dominios euclídeos

1.12.1. Definición y propiedades

Trataremos ahora la clase de anillos que son DIP porque existe una división, similar al caso del anillo de los enteros $\mathbb{Z}$ o el anillo $F[X]$ de polinomios con coeficientes en un cuerpo.

Definición 1.12.1. (1) Una norma (positiva) en un anillo R es una aplicación $N : R - \{0\} \to \mathbb{N} \cup \{0\}$.

(2) Un dominio euclídeo (DE) es un DI R junto con una norma positiva N en R tal que para cada par de elementos $a, 0 \neq b \in R$, se verifica

   a) si $b|a$, entonces $N(b) \leq N(a)$

   b) existen $q, r \in R$ con $a = bq + r$ y la condición $r = 0$ o $N(r) < N(b)$.

Proposición 1.12.2. *Sean R un DE con norma N y $0 \neq a, 0 \neq b \in R$. Si $a|b$ y $N(a) = N(b)$, entonces a, b son asociados.*

Demostración. Dividimos $a = bq + r$ con $N(r) < N(b)$ si $r \neq 0$. Puesto que $b = ac$ para algún $c \in R$. se verifica $r = a - bq = a(1 - cq)$. Así, $a|r$. Si $r \neq 0$, esto implica $N(a) \leq N(r) < N(b)$ contra la hipótesis, Así $r = 0$ y, por tanto, $b|a$. Las condiciones $a|b$ y $b|a$ equivalen a a, b asociados, puesto que R es DI. □

Corolario 1.12.3. *Sean R un DE con norma N y $0 \neq a \in R$. Entonces, a es unidad en R si, y sólo si, $N(a) = N(1)$.*

Demostración. Si a es unidad, entonces $a|1$. Por tanto, $N(a) \leq N(1)$. Como $1|a$, también se tiene $N(1) \leq N(a)$. Recíprocamente, como $1|a$ y $N(1) = N(a)$, por Proposición (1.12.2) 1 y a son asociados. Es decir, a es unidad. □

Proposición 1.12.4. *En un dominio euclídeo R todo ideal es principal, i.e. todo DE es un DIP. Con más precisión, sea $\{0\} \neq I \subset R$ un ideal no nulo. Si $d \in I - \{0\}$ es un elemento con norma mínima entre las normas de los elementos no nulos de I, entonces $I = dR$.*

Demostración. Basta probar que $I \subset dR$. Sea $x \in I$. Dividimos $x = dq + r$. Entonces $r = x - dq \in I$. Por la elección de d con norma mínima ha de ser $r = 0$. Por tanto $x = dq \in dR$. □

Ejemplos 1.12.5. (1) En $\mathbb{Z}$ la división entera con la norma valor absoluto.

(2) En $F[X]$, con F cuerpo, la división de polinomios con la norma dada por el grado.

(3) El anillo $\mathbb{Z}[i]$, de los enteros de Gauss, es un DE con la norma $N(a+bi) = a^2+b^2$. Sean $\alpha = a+bi, 0 \neq \beta = c+di \in \mathbb{Z}[i]$. Consideramos $\delta = \alpha\beta^{-1} = r+si \in \mathbb{Q}[i]$, con $r = \frac{ac+bd}{c^2+d^2}$, $s = \frac{bc-ad}{c^2+d^2} \in \mathbb{Q}$. Sean p, q los enteros más próximos a r, s, de forma que $|r-p| \leq \frac{1}{2}$, $|s-q| \leq \frac{1}{2}$. Sea $\gamma = \alpha - (p+qi)\beta = \delta\beta - (p+qi)\beta = \beta((r-p)+(s-q)i)$. Es $N((r-p)+(s-q)i) = (r-p)^2+(s-q)^2 \leq \frac{1}{4}+\frac{1}{4} = \frac{1}{2}$. Por tanto $N(\gamma) \leq \frac{1}{2}N(\beta)$.

El algoritmo de división es rápido y sencillo. Sin embargo, el cociente no es necesariamente único. Si r (ó s) es la mitad de un entero impar hay dos elecciones posibles para p (ó q).

(4) De forma similar se puede probar que $\mathbb{Z}[\sqrt{-2}], \mathbb{Z}[(1+\sqrt{-3})/2], \mathbb{Z}[(1+\sqrt{-7})/2], \mathbb{Z}[(1+\sqrt{-11})/2]$ son DE respecto de su norma. Si embargo, $\mathbb{Z}[\sqrt{-5}]$ no es DE puesto que el ideal $(3, 2+\sqrt{-5})\mathbb{Z}[\sqrt{-5}]$ no es principal. Probaremos más adelante que $\mathbb{Z}[(1+\sqrt{-19})/2]$ es un DIP que no DE respecto de ninguna norma.

1.12.2. Algoritmo de Euclides

Proposición 1.12.6 (Algoritmo de Euclides)**.** *Sean R un DE y $a, b \in R - \{0\}$. La cadena de divisiones $a = q_0b + r_0, b = q_1r_0 + r_1, r_0 = q_2r_1 + r_2, \ldots, r_{i-2} = q_ir_{i-1} + r_i, \ldots, r_{n-2} = q_nr_{n-1} + r_n, r_{n-1} = q_{n+1}r_n$, con restos no nulos y $N(b) > N(r_0) > N(r_1) > N(r_2) > \cdots > N(r_{n-1}) > N(r_n)$ alcanza un resto nulo $r_{n+1} = 0$. Se verifica la igualdad de ideales $(a,b)R = (b,r_0)R = (r_0,r_1)R = (r_1,r_2)R = \cdots = (r_{i-1},r_i)R = \cdots = (r_{n-1},r_n)R = r_nR$. En consecuencia el último resto no nulo r_n es un máximo común divisor $r_n = \mathrm{mcd}(a,b)$.*

Demostración. La igualdad $r_i = r_{i-2} - q_ir_{i-1}$ implica $(r_{i-2}, r_{i-1})R = (r_{i-1}, r_i)R$. □

Observación 1.12.7. El algoritmo proporciona una identidad de Bezout. Veamos un ejemplo, hasta la tercera división.

$$
\begin{aligned}
&r_0 = a - q_0b,\ r_1 = b - q_1r_0,\ r_2 = r_0 - q_2r_1,\ r_3 = r_1 - q_3r_2.\\
&r_1 = b - q_1(a - q_0b) = a(-q_1) + b(1 + q_0q_1),\\
&r_2 = a - q_0b - (a(-q_1) + b(1 + q_0q_1))q_2 = a(1 + q_1q_2) + b(-q_0 - q_2 - q_0q_1q_2),\\
&r_3 = a(-q_1) + b(1 + q_0q_1) - a(1 + q_1q_2)q_3 - b(-q_0 - q_2 - q_0q_1q_2)q_3 =\\
&\quad = a(-q_1 - q_3 - q_1q_2q_3) + b(1 + q_0q_1 + q_0q_3 + q_2q_3 + q_0q_1q_2q_3).
\end{aligned}
$$

Ejemplo 1.12.8. El máximo común divisor de $a = 2210, b = 1131$ es 13.

$$
\begin{aligned}
a = q_0b + r_0,&\ \ 2210 = 1 \cdot 1131 + 1079,\\
b = q_1r_0 + r_1,&\ \ 1131 = 1 \cdot 1079 + 52,\\
r_0 = q_2r_1 + r_2,&\ \ 1079 = 20 \cdot 52 + 39,\\
r_1 = q_3r_2 + r_3,&\ \ 52 = 1 \cdot 39 + 13,\\
r_2 = q_4r_3,&\ \ 39 = 3 \cdot 13.
\end{aligned}
$$

$$13 = 2210(-22) + 1131(43).$$

El algoritmo de Euclides en $\mathbb{Z}$ es extremadamente rápido. Es un teorema que el número de etapas requeridas para determinar el máximo común divisor de un par de números es, a lo más, cinco veces el número de dígitos del menor de los números. Para obtener una apreciación de la rapidez implicada aquí, observemos que en el ejemplo anterior deberíamos haber esperado $5 \cdot 4 = 20$ divisiones. Si hubiéramos comenzado con números del orden de 10^{100} (números grandes para la física estándar) habríamos esperado 500 divisiones.

1.12.3. Ecuaciones diofánticas lineales

Consideramos la ecuación $aX + bY = c$ con $0 \neq a, 0 \neq b, c \in \mathbb{Z}$. La ecuación tiene solución si, y sólo si, $c \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, donde $d = \text{mcd}(a, b)$. Por tanto, la ecuación tiene solución si, y sólo si, $d = \text{mcd}(a, b) | c$. En este caso, a partir de una identidad de Bezout $d = au + bv$ y $c = dq$ obtenemos una solución particular de la ecuación $x_0 = uq, y_0 = vq$, puesto que $c = dq = a(uq) + b(vq)$. La ecuación homogénea $aX + bY = 0$ es equivalente a $a'X + b'Y = 0$, donde $a = da', b = db'$. Puesto que $\text{mcd}(a', b') = 1$, la solución general de $a'X + b'Y = 0$ es $X = b't, Y = -a't, t \in \mathbb{Z}$. Por tanto, la solución general de la ecuación diofantica $aX + bY = c$ es $X = uq + b't, Y = vq - a't, t \in \mathbb{Z}$.

1.12.4. Un DIP que no es DE

Definición 1.12.9. Una norma de Dedekind–Hasse en un dominio de integridad R es una norma positiva tal que para todo $a, b \in R$, con $b \neq 0$, o $a \in bR$ o existe un elemento no nulo en $(a, b)R$ de norma $< N(b)$ (i.e., o bien $b \mid a$ o existen $s, t \in R$ con $0 \neq as - bt$ y $N(as - bt) < N(b)$).

Observación 1.12.10. Sea R un DE con norma N. Entonces (R, N) satisface la definición anterior con $s = 1$. De forma que la existencia de una norma de Dedekind–Hasse es un debilitamiento de la condición euclídea.

Proposición 1.12.11. *Sea R un DI. Entonces R es DIP si, y sólo si, R tiene una norma de Dedekind–Hasse.*

Demostración. Supongamos que N una norma de Dedekind–Hasse en R. Sean $I \subset R$ un ideal no nulo y $0 \neq b \in I$ con norma mínima entre los elementos no nulos de I. Sea $a \in I$, puesto que $(a, b)R \subset I$ la condición D–H y la minimalidad de b implican que $a \in bR$.
Recíprocamente, supongamos que R es un DIP. Definimos $N(u) = 1$ si $u \in R$ es unidad y $N(a) = 2^n$ si $a = p_1 \cdots p_n$ es producto de n irreducibles. Es claro que $N(ab) = N(a)N(b)$ y $N(a) > 0$ si $a \in R - \{0\}$. Sea $b \in R - \{0\}$. Entonces $(a, b)R = rR$ para cierto $r \in R$. Si $a \notin bR$ entonces $r \notin R$. Como $b = rx$, para cierto $x \in R$, se deduce que x no es unidad. Por tanto $N(b) = N(r)N(x) > N(r)$. Esto es $(a, b)R$ contiene un elemento no nulo r de norma $< N(b)$. □

Ejemplo 1.12.12. El anillo de enteros cuadráticos $R = \mathbb{Z}[(1+\sqrt{-19})/2]$ es un DIP que no es DE.
Para probar que R es DIP, comprobamos que la norma $N(a+b\frac{1+\sqrt{-19}}{2}) = a^2+ab+5b^2$ es D–H. En efecto, sean $\alpha, \beta \in R$, con $0 \neq \beta$, y $\frac{\alpha}{\beta} \notin R$. Buscamos $s, t \in R$ con $N(\alpha s - \beta t) < N(\beta)$ o, de forma equivalente,

$$N(s\frac{\alpha}{\beta} - t) < 1. \tag{1.12.12.1}$$

Escribimos $\frac{\alpha}{\beta} = \frac{a+b\sqrt{-19}}{c} \in \mathbb{Q}[\sqrt{-19}]$, con $a, b, c \in \mathbb{Z}$ enteros que no tienen divisor común y $c > 1$ (puesto que $\frac{\alpha}{\beta} \notin R$). Como a, b, c no tienen factores comunes, se puede escribir $ax + by + cz = 1$ para ciertos $x, y, z \in \mathbb{Z}$. Escribimos $ay - 19bx = cq + r$, con resto tal que $|r| \leq \frac{c}{2}$ (r puede ser negativo) y sean $s = y + x\sqrt{-19}$, $t = q - z\sqrt{-19}$. Entonces un pequeño cálculo muestra que

$$N(s\frac{\alpha}{\beta} - t) = \frac{(ay - 19bx - cq)^2 + 19(ax + by + cz)^2}{c^2} = \frac{r^2+19}{c^2} \leq \frac{1}{4} + \frac{19}{c^2},$$

y, por tanto, (1.12.12.1) se verifica para estos s, t supuesto que $c \geq 5$ (observemos que $r^2 + 19 \leq 23$ cuando $c = 5$).
Supongamos que $c = 2$. Entonces uno de los a, b es par y el otro impar (en otro caso $\frac{\alpha}{\beta} = \frac{a+b\sqrt{-19}}{2} = (\frac{a}{2} - \frac{b}{2}) + b(\frac{1+\sqrt{-19}}{2}) \in R$) y entonces un cálculo muestra que $s = 1$ y $t = \frac{(a-1)+b\sqrt{-19}}{2}$ son elementos que verifican (1.12.12.1).
Supongamos que $c = 3$. El entero $a^2 + 19b^2$ no es divisible por 3 (módulo 3 es $a^2 + b^2$ que es 0 módulo 3 si, y sólo si, a y b son 0 módulo 3; pero entonces a, b, c tienen un factor común). Escribimos $a^2 + 19b^2 = 3q + r$ con $r = 1$ ó 2. Entonces, de nuevo un cálculo rápido muestra que $s = a - b\sqrt{-19}$, $t = q$ son elementos de R que verifican (1.12.12.1).
Supongamos, finalmente, que $c = 4$, por tanto a, b no son ambos pares. Si uno de los a, b es par y el otro impar, entonces $a^2 + 19b^2$ es impar, por tanto podemos escribir $a^2 + 19b^2 = 4q + r$ para ciertos $q, r \in \mathbb{Z}$ y $0 < r < 4$. Entonces $s = a - b\sqrt{-19}$ y $t = q$ verifican (1.12.12.1). Si a, b son ambos impares, entonces $a^2 + 19b^2 \equiv 1 + 3 \pmod 8$, por tanto podemos escribir $a^2 + 19b^2 = 8q + 4$ para cierto $q \in \mathbb{Z}$. Entonces $s = \frac{a-b\sqrt{-19}}{2}$ y $t = q$ son elementos de R que satisfacen (1.12.12.1).

Probaremos ahora que $R = \mathbb{Z}[(1+\sqrt{-19})/2]$ no es DE. Para ello usaremos un criterio que, en ocasiones, permite mostrar que un DI no es DE.
Sea R un DI. Un elemento no nulo ni unidad $u \in R$ se dice "divisor lateral universal"si para cada $x \in R$ existe $z \in R$, nulo o unidad, tal que u divide a $x - z$ en R, i.e., existe un tipo de algoritmo de división para u: cada $x \in R$ se puede escribir $x = uq + z$ con $z \in R$ cero o unidad.
La existencia de divisores laterales universales es una condición más débil que DE.

Proposición 1.12.13. *Sea R un DI que no es un cuerpo. Si R es DE entonces existen divisores laterales universales en R.*

Demostración. Sean N una norma que hace de R un DE y $u \in R$ no nulo ni unidad con norma mínima entre los elementos no nulos ni unidad. Para cada $x \in R$ escribimos $x = uq+r$ con $r = 0$ o $N(r) < N(u)$. La minimalidad de u implica que r es cero o unidad. □

Podemos ahora probar que $R = \mathbb{Z}[(1 + \sqrt{-19})/2]$ no es DE (respecto de ninguna norma). Es inmediato comprobar que ± 1 son las unidades de R. Supongamos que $u \in R$ es divisor lateral universal. Sea $N(a + b(1 + \sqrt{-19}))/2 = a^2 + ab + 5b^2$ la norma del anillo cuadrático. Si $a, b \in \mathbb{Z}$ y $b \neq 0$, entonces $a^2+ab+5b^2 = (a+b/2)^2+19/(4b^2) \geq 5$ y, por tanto, los menores valores no nulos de N en R son 1 (para ± 1) y 4 (para ± 2). Tomando $x = 2$ en la definición de divisor lateral universal, se deduce que u debe dividir a alguno de los elementos $2 - 0$ ó 2 ± 1 en R, i.e., u es una no unidad divisor de 2 ó 3. Si $2 = \alpha\beta$ entonces $4 = N(\alpha)N(\beta)$, de donde se deduce que alguno de los α, β tiene norma 1, i.e., es igual a ± 1. Por tanto, los únicos divisores de 2 en R son $\pm 1, \pm 2$. De forma similar los únicos divisores de 3 en R son $\pm 1, \pm 3$. Así los únicos posibles valores para u son ± 2 o ± 3. Tomando $x = (1 + \sqrt{-19})/2$, es sencillo comprobar que ninguno de los elementos $x, x \pm 1$ son divisibles por $\pm 2, \pm 3$ en R. Así ninguno de estos es un divisor lateral universal.

1.12.5. Factorización en el anillo de enteros de Gauss

El objetivo de esta sección es obtener los elementos irreducibles del anillo $\mathbb{Z}[i]$ y aplicar esta información para demostrar un teorema de Fermat, en teoría elemental de números, que caracteriza aquellos primos que son suma de dos cuadrados.

Recordemos que si R es un anillo cuadrático de enteros y N es la norma asociada, un elemento $\alpha \in R$ es unidad si, y sólo si, $N(\alpha) = \pm 1$ y si $N(\alpha) = \pm p$, donde p es primo en $\mathbb{Z}$, entonces α es irreducible en R.

1.12.14. Sea $0 \neq \pi \in R$ un elemento primo. El ideal $\pi R \cap \mathbb{Z}$ es, por tanto, un ideal primo. Puesto que $0 \neq N(\pi) = \pi\overline{\pi} \in \pi R \cap \mathbb{Z}$, es $0 \neq \pi R \cap \mathbb{Z} = p\mathbb{Z}$ para cierto primo $p \in \mathbb{Z}$. Así, $\pi \mid p$ en R y, en consecuencia, los elementos primos de R pueden ser hallados determinando cómo los primos de $\mathbb{Z}$ factorizan en el anillo más grande R.

Supongamos que $p = \pi\pi'$ en R, con p un primo en $\mathbb{Z}$. Entonces, $p^2 = N(p) = N(\pi)N(\pi')$. Así, puesto que π no es unidad, hay sólo dos opciones: bien $N(\pi) = \pm p^2$ o bien $N(\pi) = \pm p$. En el caso $N(\pi) = \pm p^2$, es $N(\pi') = \pm 1$. Por tanto, π' es unidad y $p = \pi$, salvo unidades, es irreducible en R. En el caso $N(\pi) = \pm p$, es $N(\pi') = \pm p$. Así, también π' es irreducible y $p = \pi\pi'$ es el producto de dos irreducibles en R.

1.12.15. Consideremos ahora el caso especial $D = -1$, de los enteros de Gauss $R = \mathbb{Z}[i]$.

El anillo $R = \mathbb{Z}[i]$ es un DE con norma $N(a+bi) = a^2+b^2$, cuyas unidades son $R^* = \{\pm 1, \pm i\}$. Aplicando el argumento anterior obtenemos:

(*) Un primo p factoriza en $\mathbb{Z}[i]$ en producto de, exactamente, dos irreducibles si, y sólo si, $p = a^2 + b^2$ es la suma de dos cuadrados en $\mathbb{Z}$.

En otro caso, p permanece irreducible en $\mathbb{Z}[i]$.

(**) Si $p = a^2 + b^2 = (a+bi)(a-bi)$, entonces los irreducibles en cuyo producto p factoriza en $\mathbb{Z}[i]$ son $a \pm bi$.

En el caso $2 = 1^2 + 1^2 = (1+i)(1-i) = -i(1+i)^2$, los irreducibles $1 \pm i$ son asociados. Este es el único caso en el que los irreducibles $a \pm bi$ son asociados.
Puesto que $a^2 \equiv 0, 1 \pmod 4$, un primo impar p de la forma $a^2 + b^2$ será $p \equiv 1 \pmod 4$. Por tanto si $p \equiv 3 \pmod 4$, entonces p no es la suma de dos cuadrados y, en consecuencia, p permanece irreducible en $\mathbb{Z}[i]$.

1.12.16. Supongamos que $p \equiv 1 \pmod 4$. vamos a demostrar que p no es irreducible en $\mathbb{Z}[i]$. Esto demostrará que es $p = (a+bi)(a-bi)$, producto de dos irreducibles en $\mathbb{Z}[i]$ y, por tanto, $p = a^2 + b^2$ es suma de dos cuadrados en $\mathbb{Z}$.

Lema 1.12.17. *El primo $p \in \mathbb{Z}$ divide a un entero de la forma $n^2 + 1$ si, y sólo si, p es 2 o es un primo impar $p \equiv 1 \pmod 4$.*

Demostración. Para $p = 2$ el enunciado es trivial. Sea p un primo impar. La condición $p \mid n^2 + 1$ equivale a $\overline{n}^2 = -\overline{1}$ en $\mathbb{Z}/p\mathbb{Z}$. Esta última identidad equivale a que $\overline{n}$ sea un elemento de orden 4 en el grupo $(\mathbb{Z}/p\mathbb{Z})^*$. Esto es, $p \equiv 1 \pmod 4$, para algún $n \in \mathbb{Z}$, si, y sólo si, el grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^*$ contiene un elemento de orden 4. Esto implica que 4 divide a $p-1$. Recíprocamente, si $p \equiv 1 \pmod 4$, vamos a demostrar que $(\mathbb{Z}/p\mathbb{Z})^*$ contiene un elemento de orden 4. Este hecho se obtiene, de forma sencilla, a partir de que $(\mathbb{Z}/p\mathbb{Z})^*$ es un grupo cíclico de orden $p-1$. Si embargo, vamos a utilizar un argumento diferente. El elemento $-\overline{1} \in (\mathbb{Z}/p\mathbb{Z})^*$ tiene orden 2. Es el único elemento de orden 2, puesto que la ecuación $x^2 - 1 = 0$ tiene por solución ± 1 en el cuerpo $\mathbb{Z}/p\mathbb{Z}$.
La preimagen $H \subset (\mathbb{Z}/p\mathbb{Z})^*$ de un subgrupo de orden 2 del cociente de $(\mathbb{Z}/p\mathbb{Z})^*$ por $\{\pm 1\}$ tiene orden 4 (aquí $p \equiv 1 \pmod 4$ implica la existencia de tal subgrupo de orden 2). Puesto que $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ tiene 3 elemento de orden 2, mientras que $(\mathbb{Z}/p\mathbb{Z})^*$ y, por tanto, también H tienen un único subgrupo de orden 2, debe H ser el grupo cíclico de orden 4. □

1.12.18. Según el lema anterior, si $p \equiv 1 \pmod 4$, entonces $p \mid n^2 + 1 = (n+i)(n-i)$ en $\mathbb{Z}[i]$, para algún $n \in \mathbb{Z}$. Si p fuera irreducible en $\mathbb{Z}[i]$, dividiría a $n+i$ o su conjugado $n-i$ en $\mathbb{Z}[i]$. En esta situación, puesto que p es un número real, p ha de dividir a ambos y, en consecuencia, dividir a su diferencia $2i$. Como éste, claramente, no es el caso, hemos probado el:

Teorema 1.12.19 (Teorema de Fermat de las sumas de cuadrados)**.**

(1) El primo p es la suma de dos cuadrados de números enteros, $p = a^2 + b^2$ si, y sólo si, $p = 2$ o $p \equiv 1 \pmod 4$.

Excepto por intercambiar a, b o cambiar el signo de a, b, la representación de p como suma de cuadrados es única.

(2) Los elementos irreducibles en $\mathbb{Z}[i]$ son los siguientes:

a) $1 + i$ *(que tiene norma* 2*).*

b) *Los primos* $p \in \mathbb{Z}$ *con* $p \equiv 3 \pmod 4$ *(estos tienen norma* p^2*), y*

c) $a \pm bi$*, los factores irreducibles no asociados de* $p = a^2 + b^2 = (a + bi)(a - bi)$ *para los primos impares* $p \in \mathbb{Z}$ *con* $p \equiv 1 \pmod 4$ *(estos irreducibles tienen norma* p*).*

1.12.20. Más general, la cuestión de si ele entero $n \in \mathbb{Z}$ se puede escribir como suma de cuadrados de enteros $n^2 = A^2 + B^2$ es equivalente a la cuestión de si n es la norma de un elemento $A + Bi \in \mathbb{Z}[i]$.
Escribimos $A + Bi = \pi_1\pi_2 \cdots \pi_k$, como producto de irreducibles en $\mathbb{Z}[i]$. Se deduce del teorema anterior que n es suma de cuadrados si, y sólo si, los factores primos de n que sean congruentes con 3 módulo 4, aparecen con exponente par en la factorización de n en $\mathbb{Z}$. Además, si esta condición se satisface para n, entonces la unicidad de la factorización de $A + Bi$ en $\mathbb{Z}[i]$ prueba que ele número de representaciones de n como suma de cuadrados es $4(a_1+1)\cdots(a_r+1)$, donde si $p_1, \ldots, p_r$ son los primos $\equiv 1 \pmod 4$ que dividen al número n, entonces los a_i son los exponentes de $p_1, \ldots, p_r$ en la factorización de n.

Ejemplo 1.12.21.

$$493 = 17 \cdot 29; \quad 17 \equiv 1 (\mathrm{mod}\, 4); \quad 29 \equiv 1 (\mathrm{mod}\, 4).$$

$$17 = (4 + i)(4 - i); \quad 29 = (5 + 2i)(5 - 2i).$$

$$A + Bi = (4 \pm i)(5 \pm 2i) = \begin{cases} 18 + 13i \\ 22 - 3i \\ 22 + 3i \\ 18 - 13i. \end{cases}$$

Producto por -1 cambia el signo. Producto por i intercambia A, B y cambia el signo. Entonces las expresiones de 493 como suma de cuadrados son:

$$\begin{aligned} 493 &= (\pm 18)^2 + (\pm 13)^2 = (\pm 13)^2 + (\pm 18)^2 \\ &= (\pm 22)^2 + (\pm 3)^2 = (\pm 3)^2 + (\pm 22)^2. \end{aligned}$$

1.13. Factorialidad de los anillos de polinomios

Sean R un anillo conmutativo con unidad y $R[X]$ el anillo de polinomios con coeficientes en R. La pregunta que tratamos de responder es: ¿En qué condiciones es $R[X]$ DFU? Ya sabemos que $R[X]$ es DI si, y sólo si, R es DI. Supongamos, por tanto, que R es DI. Entonces, si F es su cuerpo de fracciones, $R[X]$ es subanillo en el dominio euclídeo $F[X]$. Podemos referir los cálculos en $R[X]$ a cálculos en $F[X]$ con el coste de permitir coeficientes fraccionarios. Esto hace aparecer la cuestión de cómo la factorización en $F[X]$ se puede usar para obtener una factorización en $R[X]$. Si $R[X]$ es DFU, los polinomios constantes factorizan de modo único en producto de polinomios, que han de ser de grado cero, esto es, R ha de ser DFU. Recíprocamente, el método que usaremos para probar que $R[X]$ es DFU si R es DFU, consiste en primero factorizar, de modo único, en $F[X]$ y luego eliminar denominadores para obtener una factorización en $R[X]$. El resultado fundamental que nos permitirá levantar la factorización en $F[X]$ a una factorización en $R[X]$ es el llamado Lema de Gauss.

1.13.1. A partir de ahora, R designa un DFU y F su cuerpo de fracciones.

Definición 1.13.2 (Contenido de un polinomio)**.**

(1) El contenido de un polinomio $0 \neq f(X) = a_0 + \cdots + a_n X^n \in R[X]$, con $n \geq 0$ y $a_n \neq 0$, es el máximo común divisor de sus coeficientes: $c(f) = \operatorname{mcd}(a_0, \ldots, a_n)$. Observemos que el contenido está definido salvo producto por unidades de R.

(2) Diremos que $0 \neq f(X) \in R[X]$ es primitivo si $c(f) = 1$. Todo $0 \neq f(X) \in R[X]$ se escribe como $f(X) = cf_1(X)$, donde $c = c(f) \in R$ y $f_1(X) \in R[X]$ es primitivo.

(3) Sea $0 \neq f(X) = \frac{a_0}{b_0} + \cdots + \frac{a_n}{b_n} X^n \in F[X]$, con $n \geq 0, a_i \in R, 0 \neq b_i \in R$ y $a_n \neq 0$. Sea $b = b_0 \cdots b_n$, de forma que $b \cdot f(X) \in R[X]$. Escribimos $b \cdot f(X) = c \cdot f_1(X)$, donde $c = c(bf(X))$ y $f_1(X) \in R[X]$ es primitivo. Entonces el contenido $c(f(X)) = \frac{c}{b}$ y $f(X) = \frac{c}{b} f_1(X)$.

Si $cf_1(X) = c'g_1(X)$, con $c, c' \in F$ y $f_1, g_1 \in R[X]$ primitivos. Ponemos $c/c' = r/s$, con $r, s \in R - \{0\}$ tales que $\operatorname{mcd}(r, s) = 1$. Entonces $sg_1(X) = rf_1(X)$ en $R[X]$. Así s divide a cada coeficiente de $f_1(X)$, que es primitivo; por tanto s es unidad en R. De forma similar r es unidad. En consecuencia, el contenido $c(f(X))$ para $f(X) \in F[X]$ está bien definido y es coherente con la definición para $f(X) \in R[X]$.

(4) Un ejemplo en $\mathbb{Q}[X]$.

$$\begin{aligned} f(X) &= 7 + \frac{28}{3}X + 42X^2 - \frac{14}{15}X^3 \\ &= \frac{1}{15}(15 \cdot 7 + 20 \cdot 7X + 90 \cdot 7X^2 - 2 \cdot 7X^3) \\ &= \frac{7}{15}(15 + 20X + 90X^2 - 2X^3). \end{aligned}$$

Esto es $c(f) = \pm\frac{7}{15}$ y $f_1(X) = 15 + 20X + 90X^2 - 2X^3$ es primitivo.

(5) Sea $d \in F - \{0\}$. Entonces $c(d \cdot f(X)) = d \cdot c(f(X))$.

(6) Sea $f(X) \in F[X] - \{0\}$. Entonces $c(f) = 1$ si, y sólo si, $f \in R[X]$ y f es primitivo.

(7) Definimos como 0 el contenido del polinomio nulo.

1.13.1. Lema de Gauss

Teorema 1.13.3 (Lema de Gauss)**.** *Sean R un DFU y F su cuerpo de fracciones. Sean $f(X), g(X) \in F[X]$. Entonces $c(fg) = c(f) \cdot c(g)$, salvo producto por unidades de R.*

Demostración. Podemos suponer $f, g \in F[X] - \{0\}$. Sean $c = c(f), d = c(g)$ y $f = c \cdot f_1$, $g = d \cdot g_1$, con $f_1, g_1 \in R[X]$ primitivos. Entonces $fg = cd \cdot f_1 g_1$ y $c(fg) = cd \cdot c(f_1 g_1)$. Por tanto, basta probar que si $f, g \in R[X]$ son primitivos, entonces fg es primitivo (Lema de Gauss). En efecto, escribamos $f(X) = a_n X^n + \cdots + a_0$, $g(X) = b_m X^m + \cdots + b_0$, con $a_i, b_j \in R, a_n \neq 0, b_m \neq 0$ y $\mathrm{mcd}(a_i) = 1$, $\mathrm{mcd}(b_j) = 1$.
Sea $p \in R$ un elemento primo, hemos de probar que p no divide a algún coeficiente de fg.

$$f(X)g(X) = a_n b_m X^{m+n} + \cdots + (\sum_{i+j=k} a_i b_j) X^k + \cdots + a_0 b_0.$$

Sea $0 \leq r \leq n$ el primero tal que $0 \neq a_r$ y $p \nmid a_r$, i.e., $p \mid a_0, \ldots, p \mid a_{r-1}$, $p \nmid a_r \neq 0$. Sea $0 \leq s \leq m$ el primero tal que $0 \neq b_s$ y $p \nmid b_s$.
El coeficiente de X^{r+s} en fg es

$$\begin{aligned} c_{r+s} = a_r b_s &+ a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \cdots + a_{r+s} b_0 \\ &+ a_{r-1} b_{s+1} + a_{r-2} b_{s+2} + \cdots + a_0 b_{r+s}, \end{aligned}$$

donde $p \nmid a_r b_s$ y p si divide a cada uno de los restantes sumandos, i.e., $p \mid c_{r+s} - a_r b_s$. Por tanto, $p \nmid c_{r+s}$. □

Damos una prueba diferente del Lema de Gauss.

Teorema 1.13.4. *Sean R un DFU y $f(X), g(X) \in R[X]$ primitivos. Entonces $f(X)g(X)$ es primitivo.*

Demostración. en $R[X]$ Sea $p \in R$ primo. Hemos de probar que p no divide a algún coeficiente de fg. Esto equivale a decir que $\overline{fg} \in (R/pR)[X]$ es no nulo. Esto es inmediato, puesto que ser primitivos implica $0 \neq \overline{f}, 0 \neq \overline{g}$ y $(R/pR)[X]$ es un DI. □

Corolario 1.13.5. *Sea $f(X) \in R[X]$, con grado ≥ 1, que factoriza $f(X) = g(X)h(X)$, con $g(X), h(X) \in F[X]$, ambos g, h de grado ≥ 1. Sean $g = c \cdot g_1$, $h = d \cdot h_1$, con $g_1, h_1 \in R[X]$ primitivos. Entonces $f = cd \cdot g_1 h_1$, con $cd \in R$ y $g_1 h_1$ primitivo. En particular $f(X) = (cdg_1(X))(h_1(X))$ factoriza en $R[X]$.*

Demostración. Lo único que hay que probar es $cd \in R$. En efecto, de $f = cd \cdot g_1 h_1$ se obtiene $c(f) = cd \cdot c(g_1 h_1) = cd$ puesto que $g_1 h_1$ es primitivo. □

Corolario 1.13.6. *Sea $f(X) \in R[X]$, con grado ≥ 1 y mónico, i.e., $f(X) = X^n + \cdots$, que factoriza como producto de dos polinomios, ambos de grado ≥ 1, en $F[X]$. Entonces $f(X)$ factoriza como producto de dos polinomios mónicos, ambos de grado ≥ 1, en $R[X]$.*

Demostración. Por Corolario 1.13.5, $f(X) = X^n + \cdots = (a_r X^r + a_{r-1} X^{r-1} + \cdots + a_0)(b_s X^s + b_{s-1} X^{s-1} + \cdots + b_0)$, con $r, s \geq 1$ en $R[X]$. Entonces $a_r b_s = 1$. Por tanto $f(X) = (X^r + b_s a_{r-1} X^{r-1} + \cdots + b_s a_0)(X^s + a_r b_{s-1} X^{s-1} + \cdots + a_r b_0)$. □

Corolario 1.13.7. *Sea $f(X) \in R[X]$, con grado ≥ 1. Entonces $f(X)$ es irreducible en $R[X]$ si, y sólo si, es primitivo e irreducible en $F[X]$.*

Demostración. Escribimos $f = c \cdot f_1$, con $c \in R$ y f_1 primitivo. Si $f(X)$ es irreducible en $R[X]$, entonces c ha de ser unidad. Esto es $c(f) = 1$. Además f es irreducible en $F[X]$. En caso contrario, por Corolario 1.13.5, una factorización en $F[X]$ puede ser levantada a $R[X]$. Recíprocamente, si f es primitivo y factoriza en $R[X]$, los factores han de tener ambos grado ≥ 1. Esto es una factorización en $F[X]$. □

Observación 1.13.8. Un elemento $0 \neq c \in R$ es irreducible en $R[X]$ si, y sólo si, c es irreducible en R. Basta observar que, puesto que R es DI, si $c = fg$, con $f, g \in R[X]$, entonces $\deg f = \deg g = 0$, i.e., $f, g \in R$.

Ejemplo 1.13.9. El polinomio $f(X) = 2X^3 - 4X^2 + 2X + 2 = 2(X^3 - 2X^2 + X + 1) \in \mathbb{Z}[X]$, es irreducible en $\mathbb{Q}[X]$, puesto que es de grado 3 y no tiene raíces en $\mathbb{Q}$; pero es reducible en $\mathbb{Z}[X]$, puesto que su contenido es 2.

Observación 1.13.10. Recordemos que R DI implica $R[X]$ DI. (Ver ejercicio 1.7.(8)).

Observación 1.13.11. Si $R[X]$ es DFU, entonces R es DFU. En efecto, R es DI, puesto que R es subanillo de $R[X]$ y, la factorización en $R[X]$ de cada elemento $c \in R$, es, de hecho, una factorización en R por la aditividad del grado en un producto de polinomios.

Teorema 1.13.12. *Sea R un DFU. Entonces el anillo de polinomios $R[X]$ es DFU. Las unidades de $R[X]$ son las unidades de R. Los elementos irreducibles de $R[X]$ son los irreducibles de R y los polinomios de grado ≥ 1 que son primitivos e irreducibles en $F[X]$.*

Demostración. Sea $0 \neq f(X) \in R[X]$ de grado ≥ 1. Por la factorización en $F[X]$ y el Corolario 1.13.5, podemos escribir $f(X) = c \cdot p_1(X) \cdots p_r(X)$, donde $c = c(f)$ y $p_i \in R[X]$, de grado ≥ 1, son primitivos e irreducibles en $F[X]$. Por tanto, los p_i son irreducibles en $R[X]$ y factorizando $c = n_1 \cdots n_t$ como producto de irreducibles en R obtenemos una factorización para f como producto de irreducibles en $R[X]$. Si $f = m_1 \cdots m_u \cdot q_1(X) \cdots q_s(X)$ es otra factorización con $m_j \in R$ irreducibles y $q_j(X) \in R[X]$, de grado ≥ 1, primitivos e irreducibles en $F[X]$, entonces, por la unicidad en $F[X]$, es $r = s$ y reordenando $p_i(X) = a_i \cdot q_i(X)$, con $0 \neq a_i \in F$. Puesto que p_i, q_i son primitivos, se deduce que $a_i \in R$ es unidad en R. Esto es p_i, q_i son asociados en $R[X]$. Cancelando los $p_i = q_i$, se concluye usando la unicidad de la factorización en R. □

Corolario 1.13.13. *Sea R un DFU. Entonces el anillo de polinomios $R[X_1, \dots, X_n]$ es DFU. Las unidades de $R[X_1, \dots, X_n]$ son las unidades de R. Los elementos irreducibles de $R[X_1, \dots, X_n]$ son los irreducibles de R y los polinomios de grado ≥ 1 que son primitivos e irreducibles en $F[X_1, \dots, X_n]$.*

Observación 1.13.14. (1) Sea $f(X) \in R[X_1, \dots, X_n]$ primitivo. Entonces f es irreducible en $R[X_1, \dots, X_n]$ si, y sólo si, f es irreducible en $F[X_1, \dots, X_n]$.

(2) Si $n \geq 2$, entonces $F[X_1, \dots, X_n]$ no es DIP.

(3) Habitualmente es difícil decidir si un polinomio es irreducible.

Ejemplo 1.13.15. Sea $R = \mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{Z}[i]$, subanillo unitario. El cuerpo de fracciones F coincide con $\mathbb{Q}[i] = \{a+bi \mid a, b \in \mathbb{Q}\}$, puesto que $\frac{r}{s}+\frac{p}{q}i = \frac{r}{s}+\frac{2p}{2q}i = \frac{2rq+2spi}{2sq} \in F$. El polinomio $f(X) = X^2+1$ factoriza de modo único $f(X) = X^2+1 = (X-i)(X+i)$ en $F[X]$. Ninguno de los factores está en $R[X]$ puesto que $i \notin R$. Por tanto, $f(X)$ es irreducible en $R[X]$. En particular, $R = \mathbb{Z}[2i]$ no es DFU.

1.13.2. Criterios de irreducibilidad

Proposición 1.13.16. *(1) Sea F un cuerpo. Un polinomio $aX + b \in F[X]$, con $0 \neq a$, es irreducible en $F[X]$.*

(2) Sea F un cuerpo. Un polinomio $f(X) \in F[X]$ de grado 2 ó 3 es irreducible en $F[X]$ si, y sólo si, no tiene raíces en F.

(3) Sean F un cuerpo, $a \in F$ y $f(X) \in F[X]$ con grado ≥ 1. Entonces $f(X)$ es irreducible si, y sólo si, $f(X + a)$ es irreducible.

(4) Sean R un DFU, F su cuerpo de fracciones y $f(X) = a_0 + \cdots + a_nX^n \in R[X]$, con $a_n \neq 0$ un polinomio de grado $n \geq 1$. Supongamos que $\frac{r}{s} \in F$ es raíz de $f(X)$, con $\operatorname{mcd}(r, s) = 1$. Entonces $r \mid a_0$ y $s \mid a_n$.

Ejemplos 1.13.17. (1) El polinomio $X^3 - 3X - 1 \in \mathbb{Z}[X]$ es irreducible en $\mathbb{Z}[X]$, puesto que es primitivo y las posibles raíces son ± 1, que no lo anulan.

(2) Para $p \in \mathbb{Z}$ primo los polinomios $X^2 - p, X^3 - p$ son irreducibles en $\mathbb{Z}[X]$.

(3) En $\mathbb{Q}[X]$ hay polinomios irreducibles de cualquier grado n, por ejemplo: $X^n - 2$.

(4) Los irreducibles de $\mathbb{C}[X]$ son los polinomios de grado 1.

(5) Los irreducibles de $\mathbb{R}[X]$ son los polinomios de grado 1 y los de grado 2 sin raíces reales.

(6) Decidir si un polinomio de $\mathbb{C}[X, Y]$ es irreducible puede ser un problema de cierta dificultad.

Proposición 1.13.18. *Sean R un DI, $P \subsetneq R$ un ideal primo y $f(X) = a_nX^n + \cdots + a_0 \in R[X]$, con grado $n \geq 1$ y tal que $a_n \notin P$. Si $f(X)$ factoriza en $R[X]$ en producto de polinomios de grado ≥ 1, entonces $\overline{f}(X) \in (R/P)[X]$ factoriza en $(R/P)[X]$ en producto de polinomios de grado ≥ 1.*

Demostración. Supongamos $f(X) = (b_rX^r + \cdots)(c_sX^s + \cdots)$, con $r, s \geq 1$ y $0 \neq b_r, 0 \neq c_s \in R$. Así $\overline{f}(X) = (\overline{b_r}X^r + \cdots)(\overline{c_s}X^s + \cdots)$, con $0 \neq \overline{b_r}, 0 \neq \overline{c_s}$, puesto que $0 \neq \overline{a_n} = \overline{b_r}\overline{c_s}$. □

Observación 1.13.19. En la demostración de la Proposición 1.13.18 basta suponer que P es un ideal propio. En el enunciado hemos incluido la condición P primo, para que $(R/P)[X]$ sea un DI, puesto que el caso típico de aplicación de este criterio supondrá que R un DIP y $P = pR$, con $p \in R$ un elemento primo.

Corolario 1.13.20. *(Criterio modular) Sea $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X], n \geq 1, a_n \neq 0$ primitivo. Supongamos que existe $p \in \mathbb{Z}$ primo con $p \nmid a_n$ y tal que $\overline{f}(X) = \overline{a_0} + \overline{a_1}X + \cdots + \overline{a_n}X^n \in \mathbb{Z}_p[X]$ es irreducible en $\mathbb{Z}_p[X]$, entonces $f(X)$ es irreducible en $\mathbb{Z}[X]$.*

Ejemplos 1.13.21. (1) $X^3 + X + 1$ es irreducible en $\mathbb{Z}[X]$ puesto que es mónico y $X^3 + X + \overline{1} \in (\mathbb{Z}/2\mathbb{Z})[X]$ no tiene raíces en $\mathbb{Z}/2\mathbb{Z}$.

(2) $X^2 + YX + 12 \in \mathbb{Z}[X, Y] = \mathbb{Z}[Y][X]$ es irreducible puesto que es mónico y módulo $P = Y\mathbb{Z}[Y]$ es $X^2 + 1$ que es irreducible en $\mathbb{Z}[X]$.

(3) $X^4 - 2X^3 + 4X^2 - X + 1 \in \mathbb{Z}[X]$ es mónico. Módulo $2\mathbb{Z}$ es $X^4 + X + \overline{1}$ que no tiene raíces en $\mathbb{Z}/2\mathbb{Z}$ y no es producto de dos polinomios mónicos irreducibles de grado 2 en $(\mathbb{Z}/2\mathbb{Z})[X]$, puesto que el único es $X^2 + X + \overline{1}$ y $(X^2 + X + \overline{1})^2 = X^4 + X^2 + \overline{1}$. En consecuencia, $X^4 - 2X^3 + 4X^2 - X + 1 \in \mathbb{Z}[X]$ es irreducible.

(4) Puesto que $X^4 - 2X^3 + 4X^2 - X + 1 \in \mathbb{Z}[X]$ es mónico y no tiene raíces en $\mathbb{Q}$, para probar que es irreducible basta ver, directamente, que $X^4 - 2X^3 + 4X^2 - X + 1 = (X^2 + aX + b)(X^2 + cX + d)$ no tiene solución con $a, b, c, d \in \mathbb{Z}$. El cálculo es inmediato.

(5) El polinomio $f(X) = X^4 - 10X^2 + 1 = (X^2 - 5)^2 - 24 \in \mathbb{Q}[X]$ es irreducible, pero factoriza en $(\mathbb{Z}/p\mathbb{Z})[X]$ para cada primo $p \in \mathbb{Z}$.

Miremos los coeficientes en $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Si $\sqrt{24} = 2\sqrt{6}$ está en $\mathbb{Z}_p$, i.e., si existe $\beta \in \mathbb{Z}_p$ tal que $\beta^2 = 6$, entonces $f(X)$ factoriza en $\mathbb{Z}_p[X]$:

$$f(X) = (X^2 - 5 + 2\beta)(X^2 - 5 - 2\beta).$$

Podemos, ahora, suponer que $X^2 - 6$ no tiene raíces en $\mathbb{Z}_p$. Así $E = \mathbb{Z}_p[X]/(X^2 - 6)\mathbb{Z}_p[X] = \mathbb{Z}_p \oplus \mathbb{Z}_p\beta$ es el cuerpo con p^2 elementos. En estas condiciones, $(a + b\beta)^2 = 5 + 2\beta$ tiene solución en E. En efecto, hay que resolver

$$\begin{cases} a^2 + 6b^2 = 5, \\ 2ab = 2. \end{cases}$$

Podemos suponer que $p \neq 2$, puesto que $f(X) = X^4 + 1$ factoriza en $\mathbb{Z}_2[X]$, de forma que $ab = 1$ y $b = a^{-1}$. Así, $a^2 + 6a^{-2} = 5$, que se reescribe como

$$0 = a^4 - 5a^2 + 6 = (a^2 - 2)(a^2 - 3).$$

Si ni 2 ni 3 es un cuadrado en $\mathbb{Z}_p$, entonces 6 es un cuadrado en E (el grupo cíclico $E - \{0\}$ está generado por β. Así $2 = \beta^m, 3 = \beta^n$, con m, n impares y $6 = \beta^{m+n}$ con $m+n$ par) en contra de la hipótesis. En consecuencia, alguno de 2 ó 3 es un cuadrado.

Hemos probado que existe $a \in \mathbb{Z}_p$ con $(a+a^{-1}\beta)^2 = 5+2\beta$. Se deduce que $(a-a^{-1}\beta)^2 = 5 - 2\beta$. Por tanto,

$$\begin{aligned} f(X) &= (X^2 - 5 + 2\beta)(X^2 - 5 - 2\beta) \\ &= (X^2 - (a - a^{-1}\beta)^2)(X^2 - (a + a^{-1}\beta)^2) \\ &= (X + a - a^{-1}\beta)(X - a + a^{-1}\beta)(X + a + a^{-1}\beta)(X - a - a^{-1}\beta) \\ &= (X - a - a^{-1}\beta)(X - a + a^{-1}\beta)(X + a + a^{-1}\beta)(X + a - a^{-1}\beta) \\ &= ((X - a)^2 - a^{-2}\beta^2)((X + a)^2 - a^{-2}\beta^2) \\ &= ((X - a)^2 - 6a^{-2})((X + a)^2 - 6a^{-2}), \end{aligned}$$

es una factorización de $f(X)$ en $\mathbb{Z}_p[X]$.

Teorema 1.13.22 (Criterio de Eisenstein)**.** *Sean R un DI, $P \subsetneq R$ un ideal primo y $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in R[X]$, con $n \geq 1$ y $a_n \neq 0$ (si a_n es una unidad en R, entonces el resultado es cierto sin imponer la condición R DI). Si $a_n \notin P, a_{n-1} \in P, \ldots, a_1 \in P, a_0 \in P$ y $a_0 \notin P^2$, entonces $f(X)$ no es producto de dos polinomios de grado ≥ 1 en $R[X]$.*

Demostración. Supongamos $f(X) = (b_rX^r + \cdots + b_0)(c_sX^s + \cdots + c_0)$, con $n > r, s \geq 1$ y $0 \neq b_r, 0 \neq c_s \in R$. En $(R/P)[X]$ obtenemos $\overline{a_n}X^n = (\overline{b_r}X^r + \cdots + \overline{b_0})(\overline{c_s}X^s + \cdots + \overline{c_0})$, con $0 \neq \overline{b_r}, 0 \neq \overline{c_s}$, puesto que $0 \neq \overline{a_n} = \overline{b_r}\overline{c_s}$. En particular, $0 = \overline{b_0}\overline{c_0}$. Esto es $\overline{b_0} = 0$ ó $\overline{c_0} = 0$. De hecho, ambos han de ser nulos. Puesto que si, e.g., $\overline{b_0} = 0$ y $\overline{c_0} \neq 0$, para el valor $j \leq r$ tal que $\overline{b_j} \neq 0$ y $\overline{b_l} = 0$ para $j > l \geq 0$, se tiene $\overline{a_j}X^j = \overline{b_j}\overline{c_0}X^j$. Como $n > r$ es $\overline{a_j} = 0$, esto es $\overline{b_j}\overline{c_0} = 0$ y $\overline{c_0} \neq 0, \overline{b_j} \neq 0$, que es contrario a la hipótesis P primo. En consecuencia $b_0, c_0 \in P$, así $a_0 = b_0c_0 \in P^2$. □

Damos otro enunciado más clásico del Criterio de Eisenstein. La demostración es, conceptualmente, la misma aunque cambiamos la redacción.

Teorema 1.13.23 (Criterio de Eisenstein)**.** *Sean R un DFU y $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in R[X]$, con $n \geq 1$ y $a_n \neq 0$ primitivo. Si existe un elemento primo $p \in R$ tal que $p \nmid a_n$, $p \mid a_{n-1}, \ldots, p \mid a_1, p \mid a_0$ y $p^2 \nmid a_0$, entonces $f(X)$ es irreducible en $R[X]$.*

Demostración. Supongamos que f factoriza $f(X) = (b_rX^r + \cdots + b_0)(c_sX^s + \cdots + c_0)$, en $R[X]$, con $n > r, s \geq 1$ y $0 \neq b_r, 0 \neq c_s \in R$. Puesto que $a_0 = b_0c_0$ es divisible por p pero no por p^2, se deduce que, por ejemplo, $p \mid b_0$ y $p \nmid c_0$. Puesto que $p \nmid a_n = b_rc_s$, es $p \nmid b_r$. Sea $r \geq j > 0$

tal que $p \nmid b_j$ y $p \mid b_l$ para $j > l \geq 0$. Entonces en la expresión $a_j = b_j c_0 + b_{j-1}c_1 + \cdots$, se tiene $p \nmid b_j c_0$, puesto que suponemos p primo y $p \nmid b_j, p \nmid c_0$; y $p \mid (b_{j-1}c_1 + \cdots)$. Así $p \nmid a_j$, en contra de la hipótesis, puesto que $n > r \geq j$. □

Si un polinomio es irreducible también lo es el polinomio obtenido escribiendo los coeficientes en "sentido contrario".

Proposición 1.13.24. *$f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in R[X], n \geq 1, a_n \neq 0, a_{\neq}0$ es irreducible si, y sólo si, $g(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n \in R[X], n \geq 1, a_n \neq 0, a_0 \neq 0$ es irreducible.*

Demostración. Es claro que $f(X) = X^n g(\frac{1}{X})$. De esta igualdad se obtiene la afirmación del enunciado, puesto que $g(X) = h(X)k(X)$ en $R[X]$ con $\deg h = r, \deg k = n - r$ si, y sólo si, $f(X) = h^*(X)k^*(X)$ en $R[X]$, donde $h^*(X) = X^r h(\frac{1}{X}), k^*(X) = X^{n-r}k(\frac{1}{X})$. □

Por tanto, tenemos un criterio de Eisenstein en "sentido contrario"

Teorema 1.13.25 (Criterio de Eisenstein *)**.** *Sean R un DFU y $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in R[X]$, con $n \geq 1$ y $a_n \neq 0$ primitivo. Si existe un elemento primo $p \in R$ tal que $p \nmid a_0$, $p \mid a_n, p \mid a_{n-1}, \ldots, p \mid a_1$ y $p^2 \nmid a_n$, entonces $f(X)$ es irreducible en $R[X]$.*

Ejemplos 1.13.26. (1) Sea $p \in \mathbb{Z}$ primo. El p–ésimo polinomio ciclotómico

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

es irreducible en $\mathbb{Q}[X]$ (y en $\mathbb{Z}[X]$, puesto que es primitivo).

Podemos aplicar Eisenstein a

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

puesto que p, siendo primo, divide a cada coeficiente binómico $\binom{p}{i}$.

(2) Veremos que si n no es primo $X^{n-1} + X^{n-2} + \cdots + X + 1$ factoriza en $\mathbb{Q}[X]$. Por ejemplo, $X^3 + X^2 + X + 1 = (X + 1)(X^2 + 1)$.

(3) El polinomio ciclotómico $\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ es irreducible en $\mathbb{Z}[i][X]$, puesto que es primitivo y a $\Phi_7(X+1) = X^6+7X^5+21X^4+35X^3+35X^2+21X+7$ se le puede aplicar el criterio de Eisenstein para el primo $7 \in \mathbb{Z}[i]$ (Teorema 1.12.19).

(4) Sea R un DI. El polinomio $Y^n - X \in R[X][Y]$ no factoriza como producto de polinomios de grado positivo en Y, puesto que verifica Eisenstein para el ideal primo $P = XR[X]$. En consecuencia es irreducible, puesto que, es claro, que no se puede escribir con un factor, no unidad, de grado cero en Y.

1.14. Ejercicios

(1) El centro de un anillo R es $Z_R = \{z \in R \mid zr = rz \text{ para todo } r \in R\}$. Demostrar que el centro de un anillo es un subanillo conmutativo que contiene a la identidad de R (si existe). Demostrar que el centro de un anillo de división es un cuerpo.

(2) Sea $\mathbb{H}$ el anillo de los cuaternios reales.

a) Describir el centro del anillo $\mathbb{H}$ de los cuaternios reales. Demostrar que $\{a+bi \mid a, b \in \mathbb{R}\}$ es un subanillo de $\mathbb{H}$ que es un cuerpo pero no está contenido en el centro de $\mathbb{H}$.

b) Demostrar que la aplicación "norma" $\mathbb{H} \xrightarrow{N} \mathbb{R}$ definida por $a + bi + cj + dk \mapsto a^2 + b^2 + c^2 + d^2$ verifica $N(\alpha) = \alpha\bar{\alpha}$, donde si $\alpha = a + bi + cj + dk$ entonces $\bar{\alpha} = a - bi - cj - dk$. Deducir que N es multiplicativa, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$ para cualesquiera $\alpha, \beta \in \mathbb{H}$.

c) Sea $\mathbb{I}$ el anillo de los cuaternios enteros. Probar que $\alpha \in \mathbb{I}$ es unidad si, y sólo si, $N(\alpha) = 1$. Escribir la tabla del grupo $\mathbb{I}^*$ que llamaremos grupo cuaternio.

(3) Demostrar que si R es un dominio de integridad y $x^2 = 1$ para $x \in R$ entonces $x = \pm 1$.

(4) Un elemento $x \in R$ se llama nilpotente si $x^m = 0$ para algún $m \in \mathbb{Z}^+$ ($m \geq 1$).

a) Demostrar que x es cero o divisor de cero.

b) Demostrar que rx es nilpotente para todo $r \in R$ tal que $rx = xr$. Exhibir un contraejemplo si $rx \neq xr$.

c) Demostrar que la suma de dos nilpotentes que conmutan es nilpotente.

d) Demostrar que $1 + x$ es unidad en R.

e) Deducir que la suma de un nilpotente y una unidad que conmutan es unidad.

f) Sea $a \in \mathbb{Z}$. Demostrar que $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ es nilpotente si, y sólo si, todo divisor primo de n es también divisor de a. En particular, determinar los nilpotentes de $\mathbb{Z}/10\mathbb{Z}$ y $\mathbb{Z}/72\mathbb{Z}$.

(5) Sean R, S anillos. Probar que $R \times S$ es una anillo con la suma $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$ y el producto $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$. Probar que $R \times S$ es conmutativo si, y sólo si, R y S son conmutativos. Probar que $R \times S$ tiene identidad si, y sólo si, R y S tiene identidad. ¿Cuáles son las unidades en este caso? ¿Es $R \times S$ dominio de integridad si R y S los son?

(6) Un anillo unitario R se llama booleano si $a^2 = a$ para todo $a \in R$.

a) Para todo elemento $a \in R$ se verifica $a + a = 0$.

b) R es conmutativo.

c) Si R es booleano y dominio de integridad entonces $R = \mathbb{Z}/2\mathbb{Z}$.

d) Sea X un conjunto no vacío. En $\mathscr{P}(X)$ definimos $A + B = (A - B) \cup (B - A)$ y $AB = A \cap B$. Comprobar que $(\mathscr{P}(X), +, .)$ es anillo (llamado anillo de conjuntos) conmutativo con identidad y booleano.

(7) Sea R un anillo con $1 \neq 0$. Un elemento no nulo a se dice divisor de cero por la izquierda en R si existe $0 \neq x \in R$ tal que $ax = 0$. Simétricamente definimos divisor de cero por la derecha. Así un divisor de cero es un elemento que es simultáneamente divisor de cero a derecha e izquierda. Un elemento $u \in R$ tiene un inverso a la izquierda en R si existe $s \in R$ tal que $su = 1$. Simétricamente inverso a derecha.

a) Demostrar que u es una unidad si, y sólo si, tiene inverso a derecha e izquierda.

b) Demostrar que si u tiene inverso a izquierda entonces u no es divisor de cero a izquierda.

c) Probar que si u tiene más de un inverso a derecha entonces es un divisor de cero a izquierda.

d) Probar que si R es un anillo finito entonces todo elemento que tiene inverso a derecha es una unidad (i.e. tiene inverso a ambos lados).

(8) Sea A un anillo conmutativo con $1 \neq 0$. Sea R el conjunto de los endomorfismos del grupo aditivo A, con la suma y la composición. Probar que R es un anillo con identidad cuyas unidades son los automorfismos de A.

(9) Sea $A = \mathbb{Z} \times \mathbb{Z} \times \cdots$ el producto directo de una cantidad numerables de copias de $\mathbb{Z}$ y sea R el anillo de los endomorfismos de $(A, +)$. Sea $\varphi \in R$ definido por $\varphi(a_1, a_2, a_3, \cdots) = (a_2, a_3, \cdots)$ y $\psi \in R$ definido por $\psi(a_1, a_2, a_3, \cdots) = (0, a_1, a_2, a_3, \cdots)$.

a) Probar que $\varphi\psi = 1_R$ pero $\psi\varphi \neq 1_R$ (i.e., ψ es un inverso a derecha de φ pero no es un inverso a izquierda).

b) Exhibir infinitos inversos a derecha de φ.

c) Hallar $0 \neq \pi \in R$ tal que $\varphi\pi = 0$ pero $\pi\varphi \neq 0$.

d) Probar que no existe $0 \neq \lambda \in R$ tal que $\lambda\varphi = 0$ (i.e., φ es un divisor de cero a izquierda pero no es divisor de cero a derecha).

(10) Sean R un anillo conmutativo, con unidad e $I \subset R$ un ideal. Demostrar que $I = R$ si, y sólo si, I contiene una unidad de R.

(11) Sea R un anillo conmutativo, con unidad. Demostrar que si R tiene un único ideal maximal M, entonces $r \in R$ es unidad si, y sólo si, $r \notin M$.

(12) En cada uno de los siguientes anillos, determinar todos sus ideales, indicando cuáles son primos o maximales.

a) $\mathbb{Z}_{12}$

b) $\mathbb{R}^2$

c) $\mathbb{Z}_4 \times \mathbb{Z}_8$

d) $\mathbb{Z}_{15}$

e) $\mathbb{Z}_{27}/(9)$

(13) Sea K un cuerpo y $f : K \to R$ un homomorfismo de anillos unitarios. Demostrar que f es inyectivo.

(14) Demostrar que la aplicación $\mathbb{C} \to \mathbb{M}_2(\mathbb{R})$ del cuerpo de los numeros complejos en el anillo de las matrices cuadradas reales de orden 2 definida por

$$a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

es un homomorfismo inyectivo.

(15) Determinar todos los homomorfisnos de anillos unitarios de $\mathbb{Z}_6 \times \mathbb{Z}_6 \to \mathbb{Z}_2$

(16) Dterminar todos los homomorfismos de anillos unitarios de $\mathbb{Z}[i] \to \mathbb{Z}[i]$ y de $\mathbb{Z}[i] \to \mathbb{Z}$.

(17) Sea R el anillo de las funciones de $\mathbb{R}$ en $\mathbb{R}$. Demostrar que le polinomio $X^2 - 1$ tiene infinitas raíces en R. ¿Cuántas raíces tiene en el anillo C de las funciones continuas de $\mathbb{R}$ en $\mathbb{R}$?

(18) Hallar dos polinomios de grado positivo en $\mathbb{Z}_6[X]$ cuyo producto sea $X + \overline{1}$.

(19) (Función de Euler) Definimos $\phi(1) =$ y para cada entero $n \geq 2$

$$\phi(n) = |\{k \mid 1 \leq k < n, \operatorname{mcd}(n,k) = 1\}|.$$

a) Demostrar que $\bar{k} \in \mathbb{Z}_n$, $n \geq 2$ es unidad si, y sólo si, $\operatorname{mcd}(n,k) = 1$ si, y sólo si, $\bar{k}$ es un generador de $(\mathbb{Z}_n, +)$. Concluir que el grupo de unidades $\mathbb{Z}_n^*$ tiene orden $\phi(n)$. En consecuencia, si $\operatorname{mcd}(n,k) = 1$, entonces $k^{\phi(n)} \equiv 1 \pmod{n}$, (teorema de Euler).

b) Si p es primo y $r \geq 1$ demostrar que $\phi(p^r) = p^r - p^{r-1}$.

c) Sean $m, n \in \mathbb{Z}$. Demostrar que la aplicación $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ dada por $f(\bar{k}) = (\bar{k}, \bar{k})$ está bien definida y es el único homomorfismo de anillos unitarios de $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$. Demostrar que f es un isomorfismo si, y sólo si, $\operatorname{mcd}(m,n) = 1$.

d) Demostrar que si $\operatorname{mcd}(m,n) = 1$, entonces $\phi(mn) = \phi(m)\phi(n)$.

e) Si $m = p_1^{r_1} \cdots p_t^{r_t}$, donde los p_i son primos distintos dos a dos y $r_i \geq 1$, entonces

$$\phi(m) = \prod_{i=1}^{t} p_i^{r_i-1}(p_i - 1) = m \prod_{i=1}^{t}(1 - \frac{1}{p_i}).$$

(20) Consideramos $\mathbb{Z}_7 = \mathbb{Z}/7\mathbb{Z}$ y $\mathbb{Z}_8 = \mathbb{Z}/8\mathbb{Z}$.

a) Escribir las tablas de la suma y el producto.

b) Obtener $\mathbb{Z}_7^*$ y $\mathbb{Z}_8^*$. ¿Son grupos cíclicos? Obtener todos los generadores en el caso de que sea cíclico.

c) Calcular si existen los inversos de $\bar{8}, \bar{9}$ y $\bar{11}$ en $\mathbb{Z}_{15}$.

(21) Calcular las soluciones enteras de las ecuaciones:

$$a)\ 25x + 40y = 24, \qquad b)\ 48x + 30y = 12,$$

$$c)\ 31x + 17y = 12, \qquad d)\ 2645x + 1955y = 230.$$

(22) Sean $a, b, n \in \mathbb{Z}$. Se dice que a es congruente con b módulo n y se escribe $a \equiv b (\mathrm{mod}\, n)$ si n divide a $b - a$. Obtener (si existen) los números enteros x que satisfagan las siguientes congruencias

$$a)\ 18x \equiv 7(\mathrm{mod}\, 35) \qquad b)\ 9x \equiv 6(\mathrm{mod}\, 45) \qquad c)\ 3x \equiv 6(\mathrm{mod}\, 45)$$

$$d)\ 5x \equiv 17(\mathrm{mod}\, 19) \qquad e)\ 5x \equiv 17(\mathrm{mod}\, 15) \qquad f)\ 34x \equiv 60(\mathrm{mod}\, 98)$$

$$g)\ 35x \equiv 119(\mathrm{mod}\, 139) \qquad h)\ 125x \equiv 27(\mathrm{mod}\, 256) \qquad i)\ 211x \equiv 659(\mathrm{mod}\, 900)$$

(23) Encontrar un entero positivo de tres cifras cuyos restos al dividirlo por 7, 9 y 11 son 1, 2 y 3.

(24) Encontrar el menor entero positivo cuyos restos al dividirlo por 5, 7 y 9 son 4, 3 y 1.

(25) Encontrar las soluciones (si existen) de los siguientes sistemas de congruencias:

$$a)\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases} \qquad b)\begin{cases} x \equiv 7 \pmod{12} \\ x \equiv 11 \pmod{15} \\ x \equiv 3 \pmod 7 \end{cases} \qquad c)\begin{cases} x \equiv 18 \pmod 7 \\ x \equiv 3 \pmod{12} \\ x \equiv 7 \pmod 5 \\ x \equiv 11 \pmod{28} \end{cases}$$

$$d)\begin{cases} 6x \equiv 8 \pmod{14} \\ 9x \equiv 36 \pmod{48} \end{cases} \qquad e)\begin{cases} x \equiv 36 \pmod{41} \\ x \equiv 5 \pmod{17} \end{cases}$$

(26) Calcula el resto de dividir 4897^{18403} entre 20. Ídem para $2^{37 \cdot 73}$ entre 37.

(27) Se dice que dos ideales I y J de un anillo conmutativo unitario R son primos entre sí (o comaximales) si $I + J = R$. Por ejemplo, $m\mathbb{Z}$ y $n\mathbb{Z}$ son primos entre sí si, y sólo si, mcd $(m, n) = 1$.

a) Se define el ideal producto IJ como el ideal generado por los productos rs de elementos $r \in I$ y $s \in J$. Probar que $IJ \subset I \cap J$ y que, si I y J son primos entre sí, entonces se tiene la igualdad.

b) (Teorema chino del resto) Sean $I_1, I_2, \cdots, I_k$ ideales en R. La aplicación $R \to R/I_1 \times R/I_2 \times \cdots \times R/I_k$ definida por $r \mapsto (r+I_1, r+I_2, \cdots, r+I_k)$ es un homomorfismo de anillos con núcleo $I_1 \cap I_2 \cap \cdots \cap I_k$. Si para cada $i \neq j$ los ideales I_i e I_j son comaximales, entonces esta aplicación es sobreyectiva y $I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k$, así $R/I_1 I_2 \cdots I_k = R/I_1 \cap I_2 \cap \cdots \cap I_k \simeq R/I_1 \times R/I_2 \times \cdots \times R/I_k$.

(28) Consideramos el ideal $I = (XY, X^2)\mathbb{R}[X, Y]$.

a) Calcular el radical de I.

b) Probar que $I = (X) \cap (X, Y)^2 = (X) \cap (X^2, Y)$.

c) Probar que (X) es primo no maximal, (X, Y) es maximal, y tanto $(X, Y)^2$ como (X^2, Y) son primarios no primos. Este ejercicio ilustra el hecho de que todo ideal (de un anillo noetheriano) se escribe (de forma **no** necesariamente única) como intersección de ideales primarios.

(29) Demostrar, para $D = 3, 5, 6, 7$, que el grupo $\mathscr{O}^\times$ de las unidades del anillo de enteros del cuerpo cuadrático $\mathbb{Q}(\sqrt{D})$ es infinito exhibiendo un elemento de orden infinito en este grupo.

(30) Sea D un entero que no es un cuadrado perfecto en $\mathbb{Z}$ y $S = \{\begin{bmatrix} a & b \\ Db & a \end{bmatrix} \mid a, b \in \mathbb{Z}\}$.

a) Demostrar que S es un subanillo de $\mathscr{M}_2(\mathbb{Z})$.

b) Si D no es un cuadrado perfecto en $\mathbb{Z}$, demostrar que la aplicación $\mathbb{Z}[\sqrt{D}] \xrightarrow{\varphi} S$ definida pro $\varphi(a + b\sqrt{D}) = \begin{bmatrix} a & b \\ Db & a \end{bmatrix}$ es un isomorfismo de anillos.

(31) Demostrar que si $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ son ideales de R entonces $\cup_{n=1}^{\infty} I_n$ es un ideal de R.

(32) La característica de un anillo R con $1 \neq 0$ es el menor entero positivo n tal que $1 + \overset{n}{\cdots} + 1 = 0$ en R. Si no existe tal entero se dice que la característica de R es cero. Por ejemplo $\mathbb{Z}/n\mathbb{Z}$ es un anillo de característica n y $\mathbb{Z}$ es un anillo de característica 0.

a) Demostrar que la aplicación $\mathbb{Z} \to R$ definida por

$$k \mapsto \begin{cases} 1 + \overset{k}{\cdots} + 1 & \text{si } k > 0, \\ 0 & \text{si } k = 0, \\ (-1) + \overset{-k}{\cdots} + (-1) & \text{si } k < 0. \end{cases}$$

es un homomorfismo de anillos cuyo núcleo es $n\mathbb{Z}$, donde n es la característica del anillo R.

b) Demostrar que si p es primo y R es una anillo conmutativo de característica p, entonces $(a+b)^p = a^p + b^p$ para todo $a, b \in R$.

c) Probar que un si un dominio de integridad tiene característica p entonces p es primo o 0.

d) El apartado (a) del ejercicio 6 muestra que la característica de un anillo booleano es 2.

(33) Supongamos que R es conmutativo. Sean I, J ideales de R y supongamos que P es un ideal primo que contiene a $I \cap J$. Demostrar que I ó J están contenidos en P.

(34) Sean I, J ideales de $\mathbb{Z}$ generados, respectivamente, por $a, b \in \mathbb{Z}$. Hallar un generador para los ideales $I + J, I \cap J, IJ, I : J, \sqrt{I}$.

(35) Sea $R \xrightarrow{\varphi} S$ un homomorfismo de anillos conmutativos.

a) Demostrar que si P es un ideal primo de S entonces $\varphi^{-1}(P) = R$ o $\varphi^{-1}(P)$ es un ideal primo de R. En el caso donde R es un subanillo de S y φ es la inclusión si P es ideal primo de S entonces $P \cap R$ es bien sea R o un ideal primo de R.

b) Probar que si M es un ideal maximal de S y φ es sobreyectivo entonces $\varphi^{-1}(M)$ es un ideal maximal de R. Dar un ejemplo para mostrar que la hipótesis sobreyectiva no se puede eliminar.

(36) Sea R un anillo unitario. Demostrar que si M es un ideal tal que R/M es un anillo de división entonces M es un ideal maximal (no suponer R conmutativo).

(37) Sea R un anillo conmutativo, unitario.

a) Probar que el conjunto de elementos nilpotentes de R es un ideal, llamado el nilradical de R y denotado $\mathcal{N}il(R)$.

b) Probar que el nilradical del cociente $R/\mathcal{N}il(R)$ es cero.

c) Escribir dos matrices nilpotentes en $\mathcal{M}_2(\mathbb{Z})$ cuya suma no es nilpotente.

d) Sea R un anillo conmutativo y con unidad. Probar que el nilradical es la intersección de todos los ideales primos de R.

e) Demostrar que si el nilradical es finitamente generado entonces es un ideal nilpotente.

f) Sea I un ideal de R. Definimos $\mathrm{rad}(I) = \{r \in R \mid r^n \in I \,\text{para cierto}\, n \in \mathbb{Z}^+\}$. Demostrar que $\mathrm{rad}(I)$ es un ideal de R que contiene a I y que $\mathrm{rad}(I)/I = \mathcal{N}il(R/I)$. El ideal $\mathrm{rad}(I)$ se llama el radical de I.

g) $\mathrm{rad}(I)$ es la intersección de todos los ideales primos que contienen a I.

h) Probar que todo ideal primo es radical.

i) Describir los ideales radicales de $\mathbb{Z}/n\mathbb{Z}$.

(38) Sea R un anillo conmutativo con unidad. Demostrar que son equivalentes.

a) R tiene exactamente un ideal primo.

b) Cada elemento de R es o nilpotente o unidad.

c) $R/\mathcal{N}il(R)$ es un cuerpo.

(39) Un ideal propio Q de un anillo conmutativo R se dice primario si siempre que $ab \in Q$ y $a \notin Q$ entonces $b^n \in Q$ para cierto $n \in \mathbb{Z}^+$.

a) Los ideales primario de $\mathbb{Z}$ son (0) y $p^n\mathbb{Z}$ para p primo.

b) Todo ideal primo es primario.

c) Un ideal Q de R es primario si, y sólo si, R/Q es no nulo y cada divisor de cero en R/Q es nilpotente.

d) Si Q es primario entonces $\mathrm{rad}(Q)$ es primo. Dar un ejemplo de ideal primo cuyo cuadrado no sea primario.

e) Probar que si $\mathrm{rad}(Q)$ es maximal entonces Q es primario. En particular las potencias de un ideal maximal son ideales primarios.

(40) Sea F un cuerpo. Probar que F contiene un subcuerpo mínimo F_0 (que denominaremos el subcuerpo primo de F) y que F_0 es isomorfo bien sea a $\mathbb{Q}$ o a $\mathbb{Z}/p\mathbb{Z}$ para cierto primo p.

(41) Sea F un cuerpo. Definimos el anillo $F((X))$ de las series formales de Laurent con coeficientes en F por

$$F((X)) = \{\sum_{n \geq N}^{\infty} a_n X^n \mid a_n \in F \,\text{and}\, N \in \mathbb{Z}\}.$$

(Cada elemento de $F((X))$ es una serie de potencias en X sumada con un polinomio en $\frac{1}{X}$, i.e., cada elemento de $F((X))$ tiene sólo un número finito de términos con potencias negativas de X.)

a) Probar que $F((X))$ es un cuerpo.

b) Probar que el cuerpo de fracciones de $F[[X]]$ es el cuerpo $F((X))$.

c) Probar que el cuerpo de fracciones de $\mathbb{Z}[[X]]$ está estrictamente contenido en el cuerpo $\mathbb{Q}((X))$.

(42) Definimos una sucesión de números reales por la fórmula de recurrencia $a_0 = a, a_1 = b, a_n = a_{n-1} + a_{n-2},\ n \geq 2$. Consideramos la serie generatriz $\varphi(t) = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \cdots \in \mathbb{R}[[t]]$. Demostrar que $\varphi(t)$ es una fracción algebraica, cuyo numerador es un polinomio invertible en $\mathbb{R}[[t]]$. Obtener la expresión del término general de a_n.

(43) Sea F un cuerpo. Demostrar que el anillo $F[X]_{(X)}$ se sumerge de manera natural en el anillo de series formales $F[[X]]$.

(44) Sean R una anillo conmutativo unitario y $U \subset R$ un sistema multiplicativamente cerrado en R. Denotemos $R \xrightarrow{\varphi} R[U^{-1}]$ el homomorfismo natural $r \mapsto r/1$.

a) Demostrar que para cada ideal $I \subset R[U^{-1}]$ se verifica $I = \varphi^{-1}(I)R[U^{-1}]$. Por tanto la aplicación $I \mapsto \varphi^{-1}(I)$ es una inyección del conjunto de ideales de $R[U^{-1}]$, en el conjunto de ideales de R. Esta aplicación inyectiva preserva inclusiones e intersecciones, y lleva ideales primos a ideales primos.

b) Un ideal $J \subset R$ es de la forma $\varphi^{-1}(I)$ para algún ideal $I \subset R[U^{-1}]$ si, y sólo si, $J = \varphi^{-1}(JR[U^{-1}])$. Este es el caso si, y sólo si, cada elemento $u \in U$ es no divisor de cero mod J en el sentido que si $r \in R$ y $ru \in J$, entonces $r \in J$. En particular, la correspondencia $I \mapsto \varphi^{-1}(I)$ es una biyección entre los primos de $R[U^{-1}]$ y los primos de R que no cortan a U.

(45) Sean $I \subset P$ ideales de R, con P primo. Probar que existe un isomorfismo natural $R_P/I_P \simeq (R/I)_{P/I}$.

(46) Sean R un anillo conmutativo unitario y $U \subset R$ una parte multiplicativamente cerrada.

a) Probar que $r \in R$ es unidad en $R[U^{-1}]$ si, y sólo si, $rR \cap U \neq \emptyset$.

b) Probar que si $r \in R$ es un elemento primo tal que $rR \cap U = \emptyset$ y $r \neq 0$ en $R[U^{-1}]$, entonces r es un elemento primo de $R[U^{-1}]$.

c) Probar que si R es DFU, para cada elemento irreducible $\frac{r}{u} \in R[U^{-1}]$ existe $x \in R$ irreducible tal que $\frac{r}{u}$ y x son asociados en $R[U^{-1}]$.

d) Demostrar que si R es DFU entonces $R[U^{-1}]$ es un DFU

(47) Sean F un cuerpo y $f(X) \in F[X]$ un polinomio mónico de grado $n \geq 1$.

a) Probar que el cociente $F[X]/(f(X))$ es un F–espacio vectorial de dimensión n con base $\{1, x, \ldots, x^{n-1}\}$, donde $x = \bar{X}$.

b) Probar que $F[X]/(f(X))$ es un cuerpo si, y sólo si, $f(X)$ es irreducible.

c) Si F es un cuerpo finito con q elementos y $f(X)$ mónico, irreducible de grado n entonces $F[X]/(f(X))$ es un cuerpo con q^n elementos.

d) El número de elementos de un cuerpo finito es de la forma p^n para cierto primo p y entero $n \geq 1$.

e) Sea F es un cuerpo finito. En $F[X]$ hay infinitos polinomios irreducibles.

(48) Construir cuerpos con $8, 27$ y 125 elementos.

(49) Sea $\mathbb{F}_8 = \mathbb{Z}[2]/(X^3 + X + \overline{1})$ y $\alpha = \overline{X} \in \mathbb{F}_8$. Demostrar

a)
$$\mathbb{F}_8 = \{\overline{0}, \overline{1}, \alpha, \overline{1} + \alpha, \alpha^2, \overline{1} + \alpha^2, \alpha + \alpha^2, \overline{1} + \alpha + \alpha^2\}.$$

b) Construir la tabla de multiplicación en $\mathbb{F}_8$.

c) Es $\mathbb{F}_8$ un cuerpo?

(50) Sean $R = \mathbb{Z}[5]/(X^2 + \overline{1})$ y $\alpha = \overline{X} \in R$. Hallar en R el inverso de $\alpha^2 + \alpha - \overline{1}$. Hallar un divisor de cero en R.

(51) Demostrar que en un DIP R dos ideales (a) y (b) son comaximales (i.e., $(a) + (b) = R$) si, y sólo si, un máximo común divisor de a y b es 1 (en cuyo caso, se dice que a y b son primos entre sí).

(52) Sea R el anillo cuadrático $\mathbb{Z}[\sqrt{-5}]$. Consideramos los ideales $I_2 = (2, 1 + \sqrt{-5})$, $I_3 = (3, 2 + \sqrt{-5})$ e $I_3' = (3, 2 - \sqrt{-5})$.

a) Demostrar que I_2, I_3 e I_3' son no principales. (Hemos probado esto para I_3.)

b)) Mostrar que el producto de dos ideales no principales puede ser principal, viendo que I_2^2 es el ideal principal generado por 2.

c) De forma similar $I_2 I_3 = (1 - \sqrt{-5})$ e $I_2 I_3' = (1 + \sqrt{-5})$ son principales. Concluir que el ideal principal (6) es el producto de cuatro ideales primos $(6) = I_2^2 I_3 I_3'$.

d) Demostrar que $2, 3, 1 + \sqrt{-5}$ y $1 - \sqrt{-5}$ son irreducibles en R, no asociados dos a dos, y $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ son dos factorizaciones distintas de 6 en producto de irreducibles en R.

e) Demostrar que los ideales I_2, I_3 e I_3' son maximales en R.

f) Las factorizaciones en *d*) implican las igualdades de ideales principales $(6) = (2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Mostrar que estas dos factorizaciones dan la misma factorización del ideal (6) en producto de ideales primos.

(53) En el anillo $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$, consideramos la aplicación $N(a + b\sqrt{-3}) = a^2 + 3b^2$. Mostrar, de forma razonada, que 2 es irreducible en $\mathbb{Z}[\sqrt{-3}]$ y, sin embargo, el ideal (2) de $\mathbb{Z}[\sqrt{-3}]$ **no** es primo.

(54) Sean $a, b \in \mathbb{Z}$ primos entre sí. Calcular $\text{mcd}(a, b)$ en $\mathbb{Z}[\sqrt{-3}]$.

(55) Para cada uno de los anillos siguientes, decidir si son DE, DIP, DFU y calcular sus unidades.

a) $R = \mathbb{Z}[\omega]$, donde ω es una raíz sexta primitiva de la unidad. Demostrar que si $N(\alpha)$ es primo, entonces α es irreducible en R. ¿Es el ideal $(1 - \omega)R$ maximal?. Factorizar 3 en producto de elementos irreducibles en R.

b) $\mathbb{Z}[\sqrt{10}]$.

(56) Demostrar que $\mathbb{Z}[\sqrt{2}]$ y $\mathbb{Z}[\sqrt{-2}]$ son DE. Hallar sus unidades.

(57) En el dominio euclídeo $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$ con la norma $N(a + b\sqrt{-2}) = a^2 + 2b^2$, consideramos el ideal:

$$I = (5 - \sqrt{-2}, 3) = \{(5 - \sqrt{-2})(a + b\sqrt{-2}) + 3(c + d\sqrt{-2}) \mid a, b, c, d \in \mathbb{Z}\}.$$

a) Demostrar que $x + y\sqrt{-2} \in I$ si y sólo si $x \equiv y \pmod 3$.

b) Comprobar que I es un ideal principal encontrando un generador de I.

c) Demostrar que I es maximal. ¿Cuántos elementos tiene el cuerpo $\mathbb{Z}[\sqrt{-2}]/I$?

(58) En el anillo $\mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$, consideramos la aplicación $N(a + b\sqrt{-6}) = a^2 + 6b^2$.

a) Demostrar que un elemento $\alpha = a + b\sqrt{-6}$ es unidad en $\mathbb{Z}[\sqrt{-6}]$ si, sólo si, $N(\alpha) = 1$. ¿Cuáles son las unidades de $\mathbb{Z}[\sqrt{-6}]$?

b) Estudiar, de forma razonada, si el elemento 3 es irreducible en $\mathbb{Z}[\sqrt{-6}]$, y si el ideal $(3) = \{3(a + b\sqrt{-6}) \mid a, b \in \mathbb{Z}\}$ es un ideal primo en $\mathbb{Z}[\sqrt{-6}]$.

(59) En el anillo $\mathbb{Z}[\sqrt{-7}] = \{a + b\sqrt{-7} \mid a, b \in \mathbb{Z}\}$, consideramos la aplicación $N(a + b\sqrt{-7}) = a^2 + 7b^2$.

a) Demostrar que un elemento $\alpha = a + b\sqrt{-7}$ es unidad en $\mathbb{Z}[\sqrt{-7}]$ si, sólo si, $N(\alpha) = 1$. ¿Cuáles son las unidades de $\mathbb{Z}[\sqrt{-7}]$?

b) Estudiar, de forma razonada, si el elemento 2 es irreducible en $\mathbb{Z}[\sqrt{-7}]$, y si el ideal $(2) = \{2(a + b\sqrt{-7}) \mid a, b \in \mathbb{Z}\}$ es un ideal primo en $\mathbb{Z}[\sqrt{-7}]$.

(60) Sean $x, y \in \mathbb{Z}$ tales que $x^3 = y^2 + 2$.

a) Demostrar que x, y son impares y primos entre sí.

b) Demostrar que $y + \sqrt{-2}, y - \sqrt{-2}$ son primos entre sí en $\mathbb{Z}[\sqrt{-2}]$.

c) Demostrar que si $y + \sqrt{-2} = (a + b\sqrt{-2})^3$ con $a, b, y \in \mathbb{Z}$, entonces $y = \pm 5$.

d) Hallar todas las soluciones enteras de la ecuación $x^3 = y^2 + 2$.

(61) Factorizar el polinomio $X^4 + 1$ en $\mathbb{Q}[X], \mathbb{R}[X], \mathbb{C}[X]$.

(62) Factorizar $X^n - 1$ en $\mathbb{Z}[X]$ para $n = 1, 2, \ldots, 10$.

(63) Factorizar $X^{12} - 1$ en $\mathbb{Q}[X]$.

(64) Demostrar que los ideales de la forma $(p, f(X))\mathbb{Z}[X]$ con p primo y $f(X)$ irreducible módulo p, son maximales.

(65) Demostrar que $X^3 - 2$ es irreducible en $\mathbb{Z}[i][X]$.

(66) Obtener un generador del ideal $(7, -2 + 3i)\mathbb{Z}[i]$.

(67) Obtener un generador del ideal $(5, 3 + 4i)\mathbb{Z}[i]$.

(68) Calcular en $\mathbb{Z}[i]$ el máximo comun divisor de $17, 10 + 11i$.

(69) Calcular una identidad de Bezout para el máximo común divisor en $\mathbb{Z}[i]$ de

a) $40 + 18i, -23 + 10i$

b) $360 + 97i, 24 + 68i$

(70) Obtener el máximo común divisor y una identidad de "Bezout" para los enteros $a = 507885$ y $b = 60808$.

(71) Comprobar que $a = 6003722857$ y $n = 77695236973$ son primos entre sí, y obtener el inverso de a módulo n.

(72) Obtener un generador del ideal $(5, -1 + 8i)\mathbb{Z}[i]$.

(73) Obtener un generador para el ideal $(85, 1 + 13i)\mathbb{Z}[i]$, i.e., un m.c.d. para 85 y $1 + 13i$, por medio del Algoritmo de Euclides. Lo mismo para $(47 - 13i, 53 + 56i)\mathbb{Z}[i]$.

(74) Mostrar, en el anillo $\mathbb{Z}[X]$, un ideal primo $\mathfrak{p}$ no maximal y un ideal maximal $\mathfrak{m}$ tales que $\mathfrak{p} \subset \mathfrak{m}$ y $\mathbb{Z}[X]/\mathfrak{m} = \mathbb{F}_9$.

(75) Mostrar, razonadamente, en el anillo $\mathbb{Z}[X]$, un ideal primo no maximal $\mathfrak{p}$ y un ideal maximal $\mathfrak{m}$ tales que $\mathfrak{p} \subsetneq \mathfrak{m}$ y $\mathbb{Z}[X]/\mathfrak{m} \simeq \mathbb{F}_{121}$.

(76) Sean R un DFU, K su cuerpo de fracciones y $p(X) = a_0 + \cdots + a_n X^n \in R[X]$, con $a_n \neq 0$ un polinomio de grado positivo. Supongamos que $\frac{r}{s} \in K$ es una raíz de $p(X)$, siendo $\mathrm{mcd}\,(r, s) = 1$. Demostrar que $r \mid a_0$ y $s \mid a_n$.

(77) Sean R un DFU, K su cuerpo de fracciones. Sean $p(X) \in R[X]$, con $a_n \neq 0$ un polinomio de grado positivo y $a + bX \in R[X]$ un polinomio primitivo de grado 1. Demostrar que $a + bX \mid p(X)$ en $R[X]$ si, y sólo si, $-\frac{a}{b} \in K$ es raíz de $p(X)$.

(78) Sea $f(X) \in \mathbb{Z}[X]$. Demostrar que si $f(0)$ y $f(1)$ son impares, entonces $f(X)$ no tiene raíces enteras.

(79) Demostrar que si F es un cuerpo de característica nula y $p(X)$ un polinomio irreducible de $F[X]$, entonces $p(X)$ no tiene raíces múltiples.

(80) Hallar una identidad de Bezout para el máximo común divisor de los polinomios $X^4 + X^3 + 3X - 9, 2X^3 - X^2 + 6X - 3$ en $\mathbb{Q}[X]$.

(81) Demostrar que los siguientes ideales son primos.

a) $(X^5 - 12X^3 + 36X - 12)\mathbb{Z}[X]$.

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

c) $(X^4 - X^3 + X + 1)\mathbb{Z}[X]$.

d) $(a_0 + a_1X_1 + \cdots + a_nX_n)F[X_1, \ldots, X_n]$, siendo $a_i \neq 0$ para algún $i = 1, \ldots, n$ y F un cuerpo.

e) $(Y^4 + 3X^2Y + X^2 + 3Y + 1)\mathbb{R}[X, Y]$.

f) $(X^3Z + 2X^2Y + 2X^2Z + XY^2 + 2XYZ + XZ^2 + Y^2 - Z^2)\mathbb{R}[X, Y, Z]$.

(82) Estudiar la irreducibilidad en $\mathbb{Z}[X], \mathbb{Q}[X]$ de los polinomios

a) $X^3 + 3X^2 + 3X + 9$.

b) $5X^{10} + 10X^7 + 20X^3 + 10$.

c) $X^3 + 5X^2 + 3X + 25$.

d) $5X^5 + 5X^4 + 10X^3 + 25X^2 + 15X + 1$.

e) $5X^5 + 5X^4 + 10X^3 - 15X + 1$.

f) $2X^4 - 8X + 1$.

g) $X^4 + 2013X + 1234567$.

h) $X^n + 22$ con $n \geq 2$.

i) $X^7 + 14X^5 + 7X^2 + 4$.

j) $3X^5 - 5X^4 + 15X^3 + 5X + 16$.

k) $2X^{13} - 13X^4 + 13X + 37$.

l) $14X^{11} - 21X^5 + 28X^2 - 5$.

(83) Demostrar que $X^3 + 2X^2 + 1$ es irreducible en $\mathbb{Z}_3[X], \mathbb{Z}[X]$ y es reducible en $\mathbb{Z}_{17[X]}$.

(84) Probar que los siguientes polinomios son irreducibles en $\mathbb{Z}[X]$.

a) $x^6 + 30x^5 - 15x^3 + 6x - 120$.

b) $x^4 + 4x^3 + 6x^2 + 2x + 1$ (sustituir x por $x - 1$).

c) $\frac{(X+2)^p - 2^p}{X}$, donde p es un primo impar.

d) $(X-1)(X-2)\cdots(X-n) - 1$, donde $n \geq 1$. (Si el polinomio factoriza considerar los valores de los factores en $X = 1, 2, \ldots, n$)

e) $(X-1)(X-2)\cdots(X-n) + 1$, donde $n \geq 1$ y $n \neq 4$. (Difícil)

f) $X^{p-1} + X^{p-2} + \cdots + X + 1$, donde p es primo.

(85) Demostrar que $R = \mathbb{C}[X, Y]/(Y^2 - X^3)$ dominio de integridad pero no es DFU (Indicación: Identificar R con el subanillo de $\mathbb{C}[T]$ generado por T^2, T^3 y probar que $x = \bar{X}$ e $y = \bar{Y}$ son irreducibles en R pero no primos).

(86) Decidir si $\mathbb{R}[X, Y]/(Y - X^5)$ es DE, DIP, DFU y calcular sus unidades.

(87) Factorizar $X^n - 1$ en producto de irreducibles en $\mathbb{Q}[X]$ para $n \leq 10$.

(88) Sean $\mathbb{R}[T]$ y $\mathbb{R}[X, Y]$ los anillos de polinomios con coeficientes en $\mathbb{R}$ en una y dos variables respectivamente. Consideramos el siguiente homomorfismo de anillos

$$\begin{array}{ccc} \mathbb{R}[X, Y] & \xrightarrow{\varphi} & \mathbb{R}[T] \\ p(X, Y) & \mapsto & p(T^2, T^5) \end{array}$$

a) Decidir si φ es sobreyectivo.

b) Demostrar que $I = (X^5 - Y^2)$ es el núcleo de φ.

c) Decidir si I es primo. Decidir si I es maximal.

(89) Sea $\mathbb{Z}[X, Y]$ el anillo de polinomios con coeficientes en $\mathbb{Z}$ en dos variables. Consideramos el siguiente homomorfismo de anillos

$$\begin{array}{ccc} \mathbb{Z}[X, Y] & \xrightarrow{F} & \mathbb{C} \\ p(X, Y) & \longmapsto & p(-i, 3) \end{array}$$

a) Demostrar que la imagen de F es $\mathbb{Z}[i]$.

b) Calcular el núcleo de F. (Indicación: el núcleo de F se puede generar con dos elementos).

c) ¿Es el núcleo de F maximal? Si el homomorfismo F partiera de $\mathbb{Q}[X, Y]$, ¿sería el núcleo de F maximal? Razonar la respuesta.

(90) Consideramos el anillo $R = \mathbb{R}[X, Y, Z]$ de polinomios en tres indeterminadas con coeficientes en $\mathbb{R}$ y el ideal $P = (Y + Z^2, Z - X^2)$.

a) Estudiar razonadamente si P es un ideal primo. Determinar un ideal maximal que contenga a P. ¿Cuál es el ideal $P \cap \mathbb{R}[Y, Z]$?

b) Consideramos el anillo $A = R/Q$, donde $Q = (Y + Z^2 + Y^2Z - X^2Y^2)R$. Sean $x = \bar{X}, z = \bar{Z} \in A$. Probar que A es un dominio de integridad y que $z - x^2$ es un elemento primo en A.

(91) Sean $R = \mathbb{R}[X, Y, Z]/(Y - X^2)$, y $x = \bar{X}, y = \bar{Y}, z = \bar{Z} \in R$.

a) Decidir, razonadamente, si el ideal $(xy - z)R$ es primo o maximal.

b) Obtener, razonadamente, el radical del ideal $(y, z)R$.

(92) Consideramos el ideal $I = (X^2 + X + 1,\ Y + X + Z + 1)$ en el anillo $R = \mathbb{Q}[X, Y, Z]$.

a) Estudiar, de forma razonada, si I es primo o maximal en R.

b) Determinar, de forma razonada, un ideal maximal M de R tal que $I \subset M$. ¿Cuál es la dimensión sobre $\mathbb{Q}$ del cuerpo R/M?

(93) Consideramos el ideal $I = (X^2 + X + 1, Y + X + Z + 1)$ en el anillo $R = \mathbb{R}[X, Y, Z]$. Estudiar, de forma razonada, si I es primo o maximal en R. Determinar, de forma razonada, un ideal maximal M de R tal que $I \subset M$.

(94) Sea $R = \mathbb{R}[X, Y, Z]/(X + Z^2 + Z + 1)$, y $x, y, z \in R$ las clases de X, Y, Z.

a) Demostrar que el ideal $(x + y - z^3)R$ es primo pero no maximal.

b) Sea $I = ((X+Z^2+Z+1)^2, X+Y-Z^3, (X+Z^2+Z+1)(X+Y)^4)\mathbb{R}[X, Y, Z]$. Calcular $\mathrm{rad}(I)$ y obtener un ideal maximal que lo contiene.

(95) Consideramos el ideal $P = (X - 4Z - 3, Y + 2Z + 1)\mathbb{R}[X, Y, Z]$.

a) Probar que $P \cap \mathbb{R}[X, Y] = (X + 2Y - 1)\mathbb{R}[X, Y]$.

b) Probar que P es primo pero no maximal, y hallar un ideal maximal que lo contiene.

(96) Sean $R = \mathbb{R}[X, Y, Z]/(Z - X + X^3)$ y $x, y \in R$ las clases de $X, Y \in \mathbb{R}[X, Y, Z]$. Demostrar que $x + y$ es irreducible en R.

(97) Consideramos el ideal $I = (7, X^2 + 1, Y + X + Z + 1)$ en el anillo $R = \mathbb{Z}[X, Y, Z]$. Estudiar, de forma razonada, si I es primo o maximal en R. Determinar, de forma razonada, un ideal maximal M de R tal que $I \subset M$.

Capítulo 2

Grupos

2.1. Definición y propiedades

Definición 2.1.1. Un grupo G es un conjunto no vacío junto con una operación binaria $G \times G \to G,\ (a,b) \mapsto ab$ que satisface los siguientes axiomas:

(1) $(ab)c = a(bc)$, para todo $a, b, c \in G$, i.e. la operación es asociativa,

(2) existe un elemento $1 \in G$, que llamamos identidad, tal que $a1 = 1a = a$ para todo $a \in G$,

(3) para cada elemento $a \in G$ existe un elemento $a^{-1} \in G$, que denominamos inverso de a, que verifica $aa^{-1} = a^{-1}a = 1$.

El grupo se dice conmutativo (o abeliano) si $ab = ba$ para todo $a, b \in G$. En un grupo conmutativo denotaremos, habitualmente, la operación por la suma $+$, el elemento neutro por 0 y el inverso de a por el opuesto $-a$.

Ejemplos 2.1.2.

(1) Grupos conmutativos: $(\mathbb{Z}, +), (\mathbb{Z}_n, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q} - \{0\}, \cdot), (\mathbb{R} - \{0\}, \cdot), (\mathbb{C} - \{0\}, \cdot)$.

(2) Sea R un anillo unitario. El conjunto de las unidades $(R^*, \cdot)$ es un grupo.

(3) Sea R un anillo conmutativo y unitario. El conjunto $\mathrm{GL}_n(R)$ de las matrices de $\mathscr{M}_n(R)$ cuyo determinante es una unidad de R con el producto de matrices es un grupo (en general, no conmutativo).

(4) Grupo de las permutaciones o grupo simétrico. Sea X un conjunto no vacío. El conjunto $S_X = \{\sigma : X \to X | \sigma \text{ biyectiva}\}$ con la composición es un grupo (en general no conmutativo).

(5) Sea $X = \{1, \ldots, n\}$. Denotaremos $S_n = S_X$. Denotaremos $\sigma \in S_n$ en la forma

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}, \sigma(i) = a_i \in \{1, 2, \ldots, n\}, i = 1, \ldots, n.$$

(6) Grupo diédrico del cuadrado D_4 formado por las isometrías del plano que dejan fijo un cuadrado de centro O. Si σ es la rotación de centro O y ángulo $\frac{\pi}{2}$ y τ una simetría respecto uno de los ejes de simetría del cuadrado, entonces:

$$D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}, \sigma^4 = 1, \tau^2 = 1, \tau\sigma^i = \sigma^{4-i}\tau.$$

Observación 2.1.3. Sean G un grupo y $a, b, c \in G$.

(1) El elemento identidad es único.

(2) Para cada a el inverso a^{-1} es único.

(3) $(a^{-1})^{-1} = a$.

(4) $(ab)^{-1} = b^{-1}a^{-1}$.

(5) $ac = bc \Rightarrow a = b, ca = cb \Rightarrow a = b$.

(6) para cualesquiera $a_1, \ldots, a_n \in G$ el elemento $a_1 \cdots a_n$ es independiente de cómo estén colocados los paréntesis en la expresión (propiedad asociativa generalizada).

Observación 2.1.4. Definimos las potencias de $a \in G$, para exponentes $n \in \mathbb{Z}$, en la forma: $a^0 = 1$, $a^n = a \cdot a^{n-1}$ si $n \geq 1$ y $a^n = (a^{-1})^{-n}$ si $n \leq -1$. Se verifican las propiedades habituales:

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

(2) $(a^m)^n = a^{mn}$.

(3) $(ab)^m = abab\overset{m}{\cdots}ab$.

(4) $(ab)^2 = a^2b^2 \Leftrightarrow ab = ba \Leftrightarrow (ab)^m = a^m b^m$ para todo $m \in \mathbb{Z}$.

Definición 2.1.5. Diremos que un grupo G es finito si su número de elementos es finito. Si G tiene n elementos diremos que G es un grupo de orden n y denotaremos $|G| = n$. Si G tiene una cantidad infinta de elementos, diremos que es de orden infinito.

Ejemplos 2.1.6.

(1) $(\mathbb{Z}_n, +)$ es finito de orden $|\mathbb{Z}_n| = n$.

(2) S_n es finito de orden $|S_n| = n!$.

Definición 2.1.7. Sea G un grupo. Un subgrupo, denotado $H \leq G$, es un subconjunto no vacío $H \subset G$ tal que si $a, b \in H$, son cualesquiera elementos de H, entonces $ab \in H$ y $a^{-1} \in H$. Es decir la operación en G hace de H un grupo. De forma equivalente, $H \neq \emptyset$ y para todo $a, b \in H, ab^{-1} \in H$.

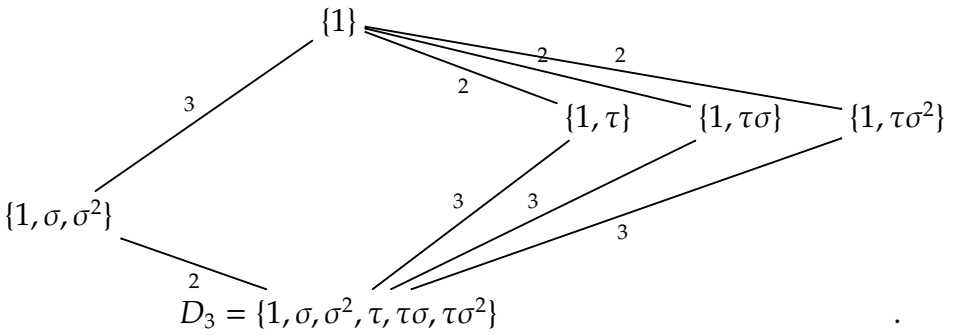
Observación 2.1.8. El trivial $\{1\} \leq G$ y el total $G \leq G$ son subgrupos de G. Si $H \leq G$ y $H \neq \{1\}, H \neq G$, diremos que H es un subgrupo propio de G.

Observación 2.1.9. Sean $H \subset G$ un subconjunto no vacío finito de G. Entonces $H \leq G$ si, y sólo si, $1 \in H$ y para todo $a, b \in H$ se verifica $ab \in H$.

Demostración. Sólo hay que probar que para cada $a \in H$ el inverso $a^{-1} \in H$. Sea $a \in H$, las aplicaciones $H \to H, b \mapsto ab, b \mapsto ba$ son inyectivas. Por tanto, puesto que H es finito, también son sobreyectivas. En consecuencia, existen $b \in H$ tales que $ab = 1, ca = 1$. Así, $b = b1 = bac = 1c = c$ y $a^{-1} = b = c \in H$. □

Ejemplos 2.1.10. (1) Los subgrupos $\mathbb{Z}$ son los subconjuntos de la forma $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$. En efecto, es claro que cada subconjunto de esa forma es subgrupo. Recíprocamente, sea $H \leq \mathbb{Z}$. Si $H = \{0\} = 0\mathbb{Z}$. Si $H \neq \{0\}$, entonces H contiene elementos positivos. Sea $d = \text{mín}\{x \in H \mid x \geq 1\}$. Entonces $d\mathbb{Z} \subset H$. Recíprocamente, si $x \in H$ dividimos $x = dq + r$ con $0 \leq r < d$. Puesto que $r = x - dq \in H$ ha de ser $r = 0$. Así $x \in d\mathbb{Z}$.

(2) Los subgrupos de $D_3 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ son



.

Observación 2.1.11. (1) La intersección $\cap_{i \in I} H_i$ de un familia cualquiera de subgrupos de G es un subgrupo.

(2) La unión de subgrupos no es, en general, subgrupo: $2\mathbb{Z} \cup 3\mathbb{Z}$ no es subgrpuo de $\mathbb{Z}$.

(3) El producto $HK = \{hk \mid h \in H, k \in K\}$ no es, en genreral, subgrupo. Daremos condiciones para que HK sea subgrupo. En D_4 el producto $\{1, \tau\sigma\}\{1, \tau\} = \{1, \tau\sigma, \tau, \tau\sigma\tau\}$, no es subgrupo, puesto que $\tau\tau\sigma = \sigma$ no pertenece al conjunto.

Observación 2.1.12. Sea $\emptyset \neq A \subset G$.

(1) El centralizador de A en G es el subgrupo

$$C_G(A) = \{g \in G \mid ga = ag, \text{ para todo } a \in A\}.$$

(2) El centro de G es $Z(G) = C_G(G) = \{g \in G \mid gx = xg, \text{ para todo } x \in G\}$.

(3) El normalizador de A en G es el subgrupo

$$N_G(A) = \{g \in G \mid gA = Ag\}.$$

(4) $C_G(A) \leq N_G(A)$.

Observación 2.1.13. Sea $\emptyset \neq A \subset G$. El subgrupo $< A > \leq G$ generado por un subconjunto $A \subset G$ es la intersección de todos los subgrupos de G que contienen a A. Es el menor subgrupo de G que contiene a A. Este subgrupo se puede describir como

$$< A >= \{a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} \mid n \in \mathbb{Z}, n \geq 0 \text{ and } a_i \in A, \epsilon_i = \pm 1 \text{ para cada } i\}.$$

Si $< A >= G$ diremos que A es un conjunto de generadores de G y si $G =< a_1, \ldots, a_n >$ diremos que G es finitamente generado.

Ejemplo 2.1.14. (1) Grupos diedrales (en general)

El grupo de movimientos (rotaciones y simetrías) en el plano que dejan invariante un polígono regular de $n \geq 3$ lados es el grupo diedro denotado D_n (o bien D_{2n} en algunos textos). Numerando los vértices del polígono $1, \ldots, n$, cada movimiento que lo deja invariante se identifica con cierta permutación de n elementos. Si denotamos σ la rotación de amplitud $\frac{2\pi}{n}$ respecto del centro del polígono, i.e. el n–ciclo $(1 \cdots n)$, y por τ la simetría respecto de la recta que pasa por el vértice 1 y el centro del polígono, i.e. la permutación $\begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix}$, entonces el grupo es

$$D_n = \{1, \sigma, \cdots, \sigma^{n-1}, \tau, \tau\sigma, \cdots, \tau\sigma^{n-1}\},$$

donde σ^i es la rotación de amplitud $2\pi i/n$ y $\tau\sigma^i$ es una simetría respecto de cada uno de los n ejes de simetría a través del centro del polígono, con las relaciones

$$\sigma^n = 1, \qquad \tau^2 = 1, \qquad \tau\sigma^i = \sigma^{n-i}\tau.$$

De hecho, dos generadores y tres relaciones determinan el grupo

$$D_n =< \sigma, \tau \mid \sigma^n = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} > .$$

En efecto, suponemos el polígono inscrito en la circunferencia de rado 1 en $\mathbb{R}^2$, y el vértice $1 = (a_0 = 1, b_0 = 0)$. Entonces $\sigma^r(1) = r + 1 = (a_r, b_r)$, donde $a_r = \cos\frac{2\pi r}{n}, b_r = \sin\frac{2\pi r}{n}$, para $0 \leq r < n$. En general, $\sigma^k(l) = j + 1$, donde $0 \leq j < n$ y $k + l - 1 = nq + j$.

Por otra parte, $\tau(r+1) = (a_r, -b_r) = n - r + 1$, puesto que $\frac{2(n-r)\pi}{n} = 2\pi - \frac{2r\pi}{n}$ y, por tanto, $a_{n-r} = a_r, b_{n-r} = -b_r$.

Los $2n$ elementos indicados son distintos: para $1 \leq i \neq j \leq n-1$ es claro que $\sigma^i \neq \sigma^j$ y $\tau\sigma^i \neq \tau\sigma^j$. Si $\tau\sigma^i = \sigma^j$, entonces $\tau = \sigma^{j-i}$ que no es posible.

Hay, a lo más, $2n$ transformaciones en D_n: sean $\rho \in D_n$ y $\rho(1) = k$. Hay n posibilidades para elegir k y, puesto que ρ conserva las distancias, $\rho(1)$ es un vértice consecutivo al vértice k, para lo que sólo hay dos opciones. Por tanto, como los vértices $1, 2$ son una base de $\mathbb{R}^2$ y las transformaciones son aplicaciones lineales hay, a lo más, $2n$ transformaciones.

(2) Grupo cuaternio.

Es el grupo $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ con el producto determinado por $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -jk = i, ki = -ik = j$, que resulta ser el grupo con dos generadores y relaciones

$$Q_8 =< i, j \mid i^4 = 1, i^2 = j^2, i^{-1}ji = j^{-1} > .$$

Observación 2.1.15. Un grupo H se dice cíclico si puede ser generado por un elemento $H =< x >= \{x^n \mid n \in \mathbb{Z}\}$. Un grupo cíclico es conmutativo. Todo subgrupo K de un grupo cíclico $H =< x >$ es cíclico $K =< x^d >$, generado por x^d, donde d es el menor entero positivo tal que $x^d \in K$, o bien $K = \{1\}$.

Proposición 2.1.16. *Sean G un grupo y $x \in G$.*

(1) Si $| < x > | = n < \infty$, entonces $< x >= \{1, x, \cdots, x^{n-1}\}$ y $x^m = 1$ si, y sólo si, $n \mid m$. En este caso $< x > \simeq \mathbb{Z}/n\mathbb{Z}$. Diremos que el orden de x es n, denotaremos $\operatorname{ord}(x) = n$. Además para $a \in \mathbb{Z} - 0$ el orden $\operatorname{ord}(x^a) = \frac{n}{\operatorname{mcd}(a,n)}$.

(2) Si $| < x > | = \infty$, entonces $x^n \neq 1$ para todo $n \neq 0$ y $x^r \neq x^s$ si $r \neq s$. En este caso $< x > \simeq \mathbb{Z}$. Diremos que x es de orden ∞, denotaremos $\operatorname{ord}(x) = \infty$. Además para $a \in \mathbb{Z} - 0$ el orden $\operatorname{ord}(x^a) = \infty$.

(3) Si $| < x > | = n < \infty$. Para cada $1 \leq a \mid n$ existe un único subgrupo de $< x >$ de orden a. Este subgrupo es $< x^{\frac{n}{a}} >$.

Demostración. Supongamos que $| < x > | = n < \infty$. Entonces existen $r > s \in \mathbb{Z}$ tales que $x^r = x^s$. Así $x^{r-s} = 1$ y $r - s > 1$. Sea $d = \min\{k > 1 \mid x^k = 1\}$. Entonces, $x^r \neq x^s$ si $1 \leq s < r < d$, puesto que $1 < r - s < d$ y, si $m = dq + r$ con $0 \leq r < d$, entonces $x^m = x^r$. Por tanto, $n = d$ y $x^m = 1 \Leftrightarrow d \mid m$.

Sean $a \neq 0, r = \frac{n}{\operatorname{mcd}(a,n)}$ y $k = \operatorname{ord}(x^a)$. Entonces $(x^a)^r = x^{\pm\operatorname{mcm}(a,n)} = 1$. Por tanto $k \mid r$. Recíprocamente, puesto que $(x^a)^k = 1$ se tiene que $n \mid ak$. Por tanto, $r \mid \frac{a}{\operatorname{mcd}(a,n)}k$. Puesto que $\operatorname{mcd}(r, \frac{a}{\operatorname{mcd}(a,n)}) = 1$, se deduce que $r \mid k$.

Sea $1 \leq a \mid n$. Entonces, $\operatorname{ord}(x^{\frac{n}{a}}) = \frac{n}{\operatorname{mcd}(\frac{n}{a},n)} = a$. Por tanto, $| < x^{\frac{n}{a}} > | = a$. Recíprocamente, si $\operatorname{ord}(x^r) = a$, entonces $\frac{n}{\operatorname{mcd}(r,n)} = a$. Por tanto, $\frac{n}{a} \mid r$. Así $< x^r > \subset < x^{\frac{n}{a}} >$ y, puesto que ambos subgrupos tienen orden a, son iguales. □

Proposición 2.1.17. *Sean G un grupo y $x, y \in G$.*

(1) $\mathrm{ord}(x) = 1 \Leftrightarrow x = 1$.

(2) $\mathrm{ord}(x) = \mathrm{ord}(x^{-1})$.

(3) $\mathrm{ord}(yxy^{-1}) = \mathrm{ord}(x)$.

(4) $\mathrm{ord}(xy) = \mathrm{ord}(yx)$.

(5) $\mathrm{ord}(x) = \infty \Leftrightarrow x^m \neq x^n$ *para todo* $m \neq n \in \mathbb{Z}$.

(6) $\mathrm{ord}(x) < \infty \Leftrightarrow x^m = x^n$ *para algún* $m \neq n \in \mathbb{Z} \Leftrightarrow x^k = 1$ *para algún* $k \in \mathbb{Z}$.

(7) Sea $1 < n < \infty$, *entonces* $\mathrm{ord}(x) = n \Leftrightarrow x^n = 1$ *y* $x^r \neq 1$ *para* $1 \leq r < n$. *Además* $x^k = 1 \Leftrightarrow n|k$.

(8) Si $\mathrm{ord}(x) = m < \infty, \mathrm{ord}(y) = n < \infty$ *y* $xy = yx$, *entonces* $\mathrm{ord}(xy) < \infty$ *y* $\mathrm{ord}(xy)|\mathrm{mcm}(m, n)$.

(9) Si $\mathrm{ord}(x) = m < \infty, \mathrm{ord}(y) = n < \infty$ *con* $\mathrm{mcd}(m, n) = 1$ *y* $xy = yx$, *entonces* $\mathrm{ord}(xy) = mn$.

(10) Si $\mathrm{ord}(x) = m < \infty$, *entonces* $\mathrm{ord}(x^a) = \frac{m}{\mathrm{mcd}(m,a)}$. *En particular, si* $a|m$, *entonces* $\mathrm{ord}(x^a) = \frac{m}{a}$

Demostración. Ejercicio. □

Clases de congruencia módulo un subgrupo

Proposición–Definición 2.1.18. (1) Dados un subgrupo $H \leq G$ y un elemento $x \in G$ denominaremos clase de congruencia módulo H a la derecha, resp. a la izquierda, de x, el conjunto $xH = \{xh \mid h \in H\}$, resp. $Hx = \{hx \mid h \in H\}$.

(2) Las relación $x \sim_H y \Leftrightarrow x^{-1}y \in H$ es de equivalencia y la clase de equivalencia de x es xH.

(3) Las relación $x_H\sim y \Leftrightarrow xy^{-1} \in H$ es de equivalencia y la clase de equivalencia de x es Hx.

(4) El conjunto cociente de clases a la izquierda, resp. clases a la derecha, es una partición de G que denotaremos G/H, resp. $H\backslash G$.

(5) La aplicación $H\backslash G \to G/H$ definida por $Hx \mapsto x^{-1}H$ está bien definida y es biyectiva.

(6) El cardinal común $|H\backslash G| = |G/H|$ es el índice de G en H denotado $[G : H]$.

Demostración. Ejercicio. □

Teorema 2.1.19 (Teorema de Lagrange)**.** *Sean G un grupo y $H \leq G$. Entonces G es finito si, y sólo si, $|H|$ y $[G : H]$ son finitos. En este caso,*

$$|G| = |H| \cdot [G : H].$$

En particular, si G es finito, entonces $|H|$ y $[G : H]$ son divisores de $|G|$.

Demostración. La implicación $\Rightarrow$ es evidente. Recíprocamente, si $|H| = s$ y $[G : H] = r$ son finitos, entonces $G = \cup_{i=1}^{r} x_i H$ es la unión disjunta de r clases de cardinal s. Por tanto, $|G| = sr$. □

Teorema 2.1.20. *Sean G un grupo y $K \leq H \leq G$ subgrupos. Entonces, $[G : K]$ es finito si, y sólo si, $[G : H]$ y $[H : K]$ son finitos. En este caso,*

$$[G : K] = [G : H][H : K].$$

Demostración. ($\Rightarrow$) Supongamos $[G : K] < \infty$, como $xK \subset xH$ y G es unión disjunta finita de clases modulo K, se deduce que $[G : H] < \infty$ y, como, $\{xK \mid x \in H\} \subset \{xK \mid x \in G\}$ se deduce que $[H : K] \leq [G : K] < \infty$.
($\Leftarrow$) Supongamos $[G : H] = r < \infty, [H : K] = s < \infty$, entonces $G = \cup_{i=1}^{r} g_i H, H = \cup_{j=1}^{s} h_j K$ (uniones disjuntas). De aquí se deduce $G = \cup_{i=1}^{r} \cup_{j=1}^{s} g_i h_j K$ es unión disjunta de clases. Por tanto $[G : K]$ es finito y $[G : K] = rs$. □

Corolario 2.1.21. *Sea G un grupo finito de orden $|G| = p$ primo. Entonces G es cíclico.*

Demostración. Sea $x \in G, x \neq 1$. Entonces $| < x > |$ es un divisor de $|G|$ distinto de 1. Por tanto, $| < x > | = p$ y $< x >= G$. □

Subgrupos normales

Proposición–Definición 2.1.22. Sean G un grupo y $N \leq G$.

(1) Las siguientes condiciones son equivalentes,

   a) $xN = Nx$, para todo $x \in G$,
   b) $xNx^{-1} = N$, para todo $x \in G$,
   c) $xNx^{-1} \subset N$, para todo $x \in G$.

   Si $N \leq G$ verifica estas condiciones diremos que N es un subgrupo normal de G, denotado $N \trianglelefteq G$.

(2) La operación en clases a la izquierda (resp. derecha) descrita por $(xN)(yN) = xyN$ (resp $(Nx)(Ny) = Nxy$) está bien definida y hace de G/N (resp. $N\backslash G$) un grupo si, y sólo si, $N \trianglelefteq G$. En este caso, los conjuntos $N\backslash G = G/N$ tienen estructura de grupo: el grupo cociente G/N. El elemento neutro de G/N es $1N = N$ y el inverso $(xN)^{-1} = x^{-1}N$.

Demostración. (1) $a) \Leftrightarrow b)$ y $b) \Rightarrow c)$ son obvias. Supongamos $c)$. Entonces $x^{-1}N(x^{-1})^{-1} \subset N$. Es decir $x^{-1}Nx \subset N$. De aquí $N \subset xNx^{-1}$.

(2) Si $N \trianglelefteq G$ y $x_1N = x_2N, y_1N = y_2N$, entonces $x_2^{-1}x_1 = n \in N, y_2^{-1}y_1 = m \in N$. Así $(x_2y_2)^{-1}x_1y_1 = y_2^{-1}x_2^{-1}x_1y_1 = y_2^{-1}ny_1$. Como $Ny_1 = y_1N$, se verifica $ny_1 = yr$ para algún $r \in N$. Así $y_2^{-1}ny_1 = y_2^{-1}y_1r = mr \in N$. Por tanto $(x_2y_2)^{-1}x_1y_1 \in N$, es decir $x_1y_1N = x_2y_2N$. □

Ejemplos 2.1.23. (1) Si G es conmutativo, entonces todo subgrupo es normal. El recíproco no es cierto. Un contraejemplo es el grupo cuaternio $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ (ejercicio).

(2) En $D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$, el subgrupo $H = \{1, \tau\}$ no es normal en D_4. En efecto, $\sigma H = \{\sigma, \sigma\tau\}$ y $H\sigma = \{\sigma, \tau\sigma\}$ son distintos, puesto que $\sigma\tau = \tau\sigma^3 \neq \sigma, \tau\sigma$. El subgrupo $N =< \sigma >= \{1, \sigma, \sigma^2, \sigma^3\}$ es normal, puesto que $D_4 =< \sigma, \tau >$ y $\tau\sigma\tau = \sigma^3 \in <\sigma >$.

(3) El cociente $D_4/ < \sigma >$ es un grupo con dos elementos. Por tanto, es isomorfo a $\mathbb{Z}_2$ y es conmutativo.

(4) Si $N \leq G$ y $[G : N] = 2$, entonces $N \trianglelefteq G$. En efecto, sea $a \in G - H$, entonces $G = H \cup aH = H \cup Ha$, uniones disjuntas, y $aH \neq H \neq Ha$. Por tanto $aH = Ha$, esto es, H es normal en G.

(5) Ser normal no es transitivo: $\{1, \tau\} \trianglelefteq \{1, \tau\sigma, \sigma^2, \tau\sigma^3\} \trianglelefteq D_4$ y $\{1, \tau\}$ no es normal en G.

Proposición 2.1.24. *Sean G un grupo y $K \leq G$.*

(1) Si $G =< g_1, \ldots, g_s >$ es finitamente generado, entonces $K \trianglelefteq G$ si, y sólo si, $g_i^{-1}Kg_i \subset K$ y $g_iKg_i^{-1} \subset K$, para todo $i = 1, \ldots, s$.

(2) Si $K =< k_1, \ldots, k_r >$ es finitamente generado, entonces $K \trianglelefteq G$ si, y sólo si, $gk_ig^{-1} \in K$, para todo $g \in G$ y todo $i = 1, \ldots, r$.

Demostración. Ejercicio. □

Definición 2.1.25. Un grupo G se dice simple si sus únicos subgrupos normales son $\{1\}, G$.

Ejemplo 2.1.26. Veremos que A_5, el subgrupo de las permutaciones pares de S_5, es simple.

Ejemplo 2.1.27 (Los grupos de orden ≤ 8)**.** Sea G un grupo finito de orden $|G| = 2, 3, 4, 5, 6, 7, 8$.

(1) Si $|G| = 2, 3, 5, 7$, entonces G es cíclico y, por tanto, isomorfo a $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$.

(2) Supongamos $|G| = 4$. Sea $x \in G, x \neq 1$. Entonces $\text{ord}(x) = 2, 4$. Si existe $x \in G$ de orden 4, entonces $G \simeq \mathbb{Z}_4$ es cíclico. En caso contrario, $G = \{1, a, b, c\}$, donde a, b, c tienen orden 2. Así $a^{-1} = a, b^{-1} = b, c^{-1} = c$. Además, $ab = c$, puesto que si $ab = a, b$, entonces $b = 1, a = 1$. Por otra parte, $abab = 1 \Rightarrow ababb = b \Rightarrow aaba = ab \Rightarrow ba = ab$, y G es conmutativo. En este caso, $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

(3) Supongamos $|G| = 6$. Si existe $x \in G$ de orden 6, entonces $G \simeq \mathbb{Z}_6$. En otro caso, supongamos que existe $a \in G$ de orden 3 y no hay elementos de orden 6. Entonces $< a >= \{1, a, a^2\}$ es de índice 2 y, por tanto, es normal en G. El cociente $G/ < a >=< a > \cup b < a >$, donde $b \notin < a >$. Así $G = \{1, a, a^2, b, ba, ba^2\}$. Veamos qué elementos son b^2 y ab. Si $b^2 = a$ o $b^2 = a^2$, entonces el orden de b es 6, que no es posible. Si $b^2 = b \Rightarrow b = 1$, falso. Si $b^2 = ba \Rightarrow b = a$, falso. Si $b^2 = ba^2 \Rightarrow b = a^2$, falso. Por tanto, $b^2 = 1$. Veamos ab. Como $b \notin < a >$ es $ab \neq 1$. Si $ab = a \Rightarrow b = 1$, falso. Si $ab = a^2 \Rightarrow b = a$, falso. Si $ab = b \Rightarrow a = 1$, falso. Si $ab = ba$, entonces el orden de ab es 6, que no es posible. Por tanto, $ab = ba^2$. En este caso, $G \simeq D_3$, que no es conmutativo. Observemos que $S_3 \simeq D_3$. Supongamos que todos los elementos de G, distintos de 1, tienen orden 2. Entonces G es conmutativo y no puede tener 6 elementos: contendría $\{1, a, b, ab, c, d\}$ y falatría d. Por tanto, los grupos de orden 6 son $\mathbb{Z}_6, D_3$.

(4) Supongamos $|G| = 8$. Si existe $x \in G$ de orden 8, entonces $G \simeq \mathbb{Z}_8$. Supongamos que existe $a \in G$ de orden 4 y no hay elementos de orden 8, entonces $< a >$ es normal en G por ser de índice 2. Por tanto $G =< a > \cup b < a >$ cob $b \notin < a >$. Así $G = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$. Razonando como en el caso de orden 6, se prueba que hay dos casos: (a) $ab = ba$, (b) $ab = ba^3$. Caso (a) $ab = ba$, G es conmutativo y $b^2 = 1$ o $b^2 = a^2$. Si $b^2 = 1$, entonces $G = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$. Si $b^2 = a^2$ entonces $(ba)^2 = 1$. Cambiando b por ba, es $G = \{1, a, a^2, a^3, ba, baa, baa^2, baa^3\} = \{1, a, a^2, a^3, ba, ba^2, ba^3, b\}$ y en los dos subcasos $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$. Caso (b) $ab = ba^3$. Si $b^2 = 1$, entonces $G \simeq D_4$. Si $b^2 = a^2$, entonces el orden de b es 4 y $G \simeq Q_8$, el grupo cuaternio

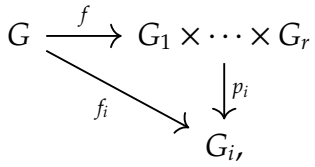
$$Q_8 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}.$$

Finalmente, si todos los elementos distintos de 1 tienen orden 2, entonces G es conmutativo y $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Producto directo de grupos

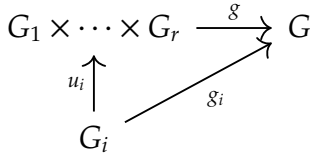
Definición 2.1.28. Sean $G_1, \ldots, G_r$ grupos. El grupo producto directo es $G_1 \times \cdots \times G_r$ con la operación $(a_1, \ldots, a_r)(b_1, \ldots, b_r) = (a_1 b_1, \ldots, a_r b_r)$. El neutro es $(1, \ldots, 1)$ y el inverso $(a_1, \ldots, a_r)^{-1} = (a_1^{-1}, \ldots, a_r^{-1})$. Si todos los grupos son conmutativos, también se usa la notación de suma directa $G_1 \oplus \cdots \oplus G_r$.

Proposición 2.1.29. *Sean $G, G_1, \ldots, G_r$ grupos y $f_i : G \to G_i$ homomorfismos. La aplicación $f = (f_1, \ldots, f_r) : G \to G_1 \times \ldots \times G_r$, definida por $f(a) = (f_1(a), \ldots, f_r(a))$ es el único homomorfismo de grupos que hace conmutativos los diagramas*



donde $p_i(a_1, \ldots, a_r) = a_i$ es la proyección i–ésima-

Proposición 2.1.30. *Sean $G, G_1, \ldots, G_r$ grupos, G conmutativo, y $g_i : G_i \to G$ homomorfismos. La aplicación $g : G_1 \times \ldots \times G_r \to G$, definida por $g(a_1, \ldots, a_r) = g_1(a) \cdots g_r(a)$ es el único homomorfismo de grupos que hace conmutativos los diagramas*



donde $u_i(a) = (1, \ldots, a, \ldots, 1)$ es la inclusión i–ésima-

Proposición 2.1.31. *Sean $G_1 =< a_1 >, \ldots, G_r =< a_r >$ grupos cíclicos de órdenes n_i. El grupo $G_1 \times \ldots \times G_r$ es cíclico si, y sólo si, los órdenes n_i de los G_i son primos entre sí, dos a dos. En este caso, $G_1 \times \ldots \times G_r =< (a_1, \ldots, a_r) >$.*

Demostración. Sean $i \neq j$. Puesto que los elementos $(1, \ldots, a_i, \ldots, 1), (1, \ldots, a_j, \ldots, 1)$ conmutan, el orden de su producto es $\text{mcm}(n_i, n_j)$. Se deduce que el orden de $(a_1, \ldots, a_r)$ es $\text{mcm}(n_1, \ldots, n_r)$. Entonces el orden de $(a_1, \ldots, a_r)$ coincide con el orden $n_1 \cdots n_r$ de $G_1 \times \ldots \times G_r$ si, y sólo si, los n_i son primos entre sí, dos a dos. □

Producto directo interno de grupos

Proposición 2.1.32. *Sean G un grupo y $H, K \leq G$.*

(1) La aplicación $\varphi : H \times K \to G$, definida por $(h, k) \mapsto hk$ es un homomorfismo si, y sólo si, $hk = kh$ para todo $h \in H, k \in K$.

(2) φ es sobreyectiva si, y sólo si, $HK = G$, donde $HK = \{hk \mid h \in H, k \in K\}$.

(3) $\ker \varphi = \{(a, a^{-1}) \mid a \in H \cap K\}$.

(4) $\ker \varphi = \{1\}$ si, y sólo si, $H \cap K = \{1\}$.

Demostración. Ejercicio. □

Definición 2.1.33. Sean G un grupo y $H, K \leq G$. Diremos que G es producto directo interno de H, K si $\varphi : H \times K \to G, \varphi(h,k) = hk$, es un isomorfismo.

Proposición 2.1.34. *Sean G un grupo y $H, K \leq G$. Entonces G es producto directo interno de H, K si, y sólo si, se verifican las condiciones:*

(1) $hk = kh$ para todo $h \in H, k \in K$.

(2) $H \cap K = \{1\}$.

(3) $G = HK$.

En este caso, todo $g \in G$ se escribe $g = hk$ de modo único con $h \in H, k \in K$.

Ejemplos 2.1.35. (1) Sean $H = \{0, 2, 4\}, K = \{0, 3\} \leq \mathbb{Z}_6$. Entonces $H+K = \mathbb{Z}_6, H \cap K = \{0\}$ y los elementos conmutan. Por tanto, $\mathbb{Z}_6 \simeq H \oplus K$ es el producto directo interno de $H \simeq \mathbb{Z}_3, K \simeq \mathbb{Z}_2$.

(2) En D_4, sean $H =< \sigma >, K = \{1, \sigma^2, \tau, \tau\sigma^2\}$. Se verifica $HK = D_4$, pero $\sigma\tau \neq \tau\sigma$ y $H \cap K = \{1, \sigma^2\}$. Por tanto, D_4 no es producto directo interno de H, K.

(3) En D_6, sean $H = \{1, \sigma^3\}, K = \{1, \sigma^2, \sigma^4, \tau, \tau\sigma^2, \tau\sigma^4\}$. Entonces $D_6 = HK, H \cap K = \{1\}$ y los elementos de H conmutan con los de K. Por tanto G es producto directo interno de H, K. Así $G \simeq H \times K \simeq \mathbb{Z}_2 \times D_3$.

Proposición 2.1.36. *Sean $H \trianglelefteq G, K \trianglelefteq G$. Si $H \cap K = \{1\}$, entonces los elementos de H conmutan con los de K.*

Demostración. Sean $h \in H, k \in K$. Entonces $hkh^{-1} \in H, kh^{-1}k^{-1} \in H$. Por tanto, $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K = \{1\}$. Así $hk = kh$. □

Definición 2.1.37. Diremos que un grupo G es producto directo interno de los subgrupos $h_1, \ldots, H_r$ si la aplicación $\varphi : H_1 \times \cdots \times H_r \to G, \varphi(h_1, \ldots, h_r) = h_1 \cdots h_r$ es un homomorfismo biyectivo.

Proposición 2.1.38. *Sean $H_1, \ldots, H_r \leq G$ y $\varphi : H_1 \times \cdots \times H_r \to G, \varphi(h_1, \ldots, h_r) = h_1 \cdots h_r$.*

(1) φ es homomorfismo si, y sólo si, $h_i h_j = h_j h_i$ para todo $h_i \in H_i, h_j \in H_j$.

(2) φ es suprayectivo si, y sólo si, $H_1 \cdots H_r = G$.

(3) Si φ es homomorfismo, entonces φ es inyectivo si, y sólo si, $H_j \cap (H_1 \cdots H_{j-1} = \{1\})$.

Demostración. Ejercicio. □

Proposición–Definición 2.1.39. Sean G un grupo y $H, K \leq G$ subgrupos.

(1) Definimos el subconjunto de $HK = \{hk \mid h \in H, k \in K\}$.

(2) Si H, K son subgrupos finitos, entonces

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

(3) $H \cap K = \{1\}$ si, y sólo si, la expresión hk de cada elemento de HK es única.

(4) $HK \leq G$ si, y sólo si, $HK = KH$.

(5) Si $H \leq N_G(K)$ (i.e. $kH = Hk$ para todo $k \in K$), entonces HK es un subgrupo de G. En particular, si $K \trianglelefteq G$, entonces $HK \leq G$ para todo $H \leq G$.

(6) Si $H \trianglelefteq G$, $K \trianglelefteq G$, entonces $HK \trianglelefteq G$.

(7) Si $H \trianglelefteq G$, $K \trianglelefteq G$ y $H \cap K = \{1\}$, entonces HK es un subgrupo, los elementos de H conmutan con los de K y, por tanto, la aplicación natural $H \times K \to HK$ definida por $(h, k) \mapsto hk$ es un homomorfismo de grupos, que es además biyectivo. Diremos que HK es el producto directo interno de los subgrupos normales H y K.

(8) Si G es finito, $H \trianglelefteq G$, $K \trianglelefteq G$, $H \cap K = \{1\}$ y $|G| = |H| \cdot |K|$, entonces $G \simeq H \times K$.

Demostración. (2) El número de elementos de HK es el número de clases de equivalencia en $H \times K$ por la relación $(h, k) \sim (h_1, k_1) \Leftrightarrow hk = h_1k_1$. Puesto que $hk = h_1k_1 \Leftrightarrow h_1^{-1}h = k_1k^{-1}$ y este último es un elemento de $H \cap K$, es claro que la clase de equivalencia de (h, k) es el conjunto $\{(hu^{-1}, uk) | u \in H \cap K\}$. Este conjunto es biyectivo con $H \cap K$. De aquí la fórmula.
(4) ($\Rightarrow$) Dado $hk \in HK$, el inverso $k^{-1}h^{-1} = h_1k_1$ para ciertos $h_1 \in H, k_1 \in K$. Así $hk = k_1^{-1}h_1^{-1} \in KH$. Dado $kh \in KH$, el inverso $h^{-1}k^{-1} \in HK$. Por tanto, el inverso del inverso, $kh \in HK$.
($\Leftarrow$) Dados $hk, h_1k_1 \in HK$, existen h_2, k_2 tales que $kh_1 = h_2k_2$. Así $hkh_1k_1 = hh_2k_2k_1 \in HK$. Dado $hk \in HK$ existen h_1, k_1 tales que $hk = k_1h_1$. Entonces $(hk)^{-1} = h_1^{-1}k_1^{-1} \in HK$.
(6) Sólo hay que probar que el subgrupo HK es normal en G. Sean $x \in G, h \in H, k \in K$. Entonces $xhkx^{-1} = xk_1x^{-1}xh_1x^{-1} \in KH = HK$.

□

Teoremas de isomorfía

Definición 2.1.40. Sean G y H dos grupos. Un homomorfismo $f : G \to H$ es una aplicación tal que $f(xy) = f(x)f(y)$ para todo $x, y \in G$.

Definición 2.1.41. Un homomorfismo inyectivo, sobreyectivo, biyectivo, se denomina monomorfismo, epimorfismo, isomorfismo.

Observación 2.1.42. (1) La composición de homomorfismos es homomorfismo.

(2) Si $f : G \to H$ es ismorfismo, entonces la aplicación inversa $f^{-1} : H \to G$ es homomorfismo (biyectivo).

Observación 2.1.43. Sea $G \xrightarrow{f} H$ un homomorfismo de grupos.

(1) $f(1_G) = 1_H$.

(2) $f(x^{-1}) = f(x)^{-1}$.

(3) $f(x^n) = f(x)^n$, para todo $n \in \mathbb{Z}$.

(4) El núcleo de f es el subgrupo normal de G definido por $\ker f = \{x \in G \mid f(x) = 1\}$.

(5) La imagen $\operatorname{im} f$ es un subgrupo de H.

(6) Un subgrupo $N \leq G$ es normal si, y sólo si, es el núcleo de algún homomorfismo $G \xrightarrow{f} H$.

Demostración. Ejercicio. □

Ejemplos 2.1.44. (1) La inclusión $i : H \hookrightarrow G$, de un subgrupo $H \leq G$, es un monomorfismo.

(2) La aplicación natural $p : G \to G/N$ definida por $x \mapsto xN$, donde $N \trianglelefteq G$, es un epimorfismo cuyo núcleo es N.

(3) La aplicación $(\mathbb{R}, +) \to (\mathbb{C} - \{0\}, \cdot)$ definida por $x \mapsto \exp(2\pi i x)$ es un homomorfimso cuyo núcleo es el subgrupo $(\mathbb{Z}, +)$ y cuya imagen es el subgrupo $(S^1 = \{z \in \mathbb{C} \mid |z| = 1\}, \cdot)$. La aplicación inducida $(\mathbb{R}/\mathbb{Z}, +) \to (S^1, \cdot)$ es un isomorfismo.

Proposición 2.1.45. *Un homomorfismo $f : G \to H$ de grupos es inyectivo si, y sólo si,* $\ker f = \{1\}$.

Demostración. ($\Rightarrow$) Si $f(x) = 1$, entonces $f(x) = f(1)$. Por tanto $x = 1$
($\Leftarrow$) Sean $x, y \in G$. Entonces $f(x) = f(y) \Leftrightarrow 1 = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \Leftrightarrow xy^{-1} \in \ker f = \{1\} \Rightarrow x = y$. □

Teorema 2.1.46 (Primer Teorema de isomorfía)**.** *Sea $f : G \to H$ un homomorfismo de grupos. Existe un único homomorfismo $\overline{f} : G/\ker f \to \operatorname{im} f$, definido por $\overline{g} \mapsto f(g)$, tal que el diagrama*

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & H \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ G/\ker f & \xrightarrow{\quad \overline{f} \quad} & \operatorname{im} f \end{array}$$

es conmutativo. El homomorfismo $\overline{f}$ es un isomorfismo.

Demostración. $f(x) = f(y) \Leftrightarrow 1 = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \Leftrightarrow xy^{-1} \in \ker f \Leftrightarrow p(x) = p(y)$. □

Teorema 2.1.47 (Teorema de la correspondencia)**.** *Sean G un grupo y $N \trianglelefteq G$. Existe una biyección*

$$\{H \leq G \mid N \leq H\} \longleftrightarrow \{\overline{H} \leq G/N\},$$

definida por $H \mapsto H/N$. Además, si $N \leq H$, entonces $H \trianglelefteq G \Leftrightarrow H/N \trianglelefteq G/N$.

Demostración. Ejercicio. □

Teorema 2.1.48 (Segundo Teorema de isomorfía)**.** *Sean G un grupo y $H \trianglelefteq G, K \trianglelefteq G$ tales que $K \leq H$. Entonces $H/K \trianglelefteq G/K$ y existe un isomorfismo*

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

Demostración. La aplicación $G/K \to G/H$ dada por $xK \mapsto xH$ está bien definida y es un homomorfismo sobreyectivo, cuyo núcleo es H/K. Aplicando el primer teorema de isomorfismo se obtiene el enunciado. □

Teorema 2.1.49 (Tercer Teorema de isomorfía)**.** *Sean G un grupo y $H \leq G, K \trianglelefteq G$. Entonces $HK \leq G$, $K \trianglelefteq HK, H \cap K \trianglelefteq H$, y existe un isomorfismo*

$$\frac{H}{H \cap K} \simeq \frac{HK}{K}.$$

Demostración. La aplicación $H \to G/K$ dada por $h \mapsto hK$ es un homomorfismo cuya imagen es $\frac{HK}{K}$ y cuyo núcleo es $H \cap K$. Aplicando el primer teorema de isomorfismo se obtiene el enunciado. □

2.2. Grupo simétrico

Definición 2.2.1. Sea S un conjunto no vacío. El conjunto de aplicaciones biyectivas $S \xrightarrow{\sigma} S$ es un grupo con el producto $\sigma\tau = \tau \circ \sigma$ (i.e. la composición de aplicaciones en el orden opuesto). El grupo de permutaciones de S.
Si $S = \{1, \cdots, n\}$ el grupo obtenido es el grupo simétrico S_n cuyo orden es $|S_n| = n!$.

Notación 2.2.2. Representamos un elemento $\sigma \in S_n$ mediante la matriz

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}^{-1} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ 1 & 2 & \cdots & n \end{pmatrix} \underset{\text{reordenando}}{=} \begin{pmatrix} 1 & 2 & \cdots & n \\ a'_1 & a'_2 & \cdots & a'_n \end{pmatrix}.$$

Definición 2.2.3. Fijados $m \leq n$ elementos $a_1, \cdots, a_m \in \{1, \cdots, n\}$, el m–ciclo $\sigma = (a_1 \cdots a_m)$ está definido por $\sigma(a_i) = a_{i+1}$, $1 \leq i \leq m-1$, $\sigma(a_m) = a_1$, $\sigma(a) = a$, $a \neq a_1, \ldots, a_m$.

Definición 2.2.4. Un 2–ciclo se denomina trasposición. Dos ciclos $(a_1 \cdots a_r), (b_1 \cdots b_s)$ se dicen disjuntos si $a_i \neq b_j$ para todo i, j.

Observación 2.2.5. (1) Ciclos disjuntos conmutan.

(2) Inverso de un m–ciclo $(a_1 \cdots a_m)^{-1} = (a_m \cdots a_1) = (a_1 a_m \cdots a_2)$.

(3) $(a_1 a_2)^{-1} = (a_1 a_2)$.

Demostración. Ejercicio. □

Ejemplos 2.2.6. (1)

$$(135)(2647) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 7 & 1 & 4 & 2 \end{pmatrix},$$

$$(2647)(135) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 7 & 1 & 4 & 2 \end{pmatrix}.$$

(2) $(2647)^{-1} = (7462)$.

Proposición 2.2.7. *(1) El orden de un m-ciclo es m.*

(2) El orden de un producto de ciclos disjuntos dos a dos es el mínimo común múltiplo de los órdenes de los ciclos.

Demostración. (1) Sea $\sigma = (a_1 \cdots a_m)$. Es claro que $\sigma^m = 1$ y $\sigma^r \neq 1$, puesto que $\sigma^r(a_1) = a_{r+1} \neq a_1$, para $1 \leq r < m$.
(2) Sean $\sigma_1, \ldots, \sigma_t$ ciclos disjuntos dos a dos, de longitudes $r_1, \ldots, r_t, m = \text{mcm}(r_1, \ldots, r_t)$ y r el orden de $\sigma_1 \cdots \sigma_t$. Como los ciclos conmutan $(\sigma_1 \cdots \sigma_t)^m = \sigma_1^m \cdots \sigma_t^m = 1$. Por tanto, $r \mid m$. Recíprocamente, de $1 = (\sigma_1 \cdots \sigma_t)^r = \sigma_1^r \cdots \sigma_t^r$, como los ciclos son disjuntos, se deduce que $\sigma_i^r = 1$, para todo i. Por tanto, $r_i \mid r$ para todo i. De aquí $m \mid r$. □

Proposición 2.2.8 (Descomposición en producto de ciclos disjuntos)**.** *Toda permutación se descompone en producto de ciclos disjuntos de modo único, salvo el orden de los ciclos.*

Demostración. Sean $\sigma \in S_n$, $i \in \{1, \ldots, n\}$ y $1 \leq r \leq n$ el primer número tal que $\sigma(i) = i$. Si $r = n$, entonces $\sigma = (\sigma(i) \cdots \sigma^{n-1}(i)\sigma^n(i) = i)$ en un n–ciclo. Si $r < n$, el primer ciclo de la descomposición es $\sigma_1 = (\sigma(i) \cdots \sigma^{r-1}(i)\sigma^r(i) = i)$. Consideramos $j \in \{1, \ldots, n\} - \{\sigma(i), \ldots, \sigma^{r-1}(i), \sigma^r(i) = i\}$, y el segundo ciclo de la descomposición es $\sigma_2 = (\sigma(j) \cdots \sigma^{s-1}(j)\sigma^s(j) = j)$. El ciclo σ_2 es disjunto de σ_1 puesto que si $\sigma^h(j) = \sigma^k(i)$, entonces $\sigma^{k-h}(i) = j$ y, de aquí, $j \in \{\sigma(i), \ldots, \sigma^{r-1}(i), \sigma^r(i) = i\}$, que no es posible. Continuando el proceso obtenemos la descomposición en producto de ciclos disjuntos. Según el procedimiento anterior, para cada $i \in \{1, \ldots, n\}$ si $\sigma(i) = j$, un ciclo $(\cdots i\ j \cdots) = (i\ j \cdots)$ pertenece a la descomposición y está unívocamente determinado por σ, i. Por tanto, sólo puede variar el orden de los ciclos en la descomposición. □

Ejemplos 2.2.9. (1)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 7 & 1 & 4 & 2 \end{pmatrix} = (135)(2647)$$

es de orden 12.

(2)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 4 & 1 & 9 & 6 & 8 & 2 & 5 \end{pmatrix} = (134)(278)(59),$$

es de orden 6.

(3)

$$(a_1a_2a_3a_4)^2 = (a_1a_2a_3a_4)(a_1a_2a_3a_4) = (a_1a_3)(a_2a_4),$$
$$(a_1a_2a_3a_4)^3 = (a_1a_3)(a_2a_4)(a_1a_2a_3a_4) = (a_1a_4a_3a_2),$$
$$(a_1a_2a_3a_4)^4 = (a_1a_4a_3a_2)(a_1a_2a_3a_4) = ().$$

Proposición–Definición 2.2.10 (Permutaciones pares e impares)**.**

(1) Sea $\sigma \in S_n$. Un par $i < j$ forma permanencia o inversión para σ según que $\sigma(i) < \sigma(j)$ o $\sigma(i) > \sigma(j)$.

(2) El índice de σ es

$$\epsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i} = (-1)^{k_\sigma},$$

donde k_σ es el número de pares en inversión en σ.

(3) Diremos que σ es par o impar según que su número de pares en inversión k_σ sea par o impar, es decir, según que $\epsilon(\sigma) = 1$ o $\epsilon(\sigma) = -1$.

(4) Toda trasposición es impar.

(5) $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$. Esto es, el índice es un homomorfismo $S_n \xrightarrow{\epsilon} \{1, -1\}$, en el grupo multiplicativo $(\{1, -1\}, \cdot) \simeq (\mathbb{Z}_2, +)$.

(6) El conjunto A_n de las permutaciones pares es el núcleo de i. Por tanto A_n es un subgrupo normal de S_n, que recibe el nombre de grupo alternado. El cociente $S_n/A_n \simeq \mathbb{Z}_2$. Por tanto, $|A_n| = \frac{1}{2}n!$.

(7) Sea $H \le S_n$ un subgrupo. Entonces o todas las permutaciones de H son pares, i.e. $H \le A_n$, o bien exactamente la mitad de ellas son pares.

(8) Un m–ciclo es producto de $m - 1$ trasposiciones: $(a_1a_2 \cdots a_m) = (a_1a_2)(a_1a_3) \cdots (a_1a_m)$. Por tanto un m ciclo es par o impar según que m sea impar o par.

(9) Toda permutación es producto de trasposiciones. La permutación es par o impar, según que el número de trasposiciones sea par o impar. En particular, la paridad del número de trasposiciones en la descomposición en producto de trasposiciones de una permutación es invariante.

Demostración. (2) Cada numerador $\sigma(j) - \sigma(i)$ es $\pm(l-k)$ para únicos $k < l$ y, por tanto, cancela en 1, con exactamente un denominador si el par $i < j$ no forma inversión para σ y cancela en -1, con exactamente un denominador si el par $i < j$ forma inversión para σ.
(4) El número de pares en inversión en la trasposición (ij), con $i < j$, es $2(j-i)-1$.
(5) Por definición

$$\epsilon(\sigma\tau) = \prod_{1\le i<j\le n} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{j-i}.$$

Hay k_σ pares $i < j$ tales que $\sigma(i) > \sigma(j)$. El producto $(-1)^{k_\sigma}\epsilon(\sigma\tau)$ actúa en el término de la derecha cambiando el signo de cada diferencia $\tau(\sigma(j)) - \tau(\sigma(i))$ para exactamente esos k_σ pares. por tanto el resultado en el término de la derecha coincide con $\epsilon(\tau)$. Es decir

$$(-1)^{k_\sigma}\epsilon(\sigma\tau) = \epsilon(\tau).$$

(7) Supongamos que $H \not\subset A_n$. Sea $\sigma \in H - A_n$, entonces en la biyección $H \to H$ dada por $\tau \mapsto \sigma\tau$, un elemento $\tau \in H$ es par o impar si, y sólo si, su imagen $\sigma\tau$ es impar o par. De aquí la afirmación. □

Ejemplo 2.2.11.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 7 & 1 & 4 & 2 \end{pmatrix} = (135)(2647) = (13)(15)(26)(24)(27),$$

es impar.

Proposición 2.2.12 (Generación por trasposiciones y 3–ciclos)**.**

(1) $(a_1a_2\cdots a_m) = (a_1a_2)(a_1a_3)\cdots(a_1a_m) = (a_{m-1}a_m)\cdots(a_2a_3)(a_1a_2)$.

(2) Si $a_1 \neq 1$ *entonces* $(a_1a_i) = (1a_i)(1a_1)(1a_i)$.

(3) S_n *está generado por las trasposiciones* $(12), (13), \cdots, (1n)$.

(4) Si $i \neq 2 \neq j$, *entonces* $(1i)(1j) = (1ij) = (12j)(12i)(12j)^2, (12)(1j) = (12j), (1i)(12) = (1i2) = (12i)^2$.

(5) Si $n \geq 3$ *el grupo alternado* A_n *está generado por los* 3*–ciclos* $(123), (124)\cdots(12n)$.

Demostración. Ejercicio. □

Teorema 2.2.13 (Teorema de Abel: Simplicidad del grupo alternado)**.**

(1) Sea $n \geq 3$. Si $H \trianglelefteq A_n$ y H contiene un 3–ciclo entonces $H = A_n$.

(2) Si $n \geq 5$ entonces A_n es simple.

Demostración. (1) Supongamos $(a_1a_2a_3) \in H$. Sea $\sigma \in S_n$ tal que $\sigma(1) = a_1, \sigma(2) = a_2, \sigma(3) = a_3$. Si $\sigma \in A_n$ entonces $(123) = \sigma(a_1a_2a_3)\sigma^{-1} \in H$. Si σ es impar $(12)\sigma \in A_n$, en este caso, $(132) = (12)\sigma(a_1a_2a_3)\sigma^{-1}(12)^{-1} \in H$. Por tanto, $(123) = (132)^{-1} \in H$. Si $n = 3$ esto prueba que $H = A_3$. Si $n > 3$ entonces para $k > 3$, el ciclo $(23k) \in A_n$, por tanto, $(1k2) = (23k)(123)(23k)^{-1} \in H$ y, en consecuencia, $(12k) = (1k2)^{-1} \in H$.
(2) Sea $\{1\} \neq H \trianglelefteq A_n$. Elegimos $1 \neq h = \alpha_1 \cdots \alpha_r \in H$, donde los α_i son ciclos disjuntos de longitud $\alpha_i \geq$ longitud α_{i+1}.
Casos:

(1) $\alpha_1 = (a_1 \cdots a_m)$, $m > 3$,

(2) α_1, α_2, 3–ciclos,

(3) α_1, 3–ciclo y para todo $i \geq 2$, α_i es trasposición,

(4) todo α_i trasposición.

Caso (1). El 3–ciclo $\sigma = (a_1a_2a_3) \in A_n$ y $H \trianglelefteq A_n$ por tanto $\sigma\alpha_1\sigma^{-1}\alpha_2 \cdots \alpha_r = \sigma h\sigma^{-1} \in H$. Así $\sigma\alpha_1\sigma^{-1}\alpha_1^{-1} = \sigma\alpha_1\sigma^{-1}\alpha_2 \cdots \alpha_r h^{-1} \in H$. De forma que

$$(a_2a_3a_m) = (a_1a_2a_3)(a_1a_2 \cdots a_m)(a_3a_2a_1)(a_m \cdots a_2a_1) = \sigma\alpha_1\sigma^{-1}\alpha_1^{-1} \in H$$

y, según (1) es $H = A_n$.
Caso (2). Sean $\alpha_1 = (a_1a_2a_3), \alpha_2 = (a_4a_5a_6)$ y $\sigma = (a_2a_3a_4a_5a_6) \in A_n$. Entonces

$$\sigma\alpha_1\alpha_2\sigma^{-1}\alpha_3 \cdots \alpha_r = \sigma h\sigma^{-1} \in H.$$

Por tanto, $(a_1a_5a_2a_3a_6) = \sigma\alpha_1\alpha_2\sigma^{-1}\alpha_2^{-1}\alpha_1^{-1} = \sigma h\sigma^{-1}h^{-1} \in H$ y se aplica el Caso (1).
Caso (3). Sean $\alpha_1 = (a_1a_2a_3), \tau = \alpha_2 \cdots \alpha_r$, donde τ es un producto de trasposiciones disjuntas. Entonces $(a_1a_3a_2) = \alpha_1\tau\alpha_1\tau \in H$.
Caso (4). Sea $h = \alpha_1 = (a_1a_2), \alpha_2 = (a_3a_4), \tau = \alpha_3 \cdots \alpha_r$, donde τ es un producto de trasposiciones disjuntas y disjuntas de α_1, α_2. Sea $\sigma = (a_1a_2a_3)$, entonces

$$(a_1a_4)(a_2a_3) = (a_1a_2)(a_3a_4)(a_1a_2a_3)(a_1a_2)(a_3a_4)(a_3a_2a_1) = h\sigma h\sigma^{-1} \in H.$$

Como $n \geq 5$, existe $a_5 \neq a_1, a_2, a_3, a_4, 1 \leq a_5 \leq n$. Entonces $\sigma = (a_1a_2a_5) \in A_n$. Así

$$(a_1a_5a_4a_3a_2) = (a_1a_4)(a_2a_3)\sigma(a_1a_4)(a_2a_3)\sigma^{-1} \in H$$

y se aplica el Caso (1). □

Observación 2.2.14. A_4 no es simple.

Demostración. En efecto, el subgrupo $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$ es normal en A_4. □

Teorema 2.2.15 (Teorema de Cayley)**.** *Todo grupo G es isomorfo a un subgrupo de un grupo de permutaciones. En particular, si G es finito de orden $|G| = n$, entonces G es isomorfo a un subgrupo de S_n.*

Demostración. Consideramos el grupo $\mathscr{P}$ de las permutaciones de G con producto la composición de aplicaciones. La aplicación $G \to \mathscr{P}$ definida por $g \mapsto \varphi_g$, donde $\varphi_g : G \to G$ es la biyección dada por $x \mapsto gx$, es un homomorfismo inyectivo. □

2.3. Grupos libres. Generadores y relaciones

Proposición–Definición 2.3.1 (Semigrupo libre)**.**

(1) Un semigrupo (o monoide) es un conjunto no vacío G con una ley asociativa con elemento identidad $1 \in G$.

(2) Sea $S = \{a, b, c, \ldots\}$ un conjunto no vacío. Una palabra en S es una sucesión finita de símbolos de S, en la que se permiten repeticiones. Por ejemplo: aa, $aabac$, b son palabras distintas. Es decir una palabra es una aplicación $\{1, \ldots, n\} \to S$ para cierto n.

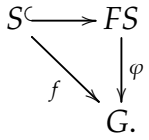
(3) Dos palabras se multiplican por yuxtaposición $aaa * aabac = aaaaabac$. Esto define una ley asociativa en el conjunto de palabras. La sucesión vacía es la unidad $1 = \ $. (Si $1 \in S$, denotaremos la sucesión vacía con otro símbolo).

(4) El conjunto FS de todas las palabras en S es el semigrupo libre sobre S.

(5) Podemos identificar S con un subconjunto de FS, i.e. $S \subset FS$.

El semigrupo libre FS está caracterizado por la siguiente propiedad universal.

Teorema 2.3.2. *Para cada aplicación $S \xrightarrow{f} G$ en un semigrupo G, existe un único homomorfismo de semigrupos $FS \to G$ que hace conmutativo el diagrama*



En concreto, $\varphi(1) = 1_G$ y $\varphi(a_1 \cdots a_n) = f(a_1) \cdots f(a_n)$. Además $f(S)$ genera G si, y sólo si, φ es sobreyectivo. En consecuencia, el semigrupo FS está determinado por la propiedad universal anterior, salvo único isomorfismo que es la identidad en S.

Proposición–Definición 2.3.3 (Grupo libre)**.**

(1) Sea $s \mapsto s^{-1}$ una biyección de S con un conjunto disjunto S^{-1} que no contiene a 1 (por ejemplo, $S^{-1} = S \times \{1\}, s^{-1} = (s, 1)$). Denotamos de la misma forma $t \mapsto t^{-1}$ la biyección inversa $S^{-1} \to S$.

(2) Formamos palabras sobre $S \cup S^{-1}$. Diremos que una palabra $p = s_1 \cdots s_n$ es reducida si no contiene letras consecutivas $s_i s_{i+1}$ tales que $s_{i+1} = s_i^{-1}$.

(3) Dadas dos palabras, diremos $p \leq q$, si p se obtiene de q mediante sucesivas eliminaciones de letras consecutivas $s_i s_{i+1}$ tales que $s_{i+1} = s_i^{-1}$.

(4) Para cada palabra p existe una única palabra reducida r tal que $r \leq p$.

(5) Escribiremos una palabra reducida en la forma $s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$, donde $s_i \in S$, $\epsilon_i = \pm 1$ y, si $s_{i+1} = s_i$ entonces $\epsilon_i = \epsilon_{i+1}$.

(6) Según nuestra definición, dos palabras reducidas son iguales $s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} = r_1^{\delta_1} \cdots r_m^{\delta_m}$ si, y sólo si, $m = n$, $s_i = r_i$, $\epsilon_i = \delta_i$ para todo i.

(7) El grupo libre sobre S es el conjunto $F(S)$ de las palabras reducidas con el producto que definimos a continuación.

Sean $r_1^{\delta_1} \cdots r_m^{\delta_m}$ y $s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$ dos palabras reducidas. Supongamos que $m \leq n$. Sea k el menor entero en el rango $1 \leq k \leq m+1$ tal que $s_k^{\epsilon_k} \neq r_{m-k+1}^{-\delta_{m-k+1}}$. Entonces,

$$(r_1^{\delta_1} \cdots r_m^{\delta_m})(s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}) = \begin{cases} r_1^{\delta_1} \cdots r_{m-k+1}^{\delta_{m-k+1}} s_k^{\epsilon_k} \cdots s_n^{\epsilon_n} & \text{si } k \leq n, \\ s_{m+1}^{\epsilon_{m+1}} \cdots s_n^{\epsilon_n} & \text{si } k = m+1 \leq n, \\ 1 & \text{si } k = m+1 \text{ y } m = n. \end{cases}$$

Ejemplo: $(aba)(a^{-1}ba) = aa$.

(8) El conjunto S genera el grupo libre $F(S)$.

Teorema 2.3.4. *$F(S)$ es un grupo.*

Demostración. El punto delicado en la demostración es la propiedad asociativa □

Teorema 2.3.5. *Para cada aplicación $S \xrightarrow{f} G$ en un grupo G, existe un único homomorfismo de grupos $F(S) \to G$ que hace conmutativo el diagrama*

$$\begin{array}{ccc} S & \hookrightarrow & F(S) \\ & {\scriptstyle f}\searrow & \downarrow{\scriptstyle \varphi} \\ & & G. \end{array}$$

En concreto, $\varphi(1) = 1_G$ y $\varphi(s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}) = f(s_1)^{\epsilon_1} \cdots f(s_n)^{\epsilon_n}$. Además $f(S)$ genera G si, y sólo si, φ es sobreyectivo. En consecuencia, $F(S)$ está determinado por la propiedad universal anterior, salvo único isomorfismo que es la identidad en S.

Demostración. Ejercicio. □

Proposición 2.3.6. *$F(S) \simeq F(S')$ si, y sólo si, $|S| = |S'|$.*

Ejemplo 2.3.7. Para abreviar, en $F(S)$, denotaremos, por ejemplo: $aaab^{-1}b^{-1} = a^3b^{-2}$.

Definición 2.3.8. (1) $F(S)$ es el grupo libre sobre el conjunto S.

(2) Un grupo G es libre si $G \simeq F(S)$ para cierto S. En este caso la imagen de S por el isomorfismo es una base libre de G.

(3) El cardinal $|S|$ es el rango de G.

Teorema 2.3.9 (Nielsen-Schreier)**.** *Todo subgrupo de un grupo libre es un grupo libre.*

Demostración. La demostración no es en absoluto trivial. Requiere un argumento topológico con espacios recubridores. □

Observación 2.3.10. Sea H un subgrupo finitamente generado de un grupo libre de rango finito F. Existe un algoritmo para construir, a partir de un conjunto finito de generadores de H una base libre finita de H. Si F tiene rango n y el índice $[F : H] = i < \infty$ entonces H tiene rango $ni - i + 1$. En particular, el rango de H puede ser mayor que el rango de F.

2.3.1. Presentaciones

Teorema 2.3.11. *Todo grupo G es cociente de un grupo libre. Con más precisión, si $S \subset G$ es un conjunto de generadores, entonces existe un subgrupo normal $K \trianglelefteq F(S)$ tal que $F(S)/K \simeq G$.*

Demostración. Por la propiedad universal existe un único epimorfismo $\varphi : F(S) \to G$ que es la identidad en S. Basta tomar $K = \ker \varphi$. □

Observación 2.3.12. Llamaremos relaciones entre los elementos del conjunto de generadores S a los elementos de K. El isomorfismo $F(S)/K \simeq G$ describe G por generadores y relaciones.

De hecho, la existencia de un epimorfismo $F(S) \to G$ se puede adoptar como definición de sistema generador S de G.

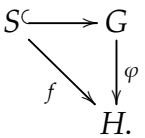
Definición 2.3.13. Consideremos un grupo $G =< S >$ con un subconjunto de generadores S.

(1) Una presentación para G es un par (S, R), donde R es un conjunto de palabras en $F(S)$ tal que el núcleo K del epimorfismo $F(S) \to G$ es el menor subgrupo normal de $F(S)$ que contiene a R. Por tanto, $G \simeq F(S)/K$. Denotaremos $G =< S \mid R >$.

(2) Diremos que G está finitamente generado si hay una presentación (S, R), donde S es un conjunto finito, y finitamente presentado si ambos S y R son finitos.

Observación 2.3.14. El subgrupo K, en $G =< S \mid R >\simeq F(S)/K$, está generado por todos los conjugados de los elementos de R.

Teorema 2.3.15. *Sea G el grupo definido por la presentación $< S \mid R >$. Para cada grupo H y cada aplicación $S \xrightarrow{f} H$ cuyo homomorfismo asociado $F(S) \to H$ lleva cada elemento de R a 1, existe un único homomorfismo de grupos $G \to H$ que hace conmutativo el diagrama*



En las condiciones del enunciado, el subgrupo normal K generado por R está contenido en el núcleo de $F(S) \to H$. En consecuencia, este homomorfismo factoriza en un homomorfismo $F(S)/K \to H$.

Ejemplos 2.3.16. (1) Veamos que $G =< a, b \mid a^n, b^2, abab >\simeq D_n$. En efecto, puesto que $\sigma, \tau \in D_n$ verifican las relaciones que definen G, el teorema anterior proporciona un homomorfismo sobreyectivo $G \to D_n$. De las relaciones $a^n = 1, b^2 = 1, ba = a^{n-1}b$ en G, se deduce que todo elemento de G es alguno de los siguientes $\{1, a, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1}\}$. Por tanto $|G| \leq n = |D_n|$ y, en consecuencia, la aplicación sobreyectiva $G \to D_n$ es una biyección.

(2) $Q_8 =< i, j \mid i^4 = 1, j^2 = i^2, j^{-1}ij = i^{-1} >$.

(3) El grupo abeliano libre con base $a_1, \ldots, a_n$ es el grupo determinado por la presentación $< a_1, \ldots, a_n \mid \{a_i a_j a_i^{-1} a_j^{-1}\}_{i<j} >$.

(4) $\mathbb{Z}_n \times \mathbb{Z}_m =< a, b \mid a^n = b^m = aba^{-1}b^{-1} = 1 >$.

(5) S_n está generado por las trasposiciones $(12), (23), \ldots, (n-1\, n)$ que satisfacen las relaciones $(i\, i+1)^2 = 1$, $((i\, i+1)(i+1\, i+2))^3 = 1$, $(i\, i+1)(j\, j+1)(i\, i+1)(j\, j+1) = 1$, si $|i-j| \geq 2$. Esto es una presentación

$$S_n =< t_1, \ldots, t_{n-1} \mid t_i^2 = 1, (t_i t_{i+1})^3 = 1, t_i t_j t_i t_j = 1 \text{ si } |i-j| \geq 2 > .$$

(6) El grupo fundamental de la esfera con r puntos eliminados tiene generadores $\sigma_1, \ldots, \sigma_r$, lazos que aíslan cada uno de los puntos eliminados, con las relación $\sigma_1 \cdots \sigma_r = 1$.

(7) El grupo fundamental de una superficie de Riemann compacta de género g tiene $2g$ generadores $u_1, v_1, \ldots, u_g, v_g$ con la relación $u_1 v_1 u_1^{-1} v_1^{-1} \cdots u_g v_g u_g^{-1} v_g^{-1} = 1$.

(8) En general es extremadamente difícil saber si $< S \mid R >$ es el grupo trivial, un grupo finito o isomorfo a algún grupo conocido. Como ejemplo, el primero de los siguientes grupos es infinito y el segundo es trivial.

$$< x_1, x_2, x_3, x_4 \mid x_2 x_1 x_2^{-1} = x_1^2,\ x_3 x_2 x_3^{-1} = x_2^2,\ x_4 x_3 x_4^{-1} = x_3^2,\ x_1 x_4 x_1^{-1} = x_4^2 >,$$

$$< x_1, x_2, x_3 \mid x_2 x_1 x_2^{-1} = x_1^2,\ x_3 x_2 x_3^{-1} = x_2^2,\ x_1 x_3 x_1^{-1} = x_3^2 > .$$

2.4. Acción de un grupo sobre un conjunto

Proposición–Definición 2.4.1. Sean G un grupo y S un conjunto no vacío. Una acción (por la izquierda) de G en S es un homomorfismo $G \xrightarrow{\rho} \mathrm{Aut}(S)$, donde $\mathrm{Aut}(S)$ es el grupo de las biyecciones de S, con la operación $fh := f \circ h$, donde $f, h \in \mathrm{Aut}(S)$. Denotaremos $\rho(g)x = gx$, para $g \in G, x \in S$.
De forma equivalente, una acción es una aplicación

$$G \times S \longrightarrow S, \quad (g, x) \mapsto gx, \tag{2.4.1.1}$$

que verifica, para cualesquiera $g_1, g_2 \in G, x \in S$

(1) $1_G x = x$,

(2) $(g_1 g_2)x = g_1(g_2 x)$.

Demostración. Ejercicio. □

Observación 2.4.2. Una acción a la derecha, $S \times G \to S$ con $x1_G = x; x(g_1 g_2) = (xg_1)g_2$, equivale a $G \xrightarrow{\rho} \mathrm{Aut}(S)$, donde $\mathrm{Aut}(S)$ es el grupo de las biyecciones de S, con la operación $fh := h \circ f$, donde $f, h \in \mathrm{Aut}(S)$.
Cada acción a la derecha xg, define una acción a la izquierda $gx := xg^{-1}$, y recíprocamente. Podemos, por tanto, considerar siempre acciones por la izquierda.

Definición 2.4.3. Diremos que G actúa de forma *efectiva* si ρ es inyectiva. Es decir, si la condición $gx = x$, para todo $x \in S$, implica que $g = 1_G$.
Denotando $K = \ker(\rho)$. La acción (2.4.1.1) induce una acción efectiva

$$G/K \times S \longrightarrow S, \quad (gK, x) \mapsto gx.$$

Ejemplo 2.4.4. El grupo de la rotaciones actúa de forma efectiva en el plano $\mathbb{R}^2$.

Ejemplos 2.4.5. (1) $S = G$. Acción (a la izquierda) por multiplicación a la izquierda.

$$G \longrightarrow \mathrm{Aut}(G), \quad g \mapsto (G \xrightarrow{g\cdot} G,\ x \mapsto gx).$$

(2) $S = G$. Acción (a la izquierda) por multiplicación a la derecha.

$$G \longrightarrow \mathrm{Aut}(G), \quad g \mapsto (G \xrightarrow{\cdot g^{-1}} G,\ x \mapsto xg^{-1}).$$

(3) $S = G$. Acción por conjugación.

$$G \longrightarrow \mathrm{Aut}(G), \quad g \mapsto (G \xrightarrow{g\{\}} G,\ x \mapsto gxg^{-1} := {}^g x).$$
$${}^{g_1 g_2}x = (g_1 g_2)x(g_1 g_2)^{-1} = g_1 g_2 x g_2^{-1} g_1^{-1} = {}^{g_1}({}^{g_2}x).$$

(4) Si G actúa sobre S entonces cada subgrupo $H \leq G$ actúa sobre S.

(5) Si $T \subset S$ es invariante por la acción (i.e. $gT := \{gx \mid x \in T\} = T$, para cada $g \in G$) entonces G actúa sobre T.

(6) Si G actúa por conjugación sobre G, cada subgrupo normal $H \trianglelefteq G$ es invariante. Por tanto G actúa sobre H por conjugación.

(7) Sean $H, K \leq G$ diremso que K es estable por conjugación de H si $hKh^{-1} = K$ para todo $h \in H$. Si K es estable por conjugación de H, entonces la acción por conjugación de H en G induce una acción por conjugación en el conjunto de clases G/K, definida por: $(h, gK) \mapsto hgKh^{-1} = hgh^{-1}hKh^{-1} = hgh^{-1}K$.

(8) Sean $H, K \leq G$. La acción por multiplicación de H en G, induce una acción en el conjunto de clases G/K, definida por $(h, gK) \mapsto (hg)K$. Esta acción es transitiva. su núcleo es $\{h \in H \mid (hg)K = gK\}$ para todo $g \in G$. Este núcleo es $H \cap (\cap_{g \in G})gKg^{-1}$.

(9) La acción de H en G por conjugación induce una acción en el conjunto de subgrupos de G, definida por: $(h, K) \mapsto hKh^{-1}$.

(10) Una acción $G \xrightarrow{\rho} \mathrm{Aut}(S)$ induce una acción de G en el conjunto de las partes de S, definida por $gA = \{gx \mid x \in A\}$.

Proposición 2.4.6. *Sean G un grupo finito y p el menor primo que divide al orden de G. Entonces todo subgrupo de G de índice p es normal en G.*

Demostración. Sea $H \leq G$ tal que $[G : H] = p$. Consideramos la acción de G en el conjunto de clases G/H por multiplicación a la izquierad. El núcleo de esta acción es el subgrupo normal $K = \cap_{g \in G} gHg^{-1}$. veamos que $K = H$. El grupo cociente G/K actúa de forma efectiva sobre el conjunto de clases G/H. Por tanto G/K es isomorformo a un subgrupo del grupo de permutaciones de G/H, cuyo orden es $p!$. En consecuencia, $[G : K]$ divide a $p!$. Como p es el menor primo que divide al orden de G, todo divisor primo de $[G : K]$ es $\geq p$. Por tanto $[G : K] = p$. Como $K \leq H$ y ambos tienen índice p, de la ecuación $[G : K] = [G : H][H : K]$, se deduce $[H : K] = 1$. Por tanto, $H = K$. □

Proposición 2.4.7. *Sean G un grupo finito simple y $H \leq G$ de índice $[G : H] = m > 1$. Entonces existe un homomorfismo inyectivo de G en el grupo alternado A_m.*

Demostración. Consideramos la acción de G en el conjunto de clases G/H, dada por $(g, g'H) \mapsto (gg')H$. Esta acción induce un homomorfismo f de G en el grupo de permutaciones de G/H que es isomorfo a S_m. Puesto que G es simple y la acción no es trivial ($m > 1$), el núcleo de f es trivial, esto es, f es inyectivo. Supongamos que $f(G) \not\subset A_m$. Entonces $[f(G) : f(G) \cap A_m] = 2$. Por tanto, $f(G) \cap A_m \trianglelefteq f(G)$. Como $f(G)$ es simple y $f(G) \cap A_m \neq \{1\}$, se deduce $A_m \subsetneq f(G)$. Esto implica $G \simeq f(G) = S_m$. Esto es imposible puesto que S_m no es simple. Por tanto $f(G) \subset A_m$. □

Proposición–Definición 2.4.8 (Órbitas y estabilizadores)**.**

(1) Una acción $G \times S \to S$ induce una relación de equivalencia en S:

$$x \sim_G y \Leftrightarrow \text{ existe } g \in G \text{ tal que } y = gx.$$

Las clases de equivalencia son las *órbitas* de la acción. La G–órbita de $x \in S$ es el conjunto

$$Gx := \{gx \mid g \in G\}.$$

El cociente $S/\sim_G$ es el conjunto de órbitas.

(2) La acción es *transitiva* si hay una única órbita. Esto es, para todo $x, y \in S$ existe $g \in G$ tal que $gx = y$.

(3) Sea $H \leq G$. Las H–órbitas de la acción de H sobre G por multiplicación a derecha (resp. izquierda) son las clases adjuntas de H en G.

(4) La G–órbita de $x \in G$ en la acción por conjugación es la clase de conjugación de x

$$^G x = \{gxg^{-1} \mid g \in G\}.$$

(5) El *estabilizador* de $x \in S$ es

$$\text{Stab}(x) = \{g \in G \mid gx = x\}.$$

(6) En la acción por conjugación.

$$\text{Stab}(x) = N_G(x) = Z_G(x) = \{g \in G \mid gx = xg\}.$$

(7) En la acción por conjugación de G en el conjunto de subgrupos de G, el estabilizador de un subgrupo $K \leq G$ es $\text{Stab}(K) = N_G(K) = \{g \in G \mid gKg^{-1} = K\}$, el normalizador de K en G. El subgrupo K es normal en $N_G(K)$ que es el mayor subgrupo de G donde K es normal.

(8) El núcleo de una acción es $\cap_{x \in S}\text{Stab}(x)$.

Ejemplos 2.4.9. (1) Un espacio afín es un conjunto con una acción transitiva del grupo aditivo de un espacio vectorial.

(2) La acción por multiplicación de G en G es transitiva.

Proposición 2.4.10. *Supongamos que G actúa sobre S entonces*

(1) $\text{Stab}(x)$ *es un subgrupo de* G*,*

(2) $|Gx| = [G : \text{Stab}(x)]$.

Demostración. (2) Consideramos el conjunto $G/\mathrm{Stab}(x)$, de clases adjuntas por la derecha respecto de $\mathrm{Stab}(x)$, y la aplicación

$$Gx \xrightarrow{\varphi} G/\mathrm{Stab}(x); \quad gx \mapsto g\mathrm{Stab}(x).$$

Las equivalencias

$$g\mathrm{Stab}(x) = g'\mathrm{Stab}(x) \Leftrightarrow (g')^{-1}g\mathrm{Stab}(x) = \mathrm{Stab}(x)$$
$$\Leftrightarrow (g')^{-1}g \in \mathrm{Stab}(x) \Leftrightarrow (g')^{-1}gx = x \Leftrightarrow gx = g'x,$$

muestran que φ está bien definida y es inyectiva. Es claro que φ es sobreyectiva. Esto es, φ es una aplicación biyectiva. □

Proposición 2.4.11 (Ecuación de clases)**.** *Sea G un grupo finito que actúa sobre un conjunto finito S. Consideramos la partición de S en órbitas de la acción*

$$S = \mathscr{O}_1 \cup \cdots \cup \mathscr{O}_r.$$

Así el número de elementos de S verifica

$$|S| = \sum_{i=1}^{r} |\mathscr{O}_i|.$$

Elegimos un representante de cada órbita $\mathscr{O}_i = Gx_i$. Según la Proposición 2.4.10

$$|\mathscr{O}_i| = [G : \mathrm{Stab}(x_i)].$$

En consecuencia

$$|S| = \sum [G : \mathrm{Stab}(x_i)],$$

donde $\{x_1, \ldots, x_r\}$ es un conjunto de representantes de las órbitas de la acción.
Sea $S_0 = \{x \in S \mid Gx = \{x\}\}$ (el conjunto de puntos fijos de la acción) y $\{x_1, \ldots, x_r\}$ un conjunto de representantes de las órbitas. Entonces cada elemento de S_0 aparece entre los x_i y la ecuación anterior se puede escribir

$$|S| = |S_0| + \sum_{\substack{x \in \{x_1, \ldots, x_r\} \\ x \notin S_0}} [G : \mathrm{Stab}(x_i)]. \tag{2.4.11.1}$$

Observemos que $x \in S_0 \Leftrightarrow |Gx| = 1 \Leftrightarrow [G : \mathrm{Stab}(x)] = 1$. Por tanto, si $x \in \{x_1, \ldots, x_r\} - S_0$, entonces $[G : \mathrm{Stab}(x)] > 1$.

En el caso de la acción de G por conjugación en G, el conjunto S_0 es el centro $Z(G)$, puesto que $x \in Z(G)$ si, y sólo si, la órbita ${}^G x = \{gxg^{-1} \mid g \in G\} = \{x\}$. Entonces, de la ecuación (2.4.11.1) *resulta la* ecuación de clases *para un grupo finito*

$$|G| = |Z(G)| + \sum_{\substack{x \in \{x_1, \ldots, x_r\} \\ x \notin Z(G)}} [G : N_G(x)], \tag{2.4.11.2}$$

donde $\{x_1, \ldots, x_r\}$ es un conjunto de representantes de las clases de conjugación.

Definición 2.4.12. Sea G un grupo finito. Un subgrupo $H \leq G$ cuyo orden $|H| = p^s$, con p primo y $s \geq 1$, se denomina un p–subgrupo de G. Si $|G| = p^r$ con p primo y $r \geq 1$, diremos que G es un p–grupo.

Corolario 2.4.13. *Sea G un p–grupo que actúa sobre S. Entonces*

$$|S| \equiv |S_0| \pmod{p}.$$

Demostración. Basta observar que en la ecuación (2.4.11.1) cada sumando $[G : \mathrm{Stab}(x_i)]$ en el miembro de la derecha es > 1 y un divisor de $|G| = p^r$. Por tanto, $p \mid [G : \mathrm{Stab}(x_i)]$. □

Corolario 2.4.14. *Sean G un grupo finito y H un p–subgrupo de G. Entonces*

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Demostración. Consideramos la acción de H en el conjunto de clases $S = G/H$ por multiplicación a la izquierda. Entonces

$$\mathrm{Stab}(gH) = \{h \in H \mid h(gH) = gH\} = \{h \in H \mid g^{-1}hgH = H\} = \{h \in H \mid g^{-1}hg \in H\}.$$

La órbita de gH tiene un único elemento $\Leftrightarrow \mathrm{Stab}(gH) = H \Leftrightarrow$ para todo $h \in H, g^{-1}hg \in H \Leftrightarrow g \in N_G(H)$. Por tanto, $S_0 = N_G(H)/H$. Así la ecuación (2.4.11.1) se escribe

$$|G/H| = |N_G(H)/H| + \sum_{\substack{gH \in \{g_1H, \ldots, g_rH\} \\ x \notin S_0}} [H : \mathrm{Stab}(g_iH)].$$

Puesto que $|H| = p^s$ y cada sumando $[H : \mathrm{Stab}(g_iH)]$ es > 1 y un divisor de $|H|$, se obtiene el resultado. □

Corolario 2.4.15. *Sean G un p–grupo. Entonces $Z(G) \neq \{1\}$.*

Demostración. Puesto que $[G : N_G(x)] \mid |G|$ y, para cada $x \notin Z(G)$ es $[G : N_G(x)] \neq 1$, resulta que $p \mid [G : N_G(x)]$, para cada $x \notin Z(G)$. Por tanto, de la ecuación de clases (2.4.11.2), se deduce que $p \mid |Z(G)|$. □

2.5. Los teoremas de Sylow

Hemos visto que si $H < G$ entonces $|H| \mid |G|$. Por otra parte, un grupo cíclico contiene un único subgrupo de orden un divisor dado del orden del grupo. La pregunta natural es: si $d \mid |G|$, ¿contiene G un subgrupo de orden d? La respuesta es, en general, negativa.

Ejemplo 2.5.1. El grupo alternado A_4, que tiene orden 12, no contiene subgrupos de orden 6. También sabemos que para $n \geq 5$ el grupo A_n es simple. Puesto que todo subgrupo de índice 2 es normal, deducimos que A_n no contiene subgrupos de orden $\frac{1}{4}n!$.

Los Teoremas de Sylow, que generalizan el teorema de Cauchy, aseguran la existencia de subgrupos de un orden dado en ciertas condiciones.

Teorema 2.5.2 (Teorema de Cauchy)**.** *Sean G un grupo de orden finito y p un divisor primo del orden de G. Entonces G contiene un subgrupo de orden p.*

Demostración. Sean $|G| = n$ y $p \mid n$. Consideramos el conjunto $X = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \cdots g_p = 1\}$. Puesto que $g_1 \cdots g_p = 1 \Leftrightarrow g_p = (g_1 \cdots g_{p-1})^{-1}$, el conjunto X está en biyección con G^{p-1}. Por tanto $|X| = n^{p-1}$.

El grupo cíclico $(\mathbb{Z}_p, +)$ actúa sobre X: dado $1 \leq k < p$, definimos $(k, (g_1, \ldots, g_p)) \mapsto (g_{k+1}, \ldots, g_p, g_1, \ldots, g_k)$. El conjunto de puntos fijos de la acción es no vacío: $(1, \ldots, 1) \in X_0 = \{(x, \ldots, x) \mid x^p = 1\}$ y, como $\mathbb{Z}_p$ es un p–grupo, por Corolario 2.4.13, se deduce que $|X| \equiv |X_0| \pmod{p}$. Como $p \mid n$ y $|X| = n^{p-1}$ se deduce que $p \mid |X_0|$ y como $|X_0| > 0$, se deduce que $|X_0| > 1$. Por tanto, existe $1 \neq g \in G$ tal que $g^p = 1$. Como p es primo, este elemento genera un subgrupo $< g >$ de orden p. □

Observación 2.5.3. Para demostrar el Teorema de Sylow, basta conocer el Teorema de Cauchy suponiendo que G es conmutativo. Damos una demostración diferente del Teorema de Cauchy, suponiendo que G es conmutativo: Escribimos $|G| = pd$. Inducción en d. Si $d = 1$ el resultado es obvio. Supongamos $d > 1$ y el resultado cierto para cualquier grupo de orden pd', donde $1 \leq d' < d$.
Sea $1 \neq a \in G$. Si $p \mid \operatorname{ord} a$, y $\operatorname{ord} a = pr$, entonces

$$\operatorname{ord} a^r = \frac{\operatorname{ord} a}{\operatorname{mcd}(r, \operatorname{ord} a)} = \frac{pr}{\operatorname{mcd}(r, pr)} = p,$$

lo que prueba el resultado.
Supongamos, por tanto, $p \nmid \operatorname{ord} a$. Puesto que suponemos G conmutativo, podemos considerar el grupo cociente $G/ < a >$. De la igualdad $|G| = | < a > 1||G/ < a > |$ deducimos $p \mid |G/ < a > |$. Por tanto $|G/ < a > | = pd'$ con $d' < d$. Por hipótesis de inducción $G/ < a >$ contiene un elemento $b < a >$ de orden p. Esto implica que $b^p \in < a >$ y $b \notin < a >$. En consecuencia $< b^p > \subsetneq < b >$. Puesto que $\operatorname{ord} b^p = \frac{\operatorname{ord} b}{\operatorname{mcd}(\operatorname{ord} b, p)}$, deducimos $\operatorname{mcd}(\operatorname{ord} b, p) \neq 1$. Esto es $p \mid \operatorname{ord} b$ y, por tanto, el subgrupo cíclico $< b >$ contiene un subgrupo de orden p.

Teorema 2.5.4 (Primer Teorema de Sylow)**.** *Sea G un grupo finito cuyo orden es divisible por p^r, donde p es un número primo y $r \geq 0$. Entonces G contiene un subgrupo de orden p^r.*

Demostración. Inducción sobre $|G|$. Si $|G| = 1$ o $r = 0$ el resultado es trivial. Supongamos $|G| > 1$, $r > 0$ y el resultado cierto para todo grupo de orden menor que $|G|$. escribimos $|G| = p^r n$, con $r > 0, n \geq 1$.
Caso 1. $p \mid |Z(G)|$.
En este caso, puesto que $Z(G)$ es conmutativo, según la Observación 2.5.3 el subgrupo $Z(G)$ tiene un elemento a de orden p. Puesto que todo subgrupo de $Z(G)$ es normal en G, podemos considerar el grupo cociente $G/ < a >$, cuyo orden es $|G/ < a > | = p^{r-1}n < |G|$. Por la hipótesis de inducción $G/ < a >$ contiene un subgrupo $\overline{H}$ de orden p^{r-1}. Este subgrupo corresponde a un subgrupo H de G (que contiene a $< a >$) cuyo orden es $|H| = p^r$.
Caso 2. $p \nmid |Z(G)|$.
En este caso, de la ecuación de clases (2.4.11.2), se deduce

$$p \nmid \sum_{\substack{x \in \{x_1, \ldots, x_r\} \\ x \notin Z(G)}} [G : N_G(x)].$$

Por tanto existe $x \notin Z(G)$ tal que $p \nmid [G : N_G(x)]$. Así de $|G| = [G : N_G(x)] \cdot (|N_G(x)|$ y $p^r \mid |G|$, se deduce, puesto que p es primo,

$$p^r \mid |N_G(x)|.$$

Ahora bien, $|N_G(x)| < |G|$, puesto que $x \notin Z(G)$. Por tanto, según la hipótesis de inducción, $N_G(x)$ contiene un subgrupo H de orden p^r, que también es subgrupo de G. □

Damos un enunciado equivalente, ligeramente distinto, del primer teorema de Sylow, en cuya prueba vamos a usar el teorema de Cauchy completo.

Teorema 2.5.5 (Primer Teorema de Sylow)**.** *Sea G un grupo finito cuyo orden es divisible por p^r, donde p es primo y $r \geq 1$. Entonces G contiene una serie de subgrupos $H_1 \trianglelefteq \cdots \trianglelefteq H_r$ de ordenes $|H_i| = p^i, i = 1, \ldots, r$.*

Demostración. Inducción en $r \geq 1$. Si $r = 1$ es el Teorema de Cauchy 2.5.2. Supongamos $r > 1$ y, el teorema cierto para p^{r-1}. Entonces existe $H_1 \trianglelefteq \cdots \trianglelefteq H_{r-1}$ de ordenes $|H_i| = p^i, i = 1, \ldots, r-1$. Como $p^r \mid |G| = |H_{r-1}|[G : H_{r-1}] = p^{r-1}[G : H_{r-1}]$, se deduce que $p \mid [G : H_{r-1}]$. Según Corolario 2.4.14, $[N_G(H_{r-1}) : H_{r-1}] \equiv [G : H_{r-1}] \pmod{p}$. Deducimos que $p \mid [N_G(H_{r-1}) : H_{r-1}]$. Por tanto, según el Teorema de Cauchy 2.5.2, el grupo cociente $N_G(H_{r-1})/H_{r-1}$ tiene un subgrupo H_r/H_{r-1} de orden p, que es normal en $N_G(H_{r-1})/H_{r-1}$, según Proposición 2.4.6. Por tanto, $H_{r-1} \trianglelefteq H_r$ y $|H_r| = p^r$. □

Definición 2.5.6. Sean G un grupo finito y p un divisor primo del orden de G. Si p^r es la mayor potencia de p que divide al orden de G y H es un subgrupo de orden p^r, diremos que H es un p–subgrupo de Sylow de G.

El Primer Teorema de Sylow dice que para cada divisor primo del orden de G existen p–subgrupos de Sylow en G.

Observación 2.5.7. La acción de G por conjugación en el conjunto $\mathscr{P}(G)$ de las partes de G, estabiliza el conjunto de p–subgrupos de Sylow. Es decir, si H es un p–subgrupo de Sylow entonces gHg^{-1} es un p–subgrupo de Sylow para cada $g \in G$. □

El Segundo Teorema de Sylow asegura que esta acción es transitiva, i.e., cualesquiera dos p–subgrupos de Sylow son conjugados.
Recordemos que el normalizador de un subgrupo P de G está definido por $N_G(P) = \{g \in G \mid gPg^{-1} = P\}$.

Lema 2.5.8. *Sean G un grupo finito y p un divisor primo del orden de G. Si P un p–subgrupo de Sylow de G y H un subgrupo de G de orden p^i contenido en $N_G(P)$ entonces $H \subset P$.*

Demostración. Las condiciones $H, P \leq G$ y $H \subset N_G(P)$ implican que $HP := \{hp \mid h \in H, p \in P\} \leq G$, $P \trianglelefteq HP$, $H \cap P \trianglelefteq H$ y $HP/P \simeq H/H \cap P$. Así HP/P es isomorfo a un cociente de H. Por tanto $|HP/P| = p^k$ para cierto $0 \leq k < i$. En consecuencia $|HP| = p^k|P|$. Ahora bien, P es un p–subgrupo de Sylow, de forma que $k = 0$ y $P = HP$. Esto es $H \subset P$. □

Teorema 2.5.9 (Segundo Teorema de Sylow)**.** *Sean G un grupo finito y p un divisor primo del orden de G.*

(1) Cualesquiera dos p–subgrupos de Sylow de G son G–conjugados.

(2) El número s_p de p–subgrupos de Sylow de G es un divisor del índice de todo p–subgrupo de Sylow y es congruente con 1 módulo p.

(3) Todo subgrupo de G cuyo orden es una potencia de p está contenido en un p–subgrupo de Sylow.

Demostración. (1) Sea $\mathscr{S}$ el conjunto de p–subgrupos de Sylow de G. Consideramos la acción de G en $\mathscr{S}$ por conjugación. Sea $\mathscr{O}$ una órbita de la acción. Entonces G actúa sobre $\mathscr{O}$. Por tanto, si P es un p–subgrupo de Sylow, entonces P actúa sobre $\mathscr{O}$. Descomponemos $\mathscr{O}$ como unión (disjunta) de P–órbitas. Según (2) de Proposición 2.4.10, el cardinal de cada P–órbita es un divisor de $|P|$. Por tanto, cada P–órbita tiene cardinal 1 o una potencia positiva de p. Ahora bien, para cada $P' \in \mathscr{O} - \{P\}$ la P–órbita de P' no tiene cardinal 1. En efecto, si $\{P'\}$ es una P–órbita entonces $P \subset N_G(P')$ y, según el Lema 2.5.8, $P \subset P'$, de donde $P = P'$, puesto que tienen el mismo cardinal.
Además, si $P \in \mathscr{O}$ entonces es claro que $\{P\}$ es una P–órbita cuyo cardinal es 1.

En consecuencia, si suponemos que P_1, P_2 son p–subgrupos de Sylow tales que $P_1 \in \mathscr{O}$ y $P_2 \notin \mathscr{O}$; descomponiendo $\mathscr{O}$ en P_1–órbitas, y teniendo en cuenta que $|\mathscr{O}| = \sum |\text{órbitas}|$, resulta que $|\mathscr{O}|$ es congruente con 1 módulo p; mientras que descomponiendo $\mathscr{O}$ en P_2–órbitas resulta que $|\mathscr{O}|$ es congruente con 0 módulo p. Esta contradicción proviene de suponer que existe un p–subgrupo de Sylow que no está en $\mathscr{O}$. Por tanto $\mathscr{S} = \mathscr{O}$, como queríamos probar.

(2) Según hemos visto en la prueba de (1) el número de p–subgrupos de Sylow $|\mathscr{S}| = |\mathscr{O}|$ es congruente con 1 módulo p.
Además, puesto que $|\mathscr{O}| = [G : \operatorname{Stab} P] = [G : N_G(P)]$, donde P es un p–subgrupo de Sylow, el Teorema de Lagrange dice que $|\mathscr{S}|$ es un divisor de $|G|$. Ahora bien, $|G| = |P|\,[G : P]$ y $|\mathscr{S}|$ y $|P|$ son primos entre sí. Por tanto $|\mathscr{S}| \mid [G : P]$.

(3) Sea H un subgrupo de G de orden p^k. Consideramos la acción de H en $\mathscr{S}$. Como antes, vemos que las H–órbitas tienen cardinal 1 o una potencia positiva de p. Puesto que $|\mathscr{S}|$ es congruente con 1 módulo p, deducimos que existe una H–órbita de cardinal 1. Sea ésta $\{P\}$. Entonces $H \subset N_G(P)$. Así, según el Lema 2.5.8, $H \subset P$. □

Corolario 2.5.10. *Sean G un grupo finito, p un divisor primo de $|G|$, y P un p–subgrupo de Sylow de G. Entonces P es el único p–subgrupo de Sylow de G si, y sólo si, $P \trianglelefteq G$.*

Demostración. En la demostración del Segundo Teorema de Sylow hemos visto que el número de p–subgrupos de Sylow es $s_p = [G : N_G(P)]$. Por tanto P es único si, y sólo si, $[G : N_G(P)] = 1$. Esta condición equivale a $N_G(P) = G$, es decir $P \trianglelefteq G$. □

Ejemplo 2.5.11. Sea G un grupo de orden $|G| = 2^2 \cdot 7$. Por el primer teorem de Sylow, existen subgrupos de órdenes $|H_2| = 2, |H_4| = 2^2, |H_7| = 7$. Por el segundo teorema, $s_2 \mid [G : H_4] = 7$ y $s_2 = 2k + 1$. Por tanto, $s_2 = 1$ o $s_2 = 7$. También $s_7 = 7k + 1 \mid [G : H_7] = 4$. Por tanto, $s_7 = 1$ y, en consecuencia, $H_7 \trianglelefteq G$. El cociente G/H_7 tiene un subgrupo H_{14}/H_7 de orden 2. Por tanto, G tiene un subgrupo H_{14} de orden 14. Así, G tiene subgrupos de órdenes cualquier divisor de $|G|$.

Como aplicación de los Teoremas de Sylow podemos clasificar los grupos de orden $2p$.

Ejemplo 2.5.12. Sean G un grupo de orden $2p$, donde $p > 2$ es primo.
El primer teorema de Sylow asegura que G tiene 2–subgrupos de Sylow de orden 2 y p–subgrupos de Sylow de orden p. El número s_2 de 2–subgrupos de Sylow divide a p y es de la forma $2k + 1$. Por tanto $s_2 = 1$ o $s_2 = p$. El número s_p de p–subgrupos de Sylow divide a 2 y es de la forma $ph + 1$. Por tanto $s_p = 1$. Es decir, G tiene un único subgrupo H de orden p, y este subgrupo es normal, y puede tener 1 ó p subgrupos de orden 2.

Caso 1. Supongamos que existe un único subgrupo K de orden 2. Entonces K es normal en G. En estas condiciones $H \cap K = \{1\}$ y $G \simeq H \times K \simeq \mathbb{Z}_p \times \mathbb{Z}_2 \simeq \mathbb{Z}_{2p}$ es cíclico.

Caso 2. Supongamos que G tiene p elementos de orden 2. Ninguno de estos p elementos están en H, puesto que H tiene orden $p > 2$ primo. Por tanto, si $H =< \sigma >$ y $\tau \notin H$ entonces $G = H \cup \tau H$ y $H \cap \tau H = \emptyset$. Esto es $G = \{1, \sigma, \ldots, \sigma^{p-1}, \tau, \tau\sigma, \ldots, \tau\sigma^{p-1}\}$. Además, el orden de $\tau\sigma^i$ es 2 para cada $i = 0, \cdots, p-1$. Ahora,

$$(\tau\sigma^i)^2 = 1 \Rightarrow \sigma^{-i}\tau^{-1} = \tau\sigma^i \Rightarrow \sigma^{p-i}\tau = \tau\sigma^i.$$

Las identidades

$$\sigma^p = 1, \quad \tau^2 = 1, \quad \sigma^{p-i}\tau = \tau\sigma^i, \quad i = 0, \ldots, p-1,$$

determinan el grupo G, que resulta ser isomorfo al grupo diedro D_p.

2.6. Grupos resolubles

Denotaremos $G \rhd H$ un subgrupo normal propio H de un grupo G.

2.6.1. Definición. Caracterización

Definición 2.6.1. Un grupo G se dice simple si sus únicos subgrupos normales son $\{1\}, G$.

Ejemplo 2.6.2. Sea G grupo conmutativo finito. Entonces, G es simple si, y sólo si, G es cíclico de orden primo (ejercicio).

Definición 2.6.3. Una sucesión de subgrupos cada uno normal en el inmediatamente anterior,

$$G = G_k \rhd G_{k-1} \rhd \cdots \rhd G_1 \rhd G_0 = \{1\}, \tag{2.6.3.1}$$

es una serie normal para el grupo G.

Ejemplos 2.6.4. (1) $S_2 \rhd \{1\}$, serie normal de longitud máxima. El cociente $S_2/\{1\} \simeq \mathbb{Z}_2$ es cíclico de orden primo.

(2) $S_3 \rhd A_3 \rhd \{1\}$, serie normal de longitud máxima. Los cocientes $S_3/A_3 \simeq \mathbb{Z}_2, A_3/\{1\} \simeq \mathbb{Z}_3$ son cíclicos de orden primo.

(3) $S_4 \rhd A_4 \rhd V \rhd W \rhd \{1\}$,
$V = \{(1), (12)(34), (13)(24), (14)(23)\}, W = \{(1), (12)(34)\}$, serie normal de longitud máxima. Los cocientes $S_4/A_4 \simeq \mathbb{Z}_2$, $A_4/V \simeq \mathbb{Z}_3$, $W/\{1\} \simeq \mathbb{Z}_2$ son cíclicos de orden primo.

(4) $S_5 \rhd A_5 \rhd \{1\}$.

Ejercicio 2.6.5. Comprobar que $A_4 \rhd V$ (puesto que V es conmutativo, es trivial que $V \rhd W$).

Observación 2.6.6. A una serie normal (2.6.3.1) le asociamos los cocientes

$$G_k/G_{k-1},\ G_{k-1}/G_{k-2},\ \ldots,\ G_1/G_0 = G_1, \tag{2.6.6.1}$$

que denominaremos *factores*.

Definición 2.6.7. *Diremos que un grupo G es resoluble si tiene una serie normal cuyos factores son todos conmutativos.*

Ejemplos 2.6.8. (1) Las series normales de (2.6.4) para S_3 y S_4, prueban que estos dos grupos simétricos son resolubles. En efecto:

El cociente S_3/A_3 es de orden 2, por tanto cíclico. El grupo A_3 es cíclico de orden 3. El cociente S_4/A_4 es de orden 2, A_4/V es de orden 3, V/W y W de orden 2.

(2) Todo grupo conmutativo es resoluble.

Teorema 2.6.9. *Todo grupo finito de orden potencia de un primo es resoluble.*

Demostración. Sea G de orden p^n, donde p es primo y $n \geq 1$. Según Corolario 2.4.15, G tiene centro no trivial Z_1. Si $G = Z_1$ entonces G es conmutativo y, por tanto, resoluble. En otro caso, ponemos $G_1 = Z_1 \lhd G$. Ahora el grupo G/G_1 tiene centro no trivial Z_2 de la forma $Z_2 = G_2/G_1$, con $G \rhd G_2 \rhd G_1$. Construimos así una serie

$$G = G_{s+1} \rhd G_s \rhd \cdots \rhd G_1 \rhd G_0 = \{1\},$$

donde cada factor $G_{i+1}/G_i = Z(G/G_i)$ es conmutativo. □

Caracterizamos ahora los grupos resolubles en términos de la serie derivada.

Definición 2.6.10 (Subgrupo derivado)**.** Sea G un grupo. Para cada $g, h \in G$ consideramos el conmutador $[g,h] = g^{-1}h^{-1}gh$. El *subgrupo derivado* G' es el subgrupo generado por todos los conmutadores. Puesto que $[g,h]^{-1} = [h,g]$, el subgrupo G' es el conjunto de los productos $[g_1,h_1]\cdots[g_r,h_r]$.

Observación 2.6.11. (1) Si $G \xrightarrow{\eta} \overline{G}$ es un homomorfismo $\eta(G') \subset \overline{G}'$, puesto que $\eta([g,h]) = [\eta(g),\eta(h)]$.

(2) Si $K \trianglelefteq G$ entonces cada automorfismo interior $G \xrightarrow{I_a} G$, $x \mapsto axa^{-1}$ induce un endomorfismo $K \xrightarrow{I_a} K$. Por tanto, $I_a(K') \subset K'$, para cada $a \in G$. En consecuencia, $K' \trianglelefteq G$.

Es decir

$$K \trianglelefteq G \Rightarrow K' \trianglelefteq G. \tag{2.6.11.1}$$

(3) En particular, de $G \trianglelefteq G$ deducimos $G' \trianglelefteq G$.

(4) Además G/G' es conmutativo, directamente de la definición de G'. Es más, si $H \trianglelefteq G$ y G/H es conmutativo entonces $G' \leq H$.

Definición 2.6.12 (Serie derivada)**.** Definimos $(G')' = (G')', \ldots, G^{(k)} = (G^{(k-1)})'$. Tenemos entonces la serie derivada

$$G \trianglerighteq G' \trianglerighteq (G')' \trianglerighteq \cdots \trianglerighteq G^{(k)} \trianglerighteq \cdots, \tag{2.6.12.1}$$

donde por inducción, usando (2.6.11.1), vemos que cada $G^{(k)} \trianglelefteq G$.

Teorema 2.6.13. *Un grupo G es resoluble si, y sólo si, $G^{(k)} = \{1\}$ para algún $k \geq 1$.*

Demostración. Si $G \neq \{1\}$ y k es el primer entero tal que $G^{(k)} = \{1\}$ entonces

$$G \rhd G' \rhd (G')' \rhd \cdots \rhd G^{(k)} = \{1\},$$

y, puesto que cada cociente $G^{(i)}/G^{(i+1)}$ es conmutativo, G es resoluble.
Recíprocamente, si G tiene una serie normal (2.6.3.1) con factores (2.6.6.1) conmutativos, entonces $G_i' \leq G_{i-1}$. En particular, $G' = G_k' \leq G_{k-1}$ y, por tanto, $(G')' \leq G_{k-1}' \leq G_{k-2}$. Además, suponiendo que $G^{(i)} \leq G_{k-i}$ entonces $G^{(i+1)} = (G^{(i)})' \leq G_{k-i}' \leq G_{k-i-1}$. Por tanto, $G^{(s)} \leq G_{k-s}$ y, puesto que $G_0 = \{1\}$ es $G^{(k)} = \{1\}$. □

Teorema 2.6.14. *Todo subgrupo y toda imagen homomorfa de un grupo resoluble es resoluble. Recíprocamente, si $K \trianglelefteq G$ es tal que K y G/K son resolubles entonces G es resoluble.*

Demostración. Si $H \leq G$ entonces $H^{(i)} \leq G^{(i)}$. Por tanto $G^{(k)} = \{1\} \Rightarrow H^{(k)} = \{1\}$. Sea $G \xrightarrow{\eta} H$ un homomorfismo. Entonces $\eta(G') = (\eta(G))'$ y $\eta((G')') = \eta((G')') = (\eta(G'))' = (\eta(G)')' = (\eta(G)')'$. Así $\eta(G^{(i)}) = (\eta(G))^{(i)}$. Por tanto $G^{(k)} = \{1\} \Rightarrow (\eta(G))^{(k)} = \{1\}$.
Supongamos ahora $K \trianglelefteq G$ y G/K resolubles. Puesto que $G \xrightarrow{\pi} G/K$ es sobreyectivo $\pi(G^{(i)}) = (G/K)^{(i)}$. Por tanto, $\pi(G^{(k)}) = \{1\}$, para algún k. Esto significa $G^{(k)} \leq K$. Puesto que K es resoluble $K^{(l)} = \{1\}$, para cierto l. En consecuencia, $G^{(k+l)} = (G^{(k)})^{(l)} \leq K^{(l)} = \{1\}$. □

Corolario 2.6.15. *Si G es resoluble y $H \trianglelefteq G$ entonces G/H es resoluble.*

Corolario 2.6.16. *El grupo simétrico S_n no es resoluble para $n \geq 5$.*

Demostración. Según el Teorema 2.6.14, si S_n fuera resoluble también lo sería A_n. Pero el Teorema de Abel asegura que A_n es simple para $n \geq 5$ y, por tanto, la única serie normal es $A_n \rhd \{1\}$. Esto es, de ser A_n resoluble sería conmutativo. Sin embargo, (123), (234) no conmutan. □

Finalmente obtendremos un criterio para decidir si un grupo finito es resoluble en términos de una serie de composición del grupo.

2.6.2. Teorema de Jordan–Holder

Definición 2.6.17. Una serie de composición de un grupo G es una serie normal

$$G = G_s \rhd G_{s-1} \rhd \cdots \rhd G_1 \rhd G_0 = \{1\},$$

tal que cada G_{i-1} es subgrupo normal maximal en G_i, es decir, G_i/G_{i-1} es simple. En este caso, los factores G_i/G_{i-1} se denominan factores de composición de G.

Observación 2.6.18. Todo grupo finito G posee una serie de composición, puesto que el conjunto de subgrupos normales es finito. □

Ejemplo 2.6.19. $(\mathbb{Z}, +)$ no admite serie de composición: entre $\{0\}$ y $\{0\} \neq n\mathbb{Z}$ hay una cadena infinita de subgrupos.

Teorema 2.6.20 (de Jordan–Holder)**.** *Sean G un grupo finito y*

$$G = G_s \rhd G_{s-1} \rhd \cdots \rhd G_1 \rhd G_0 = \{1\}, \tag{2.6.20.1}$$

$$G = H_t \rhd H_{t-1} \rhd \cdots \rhd H_1 \rhd H_0 = \{1\}, \tag{2.6.20.2}$$

dos series de composición en G. Entonces $s = t$ y existe una permutación σ de $\{1, \ldots, s\}$ tal que $G_i/G_{i-1} \simeq H_{\sigma(i)}/H_{\sigma(i)-1}$.

Demostración. Inducción en $|G|$. Si $G = \{1\}$ es trivial. Supongamos $|G| > 1$ y cierto para grupos de orden menor que $|G|$.
Caso 1. $G_{s-1} = H_{t-1}$. Entonces

$$G_{s-1} \rhd \cdots \rhd G_1 \rhd G_0 = \{1\},$$
$$H_{t-1} \rhd \cdots \rhd H_1 \rhd H_0 = \{1\},$$

son dos series para $G_{s-1} = H_{t-1}$ y, por inducción, se concluye.
Caso 2. $G_{s-1} \neq H_{t-1}$. En este caso, de $G_{s-1} \lhd G$ y $H_{t-1} \lhd G$ se deduce $G_{s-1}H_{t-1} \lhd G$. Además $G_{s-1} \lhd G_{s-1}H_{t-1}$. Puesto que G_{s-1} es normal maximal en G, se deduce $G_{s-1} = G_{s-1}H_{t-1}$ o $G_{s-1}H_{t-1} = G$. Si $G_{s-1} = G_{s-1}H_{t-1}$ entonces $H_{t-1} \leq G_{s-1}$. Así $H_{t-1} \lhd G_{s-1} \lhd G$ y, puesto que H_{t-1} es normal maximal en G y $G_{s-1} \neq G$, es $G_{s-1} = H_{t-1}$. Por tanto, $G_{s-1}H_{t-1} = G$. En esta situación, según el segundo teorema de isomorfismo, $G/G_{s-1} = G_{s-1}H_{t-1}/G_{s-1} \simeq H_{t-1}/G_{s-1}\cap H_{t-1}$ y $G/H_{t-1} = G_{s-1}H_{t-1}/H_{t-1} \simeq G_{s-1}/G_{s-1}\cap H_{t-1}$. Por tanto, puesto que G/G_{s-1} y G/H_{t-1} son grupos simples también son simples $H_{t-1}/G_{s-1} \cap H_{t-1}$ y $G_{s-1}/G_{s-1} \cap H_{t-1}$. En consecuencia, $K = G_{s-1} \cap H_{t-1}$ es normal maximal en G_{s-1} y en H_{t-1} y $G/G_{s-1} \simeq H_{t-1}/K$, $G/H_{t-1} \simeq G_{s-1}/K$.
Sea $K = K_{r-2} \rhd K_{r-3} \rhd \cdots \rhd K_1 \rhd K_0 = \{1\}$ una serie de composición para K. Puesto que $K = K_{r-2}$ es normal maximal en G_{s-1} y en H_{t-1} obtenemos series de composición

$$G = G_s \rhd G_{s-1} \rhd K_{r-2} \rhd \cdots \rhd K_1 \rhd K_0 = \{1\}, \tag{2.6.20.3}$$

$$G = H_t \rhd H_{t-1} \rhd K_{r-2} \rhd \cdots \rhd K_1 \rhd K_0 = \{1\}, \tag{2.6.20.4}$$

El caso 1 aplicado a (2.6.20.1) y (2.6.20.3) asegura que $r = s$ y $G_i/G_{i-1} \simeq K_{\sigma(i)}/K_{\sigma(i)-1}$, para cierta σ con $\sigma(1) = 1$. Aplicado a (2.6.20.2) y (2.6.20.4) dice que $t = r$ y $H_j/H_{j-1} \simeq K_{\tau(j)}/K_{\tau(j)-1}$, para cierta τ con $\tau(1) = 1$. De aquí concluimos lo afirmado en el teorema. □

Definición 2.6.21. Llamaremos factores de composición a los factores de una serie de composición de un grupo finito.

Ejemplo 2.6.22. Series de composición para el grupo diedro $D_4 =< \sigma, \tau >$.

$$D_4 \rhd < \tau, \sigma^2 > \rhd < \sigma^2 > \rhd \{1\},$$
$$D_4 \rhd < \tau, \sigma^2 > \rhd < \tau > \rhd \{1\},$$
$$D_4 \rhd < \sigma > \rhd < \sigma^2 > \rhd \{1\}.$$

Teorema 2.6.23. *Un grupo finito es resoluble si, y sólo si, todos sus factores de composición son cíclicos de orden primo.*

Demostración. Si G es finito y resoluble entonces cada factor G_i/G_{i-1} de una serie de composición resulta resoluble y simple. Por tanto G_i/G_{i-1} es conmutativo y simple. Esto implica que es cíclico de orden primo. Recíprocamente si los factores de composición son cíclicos, también son conmutativos y el grupo es resoluble. □

2.7. Grupos conmutativos finitamente generados

Definición 2.7.1. (1) Sea $(G,+)$ un grupo conmutativo. Diremos que G es un grupo conmutativo finitamente generado si existe una familia finita de elementos $S = \{x_1,\dots,x_r\}$ de elementos de G tal que cada elemento $x \in G$ se puede escribir como una combinación lineal $x = m_1x_1 + \cdots + m_rx_r$ para ciertos $m_1,\dots,m_r \in \mathbb{Z}$. Diremos que S es una familia (o conjunto) de generadores de G.

(2) Sea $S = \{x_1,\dots,x_r\}$ una familia en G. La aplicación $\varphi : \mathbb{Z}^r \to G$ definida por $(m_1,\dots,m_r) \mapsto m_1x_1 + \cdots + m_rx_r$ es un homomorfismo de grupos aditivos.

(3) La familia S es un conjunto de generadores si, y sólo si, φ es sobreyectivo. Es este caso, φ induce un isomorfismo $\mathbb{Z}^r/\ker\varphi \simeq G$. Diremos que el subgrupo $H = \ker\varphi$ es el subgrupo de las relaciones entre los generadores $S = \{\varphi(e_1) = x_1,\dots,\varphi(e_r) = x_r\}$. Es decir $(m_1,\dots,m_r) \in H \Leftrightarrow m_1x_1 + \cdots + m_rx_r = 0$.

(4) Diremos que S es una familia libre si φ es inyectivo. Es decir, si $m_1x_1 + \cdots + m_rx_r = 0 \Rightarrow m_1 = \cdots m_r = 0$.

(5) Diremos que G es un grupo conmutativo finitamente generado libre si existe una familia finita de generadores S tal que φ es un isomorfismo. Es decir, cada elemento $x \in G$ se escribe, de modo único, como combinación lineal $x = m_1x_1 + \cdots + m_rx_r$ para ciertos $m_1,\dots,m_r \in \mathbb{Z}$.

Lema 2.7.2. *Sean $d_1,\dots,d_r \in \mathbb{Z}$ y $e_i = (0,\dots,1,\dots,0) \in \mathbb{Z}^r$, $i = 1,\dots,r$. Existe un ismorfismo*

$$\frac{\mathbb{Z}^r}{< d_1e_1,\dots,d_re_r >} \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}.$$

Demostración. El homomorfismo $\mathbb{Z}^r \to \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}$ definido por $e_i \mapsto (\overline{0},\dots,\overline{1},\dots,\overline{0})$ es sobreyectivo y su núcleo es el subgrupo $< d_1e_1,\dots,d_re_r >$. Por el primer teorema de isomorfía, se tiene el isomorfismo. □

Proposición 2.7.3. *Sean L un grupo libre finitamente generado un isomorfismo y $L \simeq \mathbb{Z}^r$ y $L \simeq \mathbb{Z}^s$ ismorfismos. Entonces $r = s$. Diremos que r es el rango del grupo libre finitamente generado L.*

Demostración. Consideramos el subgrupo $2L = \{2x \mid x \in L\} \leq L$. Sea $\varphi : \mathbb{Z}^r \to L$ definido por $e_i \mapsto x_i$ un isomorfismo. Entonces $\varphi(< 2e_1,\dots,2e_r >) = 2L$. Por tanto

$$\frac{\mathbb{Z}^r}{< 2e_1,\dots,2e_r >} \simeq L/2L.$$

Según Lema 2.7.2, obtenemos un isomorfismo

$$(\mathbb{Z}_2)^r \simeq L/2L.$$

Este isomorfismo muestra que $L/2L$ tiene 2^r elementos. De forma similar, de un isomorfismo $\mathbb{Z}^s \to L$ deducimos que $L/2L$ tiene 2^s elementos. Por tanto, $r = s$. □

Proposición 2.7.4. *Sean G un grupo conmutativo finitamente generado y $H \leq G$ un subgrupo. Entonces H es finitamente generado.*

Demostración. Inducción sobre el número de generadores. Si $G =< x >$, entonces $G \simeq \mathbb{Z}$ o $G \simeq \mathbb{Z}_n$. En los dos casos los subgrupos son cíclicos. Sea G generado por $\{x_1, \ldots, x_r\}$ con $r > 1$ y cierto para grupos generados por s elementos con $1 \leq s < r$. Sea $H \leq G$. El conjunto de los coeficientes de x_1 en la expresión de los elementos de H como combinación lineal de $\{x_1, \ldots, x_r\}$ es un ideal de $\mathbb{Z}$ generado por cierto número d; y existe una combinación lineal $dx_1 + m_2x_2 + \cdots + m_rx_r \in H$. Puesto que, por hipótesis de inducción, $H \cap < x_2, \ldots, x_r >$ es finitamente generado, bastará probar que $H = (H \cap < x_2, \ldots, x_r >) + < dx_1 + m_2x_2 + \cdots + m_rx_r >$. En efecto, sea $h = n_1x_1 + n_2x_2 + \cdots + n_rx_r \in H$. Entonces, el coeficiente $n_1 = dk$, para algún k. Por tanto, se verifica que $h - k(dx_1 + m_2x_2 + \cdots + m_rx_r) \in < x_2, \ldots, x_r >$. Así $h = k(dx_1 + m_2x_2 + \cdots + m_rx_r) + (h - k(dx_1 + m_2x_2 + \cdots + m_rx_r)) \in < dx_1 + m_2x_2 + \cdots + m_rx_r > + (H \cap < x_2, \ldots, x_r >)$. □

Definición 2.7.5. Sea G un grupo conmutativo. Un elemento $x \in G$ se dice de torsión si existe $0 \neq m \in \mathbb{Z}$ tal que $mx = 0$. El conjunto $T(G)$ de los elementos de torsión de G es un subgrupo de G denominado el subgrupo de torsión de G. Diremos que G es libre de torsión si $T(G) = \{0\}$.

Lema 2.7.6. *Sean L, F grupos conmutativos (finitamente generados).*

(1) $T(L \oplus F) = T(L) \oplus T(F)$.

(2) Si L es libre, entonces $T(L) = \{0\}$.

(3) Si F es finito, entonces $T(F) = F$.

(4) $T(G/T(G)) = 0$.

Demostración. (1) Sean $x \in L$, $y \in F$. Entonces $m(x, y) = (0, 0) \Leftrightarrow mx = 0$ y $my = 0$.

(2) Sea $S = \{x_1, \ldots, x_r\}$ un sistema de generadores libre. Entonces, si $m \neq 0$ se tiene $m(m_1x_1 + \cdots + m_rx_r) = 0 \Leftrightarrow mm_1x_1 + \cdots + mm_r = 0 \Leftrightarrow mm_1 = \cdots = mm_r = 0 \Leftrightarrow m_1 = \cdots = m_r = 0 \Leftrightarrow m_1x_1 + \cdots + m_rx_r = 0$.

(3) Si F es finito, entonces todo elemento $y \in F$ es de orden finito. Por tanto, existe $m \neq 0$ tal que $my = 0$.

(4) $m\overline{x} = 0, m \neq 0 \Rightarrow \overline{mx} = 0 \Rightarrow mx \in T(G) \Rightarrow m_1mx = 0, m_1 \neq 0 \Rightarrow x \in T(G) \Rightarrow \overline{x} = 0$.

□

Ejemplo 2.7.7. $T(\mathbb{Z} \oplus \mathbb{Z}_n) = \mathbb{Z}_n$.

Proposición 2.7.8. *Sea G un grupo finitamente generado. Si $T(G) = 0$, entonces G es libre.*

Demostración. Sean r el número mínimo de elementos en un sistema de generadores de G. Supongamos que G no es libre. Entonces hay relaciones no triviales entre los elementos de cualquier sistema con r generadores. Sean m el mínimo entre los coeficientes positivos de cualquier relación no trivial entre los elementos de cualquier sistema de generadores con r elementos y $mx_1 + m_2x_2 + \cdots + m_rx_r = 0$ una relación. Dividimos $m_i = mq_i + t_i, 0 \leq t_i < m, i = 2, \ldots, r$. Entonces $m(x_1 + q_2x_2 + \cdots + q_rx_r) + t_2x_2 + \cdots + t_rx_r = 0$. Por tanto, $t_i = 0, i = 2, \ldots, r$. Así $m(x_1 + q_2x_2 + \cdots + q_rx_r) = 0$. Como $T(G) = 0$, se deduce que $x_1 + q_2x_2 + \cdots + q_rx_r = 0$. Por tanto, $\{x_2, \ldots, x_r\}$ es un sistema de generadores. Esto es contario a la elección de r. En consecuencia, la única relación entre los elementos de un sistema de r generadores es la trivial y, por tanto, G es libre. □

Corolario 2.7.9. *Sean L un grupo conmutativo finitamente genrado libre y $M \leq L$ un subgrupo. Entonces M es libre.*

Demostración. Proposición 2.7.4, $T(M) \subset T(L) = 0$ y Proposición 2.7.8. □

Proposición 2.7.10. *Sean G un grupo conmutativo finitamente generado y $L' = G/T(G)$. Entonces L' es libre y si $\{e_1, \ldots, e_r\} \in G$ son tales que $\{\overline{e_1}, \ldots, \overline{e_r}\}$ es un sistema libre de generadores de L', entonces $L =< e_1, \ldots, e_r > \simeq L'$ es libre y $G = L \oplus T(G)$.*

Demostración. Segun Lema 2.7.6 (4) y Proposición 2.7.8, L' es libre. Si $m_1e_1 + \cdots + m_re_r = 0$, entonces $m_1\overline{e_1} + \cdots + m_r\overline{e_r} = 0$. Como $\{\overline{e_1}, \ldots, \overline{e_r}\}$ es un sistema libre, se deduce que $m_1 = \cdots = m_r = 0$. Por tanto, L es libre y $L \simeq L'$. Puesto que L es libre, L es sin torsión. Por tanto $L \cap T(G) = 0$. Así, basta probar que $G = L + T(G)$. Sean $x \in G$ y $\overline{x} = m_1\overline{e_1} + \cdots m_r\overline{e_r}$. Entonces, $y = m_1e_1 + \cdots + m_re_r \in L$ y $x - y \in T(G)$, puesto que $\overline{x} = \overline{y}$. Así $x = y + (x - y) \in L + T(G)$. □

Definición 2.7.11. Sea G un grupo conmutativo finitamente generado. Llamaremos rango de G al rango del grupo libre $G/T(G)$.

Ejemplo 2.7.12. *El rango de $\mathbb{Z}^3 \oplus \mathbb{Z}_5$ es 3.*

Proposición 2.7.13. *Sean L un grupo conmutativo libre de rango r y $\{0\} \neq M \leq L$ un subgrupo. Entonces existen un sistema libre de generadores $\{e_1, \ldots, e_r\}$ de L y $d_1, \ldots, d_s$ enteros positivos con $s \leq r$, tales que $\{d_1e_1, \ldots, d_se_s\}$ es un sistema libre de generadores de M y $d_1 \mid d_2 \mid \cdots \mid d_s$.*

Demostración. Inducción en r. Si $r = 1$, entonces $L =< e_1 > \simeq \mathbb{Z}$. Por tanto, los subgrupos no nulos de L son de la forma $< de_1 >$ con $d > 0$. Sea $r > 1$ y cierto para grupos libres de rango $< r$. Puesto que $M \neq \{0\}$, el conjunto de los coeficientes positivos de la expresión de los elementos no nulos de M como combinación lineal de cualquier sistema libre de generadores de L tiene un elemento mínimo $d_1 > 0$; y existe una expresión $0 \neq d_1v_1 + m_2v_2 + \cdots + m_rv_r \in M$, donde $\{v_1, \ldots, v_r\}$ es un sistema libre de generadores de L. Dividimos $m_i = d_1q_i + t_i, 0 \leq t_i < d_1, i = 2, \cdots, r$. Entonces $0 \neq d_1(v_1 + q_2v_2 + \cdots + q_rv_r) + t_2v_2 + \cdots + t_rv_r \in M$. Por tanto, puesto que $w_1 = v_1 + q_2v_2 + \cdots + q_rv_r, w_2 = v_2, \ldots, w_r = v_r$ forman un sistema libre de generadores de L, por la elección de d_1, ha de ser $t_i = 0$ y, se deduce que $d_1w_1 \in M$. Por hipótesis de inducción, para $M \cap < w_2, \ldots, w_r >$ existen $d_2 \mid \cdots \mid d_s$

enteros positivos, con $s-1 \leq r-1$, y un sistema libre de generadores $\{e_2, \ldots, e_r\}$ del grupo libre $< w_2, \ldots, w_r >$ tales que $\{d_2e_2, \ldots, d_se_s\}$ es un sistema libre de generadores de $M \cap < w_2, \ldots, w_r >$. Los elementos $e_1 = w_1, e_2, \ldots, e_r$ son un sistema libre de generadores de L tal que $d_1e_1, d_2e_2, \ldots d_se_s \in M$, $d_2 \mid \cdots \mid d_s$ y $M \cap < e_2, \ldots, e_r > = < d_2e_2, \ldots, d_se_s >$. Por tanto, basta probar que $M = (M \cap < e_2, \ldots, e_r >) \oplus < d_1e_1 >$ y que $d_1 \mid d_2$. En efecto, sea $0 \neq x \in M$, entonces $x = n_1e_1 + n_2e_2 + \cdots + n_re_r$, para ciertos $n_1, n_2, \ldots, n_r$. Dividimos $n_1 = d_1q + t, 0 \leq t < d_1$. Así $x - q(d_1e_1) = te_1 + n_2e_2 + \cdots + n_re_r \in M$. Por tanto, según la elección de d_1, ha de ser $t = 0$ y $n_2e_2 + \cdots + n_re_r \in M$ Así $x = q(d_1e_1) + n_2e_2 + \cdots + n_re_r \in < d_1e_1 > + (M \cap < e_2, \ldots, e_r >)$. Ademas $< d_1e_1 > \cap (M \cap < e_2, \ldots, e_r >) = \{0\}$, puesto que $\{e_1, e_2, \ldots, e_r\}$ es libre y $d_1 \neq 0$. Finalmente, consideramos el elemento $d_1e_1 + d_2e_2 \in M$. Dividimos, $d_2 = d_1q + t, 0 \leq t < d_1$. Entonces $d_1(e_1 + qe_2) + te_2 + 0e_3 + \ldots + 0e_r \in M$. Por la elección de d_1 ha de ser $t = 0$. Así $d_1 \mid d_2$. □

Teorema 2.7.14 (Teorema de estructura)**.** *Sea G un grupo conmutativo finitamente generado, entonces existen enteros $0 \leq r, 1 \leq d_1 \mid \cdots \mid d_s$, únicos tales que*

$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_s}.$$

Demostración. Puesto que G es finitamente generado, existe un homomorfismo sobreyectivo $\varphi : \mathbb{Z}^n \to G$, para cierto n. Por la Proposición 2.7.13, existen un sistema libre de generadores $\{e_1, \ldots, e_n\}$ de $\mathbb{Z}^n$ y enteros $1 \leq d_1 \mid \cdots \mid d_s$ tales que $\{d_1e_1, \ldots, d_se_s\}$ es un sistema libre de generadores de $\ker \varphi$. Así

$$G \simeq \frac{\mathbb{Z}^n}{\ker \varphi} = \frac{< e_1 > \oplus \cdots \oplus < e_s > \oplus < e_{s+1} > \oplus \cdots \oplus < e_n >}{< d_1e_1 > \oplus \cdots \oplus < d_se_s >} \simeq$$

$$\simeq \frac{< e_1 >}{< d_1e_1 >} \oplus \cdots \oplus \frac{< e_s >}{< d_se_s >} \oplus < e_{s+1} > \oplus \cdots \oplus < e_n > \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_s} \oplus \mathbb{Z}^{n-s}.$$

Unicidad se prueba en la Observación 2.7.20. □

Observación 2.7.15. En el Teorema 2.7.14, el entero r es el rango de G. Los enteros $d_1 \mid \cdots \mid d_s$ se denominan factores invariantes o coeficientes de torsión de G. Además G es finito si, y sólo si, $r = 0$. En este caso $G \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_s}$.

Observación 2.7.16. Una sorprendente consecuencia del Teorema 2.7.14 es el Teorema 3.6.7, que afirma que todo subgrupo finito del grupo multiplicativo de un cuerpo es cíclico.

Observación 2.7.17 (Divisores elementales)**.** Si $d = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ donde los p_i son primos distintos y $\alpha_i \geq 1$, entonces

$$\mathbb{Z}_d \simeq \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{\alpha_m}}.$$

Dados $1 < d_1 \mid d_2 \mid \cdots \mid d_s$ escribimos

$$\begin{aligned}
d_1 &= p_{11}^{\alpha_{11}} \cdots p_{1m_1}^{\alpha_{1m_1}} \\
d_2 &= p_{11}^{\alpha_{21}} \cdots p_{1m_1}^{\alpha_{2m_1}} p_{21}^{\alpha_{2m_1+1}} \cdots p_{2m_2}^{\alpha_{2m_1+m_2}} \\
&\vdots \\
d_s &= p_{11}^{\alpha_{s1}} \cdots p_{1m_1}^{\alpha_{sm_1}} p_{21}^{\alpha_{sm_1+1}} \cdots p_{2m_2}^{\alpha_{sm_1+m_2}} \cdots p_{s1}^{\alpha_{sm_1+m_2+\cdots+m_{s-1}+1}} \cdots p_{sm_s}^{\alpha_{sm_1+m_2+\cdots+m_{s-1}+m_s}}.
\end{aligned}$$

Los $p_{ij}^{\alpha_{kl}}$ son los divisores elementales.

$$\mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_s} \simeq \oplus_{ijkl} \mathbb{Z}_{p_{ij}^{\alpha_{kl}}}.$$

Puesto que el proceso es reversible, y si $\mathbb{Z}^r \oplus \mathbb{Z}_{d_1} \oplus \ldots \oplus \mathbb{Z}_{d_s} \simeq G \simeq \mathbb{Z}_{r'} \oplus \mathbb{Z}_{d'_1} \oplus \ldots \oplus \mathbb{Z}_{d'_{s'}}$, entonces $\mathbb{Z}^r \simeq G/T(G) \simeq \mathbb{Z}^{r'} \Rightarrow r = r'$ y $\mathbb{Z}_{d_1} \oplus \ldots \oplus \mathbb{Z}_{d_s} \simeq T(G) \simeq \mathbb{Z}_{d'_1} \oplus \ldots \oplus \mathbb{Z}_{d'_{s'}}$; la unicidad de los coeficientes de torsión es equivalente a la unicidad de los divisores elementales. Demostraremos la unicidad de los factores invariantes en la Obervación 2.7.20.

Ejemplo 2.7.18. Grupos finitos de orden $1400 = 2^3 \cdot 5^2 \cdot 7$.

$$\begin{aligned}
\mathbb{Z}_2 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{70} &\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \\
\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{350} &\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{5^2} \oplus \mathbb{Z}_7 \\
\mathbb{Z}_{10} \oplus \mathbb{Z}_{140} &\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \\
\mathbb{Z}_2 \oplus \mathbb{Z}_{700} &\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{5^2} \oplus \mathbb{Z}_7 \\
\mathbb{Z}_5 \oplus \mathbb{Z}_{280} &\simeq \mathbb{Z}_{2^3} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \\
\mathbb{Z}_{1400} &\simeq \mathbb{Z}_{2^3} \oplus \mathbb{Z}_{5^2} \oplus \mathbb{Z}_7
\end{aligned}$$

Corolario 2.7.19. *Sea G un grupo conmutativo finitamente generado, entonces existen un entero $r \geq 0$ y números primos $p_1, \ldots, p_m$ junto con enteros positivos $\alpha_1, \ldots, \alpha_m$, únicos con la propiedad de que si $p_i = p_{i+1}$, entonces $\alpha_i \leq \alpha_{i+1}$, tales que*

$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{\alpha_m}}.$$

Observación 2.7.20 (Unicidad de los factores invariantes)**.** Sean G un grupo finito conmutativo y $G =< \overline{e_1} > \oplus \cdots \oplus < \overline{e_s} >$ una descomposición donde $< \overline{e_i} > \simeq \mathbb{Z}_{d_i}$ con $1 < d_1 \mid \cdots \mid d_s$. Denotaremos $G_i =< \overline{e_i} >$.
Para cada primo p definimos los subgrupos

$$G_i(p) = \{x \in G_i \mid px = 0\},\ G(p) = \{x \in G \mid px = 0\}.$$

Vamos a probar que $G(p) = G_1(p) \oplus \cdots \oplus G_s(p)$. En efecto, como cada $G_i(p) \leq G_i =< \overline{e_i} >$ y la suma de los G_i es directa, también la suma de los $G_i(p)$ es directa. Por tanto, $G_1(p) \oplus \cdots \oplus G_s(p) \leq G(p)$. Sea $x \in G(p)$, entonces $x = m_1\overline{e_1} + \cdots + m_s\overline{e_s}$, para ciertos $m_i \in \mathbb{Z}$. Como $px = 0$, se tiene $(pm_1)\overline{e_1} + \cdots + (pm_s)\overline{e_s} = 0$ y, como la suma es directa, se deduce $(pm_1)\overline{e_1} = \cdots = (pm_s)\overline{e_s} = 0$. Por tanto, cada $m_i\overline{e_i} \in G_i(p)$. Así, $G(p) = G_1(p) \oplus \cdots \oplus G_s(p)$.
Puesto que $pG(p) = pG_i(p) = 0$, los subgrupos $G(p), G_i(p)$ son espacios vectoriales sobre el cuerpo finito $\mathbb{Z}_p$ y la expresión $G(p) = G_1(p) \oplus \cdots \oplus G_s(p)$ es una suma directa de subespacios vectoriales.
Se verifica que

$$\dim G_i(p) = \begin{cases} 0 & \text{si } p \nmid d_i \\ 1 & \text{si } p \mid d_i \end{cases}.$$

En efecto, sea $x = m\overline{e_i} \in G_i(p)$ tal que $px = 0$. Entonces, $pm\overline{e_i} = 0$. De aquí $d_i \mid pm$. Si $p \nmid d_i$ se deduce $d_i \mid m$ y, por tanto, $x = 0$. Si $p \mid d_i$, entonces $m = t\frac{d_i}{p}$, para cierto $t \in \mathbb{Z}$. Por tanto, $G_i(p) =< \frac{d_i}{p}\overline{e_i} >$.
En consecuencia, la dimensión de $G(p)$ como $\mathbb{Z}_p$ espacio vectorial es el número de factores invariantes que son divisibles por p.
Si tenemos dos descomposiciones, una con s sumandos y la otra con t sumandos, tomamos un primo que divida al primer factor invariante de la primera descomposición (y que, por tanto, divide a los s factores invariantes). Como la definición de $G(p)$ no depende de la descomposición y, para un primo que divida al primer factor invariante de la primera descomposición, la dimensión de $M(p)$ es el número de factores invariantes s de dicha descomposición y, para la segunda descomposición, la dimensión de $M(p)$ es el número de factores invariantes que son divisibles por p, que es $\leq t$, se deduce que $s \leq t$. Razonando de forma simétrica, se deduce que $t \leq s$. Por tanto, el número de factores invariantes es invariante. Además, esto prueba que cualquier primo que divida al primer factor invariante de una descomposición, también divide al primer factor invariante de cualquier otra descomposición.
En una descomposición, el último factor invariante d_s es múltiplo de todos los factores invariantes, luego anula a todos los generadores $\overline{e_i}$ de la descomposición y, por tanto, a todos los elementos de G, es decir, $d_s x = 0$, para todo $x \in G$. El conjunto $\{m \in \mathbb{Z} \mid mx = 0 \text{ para todo } x \in G\}$ es un ideal de $\mathbb{Z}$ que contiene a b_m. Recíprocamente, si m está en el ideal, entonces $m\overline{e_s} = 0$ y, por tanto, $d_s \mid m$. Es decir, dicho ideal está generado por d_s. Esto prueba la unicidad del último factor invariante de cualquier descomposición.
Sean $1 < d_1 \mid \cdots \mid d_s$ y $1 < c_1 \mid \cdots \mid c_s$ los factores invariantes de dos descomposiciones; la segunda $G =< \overline{f_1} > \oplus \cdots \oplus < \overline{f_s} >$. Ya hemos probado que $d_s = c_s$. Si d_s es un número primo, entonces todos los d_i, c_i son dicho número primo y se tiene la unicidad. Supongamos que d_s es producto de $n+1$ primos y la hipótesis de unicidad cierta para descomposiciones de grupos donde el último factor es producto de n primos. Hemos probado que d_1 y c_1 son divisibles por los mismos primos. Sea p un primo que divida a ambos (luego divide a todos los d_i, c_i). Consideramos el subgrupo $pG = \{px \mid x \in G\}$. Entonces, es obvio que

$$pG =< p\overline{e_1} > \oplus \cdots \oplus < p\overline{e_s} >=< p\overline{f_1} > \oplus \cdots \oplus < p\overline{f_s} >$$

También es obvio que $\text{ord}(p\overline{e_i}) = \frac{d_i}{p}, \text{ord}(p\overline{f_i}) = \frac{c_i}{p}$. Puede ocurrir que algunos de los primeros d_i sean iguales a p, con lo que los primeros sumandos de estas descomposiciones serían nulos. Si en ambas descomposiciones eliminamos los sumandos nulos, obtenemos dos descomposiciones del grupo pG, donde el último factor invariante $\frac{d_s}{p}$ es producto de n primos. Por tanto, por la hipótesis de inducción, concluimos que el número de sumandos nulos para las dos descomposiciones coincide, y que los restantes tiene los mismos factores invariantes, es decir, el número de d_i iguales a p es el mismo que el número de c_i iguales a p, y para los restantes $\frac{d_i}{p} = \frac{c_i}{p}$. esto implica la igualdad de los d_i y los c_i.

Observación 2.7.21 (Cálculo de los factores invariantes a partir de generadores y relaciones)**.** Sea G un grupo conmutativo generado por $\{x_1, \ldots, x_m\}$ con las relaciones

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m = 0 \\ \qquad\qquad\qquad\qquad \vdots \\ a_{p1}x_1 + a_{p2}x_2 + \cdots + a_{pm}x_m = 0. \end{cases}$$

Es decir, el homomorfismo sobreyectivo $\mathbb{Z}^m \to G$, definido por $e_i \mapsto x_i$, donde $e_i = (0, \ldots, 1, \ldots, 0)$, tiene por núcleo el subgrupo H de $\mathbb{Z}^m$ generado por los elementos

$$H =< a_1 = (a_{11}, a_{12}, \ldots, a_{1m}), a_2 = (a_{21}, a_{22}, \ldots, a_{2m}), \ldots, a_p = (a_{p1}, a_{p2}, \ldots, a_{pm}) >,$$

de forma que $G \simeq \mathbb{Z}^m/H$.
Hacemos transformaciones elementales en las filas y columnas de la matriz

$$M = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{p1} & a_{p2} & \cdots & a_{pm} \end{pmatrix}.$$

Denotaremos a_i las filas de M, b_k las columnas de M. Veamos qué efecto tienen las transformaciones elementales de filas o columnas sobre $B = \{e_1, \ldots, e_m\}, H$ y $\mathbb{Z}^m/H$.

(1) $a_i \leftrightarrow a_j$. No cambia B ni H.

(2) $a_i \to -a_i$. No cambia B ni H.

(3) $a_i \to a_i + ta_j, i \neq j, t \in \mathbb{Z}$. No cambia B ni H.

(1) $c_k \leftrightarrow c_l$. Cambia

$$B = \{e_1, \ldots, e_k, \ldots, e_l, \ldots, e_m\}$$

por

$$B' = \{f_1 = e_1, \ldots, f_k = e_l, \ldots, f_l = e_k, \ldots, f_m = e_m\}$$

y

$$H =< \{a_n\}_{1,\ldots,p} >$$

por

$$H' =< \{b_q = (b_{q1} = a_{q1}, \ldots, b_{qk} = a_{ql}, \ldots, b_{ql} = a_{qk}, \ldots, b_{qm} = a_{qm})\}_{1,\ldots,p} > .$$

El cambio de base induce un isomorfismo

$$\mathbb{Z}^m =< e_1 > \oplus \cdots \oplus < e_m > \to \mathbb{Z}^m =< f_1 > \oplus \cdots \oplus < f_m >$$

, dado por $e_1 \mapsto f_1, \ldots, e_k \mapsto f_l, \ldots, e_l \mapsto f_k, \ldots, e_m \mapsto f_m$, que transforma H en H', por tanto,

$$\frac{< e_1 > \oplus \cdots \oplus < e_m >}{H} \simeq \frac{< f_1 > \oplus \cdots \oplus < f_m >}{H'}.$$

(2) $c_k \to -c_k$. Cambia

$$B = \{e_1, \ldots, e_k, \ldots, e_m\}$$

por

$$B' = \{f_1 = e_1, \ldots, f_k = -e_k, \ldots, f_m = e_m\}$$

y

$$H =< \{a_n\}_{1,\ldots,p} >$$

por

$$H' =< \{b_q = (b_{q1} = a_{q1}, \ldots, b_{qk} = -a_{qk}, \ldots, b_{qm} = a_{qm})\}_{1,\ldots,p} > .$$

El cambio de base induce un isomorfismo

$$\mathbb{Z}^m =< e_1 > \oplus \cdots \oplus < e_m > \to \mathbb{Z}^m =< f_1 > \oplus \cdots \oplus < f_m >$$

, dado por $e_1 \mapsto f_1, \ldots, e_k \mapsto -f_k, \ldots, e_m \mapsto f_m$, que transforma H en H', por tanto,

$$\frac{< e_1 > \oplus \cdots \oplus < e_m >}{H} \simeq \frac{< f_1 > \oplus \cdots \oplus < f_m >}{H'}.$$

(3) $c_k \to c_k + tc_l, k \neq l, t \in \mathbb{Z}$. Cambia

$$B = \{e_1, \ldots, e_k, \ldots, e_l, \ldots, e_m\}$$

por

$$B' = \{f_1 = e_1, \ldots, f_k = e_k, \ldots, f_l = e_l - te_k, \ldots, f_m = e_m\}$$

y

$$H =< \{a_n\}_{1,\ldots,p} >$$

por

$$H' =< \{b_q = (b_{q1} = a_{q1}, \ldots, b_{qk} = a_{qk} + ta_{ql}, \ldots, b_{ql} = a_{ql}, \ldots, b_{qm} = a_{qm})\}_{1,\ldots,p} >,$$

puesto que

$$a_{q1}e_1 + \ldots a_{qk}e_k + \ldots + a_{ql}e_l + \ldots + a_{qm}e_m = a_{q1}f_1 + \ldots + a_{qk}f_k + \ldots + a_{ql}(f_l + tf_k) + \ldots + a_m f_m =$$

$$= a_{q1}f_1 + \ldots + (a_{qk} + ta_{ql})f_k + \ldots + a_{ql}f_l + \ldots + a_{qm}f_m.$$

El cambio de base induce un isomorfismo

$$\mathbb{Z}^m =< e_1 > \oplus \cdots \oplus < e_m > \to \mathbb{Z}^m =< f_1 > \oplus \cdots \oplus < f_m >$$

, dado por $e_1 \mapsto f_1, \ldots, e_k \mapsto f_k, \ldots, e_l \mapsto f_l + tf_k, \ldots, e_m \mapsto f_m$, que transforma H en H', por tanto,

$$\frac{< e_1 > \oplus \cdots \oplus < e_m >}{H} \simeq \frac{< f_1 > \oplus \cdots \oplus < f_m >}{H'}.$$

Mediante transformaciones elementales de filas y columnas de los seis tipos anteriores se puede transformar M en una matriz de la forma (ilustraremos el proceso mediante un ejemplo)

$$M' = \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_s & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix},$$

donde $1 < d_1 \mid \cdots \mid d_s$. En la base $\{f_1, \ldots, f_s\}$ que corresponde a M', el subgrupo

$$H' = < d_1 f_1 > \oplus < d_2 f_2 > \oplus \cdots \oplus < d_s f_s > .$$

En consecuencia,

$$G \simeq \mathbb{Z}^m / H \simeq \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_s} \oplus \mathbb{Z}^{m-s}.$$

Por tanto, $d_1 \mid \cdots \mid d_s$ son los factores invariantes de G y $m - s$ es el rango de G.

Ejemplo 2.7.22. Grupo conmutativo finitamente generado G definido por generadores $\{a, b, c\}$ y relaciones

$$\begin{cases} 6a - 9b - 3c = 0 \\ 24a + 9b + 9c = 0 \\ 42a + 45b + 27c = 0 \end{cases}$$

El máximo común divisor de los coeficientes es 3. El proceso comienza transformando M en una matriz cuyo elemento m_{11} es 3.

$$\begin{pmatrix} 6 & -9 & -3 \\ 24 & 9 & 9 \\ 42 & 45 & 27 \end{pmatrix} \xrightarrow{c_1 \leftrightarrow c_3} \begin{pmatrix} -3 & -9 & 6 \\ 9 & 9 & 24 \\ 27 & 45 & 42 \end{pmatrix} \xrightarrow{f_1 \to -f_1} \begin{pmatrix} 3 & 9 & -6 \\ 9 & 9 & 24 \\ 27 & 45 & 42 \end{pmatrix} \xrightarrow{f_2 \to f_2 - 3f_1, f_3 \to f_3 - 9f_1}$$

$$\begin{pmatrix} 3 & 9 & -6 \\ 0 & -18 & 42 \\ 0 & -36 & 96 \end{pmatrix} \xrightarrow{c_2 \to c_2 - 3c_1, c_3 \to c_3 + 2c_1} \begin{pmatrix} 3 & 0 & 0 \\ 0 & -18 & 42 \\ 0 & -36 & 96 \end{pmatrix} \xrightarrow{c_3 \to c_3 + 2c_2}$$

El máximo común divisor de los coeficientes de la submatriz obtenida eliminado la fila primear y la columna primera es 6. El proceso continúa colocando un 6 en la posición m_{22}.

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & -18 & 6 \\ 0 & -36 & 24 \end{pmatrix} \xrightarrow{c_2 \leftrightarrow c_3} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & -18 \\ 0 & 24 & -36 \end{pmatrix} \xrightarrow{c_3 \to c_3 + 3c_2} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 24 & 36 \end{pmatrix} \xrightarrow{f_3 \to f_3 - 4f_2} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 36 \end{pmatrix}.$$

En consecuencia,

$$G \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{36}.$$

2.8. Ejercicios

(1) Decidir cuáles de los siguientes conjunto tienen estructura de grupo con la operación indicada. En caso afirmativo, ver si son o no conmutativos.

   a) $G = \{x \in \mathbb{R} \mid x > 0\}$ con el producto.

   b) $G = \{x \in \mathbb{C} \mid x^n = 1\}$ con el producto (donde $n \in \mathbb{N}$ está fijado).

   c) $G = \{x \in \mathbb{C} \mid x^n = 1, \text{ para algun } n \in \mathbb{N}\}$ con el producto.

   d) $G = \{x \in \mathbb{C} \mid |x| = 1\}$ con el producto.

   e) $G = \{A \in \mathscr{M}_n(\mathbb{R}) \mid A^2 = I\}$ con el producto.

   f) $G = \{a \in \mathbb{Z} \mid a \text{ es un cuadrado}\}$ con la suma.

   g) $G = \{a \in \mathbb{Q} \mid a \text{ es un cuadrado}\}$ con el producto.

(2) Sean G un grupo y $H \subset G$ un subconjunto finito no vacío tal que $ab \in H$ para todo $a, b \in H$. Demostrar que H es un subgrupode G.

(3) Sean G un grupo finito y $0 < n \in \mathbb{N}$.

   a) ¿Es cierto que si el orden de todo elemento de G divide a n, entonces el orden de G divide a n?

   b) Sea H el subconunto de elementos de G cuyo orden divide a n. ¿Es H un subgrupo de G? ¿Y si G es conmutativo?

(4) Demostrar que el producto cartesiano de dos grupos no triviales del mismo orden no puede ser un grupo cíclico.

(5) Para los valores $n = 6, 7, 8, 9, 10, 11, 12, 13, 24$, hallar el orden de los elementos del grupo $\mathbb{Z}_n^* = \{\bar{k} \in \mathbb{Z}_n \mid \text{mcd}(k, n) = 1, 1 \leq k < n\}$ con el producto. Indicar generadores para estos grupos. ¿Cuáles son cíclicos?

(6) Determinar los subgrupos finitos del grupo $(\mathbb{C} - \{0\}, \cdot)$.

(7) Determinar los subgrupos finitos del grupo $(\mathbb{R} - \{0\}, \cdot)$.

(8) Demostrar que si todo elemento $x \in G - \{1\}$ tiene orden 2, entonces el grupo G es conmutativo.

(9) Hallar el centro de los grupos diédricos D_3, D_4.

(10) Sean G un grupo y $a, b \in G$. Demostrar que

   a) $\text{ord}(a) = \text{ord}(a^{-1}) = \text{ord}(b^{-1}ab)$.

   b) $\text{ord}(ab) = \text{ord}(ba)$.

(11) Sean $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ en el grupo $G = \mathrm{GL}_2(\mathbb{Q})$.

a) Hallar los órdenes de A, B, AB.

b) Sea $T = \{C \in G \mid \mathrm{ord}(C) \text{ es finito}\}$. ¿Es T un grupo?

(12) Sean $a, b \in G$ elementos de ordenes finitos y primos entres sí tales que $ab = ba$. Demostrar que $\mathrm{ord}(ab) = \mathrm{ord}(a)\mathrm{ord}(b)$ y $< a > \cap < b >= \{1\}$.

(13) Sean G un grupo finito conmutativo y $a \in G$ un elemento de orden $m = \mathrm{máx}\{\mathrm{ord}(b) \mid b \in G\}$. Demostrar que $\mathrm{ord}(b) \mid m$ para todo $b \in G$.

(14) Consideramos las matrices complejas

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Demostrar que $G = \{\mathbf{1}, -\mathbf{1}, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$ es un subgrupo (denominaremos a G el grupo cuaternio) del grupo $\mathrm{GL}_2(\mathbb{C})$ de matrices complejas inversibles de orden 2 con el producto. Escribr la tabla de multiplicar de G y hallar el orden de los elementos de G. Estudiar si G es isomorfo a D_4.

(15) Sea $G = \mathrm{GL}_2(\mathbb{Z}_2)$. Hallar los elementos de G y sus órdenes.Hallar los subgrupos de G determinando cuáles son normales. Demostrar que G es isomorfo a S_3.

(16) Sean G un grupo y H un subgrupo de índice primo. Demostrar que no existe un subgrupo H' tal que $H \subsetneq H' \subsetneq G$.

(17) Sean K un subgrupo normal de índice primo p de un grupo G y H un subgrupo de G no contenido en K. Demostrar que $G = KH$ y $[H : H \cap K] = p$.

(18) Probar que si H es un subgrupo normal de índice n de un grupo G, entonces $x^n \in H$ para todo $x \in G$. ¿Es cierto el resultado sin la hipótesis de normalidad sobre H?

(19) ¿Es cierto que si H y K son dos subgrupo normales de un grupo G tales que G/H y G/K son isomorfos, entonces H y K son isomorfos?

(20) Encontrar un grupo finito no conmutativo todos cuyos subgrupos son normales.

(21) Demostrar que le subgrupo $\{(), (12)(34), (13)(24), (14)(23)\}$ de S_4 es un subgrupo normal.

(22) Encontrar todos los subgrupos del grupo diédrico D_4, indicando cuáles son normales.

(23) Demostrar que el grupo diédrico D_6 es isomorfo a $\mathbb{Z}_2 \times S_3$.

(24) Encontrar todos los subgruposn de A_4, indicando cuáles son normales. ¿Es A_4 isomorfo a $\mathbb{Z}_2 \times S_3$?

(25) Hallar todos los homomorfismos (calculando núcleo e imagen) entre los pares de grupos:

a) De $\mathbb{Z}_3$ en $\mathbb{Z}_3$.

b) De $\mathbb{Z}_n$ en $\mathbb{Z}$.

c) De $\mathbb{Z}_6$ en S_3.

d) De S_3 en $\mathbb{Z}_6$.

e) De S_3 en S_3.

f) De $\mathbb{Z}_3$ en $\mathbb{Z}_6$.

g) De $\mathbb{Z}_6$ en $\mathbb{Z}_3$.

h) De $\mathbb{Z}_8$ en $\mathbb{Z}_{12}$.

i) De $\mathbb{Z}_{12}$ en $\mathbb{Z}_8$.

(26) ¿Es isomorfo el grupo aditivo $\mathbb{Q}$ de los números racionales al grupo multiplicativo $\mathbb{Q}^*$ de los racionales no nulos.

(27) Sean $\zeta = \exp(\frac{2\pi i}{n})$, $n \geq 3$ y G el subgrupo de $\mathrm{GL}_2(\mathbb{C})$ generado por las matrices

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} \zeta & 0 \\ 0 & \overline{\zeta} \end{pmatrix}.$$

Demostrar que G es isomorfo al grupo diédrico D_n.

(28) Consideramos el subconjunto $G = \{\pm I, \pm A, \pm B, \pm C\}$ del grupo $\mathrm{GL}_2(\mathbb{Z}_3)$, donde

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Demostrar que G es un subgrupo de $\mathrm{GL}_2(\mathbb{Z}_3)$. Calcular el orden de sus elementos. Demostrar que G está generado por A, B. ¿Es G isomomorfo a D_4 o al grupo cuaternio Q_8?

(29) Sea $f : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ definida por $f(t) = \exp(2\pi i t) = \cos(2\pi t) + i \sin(2\pi t)$. Demostrar que f es un homomorfismo de grupos. Hallar su núcleo e imagen. Concluir que el grupo cociente aditivo $\mathbb{R}/\mathbb{Z}$ es ismorfo al grupo multiplicativo $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$.

(30) Sean $H = \{x \in \mathbb{R} \mid x > 0\}, K = \{z \in \mathbb{C} \mid |z| = 1\}$ subgrupos de $\mathbb{C}^*$. Demostrar que $\mathbb{C}^*$ es el producto directo interno de H y K.

(31) Sea G un grupo en el que todo elemento distinto de 1 tiene orden 2. Demostrar que G es conmutativo.

(32) Hallar el centro de los grupos D_3 y D_4.

(33) Hallar los subgrupos finitos del grupo multiplicativo $\mathbb{C}^*$.

(34) Sea G un grupo. Supongamos que existe un subgrupo $H \leq Z(G)$ tal que G/H es cíclico. Demostrar que G es abeliano.

(35) Sea G un grupo abeliano de orden ocho tal que el orden máximo de los elementos de G es cuatro. Demostrar que G es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_4$ y calcular cuántos subgrupos tiene de cada orden.

(36) Descomponer en producto de ciclos disjuntos las siguientes permutaciones. Calcular la permutación inversa de su potencia 1439–ésima:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 6 & 14 & 3 & 4 & 11 & 13 & 2 & 5 & 7 & 9 & 10 & 12 & 1 & 8 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 3 & 5 & 2 & 14 & 1 & 13 & 7 & 12 & 8 & 10 & 9 & 4 & 11 & 6 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 4 & 8 & 14 & 7 & 1 & 13 & 12 & 9 & 2 & 10 & 6 & 5 & 11 & 3 \end{pmatrix}$$

(37) Demostrar que S_n está generado por las trasposiciones $(1\,2), (1\,3), \ldots, (1\,n)$. Idem por las trasposiciones $(1\,2), (2\,3), \ldots, (n{-}1\,n)$. Idem por el ciclo $(1\,2\,\cdots n)$ y la trasposición $(1\,2)$.

(38) Sea $\sigma \in S_{11}$ una permutación de orden 21. Determinar el número de elementos del conjunto $\{1, 2, \ldots, 11\}$ que quedan fijos por σ.

(39) Decidir, de forma razonada, si:

a) el grupo simétrico S_5 tiene un elemento de orden 8,

b) el grupo simétrico S_5 contiene un subgrupo de orden 8.

(40) ¿Existe alguna permutación $\sigma \in S_5$ tal que $\sigma^3 = (1\,2\,4)$.

(41) Hallar las permutaciones $\tau \in S_5$ tales que $\tau^7 = (1\,2\,4)$.

(42) Demostrar que $\sigma(i_1\, i_2\, \cdots\, i_r)\sigma^{-1} = (\sigma(i_1)\, \sigma(i_2)\, \cdots\, \sigma(i_r))$.

(43) Demostrar que A_n está generado por los 3–ciclos.

(44) Hallar los órdens posibles de los elementos de S_7, S_8 y S_9.

(45) ¿Cuántos elementos de orden 10 tiene el grupo S_9?

(46) Probar que para $n \geq 3$ el único subgrupo de índice 2 de S_n es el grupo alternado A_n.

(47) Sean $\sigma = (1\,2\,3\,4)$ y $\tau = (1\,4)(2\,3)$ en S_6. Demostrar que el subgrupo $H =< \sigma, \tau >$ de S_6 es isomorfo al grupo diedral D_4.

(48) Sean $\sigma = (1\,2\,3\,4), \tau = (1\,4)(2\,3), \gamma = (5\,6)$ en S_6 y $K =< \sigma, \tau, \gamma >$. Demostrar que K es isomorfo a $D_4 \times \mathbb{Z}_2$.

(49) Determinar el grupo G generado por elementos a, b, c con las relaciones $a^2 = b^2 = c^3 = 1, ab = ba, cb = ac, ca = abc$. Demostrar que existe un homomorfismo $f : G \to S_4$ definido por $a \mapsto (1\,2)(3\,4), b \mapsto (1\,3)(2\,4), c \mapsto (1\,2\,3)$. Calcular el núcleo e imagen de f. (Indicación: G tiene 12 elementos).

(50) Demostrar que los órdenes del grupo generado por dos elementos a, b con las relaciones mostradas es el que se indica, en cada caso:

a) $a^2 = b^2 = 1, aba = bab$. Orden 1.

b) $a^2 = b^3 = 1, aba = bab$. Orden 1.

c) $a^2 = b^5 = 1, aba = b^2$. Orden 2.

d) $a^5 = b^2 = 1, ba = a^2b$. Orden 2.

e) $a^3 = b^9 = 1, a^2ba = b^8$. Orden 3.

f) $a^2 = b^2 = abab = 1$. Orden 8 (isomorfo a Q_8).

g) $a^4 = b^3 = 1, abab = 1$. Orden 24.

h) $a^3 = b^3 = 1, abab = 1$. Orden 12.

(51) Representar S_3 mediante generadores y relaciones usnado que está generado por $a = (1\,2), b = (3\,4)$.

(52) Sea G un grupo de orden 143 que actúa sobre un conjunto X de 108 elementos. Demostrar que X contiene un elemento cuyo estabilizador es G.

(53) Sea G un grupo de orden 35 que actúa, sin puntos fijos, sobre un conjunto X de 19 elementos. Hallar el número de órbitas de X y el número de elementos de cada órbita.

(54) Sean $1 < k < p$ enteros con p primo. Demostrar que todo grupo de orden kp es no simple.

(55) Sean G un grupo finito simple y H un subgrupo de índice primo p. Probar que p^2 no divide al orden de G y que p es el mayor divisor primo del orden de G.

(56) Sea G un grupo de orden 30. Probra que G tiene un único subgrupo de orden 3 o un único subgrupo de orden 5. Con cluir que G tiene un subgrupo de orden 15.

(57) Sea G un grupo de orden 3304. Demostrar que G contiene un subgrupo normal H de orden 59 y que G/H también contiene un subgrupo normal.

(58) Sea G un grupo de orden 616. Demostrar que G contiene algún p–subgrupo de Sylow normal para algún primo p.

(59) Sea G un grupo de orden 868.

   a) Demostrar que G tiene un único subgrupo normal de orden 217.

   b) Demostrar que G tiene subgrupos de todos los órdenes posibles.

   c) Demostrar que G es resoluble.

(60) Sea G un grupo de orden 440. Demostrar que G tiene algún subgrupo normal y contiene un único subgrupo de orden 55.

(61) Sean p, q, r primos distintos y $k \geq 2$. Demostrar que los grupos de órdenes p^k, pq, p^2q, p^2q^2, pqr no son simples. Si, además, $p > q$, entonces los grupos de orden p^nq no son simples.

(62) Demostrar que si G es simple de orden 6 =, entonces G es isomorfo al grupo alternado A_5.

(63) Demostrar que los grupos de orden 114 o 180 no son simples.

(64) Sea p un número primo. Demostrar que los grupos de orden p^2 son abelianos.

(65) Demostrar que todo grupo de orden 299 es cíclico.

(66) Demostrar que S_4 tiene subgrupos de todos los órdenes posibles. Hallar el número de subgrupos de S_4 de órdenes $2, 3, 8$.

(67) Sea G un grupo de orden 20. Probar que G tiene subgrupos de todos los órdenes posibles.

(68) Sean G un grupo finito y p el menor divisor primo del orden de G. Entonces todo subgrupo de índice p es normal en G.

(69) Demostrar que cualquier grupo de orden $3 \cdot 23 \cdot 29$ es conmutativo. ¿Es necesariamente cíclico?

(70) Sea G un grupo de orden $2^2 \cdot 3 \cdot 7$.

   a) Demostrar que G no es simple.

   b) Probar que G tiene subgrupos de orden 21.

(71) Sea G un grupo de orden $p^r q$, donde p, q primos distintos, $r \geq 1$ y $p^r < q$.

a) G no es simple.

b) G tiene subgrupos de todos los órdenes posibles.

c) G es resoluble.

(72) Sea G un grupo de orden $88 = 2^3 \cdot 11$. Se pide:

a) Demostrar que G no es simple.

b) Estudiar, de forma razonada, si G tiene subgrupos de todos los órdenes posibles.

(73) Sea G un grupo de orden $783 = 3^3 \cdot 29$.

a) Probar que G es resoluble.

b) Estudiar si G posee subgrupos de órdenes cada uno de los divisores de 783.

(74) Sea G un grupo de orden $2^2 \cdot 19 \cdot 79$. Se pide:

a) Decidir, de forma razonada, si G es resoluble.

b) Estudiar, de forma razonada, si G posee subgrupos de todos los órdenes permitidos por el teorema de Lagrange.

(75) Sea G un grupo de orden pq, donde $p \neq q$ son primos. Demostrar que G no es simple y que G es resoluble. (Existen dos grupos de orden pq, el cíclico y un grupo no abeliano).

(76) Demostrar que todo p–grupo es resoluble.

(77) Descomponer, según el teorema de estructura, los grupos de unidades de $\mathbb{Z}_{11}, \mathbb{Z}_{12}, \mathbb{Z}_{14}, \mathbb{Z}_{16}, \mathbb{Z}_{18}, \mathbb{Z}_{20}$.

(78) ¿Contiene el grupo S_9 algún subgrupo conmutativo de orden 21?

(79) ¿Cuál es el número de grupos conmutativos, salvo isomorfismo, de orden 1008? Hallar los coeficientes de torsión de cada modelo.

(80) ¿Cuál es el número de grupos conmutativos, salvo isomorfismo, de orden 360? Hallar los coeficientes de torsión de cada modelo.

(81) Descomponer, según el teorema de estructura, el grupo conmutativo generado por cuatro elementos a, b, c, d con las relaciones:

$$\begin{cases} 6b - 9c - 3d & = 0 \\ 12a + 24b + 9c + 9d & = 0 \\ 30a + 42b + 45c + 27d & = 0. \end{cases}$$

(82) Descomponer, según el teorema de estructura, el grupo conmutativo generado por cuatro elementos a, b, c, d con las relaciones:

$$\begin{cases} 2b + 4c - d & = 0 \\ 6a + 12b + 14c + 5d & = 0 \\ 4b + 14c - d & = 0. \end{cases}$$

Capítulo 3

Teoría de cuerpos

3.1. Extensiones de cuerpos

Definición 3.1.1. (1) Un cuerpo F es un anillo conmutativo unitario donde todo elemento no nulo es unidad.

(2) La característica de F es el número primo positivo generador del núcleo del único homomorfismo de anillos unitarios $\mathbb{Z} \to F$ o es 0 si este homomorfismo es inyectivo. La característica es el número primo que es el menor entero $p > 0$ tal que

$$1_F + \overset{p}{\cdots} + 1_F = 0_F,$$

ó 0 si ningún múltiplo de 1_F es 0_F.

(3) El subcuerpo primo de F es la intersección de todos los subcuerpos de F, i.e., el menor subcuerpo de F. El subcuerpo primo es isomorfo a $\mathbb{Q}$ o a $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ según que la característica de F sea 0 ó p.

Observación 3.1.2. Todo homomorfismo de anillos unitarios de un cuerpo F en un anillo R es inyectivo.

Definición 3.1.3. (1) Sea K un cuerpo que contiene a F como subcuerpo. Diremos que K es un cuerpo extensión de F. Diremos que F es el cuerpo base de la extensión y denotaremos K/F o $F \subset K$ o, a veces, $\begin{matrix} K \\ | \\ F \end{matrix}$. En particular, todo cuerpo es extensión de su cuerpo primo.

(2) El grado de la extensión K/F es la dimensión de K como espacio vectorial sobre F. Denotaremos $[K : F]$. La extensión es finita si $[K : F] < \infty$.

Ejemplos 3.1.4. (1) $\mathbb{C}/\mathbb{R}$ extensión finita de grado $[\mathbb{C} : \mathbb{R}] = 2$.

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

(3) $[\mathbb{R} : \mathbb{Q}] = 2^{\aleph_0}$.

Proposición 3.1.5 (Fórmula de los grados). *Sean $F \subset E \subset K$ extensiones tales que $[E : F] < \infty$ y $[K : E] < \infty$. Entonces $[K : F] < \infty$ y*

$$[K : F] = [K : E][E : F]. \tag{3.1.5.1}$$

Demostración. Si $\{\alpha_1, \ldots, \alpha_n\}$ es una base de K/E y $\{\beta_1, \ldots, \beta_m\}$ es una base de E/F, entonces $\{\alpha_i\beta_j\}_{\substack{i=1,\ldots,n,\\ j=1,\ldots,m}}$ es una base de K/F. □

Observación 3.1.6. La fórmula (3.1.5.1) sigue siendo correcta, en el sentido de la aritmética de los cardinales infinitos, si alguna de las extensiones tiene por grado un cardinal infinito.

Observación 3.1.7. Sea K/F una extensión. Entonces $[K : F] = 1$ si, y sólo si, $K = F$.

Definición 3.1.8. (1) Sean K/F una extensión y $S \subset K$ un subconjunto. El subcuerpo de K extensión de F generado por S, que denotaremos $F(S)$, es la intersección de todos los subcuerpos de K extensiones de F que contienen a S:

$$F(S) = \bigcap_{\substack{F \subset E \subset K \\ E \text{ subcuerpo y} \\ S \subset E}} E.$$

El cuerpo $F(S)$ es el menor subcuerpo de K extensión de F que contiene a S. Diremos que $F(S)$ es el subcuerpo de K obtenido por adjunción a F de los elementos de S.

Sea $F[S]$ es el menor subanillo de K extensión de F que contiene a S, esto es la intersección de todos los subanillos de K extensión de F que contienen a S. Entonces

$$F[S] = \{\alpha \in K \mid \text{existen } n \geq 0,\ s_1, \ldots, s_n \in S \text{ tales que } \alpha = f(s_1, \ldots, s_n), \\ \text{para algún polinomio con coeficientes en } F\},$$

y $F(S)$ es el cuerpo de fracciones de $F[S]$ en K. Es decir $F(S) = \{\alpha/\beta \mid 0 \neq \beta, \alpha \in F[S]\}$.

(2) Diremos que K/F es una extensión finitamente generada si existen $\alpha_1, \ldots, \alpha_n \in K$ tales que $K = F(\alpha_1, \ldots, \alpha_n)$.

(3) Diremos que la extensión K/F es simple si existe $\alpha \in K$ tal que $K = F(\alpha)$.

Observación 3.1.9. (1) $F(S_1 \cup S_2) = F(S_1)(S_2) = F(S_2)(S_1)$.

(2) $F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \cdots \subset F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

3.1.1. Extensiones algebraicas

Definición 3.1.10. *Sea K/F una extensión. Diremos que un elemento $\alpha \in K$ es algebraico sobre F si existe un polinomio no nulo $f(X) \in F[X]$ tal que $f(\alpha) = 0$. En caso contrario, diremos que $\alpha \in K$ es trascendente sobre F.*
Diremos que K/F es una extensión algebraica, o que K es una extensión algebraica de F, si todo elemento de K es algebraico sobre F.

Observación 3.1.11. Sean $K/E/F$ y $\alpha \in K$ algebraico sobre F. Entonces α es algebraico sobre E.

Ejemplos 3.1.12. (1) $\sqrt{-1} \in \mathbb{C}$ es algebraico sobre $\mathbb{Q}$. Es una raíz del polinomio $X^2+1 \in \mathbb{Q}[X]$.

(2) $\sqrt[3]{2} \in \mathbb{C}$ es algebraico sobre $\mathbb{Q}$. Es una raíz de $X^3 - 2 \in \mathbb{Q}[X]$.

(3) $\pi, e \in \mathbb{C}$ son trascendentes sobre $\mathbb{Q}$.

Proposición–Definición 3.1.13. *(1) Sean F un cuerpo y α, en cierto cuerpo extensión de F, algebraico sobre F. Existe un único polinomio mónico e irreducible $m_{\alpha,F}(X) \in F[X]$ que tiene a α por raíz. Además, un polinomio $f(X) \in F[X]$ tiene a α por raíz si, y sólo si, $m_{\alpha,F}(X) \mid f(X)$ en $F[X]$.*

(2) Sea α algebraico sobre F. Entonces $F(\alpha) = F[\alpha] \simeq F[X]/m_{\alpha,F}(X)F[X]$ es una extensión finita de F con grado $[F(\alpha) : F] = \deg m_{\alpha,F}(X) = n$ y base $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

Diremos que $m_{\alpha,F}(X)$ es el polinomio mínimo de α sobre F y que $\deg m_{\alpha,F}(X)$ es el grado de α sobre F.

(3) Sea α algebraico sobre F. Un polinomio mónico $p(X) \in F[X]$ que tiene a α por raíz, es el polinomio mínimo de α sobre F si, y sólo si, es irreducible.

(4) Sean K/F una extensión. Un elemento $\alpha \in K$ es algebraico sobre F si, y sólo si, $F[\alpha] = F(\alpha)$.

(5) Sean K/F una extensión. Un elemento $\alpha \in K$ es trascendente si, y sólo si, el homomorfismo de sustitución $F[X] \to F[\alpha]$ definido por $X \mapsto \alpha$, es inyectivo. En este caso, es un isomorfismo.

(6) Sean E/F y α, en cierto cuerpo extensión de E, algebraico sobre F. Entonces α es algebraico sobre E y $m_{\alpha,E}(X) \mid m_{\alpha,F}(X)$ en $E[X]$.

Demostración. (1) − (3) Sea $0 \neq g(X) \in F[X]$ de grado mínimo y mónico, entre los polinomios no nulos que tienen a α por raíz. Entonces, si $g(X) = a(X)b(X)$ en $F[X]$, de $0 = g(\alpha) = a(\alpha)b(\alpha)$, se deduce $a(\alpha) = 0$ ó $b(\alpha) = 0$. De donde $a(X)$ ó $b(X)$ es constante. Así $g(X)$ es irreducible. Sea $f(X) \in F[X]$ con $f(\alpha) = 0$. Dividimos $f(X) = g(X)q(X) + r(X)$, con $r(X) = 0$ ó $\deg r < \deg g$. Entonces $r(\alpha) = 0$ y, por tanto, $r(X) = 0$.

Si $p(X) \in F[X]$ es mónico e irreducible con α por raíz, entonces $p(X)$ es de mínimo grado entre los que tienen a α por raíz. Obtenemos $g(X) \mid p(X)$ y $p(X) \mid g(X)$. Esto implica que $g(X) = p(X)$, puesto que ambos son mónicos.
Hemos probado que el epimorfismo de sustitución $F[X] \to F[\alpha]$ tiene por núcleo $m_{\alpha,F}(X)F[X]$. Este ideal es maximal. Así obtenemos $F(\alpha) = F[\alpha] \simeq F[X]/m_{\alpha,F}(X)F[X]$.
Sea $m_{\alpha,F} = X^n - a_{n-1}X^{n-1} - \cdots - a_1X - a_0$. Entonces

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

De aquí $F[\alpha] = F \cdot 1 + F \cdot \alpha + \cdots + F \cdot \alpha^{n-1}$. Además la suma es directa, puesto que α no es raíz de polinomios de grado menor que n.
(4) La igualdad $F[\alpha] = F(\alpha)$ equivale (si $0 \neq \alpha$) a $\alpha^{-1} \in F[\alpha]$. Entonces $\alpha^{-1} = b_m\alpha^m + \cdots + b_0$, con $b_i \in F$. De donde $b_m\alpha^{m+1} + \cdots + b_0\alpha - 1 = 0$ es una ecuación polinomial para α con coeficientes en F. □

Ejemplo 3.1.14. Sea $\alpha = \sqrt{2+\sqrt{6}}$. Entonces $(\alpha^2-2)^2 = 6$. Esto es, $\alpha^4 - 4\alpha^2 - 2 = 0$. El polinomio $X^4-4X^2-2 \in \mathbb{Q}[X]$ es irreducible (Eisenstein). Por tanto $m_{\alpha,\mathbb{Q}}(X) = X^4-4X^2-2$. Ahora bien, $X^4-4X^2-2 = (X-\sqrt{2+\sqrt{6}})(X+\sqrt{2+\sqrt{6}})(X-\sqrt{2-\sqrt{6}})(X+\sqrt{2-\sqrt{6}}) = (X^2-(2+\sqrt{6}))(X^2-(2-\sqrt{6}))$. Puesto que $\alpha \notin \mathbb{Q}(\sqrt{6})$, el polinomio mínimo $m_{\alpha,\mathbb{Q}(\sqrt{6})}(X) = X^2-(2+\sqrt{6})$. Además $\beta = \sqrt{2-\sqrt{6}} \notin \mathbb{Q}(\alpha)$ (puesto que $\beta \notin \mathbb{R}$) y, por tanto $X^2-(2-\sqrt{6}) = m_{\beta,\mathbb{Q}(\sqrt{6})}(X) = m_{\beta,\mathbb{Q}(\alpha)}(X)$. El grado $[\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha,\alpha\beta) = \mathbb{Q}(\alpha,\sqrt{-2}) : \mathbb{Q}] = [\mathbb{Q}(\alpha)(\sqrt{-2}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8$.

Podemos preguntarnos si dado un polinomio $p(X) \in F[X]$ existe un cuerpo K extensión de F donde p tenga una raíz α. La respuesta es afirmativa.

Teorema 3.1.15. *Sean F un cuerpo y $p(X) \in F[X]$ un polinomio de grado* $\deg p \geq 1$. *Existe un cuerpo K extensión de F, donde $p(X)$ tiene una raíz α. Además podemos elegir K de forma que $K = F(\alpha) = F[\alpha] \simeq F[X]/pF[X]$ (el isomorfismo si p es irreducible).*

Demostración. Cambiando $p(X)$ por uno de sus factores irreducibles, podemos suponer $p(X)$ irreducible (y mónico).
Consideramos el cuerpo $K_1 = F[X]/p(X)F[X] = F[x]$, con $x = \bar{X}$. El homomorfismo $F \xrightarrow{i} K$ es inyectivo y ${}^ip(x) = 0$.
Sea T_2 un conjunto biyectivo con $K_1 - i(F)$ y disjunto de F. El conjunto $K = F \cup T_2$, que es biyectivo con K_1, hereda de K_1 una estructura de cuerpo, con $F \subset K$. Sea $\alpha \in K$ el elemento que corresponde a $x \in K_1$ (puesto que p es irreducible, $x \notin i(F)$ y, por tanto, $\alpha \in T_2$). Entonces $p(\alpha) = 0$ y $K = F(\alpha)$. □

Teorema 3.1.16. *Sean $p(X) \in F[X]$ un polinomio mónico e irreducible, con grado* $\deg p = n \geq 1$ *y $K = F(\alpha)$ una extensión simple de F con $p(\alpha) = 0$. Entonces $[K : F] = n$ con base $\{1, \alpha, \ldots, \alpha^{n-1}\}$.*

Teorema 3.1.17. *Sean $F \xrightarrow[\sim]{\varphi} F'$ un isomorfismo de cuerpos, $p(X) \in F[X]$ irreducible y $p^\varphi(X) \in F'[X]$ el polinomio irreducible obtenido aplicando φ a los coeficientes de $p(X)$. Sean α una raíz de $p(X)$, en alguna extensión de F, y β una raíz de $p^\varphi(X)$, en alguna extensión de F'. En estas condiciones, existe un único isomorfismo $F(\alpha) \xrightarrow[\sim]{} F'(\beta)$ que extiende a φ y transforma α en β.*

Demostración. El isomorfismo φ induce un único isomorfismo $F[X]/pF[X] \xrightarrow[\sim]{} F'[X]/p^\varphi F'[X]$ que extiende a φ y transforma $X + pF[X]$ en $X + p^\varphi F'[X]$. Ahora, componemos con los isomorfismos $F[\alpha] \simeq F[X]/pF[X]$ y $F'[\beta] \simeq F'[X]/p^\varphi F'[X]$ dados por Teorema 3.1.15. □

Ejemplos 3.1.18. (1) Si $\alpha \in F$, entonces $m_{\alpha,F}(X) = X - \alpha$.

(2) $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{R}[i] = \mathbb{C} = \mathbb{R}(i)$. El grado $[\mathbb{C} : \mathbb{R}] = 2$.

(3) $\mathbb{Q}[X]/(X^2+1) \simeq \mathbb{Q}[i] = \mathbb{Q}(i)$. El grado $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

(4) $\mathbb{Q}[X]/(X^2-2) \simeq \mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Además $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$ como subcuerpos de $\mathbb{C}$ (o de $\mathbb{R}$) y $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$, $\sqrt{2} \mapsto -\sqrt{2}$ es automorfismo. El grado $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

(5) El polinomio $X^3 - 2$ es irreducible (Eisenstein). Las raíces cúbicas de 2 en $\mathbb{C}$ son: $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$, con $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ una raíz cúbica primitiva de la unidad.

$$\mathbb{Q}[X]/(X^3-2) \simeq \mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}(\sqrt[3]{2}\omega) \simeq \mathbb{Q}(\sqrt[3]{2}\omega^2).$$

Por ejemplo, el isomorfismo

$$\mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\sim} \mathbb{Q}(\sqrt[3]{2}\omega)$$

está definido por

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \mapsto a + b\sqrt[3]{2}\omega + c\sqrt[3]{4}\omega^2. \tag{3.1.18.1}$$

Es un ejercicio recomendable comprobar directamente que la asignación (3.1.18.1) define una aplicación multiplicativa.

El grado

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

Los subcuerpos, $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\omega), \mathbb{Q}(\sqrt[3]{2}\omega^2)$ son distintos. En efecto, si dos de ellos fueran el mismo subcuerpo L de grado 3 sobre $\mathbb{Q}$, entonces, para $0 \le i < j \le 2$, el elemento $\frac{\sqrt[3]{2}\omega^j}{\sqrt[3]{2}\omega^i} = \omega^{j-i} \in L$. Esto no es posible, puesto que $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^2)$ es de grado 2 sobre $\mathbb{Q}$: la ecuación irreducible $X^2 + X + 1 = 0$ tiene por raíces ω, ω^2.

Sea $t = \bar{X}$ una raíz cúbica de 2. Entonces

$$\mathbb{Q}[X]/(X^3-2) = \mathbb{Q}[t] = \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot t \oplus \mathbb{Q} \cdot t^2. \text{ con } t^3 = 2.$$

Podemos calcular el inverso de, por ejemplo, $1+t$ en $\mathbb{Q}[t]$. Para ello hay que resolver

$$(1+t)(a+bt+ct^2) = 1, \text{ con } a,b,c \in \mathbb{Q}.$$

Esto es, $a+bt+ct^2+at+bt^2+c2 = (a+2c)+(a+b)t+(b+c)t^2 = 1$. Así, $a+2c = 1, a+b = 0, b+c = 0$. Cuya solución es $a = \frac{1}{3}, b = -\frac{1}{3}, c = \frac{1}{3}$. Por tanto,

$$(1+t)^{-1} = \frac{1}{3} - \frac{1}{3}t + \frac{1}{3}t^2.$$

Por ejemplo, para $t = \sqrt[3]{2}\omega$ obtenemos la fórmula:

$$\frac{1}{1+\sqrt[3]{2}\omega} = \frac{1}{3} - \frac{1}{3}\sqrt[3]{2}\omega + \frac{1}{3}\sqrt[3]{4}\omega^2.$$

Podemos, también, obtener el inverso a partir de la identidad de Bezout

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

Tomando clases módulo $(X^3 - 2)$ obtenemos

$$(1+t)(\frac{1}{3}(t^2 - t + 1)) = 1.$$

(6) En general, $X^n - q$, con $q \in \mathbb{Z}^+$ que tiene un divisor primo simple, es irreducible (Eisenstein). Las raíces de $X^n - q$ en $\mathbb{C}$ son $\{\sqrt[n]{q}\ \zeta^j\}$, con $\zeta = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ una raíz primitiva de la unidad y $j = 0, 1, \ldots, n-1$. El grado

$$[\mathbb{Q}(\sqrt[n]{q}\ \zeta^j) : \mathbb{Q}] = n.$$

El polinomio mínimo sobre $\mathbb{Q}$, de cada raíz $\sqrt[n]{q}\ \zeta^j$ es $p(X) = X^n - q$.

(7) $m_{\sqrt[n]{q},\mathbb{R}}(X) = X - \sqrt[n]{q}$.

(8) Sea $F = K(u)$ el cuerpo de fracciones algebraicas sobre el cuerpo K, i.e., el cuerpo de fracciones del anillo de polinomios $K[u]$. El polinomio $p(X) = X^2 - u \in F[X]$ resulta ser irreducible, según el criterio de Eisenstein para el primo u.

Sea $t = u^{\frac{1}{2}}$ una raíz de $p(X)$ en algún cuerpo extensión de F. Entonces el grado $[F(t) : F] = 2$ y

$$F[t] = \{a(u) + b(u)t \mid a(u), b(u) \in F\}.$$

(9) El polinomio $p(X) = X^3 - 3X - 1$ es irreducible en $\mathbb{Q}[X]$, puesto que es de grado 3 y no tiene raíces en $\mathbb{Q}$. Sea α una raíz de $p(X) = m_{\alpha,\mathbb{Q}}(X)$. Entonces

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3.$$

Proposición 3.1.19. *Sea K/F una extensión finita de grado $[K : F] = n$. Entonces todo elemento $\alpha \in K$ es raíz de un polinomio de grado $\leq n$ sobre F. Con más precisión, K/F es algebraica y $[F(\alpha) : F]$ es un divisor de $[K : F]$,*

$$[K : F] = [K : F(\alpha)][F(\alpha) : F]. \tag{3.1.19.1}$$

Además $K = F(\alpha)$ si, y sólo si, $[F(\alpha) : F] = n$.

Este último resultado significa que toda extensión finita es algebraica y finitamente generada por elementos algebraicos.

3.1.2. Caracterización de las extensiones finitas

Proposición 3.1.20. *Sean K/F una extensión y $\alpha_1, \ldots, \alpha_n \in K$ algebraicos sobre F. Sean $m_1(X) = m_{\alpha_1,F}(X)$ y, $m_i(X) = m_{\alpha_i,F(\alpha_1,\ldots,\alpha_{i-1})}(X)$, para cada $i = 2, \ldots, n$. Entonces*

(1) $F(\alpha_1, \ldots, \alpha_n) = F[\alpha_1, \ldots, \alpha_n]$.

(2) $F(\alpha_1, \ldots, \alpha_n)$ es una extensión finita de F y

$$[F(\alpha_1, \ldots, \alpha_n) : F] = \prod_{i=1}^{n} \deg m_i(X). \tag{3.1.20.1}$$

Demostración. El caso $n = 1$ es parte de Proposición 3.1.13. Supongamos que $n > 1$ y que, por hipótesis de inducción, $F(\alpha_1, \ldots, \alpha_{n-1}) = F[\alpha_1, \ldots, \alpha_{n-1}]$, junto con la igualdad de grados correspondiente. Entonces α_n es algebraico sobre $F(\alpha_1, \ldots, \alpha_{n-1})$, puesto que lo es sobre F. Así $F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = F(\alpha_1, \ldots, \alpha_{n-1})[\alpha_n]$. Ahora, la hipótesis de inducción implica que $F(\alpha_1, \ldots, \alpha_{n-1})[\alpha_n] = F[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n]$. Por tanto, $F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = F[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n] = F[\alpha_1, \ldots, \alpha_{n-1}, \alpha_n]$.
Respecto del grado, de Proposición 3.1.13, obtenemos

$$[F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})] = \deg m_n(X). \tag{3.1.20.2}$$

Por otra parte, la fórmula de los grados (3.1.5.1), se escribe
(3.1.20.3)

$$[F(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) : F] = [F(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) : F(\alpha_1, \ldots, \alpha_{n-1})][F(\alpha_1, \ldots, \alpha_{n-1}) : F].$$

De (3.1.20.2), (3.1.20.3) y la hipótesis de inducción $[F(\alpha_1, \ldots, \alpha_{n-1}) : F] = \prod_{i=1}^{n-1} \deg m_i(X)$, se obtiene la fórmula (3.1.20.1). □

La Proposición 3.1.20, que acabamos de demostrar, dice que una extensión generada por una cantidad finita de elementos algebraicos es finita y, por tanto, según la Proposición 3.1.19, algebraica. En general, una extensión generada por elementos algebraicos es algebraica, aunque no necesariamente finita.

Corolario 3.1.21. *Sea K/F una extensión generada por un subconjunto $S \subset K$, tal que todo elemento $\alpha \in S$ es algebraico sobre F. Entonces todo elemento de K es algebraico sobre F.*

Demostración. Sea $\beta \in K$. Puesto que $K = F(S)$, existe una cantidad finita de elementos $\alpha_1, \ldots, \alpha_n \in S$ tal que $\beta \in F(\alpha_1, \ldots, \alpha_n)$. Concluimos, ahora, con la Proposición 3.1.20. □

Ejemplo 3.1.22. La extensión $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \ldots, \sqrt[n]{2}, \ldots)$ no es finita, puesto que contiene elementos, $\sqrt[n]{2}$, de grado n, arbitrariamente grande, sobre $\mathbb{Q}$.

Usaremos, repetidamente, un caso particular de la demostración de Proposición 3.1.5.

Observación 3.1.23. Sea $F(\alpha, \beta)/F$ tal que $[F(\alpha)(\beta) : F(\alpha)] = d$ y $[F(\alpha) : F] = n$. Entonces una base de $F(\alpha, \beta)$ como F–espacio vectorial es

$$\{\alpha^i \beta^j\}_{\substack{i = 0, \ldots, n-1 \cdot \\ j = 0, \ldots, d-1}}$$

Corolario 3.1.24. *Transitividad Sean K/F una extensión algebraica y $\alpha \in L$, con L extensión de K. Si α es algebraico sobre K, entonces α es algebraico sobre F.*

Demostración. El elemento α es raíz de cierto polinomio $p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$. Esto significa que α es algebraico sobre $F(a_{n-1}, \ldots, a_0)$. Esta última extensión está finitamente generada por elementos algebraicos $a_{n-1}, \ldots, a_0$ sobre F. Según Proposición 3.1.20, $F(a_{n-1}, \ldots, a_0)$ es una extensión finita de F. Ahora de la Proposición 3.1.5 y de Proposición 3.1.19, deducimos que $F(\alpha, a_{n-1}, \ldots, a_0)$ es finita, y, por tanto, algebraica sobre F. En particular, α es algebraico sobre F. □

Corolario 3.1.25. *Sea L/F una extensión. El conjunto K, formado por los elementos de L que son algebraicos sobre F, es un subcuerpo de L. Diremos que la extensión algebraica K/F es el cierre algebraico de F en L.*

Demostración. Sean $0 \neq \alpha, \beta \in K$. La extensión $F(\alpha, \beta)/F$ es finita y, por tanto, algebraica. Así $\alpha \pm \beta, \alpha\beta, \alpha^{-1} \in F(\alpha, \beta)$ son algebraicos sobre F. Esto es, $\alpha \pm \beta, \alpha\beta, \alpha^{-1} \in K$. □

Resumiendo todo lo anterior:

Proposición 3.1.26. *(1) Sea K/F extensión finita. Entonces K/F es algebraica y para cada $\alpha \in K$ es $[K : F] = [K : F(\alpha)] \cdot (\deg m_{\alpha,F}(X))$.*

(2) Una extensión finitamente generada $F(\alpha_1, \ldots, \alpha_n)/F$ es finita si, y sólo si, cada α_i es algebraico sobre F.

(3) K/F finita si, y sólo si, K/F algebraica finitamente generada si, y sólo si, K/F finitamente generada por elementos algebraicos sobre F.

Ejemplos 3.1.27. (1) *Extensiones cuadráticas*

Sean F un cuerpo de característica $\neq 2$ y K/F de grado $[K : F] = 2$. Tomamos $\alpha \in K - F$. Entonces $\deg m_{\alpha,F}(X) = 2$ y, por tanto, $K = F(\alpha)$. Sea $m_{\alpha,F}(X) = X^2 + bX + c$. Entonces $\alpha = \frac{-b \pm \sqrt{b^2-4c}}{2}$. Además $D = b^2 - 4c$ no es un cuadrado en F puesto que $\alpha \notin F$. El símbolo $\sqrt{b^2 - 4c}$ denota una raíz de la ecuación $X^2 - (b^2 - 4c) = 0$. Así $\sqrt{D} \in K$ y $K = F(\sqrt{D})$.

Observemos que no hay una forma canónica de elegir "la" raíz cuadrada, análoga a elegir "la" raíz positiva en $\mathbb{R}$, i.e., las raíces son algebraicamente independientes.

En resumen, si char $F \neq 2$, entonces $[K : F] = 2$ si, y sólo si, $K = F(\sqrt{D})$, donde $D \in F$ no es un cuadrado en F.

(2) Sea α una raíz de $p(X) = X^3 - 3X - 1$. Entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Podemos preguntarnos si $\sqrt{2} \in \mathbb{Q}(\alpha)$. Si así fuera, se tendría $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2} : \mathbb{Q}]$. Esto es $3 = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})]2$. Por tanto $\sqrt{2} \notin \mathbb{Q}(\alpha)$, i.e., $\sqrt{2} \neq a_0 + a_1\alpha + a_2\alpha^2$ para todo $a_0, a_1, a_2 \in \mathbb{Q}$.

(3) Sea $\sqrt[6]{2}$ la raíz sexta real positiva de 2. Entonces $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$, puesto que $X^6 - 2$ es irreducible.

Por otra parte, $(\sqrt[6]{2})^3 = \sqrt{2}$. Por tanto, $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[6]{2})$ y

$$6 = [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})].[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

Así $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$ y, puesto que, $\sqrt[6]{2}$ es una raíz de $X^3 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[X]$, se deduce que $X^3 - \sqrt{2}$ es irreducible sobre $\mathbb{Q}(\sqrt{2})$ y

$$m_{\sqrt[6]{2},\mathbb{Q}(\sqrt{2})}(X) = X^3 - \sqrt{2}.$$

(4) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}] = 4$. En efecto,

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

donde $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ y $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, puesto que $\sqrt{3}$ es raíz de $X^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$ y $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$: si $\sqrt{3} = a + b\sqrt{2}$, entonces $3 = a^2 + 2b + 2ab\sqrt{2}$ y, de aquí, $\sqrt{2} \in \mathbb{Q}$ si $ab \neq 0$; ó $\sqrt{3} \in \mathbb{Q}$ si $b = 0$. Así $a = 0$ y $\sqrt{3} = b\sqrt{2}$, de donde $\sqrt{6} = 2b \in \mathbb{Q}$, que es falso.

De $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ se deduce que una base de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$ es $\{1, \sqrt{2}\}$ y, de $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ se deduce que una base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$ es $\{1, \sqrt{3}\}$. Por tanto, según la Observación 3.1.23, una base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$ es $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

Definición 3.1.28. *Sean $K_1, K_2 \subset K$. Denotaremos K_1K_2 al subcuerpo intersección de todos los subcuerpos de K que contienen a K_1 y a K_2. Es el menor subcuerpo de K que contiene a K_1 y a K_2. Diremos que es el subcuerpo compuesto de ambos.*

Proposición 3.1.29. *Sean $K_1/F, K_2/F$ finitas en K/F, con $[K_1 : F] = m, [K_2 : F] = n$ y bases $\{\alpha_1, \ldots, \alpha_m\}, \{\beta_1, \ldots, \beta_n\}$. Entonces $K_1K_2 = F(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$ y $[K_1K_2 : F] \leq mn$, con igualdad si, y sólo si, una F–base de uno de los subcuerpos permanece linealmente independiente sobre el otro.*

Corolario 3.1.30. *En las condiciones de Proposición 3.1.29, si* mcd $(m, n) = 1$, *entonces* $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.

Demostración. De $F \subset K_i \subset K_1K_2$ se deduce $m, n \mid [K_1K_2 : F] \leq mn$. □

Ejemplo 3.1.31. En $K = \mathbb{R}$, es $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$. En efecto, puesto que $(\sqrt[6]{2})^3 = \sqrt{2}$ y $(\sqrt[6]{2})^2 = \sqrt[3]{2}$ se tiene $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[6]{2})$. Por otra parte, es claro que todo cuerpo que contiene a $\sqrt{2}$ y $\sqrt[3]{2}$ también contiene a $\sqrt[6]{2}$.

Observación 3.1.32. Con la teoría desarrollada hasta el momento, podemos dar respuesta negativa al problema de la duplicación del cubo con regla y compás: construir, con regla y compás, la arista de un cubo cuyo volumen duplica el de un cubo dado. Esto equivale a construir el número $\sqrt[3]{2}$.
De forma resumida, podemos decir que los puntos del plano complejo constructibles con regla y compás son aquellos que se obtienen, a partir de $0, 1$, mediante una sucesión finita de: intersecciones de dos rectas, de recta y circunferencia o de dos circunferencias. Es decir, soluciones de ecuaciones lineales o cuadráticas. Por tanto, un punto constructible aparece, a partir de $\mathbb{Q}$, tras una sucesión finita de extensiones de grado 2. En consecuencia, si α es constructible, entonces $\alpha \in K$, con $[K : \mathbb{Q}] = 2^n$. Así, si $\sqrt[3]{2}$ fuera constructible tendríamos

$$2^n = [K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

Esto no es posible, puesto que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

3.2. Cuerpos de descomposición. Cierre algebraico

3.2.1. Sean F un cuerpo y $f(X) = a_nX^n + \cdots + a_0 \in F[X]$, con $0 \neq a_n$, un polinomio de grado $n \geq 1$. Hemos probado, Teorema 3.1.15, que existe un cuerpo $K_1 = F(\alpha_1)$, donde $f(X) = (X - \alpha_1)f_1(X)$, con $f_1(X) \in K_1[X]$. El mismo argumento para $f_1(X) \in K_1[X]$, si $\deg f_1 \geq 1$, prueba que existe $K_2 = F(\alpha_1, \alpha_2)$, donde $f(X) = a_n(X - \alpha_1)(X - \alpha_2)f_2(X)$, con $f_2(X) \in K_2[X]$. Usando inducción, es claro que existe un cuerpo $K = F(\alpha_1, \ldots, \alpha_n)$, donde $f(X) = a_n(X - \alpha_1)\cdots(X - \alpha_n)$ y $K = F(\alpha_1, \ldots, \alpha_n)$.
Si $f(X) = a_n(X - \beta_1)\cdots(X - \beta_n)$, con $\beta_i \in K' \subset K$. Entonces la unicidad de la factorización en $K[X]$ implica $X - \alpha_i = X - \beta_{\sigma i}$ para cierta permutación de n elementos σ. Así $K' = K$ y K es el menor subcuerpo de K, extensión de F, donde $f(X)$ factoriza en producto de factores lineales.

Definición 3.2.2. Diremos que K es un cuerpo de descomposición de $f(X)$ sobre F.

Observación 3.2.3. En las condiciones de (3.2.1).

(1) La extensión K/F es finita, puesto que está generada por una cantidad finita $\{\alpha_1, \ldots, \alpha_n\}$ de elementos algebraicos sobre F.

(2) El grado $[K_1 : F] \leq n$, puesto que α_1 es raíz de un polinomio $f(X) \in F[X]$ de grado n. El grado $[K_2 : F] = [K_2 : K_1][K_1 : F] \leq (n - 1)n$, puesto que α_2 es raíz de un polinomio $f_1(X) \in K_1[X]$ de grado $n - 1$. Así $[K : F] \leq n!$.

(3) Para cualquier $1 \leq i \leq$ es $F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n)$.

En efecto, $f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots = a_nX^n - a_n(\alpha_1 + \cdots + \alpha_n)X^{n-1} + \cdots$. Así $a_{n-1} = a_n(\alpha_1 + \cdots + \alpha_n)$, de donde $\alpha_i = -\frac{a_{n-1}}{a_n} - (\alpha_1 + \cdots + \alpha_{i-1} + \alpha_{i+1} + \cdots + \alpha_n) \in F(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n)$.

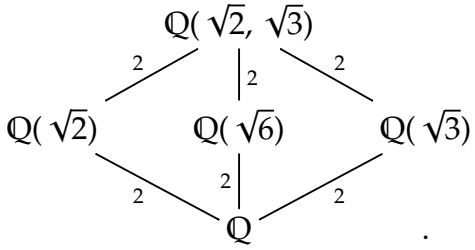
Observemos también que si $s_i = \sum_{1 \leq r_1 < \cdots < r_i \leq n} X_{r_1} \cdots X_{r_i}$ es la i–ésima función simétrica elemental, entonces el coeficiente de X^i en $f(X)$ es $a_i = a_n s_i(\alpha_1, \ldots, \alpha_n)$. Por tanto $s_i(\alpha_1, \ldots, \alpha_n) \in F$

(4) Demostraremos, a continuación, que dos cuerpos de descomposición de un polinomio $f(X)$ sobre F son isomorfos, con un isomorfismo que es la identidad en F. Diremos que son isomorfos sobre F.

Ejemplos 3.2.4. (1) El cuerpo de descomposición de $X^2 - 2$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\pm\sqrt{2}) = \mathbb{Q}(\sqrt{2})$.

(2) El cuerpo de descomposición sobre $\mathbb{Q}$ de $f(X) = (X^2 - 2)(X^2 - 3)$ es $\mathbb{Q}(\pm\sqrt{2}, \pm\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, cuyo grado es $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

El Teorema Fundamental de la Teoría de Galois nos permitirá demostrar que el retículo de subcuerpos de la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ es



(3) El cuerpo de descomposición de $X^3 - 2$.

Las raíces son $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$, con $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, $\omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$ las raíces cúbicas primitivas de 1.

El cuerpo de descomposición es

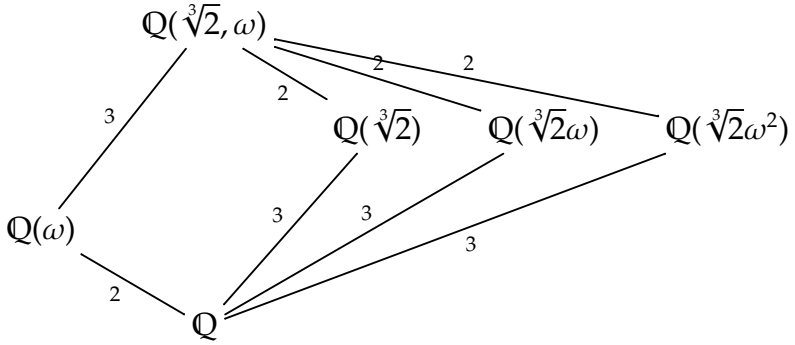
$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i).$$

El polinomio mínimo de ω, ω^2 sobre $\mathbb{Q}$ es $X^2 + X + 1$ y, es claro que $\omega \notin \mathbb{Q}(\sqrt[3]{2})$. Por tanto $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = 2$. Así

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

Los subcuerpos, $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\omega), \mathbb{Q}(\sqrt[3]{2}\omega^2)$ son distintos. En efecto, si dos de ellos fueran el mismo subcuerpo L de grado 3 sobre $\mathbb{Q}$, entonces, para $0 \leq i < j \leq 2$, el elemento $\frac{\sqrt[3]{2}\omega^j}{\sqrt[3]{2}\omega^i} = \omega^{j-i} \in L$. Esto no es posible, puesto que $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^2)$ es de grado 2 sobre $\mathbb{Q}$: la ecuación irreducible $X^2 + X + 1 = 0$ tiene por raíces ω, ω^2.

El Teorema Fundamental de la Teoría de Galois nos permitirá demostrar que el retículo de subcuerpos de la extensión $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ es



(4) El polinomio $X^4 + 4 = (X^2 + 2X + 2)(X^2 - 2X + 2)$ tiene raíces $1 \pm i, -1 \pm i$. Por tanto, el cuerpo de descomposición de $X^4 + 4$ sobre $\mathbb{Q}$ es $\mathbb{Q}(1 \pm i, -1 \pm i) = \mathbb{Q}(i)$.

(5) Cuerpo de descomposición de $X^n - 1$ sobre $\mathbb{Q}$ (cuerpo ciclotómico).

El conjunto

$$\mu_n = \{e^{\frac{2\pi ik}{n}} | k = 0, \ldots, n-1\} =< \zeta >=< \zeta^a >,\ \text{mcd}\ (a,n) = 1,\ 1 \leq a < n.$$

de las raíces n–ésimas de 1, es un subgrupo cíclico de $\mathbb{C}^*$ generado por cada una de las raíces primitivas $\zeta = e^{\frac{2\pi i}{n}}$ ó ζ^a, con mcd $(a,n) = 1,\ 1 \leq a < n$.

Algunos valores de $\zeta = e^{\frac{2\pi i}{n}}$:

n	$\zeta = e^{\frac{2\pi i}{n}}$
1	1
2	-1
3	$-\frac{1}{2} + \frac{\sqrt{3}}{2}\, i$
4	i
5	$\frac{-1+\sqrt{5}}{4} + \frac{\sqrt{10+2\sqrt{5}}}{4}\, i$
6	$\frac{1}{2} + \frac{\sqrt{3}}{2}\, i$
7	$-\frac{1}{6} + \frac{1}{6}\sqrt[3]{\frac{7}{2}(1+3\,i\,\sqrt{3})} + \frac{1}{6}\sqrt[3]{\frac{7}{2}(1-3\,i\,\sqrt{3})} + \\ + \frac{i}{2}\sqrt{1 - \left(\frac{1}{3} - \frac{1}{3}\sqrt[3]{\frac{7}{2}(1+3\,i\,\sqrt{3})} - \frac{1}{3}\sqrt[3]{\frac{7}{2}(1-3\,i\,\sqrt{3})}\right)^2}$
8	$\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\, i$

El cuerpo de descomposición de $X^n - 1$ es

$$\mathbb{Q}(\{e^{\frac{2\pi ik}{n}} | k = 0, \ldots, n-1\}) = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^a),\ \ \text{mcd}\ (a,n) = 1,\ 1 \leq a < n.$$

Veremos que el polinomio mínimo de ζ es

$$\prod_{\substack{1 \leq a < n \\ \text{mcd}\,(a,n) = 1}} (X - \zeta^a).$$

Por tanto, el grado es

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) := |\{a \mid \text{mcd}\ (a,n) = 1,\ 1 \leq a < n\}|.$$

(6) Cuerpo de descomposición del polinomio irreducible (Eisenstein) $X^p - q$, con $p \geq 3$ primo y q entero positivo con un factor primo simple.

Las raíces son $\{\sqrt[p]{q}\,\zeta^j \mid 0 \leq j \leq p-1\}$, con $\zeta = e^{\frac{2\pi\, i}{p}}$. El cuerpo de descomposición es

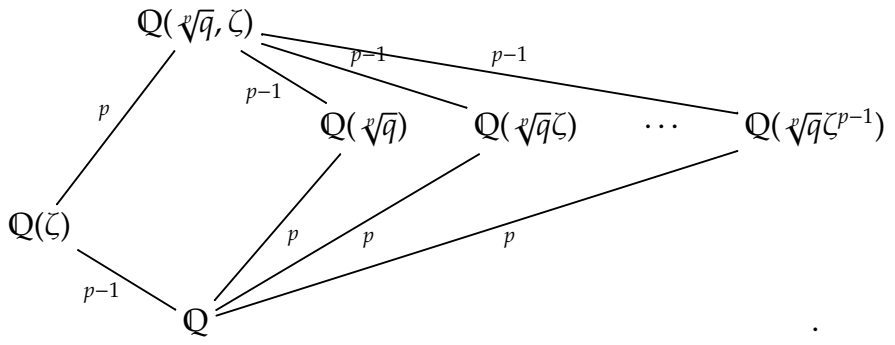
$$\mathbb{Q}(\{\sqrt[p]{q}\,\zeta^j \mid 0 \leq j \leq p-1\}) = \mathbb{Q}(\sqrt[p]{q}, \zeta).$$

Los grados $[\mathbb{Q}(\sqrt[p]{q} : \mathbb{Q}] = p$ y $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. Así, puesto que mcd $(p, p-1) = 1$, el grado es

$$[\mathbb{Q}(\sqrt[p]{q}, \zeta) : \mathbb{Q}] = p(p-1).$$

Los subcuerpos, $\mathbb{Q}(\sqrt[p]{q}\zeta^j)$, $j = 0, \ldots, p-1$ son distintos. En efecto, si dos de ellos fueran el mismo subcuerpo L de grado p sobre $\mathbb{Q}$, entonces, para $0 \leq i < j \leq p-1$, el elemento $\frac{\sqrt[p]{q}\zeta^j}{\sqrt[p]{q}\zeta^i} = \zeta^{j-i} \in L$. Esto no es posible, puesto que $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^j)$, $j = 0, \ldots, p-1$ es de grado $p-1$ sobre $\mathbb{Q}$: la ecuación irreducible $X^{p-1} + X^{p-2} + \cdots + X + 1 = 0$ tiene por raíces $\zeta, \zeta^2, \ldots, \zeta^{p-1}$.

Una *parte* del retículo de subcuerpos es



El Teorema Fundamental de la Teoría de Galois afirma que el retículo de subcuerpos de la extensión es dual del retículo de subgrupos de cierto grupo de orden finito (igual al grado de la extensión) asociado a la extensión. En particular el retículo de subcuerpos es finito.

En este ejemplo, veremos que el grupo es el llamado *grupo lineal afín unidimesional módulo p*: AGL$(1, \mathbb{F}_p)$. Es el grupo de las aplicaciones afines $\gamma_{a,b} : \mathbb{F}_p \to \mathbb{F}_p$, $x \mapsto ax + b$; $0 \neq a, b \in \mathbb{F}_p$, donde $\gamma_{a,b}\,\gamma_{c,d} = \gamma_{ac,ad+b}$. Este grupo es isomorfo al producto semidirecto $\mathbb{F}_p \rtimes \mathbb{F}_{p-1}$, esto es, el producto $\mathbb{F}_p \times \mathbb{F}_{p-1}$ con la operación $(b, a)\cdot(d, c) = (ad + b, ac)$. Completar el retículo de subgrupos de este grupo o, de forma equivalente, el retículo de subcuerpos de la extensión, no es un problema sencillo.

Teorema 3.2.5. *Sean $\varphi : F \xrightarrow{\sim} F'$ un isomorfismo de cuerpos, $f(X) \in F[X]$ un polinomio de grado ≥ 1 y $f^\varphi(X) \in F'[X]$ el polinomio obtenido aplicando φ a los coeficientes de f. Sean E un cuerpo de descomposición de f sobre F y E' un cuerpo de descomposición de f^φ sobre F'. Entonces existe un isomorfismo $\sigma : E \to E'$ que extiende a φ.*

Demostración. Si $n = 1$, entonces $E = F, E' = F'$ y la conclusión es trivial. Sea $n > 1$ y supongamos el resultado cierto para polinomios de grado $< n$.
Sean $p(X) \in F[X]$ un factor irreducible de $f(X)$ y $p^\varphi(X) \in F'[X]$ el correspondiente factor irreducible de $f^\varphi(X)$. Sean $\alpha \in E$ una raíz de p y $\beta \in E'$ una raíz de p^φ. Según el Teorema 3.1.17, existe un isomorfismo $\varphi_1 : F(\alpha) \to F'(\beta)$ que extiende a φ y aplica α en β. Por tanto, en $F(\alpha)[X]$ y $F'(\beta)[X]$, se tiene $f(X) = (X - \alpha)f_1(X)$ y $f^\varphi(X) = f^{\varphi_1}(X) =$

$(X-\alpha)^{\varphi_1} f_1^{\varphi_1}(X) = (X-\beta) f_1^{\varphi_1}(X)$, con $\deg f(X) = n-1$. Además E es un cuerpo de descomposición de f_1 sobre $F(\alpha)$ y E' es un cuerpo de descomposición de $f_1^{\varphi_1}$ sobre $F'(\beta)$. Podemos, así, aplicar la hipótesis de inducción para obtener un isomorfismo $\sigma : E \to E'$ que extiende a φ_1 y, por tanto, a φ. □

Corolario 3.2.6. *Sean $f(X) \in F[X]$ un polinomio de grado ≥ 1 y E, E' cuerpos de descomposición de f sobre F. Existe un isomorfismo $E \xrightarrow{\sim} E'$ que es la identidad en F.*

Observación 3.2.7. El isomorfismo $E \xrightarrow{\sim} E'$ dista mucho de ser único y no existe un isomorfismo distinguido o "canónico" $E \xrightarrow{\sim} E'$ sobre F.

Construiremos ahora, un cuerpo extensión de F que contiene todas las raíces de todos los polinomios con coeficientes en F.

Definición 3.2.8. (1) Sea F un cuerpo. Un cuerpo $\overline{F}$ extensión algebraica de F se dice un cierre algebraico de F si $\overline{F}$ contiene un cuerpo de descomposición de cada polinomio de grado ≥ 1 con coeficientes en F. Esto es $\overline{F}$ es algebraico sobre F y contiene todos los elementos algebraicos sobre F.

(2) Diremos que un cuerpo K es algebraicamente cerrado si cada polinomio de grado ≥ 1 con coeficientes en K tiene una raíz en K.

Observación 3.2.9. Si K es algebraicamente cerrado entonces K contiene un cuerpo de descomposición de cada polinomio de grado ≥ 1 con coeficientes en K. Esto es, si K es algebraicamente cerrado, entonces K es un cierre algebraico de K. Recíprocamente si $\overline{K} = K$ entonces K es algebraicamente cerrado.
En otras palabras, K es algebraicamente cerrado si, y sólo si, la condición α algebraico sobre K implica $\alpha \in K$.

Proposición 3.2.10. *Un cuerpo $\overline{F}$ extensión de F es un cierre algebraico de F si, y sólo si, $\overline{F}$ es algebraicamente cerrado y algebraico sobre F.*

Demostración. Sean $\overline{F}$ un cierre algebraico de F y α una raíz de un polinomio $f(X) = a_0 + \cdots + a_n X^n \in \overline{F}[X]$. Se trata de probar que $\alpha \in \overline{F}$. En efecto, α es algebraico sobre $F(a_0, \ldots, a_n)$, de forma que $[F(a_0, \ldots, a_n, \alpha) : F(a_0, \ldots, a_n)]$ es finito. también $[F(a_0, \ldots, a_n) : F]$ es finito, puesto que los a_i son algebraicos sobre F. Por tanto $F(a_0, \ldots, a_n, \alpha)/F$ es una extensión finita y, por tanto, algebraica, de forma que α es algebraico sobre F. Así $\alpha \in \overline{F}$. El recíproco es claro. □

Teorema 3.2.11. *Para cada cuerpo F existe un cuerpo algebraicamente cerrado K que contiene a F como subcuerpo.*

Demostración. Para cada polinomio $f(X) \in F[X]$ mónico de grado ≥ 1, denotamos X_f una indeterminada y consideramos el anillo de polinomios $F[\{X_f\}]$ en la familia de variables $\{X_f \mid f \in F[X],\ f \text{ mónico, } \deg f \geq 1\}$.

En este anillo de polinomios consideramos el ideal I generado por la familia $\{f(X_f) \mid f \in F[X],\ f \text{ mónico, } \deg f \geq 1\}$.
Afirmamos que I es un ideal propio. En efecto, si $1 \in I$, entonces para una familia finita de variables $\{X_{f_1}, \ldots, X_{f_n}\}$, se tiene una igualdad

$$1 = g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}), \tag{3.2.11.1}$$

donde los $g_i \in F[\{X_f\}]$. Sean $X_1 = X_{f_1}, \ldots, X_n = X_{f_n}$ y $X_{n+1}, \ldots, X_m$ las variables que aparecen en los g_i. Entonces la igualdad (3.2.11.1) tiene lugar en el anillo de polinomios $F[X_1, \ldots, X_m]$. Sea F' una extensión de F donde cada uno de los $f_i(X_i)$, $i = 1, \ldots, n$, tenga una raíz α_i. Existe un homomorfismo de sustitución $F[X_1, \ldots, X_m] \to F'$ que asigna $X_i \mapsto \alpha_i$, $i = 1, \ldots, n$. Aplicando esta sustitución en (3.2.11.1) se obtiene $1 = 0$.
En consecuencia, I es un ideal propio y sabemos que, como consecuencia del Lema de Zorn, I está contenido en un ideal maximal M de $F[\{X_f\}]$. El cuerpo $K_1 = F[\{X_f\}]/M$ es un cuerpo extensión de F donde cada polinomio $f \in F[X]$ mónico y de grado ≥ 1 tiene una raíz $f(\overline{X_f}) = 0$, puesto que $X_f \in I \subset M$.
Repetimos, inductivamente, la construcción para obtener

$$F = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset K_{n+1} \subset \cdots,$$

sucesión de extensiones, donde cada polinomio de grado positivo con coeficientes en K_n tiene una raíz en K_{n+1}.
La unión $K = \cup_{n \geq 0} K_n$ es un cuerpo extensión de F. Los coeficientes de un polinomio de grado positivo $h(X) \in K[X]$ están en cierto K_m, por tanto h tiene una raíz en $K_{m+1} \subset K$. Esto es K es algebraicamente cerrado. □

Observación 3.2.12. La demostración de la existencia de un cuerpo algebraicamente cerrado que contiene a un cuerpo dado, hace uso del Lema de Zorn, que es una de las formas equivalentes del axioma de elección

Podemos ahora obtener un cierre algebraico de F.

Proposición 3.2.13. *Sean K un cuerpo algebraicamente cerrado y F un subcuerpo de K. El conjunto $\overline{F}$ formado por los elementos de K que son algebraicos sobre F es un cierre algebraico de F.*

Demostración. Por definición, $\overline{F}$ es algebraico sobre F. El cuerpo K contiene un cuerpo de descomposición de cada polinomio de grado positivo $f \in F[X]$. Puesto que estos cuerpos de descomposición son algebraicos sobre F, están contenidos en $\overline{F}$. □

Corolario 3.2.14. *Todo cuerpo F tiene un cierre algebraico $\overline{F}$.*

Demostración. Teorema 3.2.11 y Proposición 3.2.13. □

Proposición 3.2.15. *Sean K/F una extensión algebraica y L un cierre algebraico de K. Entonces L es un cierre algebraico de F.*

Demostración. Basta aplicar la transitividad en extensiones algebraicas, Corolario 3.1.24. □

El siguiente resultado muestra que dos cierres algebraicos de un cuerpo son isomorfos.

Teorema 3.2.16. *Sean $\varphi : F \xrightarrow{\sim} F'$ un isomorfismo de cuerpos y E, E' cierres algebraicos de F, F'. Existe un isomorfismo $E \xrightarrow{\sim} E'$ extensión de φ.*

Demostración. Sea

$$\Sigma = \{(\varphi, K, K') \mid F \subset K \subset E, F' \subset K' \subset E'; K \xrightarrow{\varphi} K', F - \text{isomorfismo}\}.$$

En Σ definimos un orden por

$$(\varphi, K, K') \leq (\psi, L, L') \Leftrightarrow K \subset L,\ K' \subset L',\ \psi_{|K} = \varphi.$$

Probemos que se verifican las hipótesis del Lema de Zorn para $(\Sigma, \leq)$.
Sea $\{(\varphi_i, K_i, K_i')\}_{i\in I} \subset \Sigma$ un subconjunto totalmente ordenado. Entonces $K = \cup K_i$ es subcuerpo de E, $K' = \cup K_i'$ es subcuerpo de E' y $\varphi : K \to K'$ tal que $x \mapsto \varphi_i(x)$ si $x \in K_i$, está bien definido, puesto que si $K_j \subset K_i$, entonces $\varphi_{i_{|K_j}} = \varphi_j$, y es F–isomorfismo. Así (K, K', φ) es una cota superior de $\{(\varphi_i, K_i, K_i')\}_{i\in I}$ en $(\Sigma, \leq)$.
El lema de Zorn asegura que existe (σ, H, H') maximal en $(\Sigma, \leq)$. Afirmamos que $H = E$ y $H' = E'$. En efecto, supongamos que existe $\alpha \in E - H$. Se tiene, entonces, $F \subset H \subsetneq H(\alpha) \subset E$. Puesto que E es una extensión algebraica de F y $F \subset H \subset E$, el elemento $\alpha \in E$ es algebraico sobre H. Por tanto, según Teorema 3.1.17, $H \xrightarrow{\sigma} E'$ se puede extender a un F–isomorfismo $\eta : H(\alpha) \xrightarrow{\sim} H'(\beta)$, donde β es una raíz del polinomio de $E'[X]$ obtenido aplicando σ a los coeficientes del polinomio mínimo de α sobre H. Ahora bien, $\beta \in E'$, puesto que E' es algebraicamente cerrado. Así $H'(\beta) \subset E'$ y, por tanto, $(\sigma, H, H') < (\eta, H(\alpha), H'(\beta)) \in \Sigma$, en contra de la maximalidad de (σ, H, H').
Hemos probado que $H = E$. En consecuencia H', que es $H' \simeq E'$, es algebraicamente cerrado y E' es extensión algebraica de H'. Por tanto $E' = H'$. □

Como consecuencia obtenemos:

Teorema 3.2.17. *Sean K/F una extensión algebraica y $F \xrightarrow{\sigma} L$ un homomorfismo (inmersión) de F en un cuerpo algebraicamente cerrado. Existe una extensión $K \xrightarrow{\tau} L$ de σ. Si K es algebraicamente cerrado y L es algebraico sobre $\sigma(F)$, entonces cada tal extensión es un isomorfismo de K sobre L*

Demostración. Sean $F' = \sigma(F) \subset L$ y E' el cierre algebraico de F' en L. Sea E un cierre algebraico de K. Entonces, por Proposición 3.2.15, E es un cierre algebraico de F. Aplicamos el Teorema 3.2.16 al isomorfismo $F \xrightarrow{\sigma} F'$, a E cierre algebraico de E y E' cierre algebraico de F', para obtener un isomorfismo $E \xrightarrow{\tau_1} E'$ que extiende a $\sigma_{|F}$. La restricción $\tau = \tau_{1|K}$ es la extensión buscada.
En las condiciones de la segunda parte del enunciado $K = E$ y $L = E'$. □

Ejemplos 3.2.18. (1) El Teorema Fundamental del Álgebra afirma que $\mathbb{C}$ es algebraicamente cerrado. Por tanto, $\mathbb{C} = \mathbb{R}(i)$ es un cierre algebraico de $\mathbb{R}$. Más aun, $\mathbb{C}$ contiene un cierre algebraico de cada uno de sus subcuerpos.

(2) El cuerpo de los números algebraicos

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ es algebraico sobre } \mathbb{Q}\},$$

es un cierre algebraico de $\mathbb{Q}$.

3.2.19. El cuerpo de los números algebraicos $\overline{\mathbb{Q}}$ es numerable.

Demostración. Definimos la altura $h(r)$ de un número racional como máx($| m |, | n |$), donde $r = m/n$, con mcd$(m, n) = 1$. Hay sólo una cantidad finita de números racionales con altura menor que un número fijado $N \in \mathbb{N}$. Sea $A(N)$ el conjunto de números algebraicos cuyo polinomio mínimo sobre $\mathbb{Q}$ tiene grado $\leq N$ y tiene coeficientes de altura $< N$. Entonces $A(N)$ es finito para cada N. Elegimos una biyección de $A(10)$ con cierto segmento $[0, n(1)] \subset \mathbb{N}$. Extendemos esta biyección a una biyección de $A(100)$ con un segmento $[0, n(2)] \subset \mathbb{N}$, donde $n(2) > n(1)$. Esta construcción define, de forma inductiva, una biyección entre $\overline{\mathbb{Q}}$ y $\mathbb{N}$. □

(3) (1844) Liouville prueba que ciertos números del tipo $\sum_{n=0}^{\infty} 10^{-n!}$ son trascendentes.

Teorema 3.2.20 (Lindemann–Weierstrass)**.** *Sean $\alpha_1, \ldots, \alpha_n$ números algebraicos distintos. Entonces $e^{\alpha_1}, \ldots, e^{\alpha_n}$ son linealmente independientes sobre $\mathbb{Q}$.*

Corolario 3.2.21. *Si $\alpha \neq 0$ es algebraico, entonces e^{α} es trascendente. En particular, e es trascendente.*

Demostración. El Teorema (3.2.20) afirma que $e^0, e^{\alpha}, \cdots, e^{n\alpha}$ son linealmente independientes sobre $\mathbb{Q}$ para cada n. □

Corolario 3.2.22. *Si $\beta \neq 1$ es algebraico, entonces $\alpha = \log_e \beta$ es trascendente.*

Corolario 3.2.23. *El número π es trascendente.*

Demostración. Si π fuera algebraico, entonces πi sería algebraico y, por tanto, $e^{\pi i} = -1$ sería trascendente. □

(4) (1873) Hermite prueba que e es trascendente.

(5) (1874) Cantor prueba que $\overline{\mathbb{Q}}$ es numerable y $\mathbb{R}$ es no numerable.

(6) (1882) Lindemann prueba que π es trascendente.

(7) (1934) (Gelfand–Schneider) Si $0,1 \neq \alpha$ y $\beta \notin \mathbb{Q}$ son algebraicos, entonces α^β es trascendente (7^{th} problema de Hilbert).

(8) *Ejemplos.*

a) $2^{\sqrt{2}} = 2{,}66514414\ldots$, y su raíz cuadrada $\sqrt{2}^{\sqrt{2}}$, son trascendentes.

b) $e^\pi = (e^{i\pi})^{-i} = (-1)^{-i} = 23{,}140692632\ldots$, es trascendente (constante de Gelfand).

c) $e^{-\frac{\pi}{2}} = (e^{i\frac{\pi}{2}})^i = i^i = 0{,}207879\ldots$, es trascendente.

(9) (1994) La trascendencia de la constante de Euler

$$\gamma = \lim_{n\to\infty}(\sum_{k=1}^{n} \frac{1}{k} - \log n),$$

no ha sido probado probada todavía.

(10) (1994) ¿Es $e \pm \pi$ trascendente? ¿Es e trascendente sobre $\mathbb{Q}(\pi)$? ¿Es π trascendente sobre $\mathbb{Q}(e)$?

Proposición 3.2.24. *Si K/F es algebraica, entonces $|K| \leq$ máx$\{|F|, |\mathbb{N}|\}$, donde $||$ denota la cardinalidad del conjunto.*

Demostración. Para cada $\alpha \in K$ fijamos una ordenación $\alpha_1, \ldots, \alpha_n$ de las raíces distintas de $m_{\alpha,F}(X)$ en K. Sea $\mathscr{M}$ el conjunto de polinomios mónicos con coeficientes en F. Definimos una aplicación

$$\begin{aligned} \varphi : K &\to \mathscr{M} \times \mathbb{N} \\ \alpha &\mapsto (m_{\alpha,F}(X), r), \end{aligned}$$

si α es $\alpha = \alpha_r$.
La aplicación es inyectiva. Así $|K| \leq |\mathscr{M} \times \mathbb{N}| =$ máx$\{|\mathscr{M}|, |\mathbb{N}|\}$.
Probemos ahora que $|\mathscr{M}| \leq$ máx$\{|F|, |\mathbb{N}|\}$.
Sea $\mathscr{M}_n \subset \mathscr{M}$ el conjunto de polinomios mónicos de grado n. Entonces $|\mathscr{M}_n| = |F^n|$. Si F es finito, entonces $|F^n| = |F|^n$ es finito y, si F es infinito $|F^n| = |F|$. Por tanto, $|\mathscr{M}| = |\cup \mathscr{M}_n| =$ máx$\{|F|, |\mathbb{N}|\}$. □

3.3. Extensiones separables

3.3.1. Recordemos, Teorema 3.2.17, que dada una extensión algebraica K/F y una inmersión (homomorfismo) $F \xrightarrow{\sigma} L$ en un cuerpo algebraicamente cerrado existe una extensión $K \xrightarrow{\tau} L$ de σ.
Consideramos el caso particular $K = F(\alpha)$. Cada extensión $F(\alpha) \to L$ está determinada por $\tau(\alpha) = \beta$, que ha de ser una raíz de $m^{\sigma}_{\alpha,F}(X)$ en L. Denotemos $p(X) = m_{\alpha,F}(X)$. Para cada raíz β de $p^{\sigma}(X)$ en L, la aplicación

$$\begin{gathered} F(\alpha) \xrightarrow{\tau} L \\ a_m\alpha^m + \cdots + a_0 \mapsto \sigma(a_m)\beta^m + \cdots + \sigma(a_0), \end{gathered}$$

está bien definida y es un homomorfismo extensión de σ.
Por otra parte, podemos suponer que L es un cierre algebraico de σF, puesto que toda extensión de σ aplica K en una extensión algebraica de σF y, si $\overline{K}$ es un cierre algebraico de K, el Teorema 3.2.17, asegura que existe un isomorfismo $\overline{K} \to L$ que extiende a σ. Este isomorfismo transforma las raíces de $m_{\alpha,F}(X)$ en $\overline{K}$ en las raíces de $m^{\sigma}_{\alpha,F}(X)$. Hemos, en consecuencia, demostrado:

Proposición 3.3.2. *El número de extensiones de $F \xrightarrow{\sigma} L$, con L algebraicamente cerrado, a $F(\alpha)$, donde α es algebraico sobre F, coincide con el número de raíces distintas de $m_{\alpha,F}(X)$.*

Definición 3.3.3. (1) Sea K/F una extensión algebraica. Diremos que $\alpha \in K$ es separable sobre F si su polinomio mínimo $m_{\alpha,F}(X)$ no tiene raíces múltiples. La extensión K/F es separable si todo elemento de K es separable sobre F.

(2) Un polinomio $f(X) \in F[X]$ es separable si no tiene raíces múltiples.

Observación 3.3.4. Un elemento α algebraico sobre F es separable sobre F si, y sólo si, para cada inmersión $F \xrightarrow{\sigma} L$ en un cuerpo algebraicamente cerrado L, el número de extensiones de σ a $F(\alpha) \to L$ coincide con $[F(\alpha) : F]$.

Ejemplos 3.3.5. (1) Todo polinomio irreducible sobre un cuerpo de característica cero, o característica p que no divide a $\deg p = n$, es separable. En efecto, sea $p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in F[X]$ irreducible, con F de característica cero. Entonces el polinomio derivado $p'(X) = nX^{n-1} + \cdots$ es no nulo y de grado $< n$, por tanto las raíces de $p(X)$ no son raíces de $p'(X)$. Esto es $p(X)$ no tiene raíces múltiples.

(2) Sea $p(X) \in F[X]$ irreducible de grado $n \geq 1$, con $\operatorname{char} F = p$. Si $p'(X) \neq 0$ (e.g. si $p = \operatorname{char} F$ no divide a $n = \deg p(X)$), entonces $p(X)$ no tiene raíces múltiples.

(3) $p(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$ es irreducible y separable, puesto que no tiene raíces en $\mathbb{F}_2$ y si α es una raíz de p, entonces la otra raíz es $\alpha+1$. En efecto, $(X-\alpha)(X-(\alpha+1)) = X^2 - (2\alpha+1)X + (\alpha^2+\alpha) = X^2 - X - 1 = X^2 + X + 1$.

(4) Sea F de característica p. Supongamos que existe $a \in F - F^p$, i.e., $a \neq b^p$ para cada $b \in F$. Entonces $p(X) = X^p - a$ es irreducible sobre F. En efecto, supongamos $X^p - a = h(X)g(X)$, con $\deg h, \deg g \geq 1$. Sea α una raíz de h, entonces, en $F(\alpha)[X]$, se tiene $X^p - a = X^p - \alpha^p = (X-\alpha)^p = h(X)g(X)$. Por tanto, $h(X) = (X-\alpha)^r$, $g(X) = (X-\alpha)^s$, con $1 \leq r, s < p, r + s = p$. Así $h(X) = X^r - r\alpha X^{r-1} + \cdots \in F[X]$, de donde $r\alpha \in F$ y, como $r \neq 0$ en F, se deduce $\alpha \in F$, esto es $a \in F^p$.

(5) El polinomio $X^2 - t = X^2 + t$, con t una indeterminada, es irreducible sobre $F = \mathbb{F}_2(t)$, puesto que $\pm\sqrt{t} \notin \mathbb{F}_2(t)$, i.e., $t \neq (f(t)/g(t))^2$, para todo $0 \neq g(t), f(t) \in \mathbb{F}_2(t)$. Pero, en característica 2, el sueño del alumno de secundaria se hace realidad: $(a \pm b)^2 = a^2 \pm b^2 = a^2 + b^2$. Esto es $(X - \sqrt{t})^2 = X^2 + t$. Por tanto, $X^2 - t$ no es separable sobre $\mathbb{F}_2(t)$.

(6) El polinomio $f(x) = X^{p^n} - X$ sobre $\mathbb{F}_p$ tiene derivada $f'(X) = -1$. Por tanto, no tiene raíces múltiples y es, en consecuencia, separable. Veremos que su cuerpo de descomposición sobre $\mathbb{F}_p$ es el cuerpo finito $\mathbb{F}_{p^n}$ de p^n elementos.

(7) El polinomio $f(X) = X^n - 1 \in F[X]$ tiene derivada $f'(X) = nX^{n-1}$. Si $\operatorname{char} F = 0$ ó $\operatorname{char} F = p \nmid n$, entonces la única raíz de f' es 0, que no es raíz de f. Por tanto, $f(X) = X^n - 1$ es separable si $\operatorname{char} F = 0, p$ tal que $p \nmid n$. Además, sobre F hay n raíces distintas de la unidad. Esto es bien conocido sobre $\mathbb{Q}$: las raíces son, en este caso, $\{e^{2\pi ik/n} \mid 0 \leq k \leq n-1\} \subset \mathbb{C}$.

(8) Si $\operatorname{char} F = p \mid n$, cada raíz de $f(X) = X^n - 1$ es múltiple. En efecto, si $n = p^s \cdot m$, $p \nmid m$, entonces $X^n - 1 = (X^m - 1)^{p^s}$ (recordemos que, en característica p, es $(a \pm b)^{p^s} = a^{p^s} \pm b^{p^s}$).

3.3.6. Sea $f(X) = a_m X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0 \in F[X]$, con $m \geq 1, a_m \neq 0$, donde $\operatorname{char} F = p$. Entonces $f'(X) = \sum j a_j X^{j-1} = 0$ si, y sólo si, para cada j tal que $a_j \neq 0$, se verifica $p \mid j$. De forma equivalente, podemos escribir $f(X)$ en la forma $f(X) = b_r(X^p)^r + b_{r-1}(X^p)^{r-1} + \cdots + b_1(X^p) + b_0$, con $b_r = a_m$. Esto es $f(X) = g(X^p)$. De forma inductiva, podemos escribir $f(X) = h(X^{p^k})$ con $h'(X) \neq 0$.
En el caso $f(X)$ irreducible, el polinomio $h(X) \in F[X]$ es irreducible y separable. En este caso, denotamos $h(X) = f_{\text{sep}}(X)$. El grado de $f_{\text{sep}}(X)$ se denomina el grado separable del irreducible $f(X)$, denotado $\deg_s f(X)$. El entero p^k se denomina el grado inseparable del irreducible $f(X)$, denotado $\deg_i f(X)$. Obviamente $\deg f = (\deg_s f) \cdot (\deg_i f)$. Además, un irreducible $f(X)$ es separable si, y sólo si, $\deg_i f(X) = 1$ si, y sólo si, $\deg f(X) = \deg_s f(X)$.

3.3.7. *Endomorfismo de Frobenius.*
Sea F un cuerpo de característica p. Para cada $a, b \in (a \pm b)^{p^s} = a^{p^s} \pm b^{p^s}$; $(ab)^{p^s} = a^{p^s} b^{p^s}$. Esto es, la aplicación $F \to F$, $a \mapsto a^p$ es un endomorfismo de F.

Corolario 3.3.8. *Sea $\mathbb{F}$ un cuerpo finito. La aplicación $\mathbb{F} \to \mathbb{F}$, $a \mapsto a^p$ es un automorfismo de $\mathbb{F}$.*

Proposición 3.3.9. *Cada polinomio irreducible sobre un cuerpo finito es separable.*

Demostración. Supongamos $p^k = \deg_i f > 1$. Esto es $f(X) = a_m(X^{p^k})^m + \cdots + a_1(X^{p^k}) + a_0 = b_m^{p^k}(X^{p^k})^m + \cdots + b_1^{p^k}(X^{p^k}) + b_0^{p^k} = (b_m X^m + \cdots + b_1 X + b_0)^{p^k}$, en contra de la irreducibilidad de f. □

El punto clave en la prueba es $\mathbb{F} = \mathbb{F}^p$. Esto sugiere

Definición 3.3.10. Un cuerpo F se dice perfecto si F es de característica cero o F es de característica p y $F = F^p$.

Observación 3.3.11. Todo cuerpo finito es perfecto.

Proposición 3.3.12. *Cada polinomio irreducible sobre un cuerpo perfecto es separable.*

Corolario 3.3.13. *Toda extensión algebraica de un cuerpo perfecto es separable.*

Proposición 3.3.14. *Un cuerpo F es perfecto si, y sólo si, toda extensión algebraica de F es separable.*

Demostración. Sólo queda por demostrar que si char$F = p$ y toda extensión algebraica de F es separable, entonces $F = F^p$. En efecto, sea $a \in F$. consideramos $k = F(\alpha)$, con α raíz de $X^p - a$. El polinomio mínimo $m_{\alpha,F}(X) \mid X^p - a = (X - \alpha)^p$. Por hipótesis, $F(\alpha)/F$ es separable, por tanto, $m_{\alpha,F}$, que no tiene raíces múltiples, ha de ser $m_{\alpha,F} = (X - \alpha)$. Así $\alpha \in F$. Esto es $a \in F^p$. □

Proposición 3.3.15. *Sea K/F extensión finita. Si* $\operatorname{char} F = 0$ *ó* $\operatorname{char} F = p \nmid n$, *entonces K/F es separable.*

Demostración. Sea $\operatorname{char} F = pn$. Supongamos que para algún $\alpha \in K$ el polinomio mínimo $m_{\alpha,F}(X) = h(X^p)$. Entonces $p \mid \deg m_{\alpha,F} \mid [K : F]$. □

3.3.16. Sean E/F una extensión algebraica y $\sigma : F \to L$ una inmersión en un cuerpo algebraicamente cerrado L. Según el Teorema 3.2.17, el conjunto S_σ formado por las extensiones de σ a E es no vacío. Estamos interesados en el cardinal de S_σ. Una tal extensión aplica E en un subcuerpo de L algebraico sobre σF. Podemos, por tanto, suponer que L es un cierre algebraico de σF. Sean L' algebraicamente cerrado y $\tau : F \to L'$ una inmersión. Consideramos el conjunto S_τ de extensiones de τ a una inmersión de E en L'. Suponemos, también, que L' es un cierre algebraico de τF. Según el Teorema 3.2.16, existe un isomorfismo $\lambda : L \to L'$ que extiende al isomorfismo $\tau\sigma^{-1} : \sigma F \to \tau F$. Si $\sigma^* \in S_\sigma$ es una extensión de σ, entonces $\lambda\sigma^*$ es una extensión de τ. Por tanto, λ induce una aplicación $S_\sigma \to S_\tau$. Es claro que λ^{-1} induce una aplicación $S_\tau \to S_\sigma$ y que una es inversa de la otra. Esto es S_σ y S_τ están en biyección. En particular, el cardinal de ambos conjuntos coincide. Por tanto, este cardinal sólo depende de la extensión E/F, y lo denotaremos $[E : F]_s$. Diremos que es el *grado separable* de E sobre F.
En el caso $E = F(\alpha)$, con α algebraico sobre F, según la Proposición 3.3.2, el grado separable $[E : F]_s$ coincide con el número de raíces distintas de $m_{\alpha,F}(X)$. En consecuencia, $[F(\alpha) : F]_s \leq [F(\alpha) : F]$. Por otra parte, este número de raíces distintas de $m_{\alpha,F}(X)$ coincide

con el grado separable de $m_{\alpha,F}(X)$. Por tanto $[F(\alpha) : F]_s = \deg_s m_{\alpha,F}(X) \mid \deg m_{\alpha,F}(X) = [F(\alpha) : F]$ y el cociente $[F(\alpha) : F]/[F(\alpha) : F]_s$, que llamaremos grado inseparable de la extensión $[F(\alpha) : F]_i$ coincide con el grado inseparable $\deg_i m_{\alpha,F}(X)$

En el caso general,

Teorema 3.3.17. *Sean $E/K/F$ algebraicas. Entonces $[E : F]_s = [E : K]_s[K : F]_s$. Además, si E/F es finita, entonces $[E : F]_s$ es finito y $[E : F]_s \mid [E : F]$ y, el cociente $[E : F]/[E : F]_s$, que denominaremos grado inseparable $[E : F]_i$, verifica $[E : F]_i = [E : K]_i[K : F]_i$.*

Demostración. Sea $\sigma : F \to L$ una inmersión de F en un cuerpo algebraicamente cerrado L. Sea $\{\sigma_i\}_{i\in I}$ la familia de las distintas extensiones de σ a K y, para cada $i \in I$, sea $\{\tau_{ij}\}$ la familia de las distintas extensiones de σ_i a E. Como hemos visto cada σ_i tiene precisamente $[E : F]_s$ extensiones a E. El conjunto de extensiones $\{\tau_{ij}\}$ contiene precisamente $[E : K]_s[K : F]_s$ elementos. Cada inmersión de E en L sobre σ ha de ser una de las τ_{ij} y, por tanto, obtenemos la fórmula $[E : F]_s = [E : K]_s[K : F]_s$.
Para la segunda parte, supongamos E/F finita. Entonces podemos obtener E en una torre de extensiones $F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \cdots \subset F(\alpha_1, \ldots, \alpha_n) = E$. Denotemos, inductivamente, $F_0 = F, F_{i+1} = F_i(\alpha_{i+1}), i = 0, \ldots, n-1$. Según hemos visto en 3.3.16, para $F_{i+1} = F_i(\alpha_{i+1})/F_i$ se verifica $[F_{i+1} : F_i] = [F_{i+1} : F_i]_s[F_{i+1} : F_i]_i$. Así $[E : F] = \prod_{i=0}^{n-1}[F_{i+1} : F_i]_s \prod_{i=0}^{n-1}[F_{i+1} : F_i]_i$.
Por otra parte, de la fórmula $[E : F]_s = [E : K]_s[K : F]_s$, se deduce que $[E : F]_s = \prod_{i=0}^{n-1}[F_{i+1} : F_i]_s$. Por tanto $[E : F] = [E : F]_s \prod_{i=0}^{n-1}[F_{i+1} : F_i]_i$.
Finalmente, es claro que de $[E : F] = [E : K][K : F], [E : F]_s = [E : K]_s[K : F]_s$ y $[E : F] = [E : F]_s[E : F]_i$, se deduce $[E : F]_i = [E : K]_i[K : F]_i$. □

Corolario 3.3.18. *Sean $E/K/F$ con E/F finita. Entonces $[E : F]_s = [E : F]$ si, y sólo si, $[E : K]_s = [E : K]$ y $[K : F]_s = [K : F]$*

Teorema 3.3.19. *Sea $E = F(\alpha_1, \ldots, \alpha_n)/F$ una extensión finita. Son equivalentes.*

(1) E/F es separable, i.e., cada $\alpha \in E$ es separable sobre F.

(2) Cada $\alpha_1, \ldots, \alpha_n$ es separable sobre F.

(3) $[E : F]_s = [E : F]$

Demostración. (2) $\Rightarrow$ (3) Se deduce de Corolario 3.3.18, aplicado a la torre $F \subset F(\alpha_1) \subset \cdots \subset F(\alpha_1, \ldots, \alpha_n)$.
(3) $\Rightarrow$ (1) Sea $\alpha \in E$. De Corolario 3.3.18, aplicado a la torre $F \subset F(\alpha) \subset E$ se deduce que $[F(\alpha) : F]_s = [F(\alpha) : F]$. Esto significa que α es separable sobre F. □

Como consecuencia inmediata obtenemos:

Teorema 3.3.20. *Sean F un cuerpo y $f(X) \in F[X]$ un polinomio de grado $\deg f \geq 1$ separable y E un cuerpo de descomposición de f sobre F. Entonces E/F es separable.*

Observación 3.3.21. *Sean $K = F(\alpha_1, \ldots, \alpha_r)/F$ una extensión finita y $\sigma : F \to L$ una inmersión de F en un cuerpo algebraicamente cerrado L. Entonces*

(1) $|\{\tau : K \to L \mid \tau_{|F} = \sigma\}| \leq [K : F]$.

(2) La desigualdad anterior es una igualdad si, y sólo si, cada uno de los α_i es separable sobre F.

3.4. Extensiones normales

Definición 3.4.1. Sean K/F y L/F extensiones de un cuerpo F. Denominaremos F–homomorfismo o F–inmersión de K en L a todo homomorfismo $K \to L$ que es la identidad en F.

Lema 3.4.2. *Sean K/F una extensión algebraica y $\sigma : K \to K$ una F–inmersión. Entonces σ es un automorfismo de K.*

Demostración. Hemos de probar que σ es sobreyectivo. Sean $\alpha \in K$ y $m_{\alpha,F}(X)$ su polinomio mínimo sobre F. Sea K' el subcuerpo de K generado sobre F por aquellas raíces de $m_{\alpha,F}(X)$ que están en K. Entonces K'/F es una extensión finita. Además σ envía raíces de $m_{\alpha,F}(X)$ en K a raíces de $m_{\alpha,F}(X)$ en K. Por tanto, $\sigma(K') \subset K'$. Así, podemos ver $\sigma : K' \to K'$ como endomorfismo del F–espacio vectorial de dimensión finita K'. Este endomorfismo es inyectivo y, por tanto, sobreyectivo a causa de la dimensión finita. Ahora bien, $\alpha \in K'$. Por tanto, $\alpha \in \sigma(K)$. □

Definición 3.4.3. Sean F un cuerpo, $\overline{F}$ un cierre algebraico de F y $\alpha \in \overline{F}$. Denominaremos F–conjugados de α a las raíces en $\overline{F}$ de su polinomio mínimo $m_{\alpha,F}(X)$ sobre F.

Teorema 3.4.4. *Sean F un cuerpo, $f(X) \in F[X]$ de grado ≥ 1 y E un cuerpo de descomposición de f en un cierre algebraico $\overline{F}$ de F. Entonces cada F–inmersión de E en $\overline{F}$ es un F–automorfismo de E.*

Demostración. Sea $\sigma : E \to \overline{F}$ una F–inmersión. El cuerpo $E = F(\alpha_1, \ldots, \alpha_n) \subset \overline{F}$ con $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$, $c \in F-\{0\}$. Entonces $f(X) = f^\sigma(X) = c(X-\sigma\alpha_1)\cdots(X-\sigma\alpha_n)$. La factorización única en $\overline{F}[X]$ implica que $(\sigma\alpha_1, \ldots, \sigma\alpha_n)$ es una permutación de $(\alpha_1, \ldots, \alpha_n)$. Por tanto $\sigma(E) = F(\sigma\alpha_1, \ldots, \sigma\alpha_n) = F(\alpha_1, \ldots, \alpha_n) = E$. □

Definición 3.4.5. Sean F un cuerpo y $\{f_i\}_{i\in I}$ una familia de polinomios de $F[X]$. El cuerpo de descomposición E de la familia en un cierre algebraico $\overline{F}$ de F, es el menor subcuerpo de $\overline{F}$ que contiene un cuerpo de descomposición en $\overline{F}$ de cada polinomio de la familia. Es decir, es el subcuerpo de $\overline{F}$ generado sobre F por todas las raíces de los polinomios de la familia (que están todas en $\overline{F}$).

Teorema 3.4.6. *Sea $E \subset \overline{F}$ el cuerpo de descomposición de una familia $\{f_i(X)\}_{i\in I} \subset F[X]$. Cada F–inmersión $\sigma : E \to \overline{F}$ es un F–automorfismo de E*

Demostración. Basta probar, según Lema 3.4.2, que $\sigma(E) \subset E$.
Sea $\alpha \in E$. Puesto que E está generado sobre F por las raíces de los todos los polinomios de la familia, existe una cantidad finita de estos polinomios, tales que α está en el subcuerpo de E generado sobre F por las raíces de esta cantidad finita de polinomios. Por tanto α está en el cuerpo $K \subset E$ de descomposición sobre F del polinomio producto de esta cantidad finita de polinomios. Aplicando Teorema 3.4.4 a $\sigma : K \to \overline{F}$ se tiene $\sigma(K) \subset K$. Por tanto $\sigma(\alpha) \in E$. □

Teorema–Definición 3.4.7. *Sea K/F una extensión algebraica (extensión finita) contenida en un cierre algebraico $\overline{F}$. Las siguientes condiciones son equivalentes y definen el concepto de extensión algebraica (extensión finita) normal.*

NOR1 *Cada F–inmersión $\sigma : K \to \overline{F}$ induce un automorfismo σ de K, i.e., $\sigma(K) = K$.*

NOR1' *Cada F–inmersión $\sigma : K \to \overline{F}$ verifica $\sigma(K) \subset K$.*

NOR2 *K es el cuerpo de descomposición en $\overline{F}$ de una familia (familia finita o, equivalente, un polinomio) sobre F.*

NOR3 *Cada polinomio irreducible de $F[X]$ que tiene una raíz en K factoriza en producto de factores lineales en $K[X]$, i.e., K contiene el cuerpo de descomposición en $\overline{F}$ de cada polinomio irreducible de $F[X]$ que tiene una raíz en K.*

NOR4 *Para cada $\alpha \in K$, todos los F–conjugados de α en $\overline{F}$ están en K.*

NOR4' *Si $K = F(\{\alpha_i\}_{i\in I})$ $(= F(\alpha_1, \ldots, \alpha_n))$, entonces los conjugados de cada generador α_i están en K.*

Demostración. **NOR1** $\Rightarrow$ **NOR1'** es trivial.

NOR1' $\Rightarrow$ **NOR1** es el Lema 3.4.2.

NOR4 no es más que una forma de reescribir **NOR3**.

NOR1' $\Rightarrow$ **NOR4**. Sean $\alpha \in K$ y $\beta \in \overline{F}$ un F–conjugado de α, i.e., una raíz de $m_{\alpha,F}(X)$ en $\overline{F}$ (cuerpo donde $m_{\alpha,F}(X)$ tiene todas sus raíces). Existe un isomorfismo $F(\alpha) \to F(\beta)$ que lleva α a β. Extendemos este isomorfismo a una inmersión $\sigma : K \to \overline{F}$. Por la hipótesis **NOR1'**, esta extensión verifica $\sigma(K) \subset K$. Por tanto, $\beta = \sigma(\alpha) \in K$.

NOR4 $\Rightarrow$ **NOR4'** es trivial.

NOR4' $\Rightarrow$ **NOR2**. La condición **NOR4'** significa que para cada generador α_i, el polinomio mínimo $m_{\alpha_i,F}(X)$ tiene todas sus raíces en K, i.e, el cuerpo de descomposición de $m_{\alpha_i,F}(X)$ en $\overline{F}$ está contenido en K. Así, K es el cuerpo de descomposición de la familia $\{m_{\alpha_i,F}\}_{\alpha_i\in I}$. En el caso finito, $K = F(\alpha_1, \ldots, \alpha_n)$ basta tomar como polinomio, el producto $f(X)$ de los polinomios $m_{\alpha_i,F}(X), i = 1, \ldots, n$ y K es el cuerpo de descomposición de f.

NOR2 $\Rightarrow$ **NOR1'**. Es el Teorema 3.4.6. □

Ejemplos 3.4.8. (1) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal. El elemento $\sqrt[3]{2}\omega$ es conjugado de $\sqrt[3]{2}$ y $\sqrt[3]{2}\omega \notin \mathbb{Q}(\sqrt[3]{2})$.

(2) $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ es normal. Es el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $X^3 - 2$.

(3) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt{2 + \sqrt{5}})$, muestra que normal no es propiedad transitiva. ($\sqrt{2 - \sqrt{5}} \notin \mathbb{Q}(\sqrt{2 + \sqrt{5}})$ y $\sqrt{2 - \sqrt{5}}$ es conjugado de $\sqrt{2 + \sqrt{5}}$ sobre $\mathbb{Q}$).

3.5. Una aproximación al teorema del elemento primitivo

Definición 3.5.1. Una extensión finita K/F se dice simple si existe un elemento $\alpha \in K$ tal que $K = F(\alpha)$. Diremos que α es un elemento primitivo de la extensión.

Teorema 3.5.2. *(1) Una extensión finita es simple si, y sólo si, tiene una cantidad finita de cuerpos intermedios.*

(2) Toda extensión finita separable es simple

Demostración. Si $F = \mathbb{F}_q$ es un cuerpo finito, entonces el grupo multiplicativo K^* es cíclico. Un generador del grupo es también un elemento primitivo de la extensión. Podemos pues suponer F infinito. Supongamos que sólo hay una cantidad finita de cuerpos intermedios. Sean $\alpha, \beta \in K$. Los subcuerpos $F(\alpha + c\beta)$ obtenidos variando $c \in F$ son en cantidad finita. Por tanto existen $c_1 \neq c_2 \in F$ tales que

$$F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$$

Denotemos $K_1 = F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$. Entonces $(c_1 - c_2)\beta \in K_1$ y, puesto que $0 \neq c_1 - c_2 \in F \subset K_1$, vemos que $\beta \in K_1$. Por tanto, también $\alpha \in K_1$ y así $K_1 = F(\alpha, \beta)$. Es decir, un cuerpo intermedio generado por dos elementos es una extensión simple. Puesto que $K = F(\alpha_1, \ldots, \alpha_n)$, por inducción obtenemos $K = F(\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n)$, para ciertos $c_2, \ldots, c_n \in F$.
Recíprocamente si $K = F(\alpha)$, a cada cuerpo intermedio $F \subset E \subset K$ le asociamos el polinomio $m_{\alpha,E}(X)$ que es un divisor del polinomio $m_{\alpha,F}(X)$. Es claro, que los posibles polinomios $m_{\alpha,E}(X)$ son, pues, en cantidad finita. Basta ahora probar que el polinomio $m_{\alpha,E}(X)$ determina el cuerpo intermedio E. En efecto, si E_0 es el cuerpo intermedio generado sobre F por los coeficientes de $m_{\alpha,E}(X)$, entonces $m_{\alpha,E}(X) \in E_0[X]$ y es irreducible sobre E_0 puesto que lo es sobre E (atención: $m_{\alpha,E}(X) | m_{\alpha,F}(X)$ ocurre en $E[X]$; pero $m_{\alpha,E}(X) | m_{\alpha,E_0}(X)$ ocurre, no sólo en $E[X]$, sino también en $E_0[X]$). Por tanto, $m_{\alpha,E_0}(X) = m_{\alpha,E}(X)$ y así

$$[E_0(\alpha) : E_0] = \deg m_{\alpha,E_0}(X) = \deg m_{\alpha,E}(X) = [E(\alpha) : E].$$

De donde obtenemos

$$[E : E_0] = [E(\alpha) : E_0(\alpha)].$$

De esta última igualdad, y puesto que $F \subset E_0 \subset E \subset K = F(\alpha)$ vemos que $E(\alpha) = K = E_0(\alpha)$ y, por tanto, $[E : E_0] = 1$. Esto es $E_0 = E$.

Para la segunda parte, basta demostrar que una extensión separable $K = F(\alpha, \beta)$, con F infinito, es primitiva.
En un cierre algebraico $\bar{K} = \bar{F}$ los polinomios mínimos factorizan

$$m_{\alpha,F}(X) = (X - \alpha_1) \cdots (X - \alpha_n)$$
$$m_{\beta,F}(X) = (X - \beta_1) \cdots (X - \beta_m),$$

donde $\alpha = \alpha_1, \beta = \beta_1$ y los $\alpha_i \neq \alpha_j$ y $\beta_i \neq \beta_j$ si $i \neq j$ puesto que, por hipótesis, la extensión K/F es separable.
Consideramos el conjunto

$$Q = \{ \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} \mid 1 \leq i \leq n \, , \, 1 < j \leq n\}.$$

Puesto que F es infinito existe $c \in F$ tal que $c \notin Q$. Afirmamos que $K = F(\alpha + c\beta)$. En efecto, denotemos $\gamma = \alpha + c\beta$ y $h(X) = m_{\alpha,F}(\gamma - cX) \in F(\gamma)[X] \subset \bar{F}[X]$. Entonces $h(\beta) = 0$. Por tanto, $X - \beta$ divide a $h(X)$ en $\bar{F}[X]$. Por otra parte, si $X - \beta_j$ divide a $h(X)$ para algún $j \neq 1$, entonces $m_{\alpha,F}(\gamma - c\beta_j) = 0$. Esto significa que $\gamma - c\beta_j = \alpha_i$ para algún i y, en este caso, tendríamos $c \in Q$, en contra de la elección de c. Por tanto, en $\bar{F}[X]$ los polinomios $m_{\beta,F}(X)$ y $h(X)$ tienen $X - \beta$ como máximo común divisor. Así, su máximo común divisor en $F(\gamma)$ será $X - \beta$ o bien 1. Si ocurre la segunda opción, se tendrá $1 = a(X)m_{\beta,F}(X) + b(X)h(X)$ en $F(\gamma)[X]$. Sustituyendo $X = \beta$ se obtiene una contradicción. En consecuencia, el máximo común divisor en $F(\gamma)[X]$ es $X - \beta$. Esto implica $\beta \in F(\gamma)$, y también $\alpha = \gamma - c\beta \in F(\gamma)$. Esto es $K \subset F(\gamma)$. □

Ejemplo 3.5.3. Sea $\overline{\mathbb{F}_p}(x, y)$ el cuerpo de funciones racionales en dos variables sobre el cierre algebraico $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$. Entonces $K = \overline{\mathbb{F}_p}(x, y)$ es una extensión finita *no simple* de $F = \overline{\mathbb{F}_p}(x^p, y^p)$. En efecto, es sencillo ver que $[K : F] = p^2$ y que los todos los subcuerpos $F(x+cy)$, $c \in \overline{\mathbb{F}_p}$ son de grado p sobre F (observemos que $(x+cy)^p = x^p + c^p y^p \in F$). Si dos de estos cuerpos coincidieran, entonces, razonando como en el Teorema 3.5.2, tendríamos $K = F(x + cy)$. Esto no es posible a causa de los grados. Por tanto hay infinitos cuerpos intermedios de la forma $F(x + cy)$.

Definición 3.5.4. El grupo de automorfismos de la extensión K/F es el subgrupo $\mathrm{Aut}(K/F)$ del grupo de automorfismos de K formado por los automorfismos de K que son la identidad en F.

Ejemplo 3.5.5. Sea $K = F(\sqrt{D})/F$ una extensión cuadrática, en característica distinta de 2. El polinomio mínimo de $\alpha = \sqrt{D}$ sobre F es $X^2 - D \in F[X]$. Por tanto, los F–conjugados de α son $\pm\alpha$.
Sea $\sigma \in \mathrm{Aut}(K/F)$. Entonces $\sigma(a + b\alpha) = a + b\sigma(\alpha)$, para cada $a + b\alpha \in K$, donde $a, b \in F$. Esto muestra que α está determinado por $\sigma(\alpha)$, que ha de ser uno de sus F–conjugados. Por otra parte, $K = F(-\alpha)$ y, por tanto, según Teorema 3.1.17 existe un $\sigma \in \mathrm{Aut}(K/F)$ tal que $\sigma(\alpha) = -\alpha$. Esto muestra que

$$\mathrm{Aut}(K/F) = \{1, \sigma\},$$

donde

$$\sigma(a + b\alpha) = a - b\alpha.$$

En particular, esto se aplica a $\mathrm{Aut}(\mathbb{C} = \mathbb{R}(i)/\mathbb{R})$, donde $i = \sqrt{-1}$.

Corolario 3.5.6. *Sea K/F una extensión finita, separable y normal. Entonces* $|\mathrm{Aut}(K/F)| = [K : F]$.

Demostración. Podemos escribir $K = F(\alpha)$. Según la hipótesis $m_{\alpha,F}(X) = (X-\alpha_1)\cdots(X-\alpha_n)$, donde $\alpha = \alpha_1, \cdots, \alpha_n \in K$ son $n = [K : F]$ elementos distintos. Cada automorfismo de K/F está determinado por la imagen de α que debe ser uno de los α_i. Además, puesto que $K = F(\alpha_i)$, para cada α_i, se deduce de Teorema 3.1.17 que existe un F–automorfismo $\sigma_i : K \to K$ tal que $\sigma(\alpha) = \alpha_i$. Esto muestra que hay exactamente n automorfismos de K/F. □

Observación 3.5.7. La parte (2) del Teorema 3.5.2 puede también ser obtenida como consecuencia de la parte (1) y del Teorema fundamental, que demostraremos más adelante sin usar, por supuesto, la existencia de un elemento primitivo. El argumento es sencillo: una extensión finita y separable K/F está contenida en una extensión de Galois E/F, minimal en un cierre algebraico. Los cuerpos intermedios de K/F son también cuerpos intermedios de E/F que corresponden, según el Teorema fundamental, a subgrupos del grupo finito de Galois de E/F. En consecuencia, los cuerpos intermedios de la extensión K/F son en cantidad finita.

3.6. Cuerpos finitos

Sea $\mathbb{F}$ un cuerpo finito con q elementos.

3.6.1. Sabemos que el núcleo del único homomorfismo de anillos unitarios $\mathbb{Z} \to \mathbb{F}$ tiene núcleo el ideal $p\mathbb{Z}$, donde $p = \text{char}(\mathbb{F})$ es el número primo que denominamos la característica de $\mathbb{F}$. Esto significa que $\mathbb{F}$ es una extensión del cuerpo $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ de p elementos. En esta situación el grado $[\mathbb{F} : \mathbb{F}_p] = n$ es finito y obtenemos $q = p^n$.

3.6.2. El grupo multiplicativo $\mathbb{F}^*$ tiene orden $q-1$. Por tanto, para cada $\alpha \in \mathbb{F}^*$ verifica la ecuación $X^{q-1} - 1 = 0$. En consecuencia, todo elemento de $\mathbb{F}$ satisface la ecuación $X^q - X = 0$. Esto significa que el polinomio $X^q - X$ tiene q raíces distintas en $\mathbb{F}$. Esto es, todos los elementos de $\mathbb{F}$ son raíces del polinomio $X^q - X$. Por tanto

$$X^q - X = \prod_{\alpha \in \mathbb{F}} (X - \alpha).$$

Esto significa que $\mathbb{F}$ es un cuerpo de descomposición para el polinomio $X^q - X$ sobre $\mathbb{F}_p$. Pero un tal cuerpo de descomposición está determinado, salvo isomorfismo, como el cuerpo de descomposición de $X^{p^n} - X$ sobre $\mathbb{F}_p$.

3.6.3. Recíprocamente, denotemos $\mathbb{F}_{p^n}$ el cuerpo de descomposición del polinomio $X^{p^n} - X$ sobre $\mathbb{F}_p$ en un cierre algebraico $\overline{\mathbb{F}_p}$. Afirmamos que este cuerpo $\mathbb{F}_{p^n}$ es el conjunto de las p^n raíces distintas de $X^{p^n} - X$ en $\overline{\mathbb{F}_p}$.
En efecto, el polinomio derivado de $X^{p^n} - X$ es -1, que no tiene raíces. Por tanto $X^{p^n} - X$ no tiene raíces múltiples.
Sean α, β raíces. Entonces

$$(\alpha - \beta)^{p^n} - (\alpha - \beta) = \alpha^{p^n} - \beta^{p^n} - (\alpha - \beta) = 0.$$

Por tanto, $\alpha - \beta$ es una raíz.
También

$$(\alpha\beta)^{p^n} - (\alpha\beta) = \alpha^{p^n}\beta^{p^n} - \alpha\beta = 0,$$

y $\alpha\beta$ es una raíz. Observemos que $0, 1$ son raíces. Finalmente, si $\alpha \neq 0$ es una raíz, entonces

$$(\beta^{-1})^{p^n} - \beta^{-1} = (\beta^{p^n})^{-1} - \beta^{-1} = 0.$$

Así que β^{-1} es raíz.

En resumen, hemos demostrado:

Teorema 3.6.4. *Para cada primo p y cada entero $n \geq 1$ existe un cuerpo finito con p^n elementos, denotado $\mathbb{F}_{p^n}$, unívocamente determinado como subcuerpo de un cierre algebraico $\overline{\mathbb{F}_p}$. Es el cuerpo de descomposición del polinomio $X^{p^n} - X$. Los elementos de $\mathbb{F}_{p^n}$ son las raíces de este polinomio. Cada cuerpo finito es isomorfo a exactamente un $\mathbb{F}_{p^n}$.*

Corolario 3.6.5. *Para cada n existen polinomios irreducibles de grado n en* $\mathbb{F}_p[X]$.

Demostración. La extensión $\mathbb{F}_{p^n}/\mathbb{F}_p$ es separable de grado n. Por tanto, por el Teorema del elemento primitivo, existe $\alpha \in \mathbb{F}_{p^n}$ tal que $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$. Entonces, el polinomio mínimo de α sobre $\mathbb{F}_p$ es irreducible de grado n. □

Corolario 3.6.6. *Sean* $\mathbb{F}_q$ *un cuerpo finito y* $n \geq 1$ *un entero. En un cierre algebraico fijado* $\overline{\mathbb{F}_p}$*, existe una única extensión de* $\mathbb{F}_q$ *de grado n. Esta extensión es el cuerpo* $\mathbb{F}_{q^n}$.

Demostración. Sea $q = p^m$, entonces $q^n = p^{mn}$. El cuerpo de descomposición de $X^{q^n} - X$ es $\mathbb{F}_{p^{mn}}$, cuyo grado sobre $\mathbb{F}_p$ es mn. Puesto que $\mathbb{F}_q$ tiene grado m sobre $\mathbb{F}_p$, deducimos que $\mathbb{F}_{q^n}$ tiene grado n sobre $\mathbb{F}_q$. Recíprocamente, cada extensión de grado n de $\mathbb{F}_q$ tiene grado mn sobre $\mathbb{F}_p$ y, por tanto, ha de ser $\mathbb{F}_{p^{mn}}$. □

Teorema 3.6.7. *Todo subgrupo finito del grupo multiplicativo de un cuerpo es cíclico. En particular, el grupo multiplicativo* $\mathbb{F}_{p^n}^*$*, de un cuerpo finito, es cíclico.*

Demostración. Sea G un subgrupo finito del grupo multiplicativo F^* de un cuerpo F. El teorema de clasificación de grupos abelianos finitamente generados asegura que G es de la forma

$$G \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r},$$

donde, $1 < d_1 \mid \cdots \mid d_r$. Así $|G| = d_1 \cdots d_r$. Además todo elemento de G verifica la ecuación $x^{d_r} = 1$. Por tanto, todo elemento de G es raíz del polinomio $X^{d_r} - 1$ en F. Como este polinomio tiene a lo más d_r raíces, deducimos que $\operatorname{ord} G \leq d_r$. Esto es $d_1 \cdots d_r \leq d_r$. Por tanto $r = 1$ y $G = \mathbb{Z}_{d_1}$ es cíclico. □

Teorema 3.6.8. *El grupo de automorfismos del cuerpo finito* $\mathbb{F}_q$*, donde* $q = p^n$*, es cíclico de grado n generado por el automorfismo de Fröbenius* $\mathbb{F}_q \xrightarrow{\varphi} \mathbb{F}_q$*, definido por* $\varphi(\alpha) = \alpha^p$*. Además* $\operatorname{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \operatorname{Aut}(\mathbb{F}_{p^n})$.

Demostración. Puesto que $\mathbb{F}_{p^n}/\mathbb{F}_p$ es finita, normal y separable de grado n, sabemos que $\operatorname{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ es un grupo finito de orden n.
Sean G el grupo generado por φ y d el orden de φ. Se verifica $\varphi^n = 1_G$, puesto que $\varphi^n(\alpha) = \alpha^{p^n} = \alpha$, para todo $\alpha \in \mathbb{F}_q$. por tanto $d \mid n$. Además $\alpha^{p^d} = \alpha$, para todo $\alpha \in \mathbb{F}_q$. Por tanto, todo $\alpha \in \mathbb{F}_q$ es raíz de $X^{p^d} - X$, que tiene a lo más p^d raíces. Deducimos que $d = n$. □

3.6.9. Observemos que todo automorfismo ψ de $\mathbb{F}_q$ fija $\mathbb{F}_p$. Por tanto es un automorfismo de $\mathbb{F}_q$ sobre $\mathbb{F}_p$. Vemos así que el número de tales automorfismos coincide con el grado $[\mathbb{F}_q : \mathbb{F}_p]$. Veremos que esto corresponde con el hecho de que la extensión $\mathbb{F}_q/\mathbb{F}_p$ es normal y separable.

Finalmente, dejaremos como ejercicio la demostración del siguiente

Teorema 3.6.10. *Sean* $m, n \geq 1$ *enteros. Entonces, en un cierre algebraico de* $\mathbb{F}_p$*, el subcuerpo* $\mathbb{F}_{p^n}$ *está contenido en* $\mathbb{F}_{p^m}$ *si, y sólo si, n divide a m. En este caso,* $m = nd$*, entonces* $\mathbb{F}_{p^m}$ *es finita normal y separable sobre* $\mathbb{F}_{p^n}$ *de grado d, y el grupo de automorfismos de* $\mathbb{F}_{p^m}$ *sobre* $\mathbb{F}_{p^n}$ *es cíclico de orden d, generado por* φ^n*, donde* $\mathbb{F}_{p^m} \xrightarrow{\varphi} \mathbb{F}_{p^m}$ *es el automorfismo de Fröbenius.*

3.7. Extensiones ciclotómicas

Tratamos de demostrar que la extensión ciclotómica $\mathbb{Q}(\zeta)/\mathbb{Q}$ generada por una raíz primitiva n–ésima de la unidad ($\zeta = \exp(2\pi ia/n)$, $1 \leq a < n$ & $\operatorname{mcd}(a,n) = 1$), tiene grado

$$\varphi(n) = |\{a \mid 1 \leq a < n \ \ \& \ \ \operatorname{mcd}(a,n) = 1\}| = |(\mathbb{Z}/n\mathbb{Z})^*|.$$

3.7.1. Escribimos $n = p_1^{a_1} \cdots p_s^{a_s}$, donde p_i primos distintos y $a_i \geq 1$. Entonces el isomorfismo de anillos

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{a_s}\mathbb{Z}$$

induce un isomorfismo entre los grupos de unidades

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_s^{a_s}\mathbb{Z})^*.$$

Por tanto,

$$\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_s^{a_s}).$$

Para calcular $\varphi(p^s)$, restamos de $p^s - 1$ el número de múltiplos de p entre 1 y $p^s - 1$, que es $p^{s-1} - 1$. Obtenemos, por tanto,

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

3.7.2. Denotemos por μ_n el grupo de las raíces n–ésimas de la unidad sobre $\mathbb{Q}$. Hemos visto que

$$\mu_n = <\zeta> := \{\zeta^m \mid m \in \mathbb{Z}\} = \{\zeta^r \mid 0 \leq r < n\}.$$

es cíclico generado por una raíz primitiva n-ésima ζ.

Ejercicio 3.7.3. $\mu_d \subset \mu_n \Leftrightarrow d \mid n$.

Definición 3.7.4. El n–ésimo polinomio ciclotómico $\phi_n(X)$ es el polinomio cuyas raíces son las raíces primitivas n–ésimas de la unidad

$$\phi_n(X) = \prod_{\substack{\zeta \in \mu_n \\ \zeta \text{ primitiva}}} (X - \zeta).$$

3.7.5. Podemos obtener recursivamente los polinomios $\phi_n(X)$, a partir de la identidad

$$X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{d \mid n} \prod_{\substack{\zeta \in \mu_d \\ \zeta \text{ primitiva}}} (X - \zeta) = \prod_{d \mid n} \phi_d(X). \tag{3.7.5.1}$$

3.7.6. Comparando grados en la identidad anterior obtenemos la igualdad

$$n = \sum_{d \mid n} \varphi(d).$$

3.7.7. Calculamos recursivamente los polinomios $\phi_n(X)$ a partir de (3.7.5.1). Por ejemplo:

$$\phi_1(X) = X - 1, \qquad \phi_2(X) = X + 1.$$

$$X^3 - 1 = \phi_1(X)\phi_3(X) = (X-1)\phi_3(X) \;\Rightarrow\; \phi_3(X) = X^2 + X + 1.$$

$$X^4 - 1 = \phi_1(X)\phi_2(X)\phi_4(X) = (X-1)(X+1)\phi_4(X) \;\Rightarrow\; \phi_4(X) = X^2 + 1.$$

$$\phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \;\text{ si } p \text{ es primo.}$$

$$\phi_6(X) = X^2 - X + 1, \;\; \phi_8(X) = X^4 + 1,$$
$$\phi_9(X) = X^6 + X^3 + 1,$$
$$\phi_{10}(X) = X^4 - X^3 + X^2 - X + 1,$$
$$\phi_{12}(X) = X^4 - X^2 + 1.$$

3.7.8.

$$\phi_{2n}(X) = \phi_n(-X).$$

3.7.9.

$$\phi_{2^n}(X) = X^{2^{n-1}} + 1.$$

Para todos los valores anteriores $\phi_n(X)$ es un polinomio mónico con coeficientes enteros. Este siempre es el caso.

Lema 3.7.10. *El polinomio $\phi_n(X) \in \mathbb{Z}[X]$ y es mónico de grado $\varphi(n)$.*

Demostración. Es claro que el polinomio es mónico y tiene grado $\varphi(n)$. Veamos que tiene sus coeficientes en $\mathbb{Z}$.
Inducción sobre n.
Hemos visto que es cierto para $n = 1$. Supongamos $n > 1$ y $\varphi_d(X) \in \mathbb{Z}[X]$ para $1 \le d < n$. Entonces

$$X^n - 1 = \Big(\prod_{d|n,\, d<n} \phi_d(X)\Big)\, \phi_n(X) = f(X)\phi_n(X),$$

donde $f(X) \in \mathbb{Z}[X]$ y es mónico. La división anterior ocurre en $\mathbb{Q}(\zeta)[X]$. La unicidad de la división muestra que $\phi_n(X) \in \mathbb{Q}[X]$. Ahora tomando contenidos vemos que $\phi_n(X)$ tiene contenido 1 y, por tanto, $\phi_n(X) \in \mathbb{Z}[X]$. □

Conviene observar que, aunque los coeficientes de los polinomios ciclotómicos calculados antes son ± 1, es conocido que hay polinomios ciclotómicos con coeficientes arbitrariamente grandes.

Teorema 3.7.11. *El polinomio ciclotómico $\phi_n(X)$ es irreducible en $\mathbb{Z}[X]$.*

Demostración. Supongamos que $\phi_n(X) = f(X)g(X)$ en $\mathbb{Z}[X]$ donde podemos suponer $f(X), g(X)$ mónicos y $f(X)$ factor irreducible de $\phi_n(X)$. Elegimos una raíz primitiva n–ésima ζ que sea raíz de $f(X)$, de forma que el polinomio mínimo de ζ es $f(X)$. Sea p un primo cualquiera que no sea divisor de n. Entonces ζ^p es raíz primitiva n–ésima y, por tanto, es raíz de $f(X)$ o de $g(X)$. Supongamos que $g(\zeta^p) = 0$. Entonces ζ es raíz de

$g(X^p)$ y, por tanto, $f(X)$ divide a $g(X^p)$ en $\mathbb{Q}[X]$ y, en consecuencia en $\mathbb{Z}[X]$; pongamos $g(X^p) = f(X)h(X)$ con $h(X) \in \mathbb{Z}[X]$. Reduciendo módulo p, obtenemos $\bar{g}(X^p) = \bar{f}(X)\bar{h}(X)$ en $\mathbb{F}_p(X)$. Ahora bien $\bar{g}(X^p) = (\bar{g}(X))^p$, y así $(\bar{g}(X))^p = \bar{f}(X)\bar{h}(X)$ en $\mathbb{F}_p[X]$. Esta igualdad implica que $\bar{f}(X)$ y $\bar{g}(X)$ tienen un factor irreducible común en $\mathbb{F}_p[X]$. Por tanto reduciendo módulo p la igualdad $\phi_n(X) = f(X)g(X)$ vemos que $\bar{\phi}_n(X) \in \mathbb{F}_p[X]$ tiene una raíz múltiple. En consecuencia, también $X^n - \bar{1} \in \mathbb{F}_p[X]$ tiene una raíz múltiple; pero esto sólo es posible si p divide a n. Por tanto ζ^p es una raíz de $f(X)$. Puesto que esto se aplica a toda raíz primitiva n–ésima ζ que sea raíz de $f(X)$, se deduce que toda raíz primitiva n–ésima es raíz de $f(X)$ (si ζ es una raíz primitiva que sea raíz de $f(X)$ y $a = p_1p_2\cdots p_s$ es primo con n entonces ζ^{p_1} es raíz de $f(X)$, y, por tanto $(\zeta^{p_1})^{p_2}$ es raíz de $f(X)$, . . ., y, por tanto ζ^a es raíz de $f(X)$). Pero esto significa que $\phi_n(X)$ divide a $f(X)$ y, en consecuencia $\phi_n(X) = f(X)$. □

Corolario 3.7.12. *El polinomio mínimo sobre* $\mathbb{Q}$ *de toda raíz primitiva n–ésima de la unidad* ζ *es el polinomio ciclotómico*

$$\phi_n(X) = \prod_{\substack{\zeta \in \mu_n \\ \zeta \text{ primitiva}}} (X - \zeta),$$

y

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n).$$

Ejemplo 3.7.13. Pongamos $\zeta_8 = \exp(2\pi i/8)$. Entonces $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = \varphi(8) = 4$. El cuerpo $\mathbb{Q}(\zeta_8)$ contiene las raíces cuartas, esto es $\mathbb{Q}(i) \subset \mathbb{Q}(\zeta_8)$. Además $\zeta_8 + \zeta_8^7 = \sqrt{2}$. Por tanto $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$.

3.7.14. Veremos en la Proposición 3.10.40 que $\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$, si ζ es raíz primitiva n–ésima de la unidad.

3.8. Teoría de Galois I

Hemos demostrado la existencia de una menor extensión finita de un cuerpo F que contiene todas las raíces de un polinomio dado $f(X) \in F[X]$, el cuerpo de descomposición de f sobre F. Estudiar las raíces de f equivale a estudiar las propiedades algebraicas de este cuerpo de descomposición. La idea principal de la teoría de Galois (Evariste Galois 1811–1832) consiste en considerar la relación del grupo formado por aquellas permutaciones de las raíces que respetan las relaciones algebraicas entre ellas, con la estructura algebraica del cuerpo de descomposición. La conexión aparecerá enunciada en el Teorema Fundamental.

3.8.1. Preliminares. Ejemplos

Observación 3.8.1. (1) Recordemos que si K/F es una extensión algebraica contenida en un cierre algebraico $\overline{F}$, según Lema 3.4.2, un F–automorfismo de K, i.e., un automorfismo $\sigma : K \to K$ que es la identidad en F equivale a una F–inmersión $\sigma : K \to \overline{F}$ tal que $\sigma(K) \subset K$.

(2) Sea L un cuerpo. Todo homomorfismo $L \to L$ induce la identidad en el subcuerpo primo de L.

(3) El conjunto $\mathrm{Aut}(K)$ formado por los automorfismos de K es un grupo con la composición. Sea K/F una extensión. El subconjunto formado por los F–automorfismos de K es un subgrupo $\mathrm{Aut}(K/F)$ de $\mathrm{Aut}(K)$.

(4) Diremos que un automorfismo $\sigma : K \to K$ fija un elemento $\alpha \in K$ si $\sigma(\alpha) = \alpha$. Diremos que un automorfismo σ fija un subconjunto $S \subset K$ si fija cada elemento de S.

(5) Sea $F \subset E \subset K$, una extensión K/F y un cuerpo intermedio E. Entonces

$$\mathrm{Aut}(K/E) \leq \mathrm{Aut}(K/F).$$

Es el subgrupo formado por los F–automorfismos de K que fijan $E \subset K$.

(6) Sean K/F una extensión y $H \leq \mathrm{Aut}(K/F)$ un subgrupo. Entonces

$$\mathrm{Fix}(H) = \{\alpha \in K \mid \sigma(\alpha) = \alpha, \text{ para todo } \sigma \in H\}$$

es un cuerpo intermedio $F \subset \mathrm{Fix}(H) \subset K$.

(7) Sean $F \subset E_2 \subset E_1 \subset K$. Entonces $\mathrm{Aut}(K/E_1) \leq \mathrm{Aut}(K/E_2) \leq \mathrm{Aut}(K/F)$.

(8) Sean $H_2 \leq H_1 \leq \mathrm{Aut}(K/F)$. Entonces $F \subset \mathrm{Fix}(H_1) \subset \mathrm{Fix}(H_2) \subset K$.

(9) Sean K/F una extensión algebraica y $\alpha \in K$. Entonces para todo $\sigma \in \mathrm{Aut}(K/F)$, el elemento $\sigma(\alpha)$ es una raíz de $m_{\alpha,F}(X)$, i.e., los elementos de $\mathrm{Aut}(K/F)$ permutan las raíces de los polinomios irreducibles de $F[X]$.

Ejemplos 3.8.2. (1) $K = \mathbb{Q}(\sqrt{2})/F = \mathbb{Q}$. Un automorfismo $\tau \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ está determinado por $\tau(\sqrt{2})$ que ha de ser un $\mathbb{Q}$–conjugado de $\sqrt{2}$. Esto es $\tau(\sqrt{2}) = \pm\sqrt{2}$. Por tanto, $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$, donde $\sigma(\sqrt{2}) = -\sqrt{2}$.

(2) $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$. Puesto que los $\mathbb{Q}$–conjugados de $\sqrt[3]{2}$ son $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ y $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2 \notin \mathbb{Q}(\sqrt[3]{2})$.

3.8.3. Sea $K = F(\{\alpha_i\}_{i\in I})$ extensión algebraica de F contenida en un cierre algebraico $\overline{F}$. Cada automorfismo $\sigma \in \mathrm{Aut}(K/F)$ está determinado por los $\{\sigma(\alpha_i)\}_{i\in I}$, donde $\sigma(\alpha_i)$ ha de ser un F–conjugado de α_i en $\overline{F}$.
Si $K = F(\alpha_1, \ldots, \alpha_n)/F$ es finita, cada $\sigma \in \mathrm{Aut}(K/F)$ está determinado por los $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$, donde $\sigma(\alpha_i)$ es un F–conjugado de α_i. Por tanto, $\mathrm{Aut}(K/F)$ es un grupo finito. De hecho, hemos demostrado un resultado más fuerte en la sección de extensiones separables. El grupo

$$\mathrm{Aut}(K/F) = \{\sigma : K \to \overline{F} \mid \sigma \text{ es extensión de } F \hookrightarrow \overline{F} \text{ y } \sigma(K) \subset K\}.$$

Hemos demostrado, en Teorema 3.3.17, que

$$|\{\sigma : K \to \overline{F} \mid \sigma \text{ es extensión de } F \hookrightarrow \overline{F}\}| \leq [K : F].$$

Por tanto, si K/F es finita, entonces

$$|\mathrm{Aut}(K/F)| \leq [K : F].$$

Daremos, no obstante, otra demostración de este hecho para una extensión normal.

Teorema 3.8.4. *Sea K/F una extensión finita normal. Entonces $|\mathrm{Aut}(K/F)| \leq [K : F]$, con igualdad si, y sólo si, K/F es separable.*

Este resultado es consecuencia de el siguiente, aparentemente más general, enunciado.

Teorema 3.8.5. *Sean $\varphi : F \xrightarrow{\sim} F'$ un isomorfismo de cuerpos, E un cuerpo de descomposición de un polinomio de grado positivo $f(X) \in F[X]$ sobre F y E' un cuerpo de descomposición del polinomio $f^{\varphi}(X)$ sobre F'. El número de extensiones de φ a un isomorfismo $E \xrightarrow{\sim} E'$ es $\leq [E : F]$, con igualdad si, y sólo si, $f(X)$ es separable.*

Demostración. Hemos probado, en Teorema 3.2.5, que el conjunto de extensiones es no vacío. Una versión más cuidadosa de la demostración proporciona la desigualdad.
Inducción sobre $[E : F]$.
Si $[E : F] = 1$, entonces $E = F, E' = F'$ y hay una única extensión, el propio φ.
Supongamos $[E : F] > 1$. Entonces $f(X)$ tiene un factor irreducible $p(X) \in F[X]$ de grado ≥ 2. Sea α una raíz de $p(X)$. Si σ es una extensión de φ a E, entonces $\sigma_{|F(\alpha)}$ es un

isomorfismo τ de $F(\alpha)$ con $F'(\beta)$, donde $\beta = \sigma(\alpha)$ es raíz de $p^{\varphi}(X)$ factor irreducible de $f^{\varphi}(X)$. El isomorfismo τ está unívocamente determinado por $\tau(\alpha) = \sigma(\alpha)$. Por tanto se tiene un diagrama

(3.8.5.1)
$$\begin{array}{ccc} E & \xrightarrow[\sim]{\sigma} & E' \\ | & & | \\ F(\alpha) & \xrightarrow[\sim]{\tau} & F'(\beta) \\ | & & | \\ F & \xrightarrow[\sim]{\varphi} & F'. \end{array}$$

Recíprocamente, para cada raíz β de $p^{\varphi}(X)$ hay extensiones τ y σ de φ que proporcionan un diagrama (3.8.5.1). Por tanto, para contar el número de extensiones σ debemos contar el número de tales diagramas. El número de extensiones de φ a un isomorfismo τ es el número de raíces distintas β de $p^{\varphi}(X)$. Puesto que $\deg p(X) = \deg p^{\varphi}(X) = [F(\alpha) : F] = [F'(\beta) : F']$, vemos que el número de extensiones de φ a un τ es $\leq [F(\alpha) : F]$, con igualdad si, y sólo si, las raíces de $p(x)$ son todas distintas. Puesto que E es también el cuerpo de descomposición de $f(X)$ sobre $F(\alpha)$ y E' el cuerpo de descomposición de $f^{\varphi}(X)$ sobre $F'(\beta)$ y $[E : F(\alpha)] < [E : F]$, podemos aplicar la hipótesis de inducción para obtener que el número de extensiones de τ a un σ es $\leq [E : F(\alpha)]$, con igualdad si, y sólo si, $f(X)$ es separable (i.e., sus factores irreducibles no tienen raíces múltiples). De la igualdad $[E : F] = [E : F(\alpha)][F(\alpha) : F]$ se deduce que el número de extensiones de φ a un tal σ es $\leq [E : F]$. Tendremos igualdad si, y sólo si, se tiene igualdad en cada etapa si, y sólo si, $p(X)$ y $f(X)$ son separables si, y sólo si, $f(X)$ es separable, puesto $p(X)$ es un factor irreducible de $f(X)$. □

Observación 3.8.6. Aplicando Teorema 3.8.5 con $E = E' = K$, $F = F'$ y $\varphi = 1_F$ obtenemos Teorema 3.8.4: Si K/F es finita y normal, entonces $|\mathrm{Aut}(K/F)| \leq [K : F]$, con igualdad si K/F separable.

3.8.2. El Teorema Fundamental de la Teoría de Galois

Definición 3.8.7. Sea K/F una extensión finita. Diremos que K/F es una extensión de Galois si $|\mathrm{Aut}(K/F)| = [K : F]$. En este caso, denotaremos $\mathrm{Gal}(K/F)$ el grupo $\mathrm{Aut}(K/F)$.

Observación 3.8.8. (1) Recordemos que para toda extensión finita $|\mathrm{Aut}(K/F)| \leq [K : F]$.

(2) Hemos demostrado, Teorema 3.8.4, que toda extensión finita, normal y separable es de Galois.

(3) Demostraremos que el recíproco es cierto. Sea K/F una extensión finita. Si $|\mathrm{Aut}(K/F)| = [K : F]$, entonces K/F es normal y separable.

Corolario 3.8.9. *El cuerpo de descomposición sobre F de un polinomio separable sobre F es una extensión de Galois sobre F.*

Demostración. Teorema 3.8.5 □

Definición 3.8.10. *Sean F un cuerpo y $f(X)$ un polinomio de grado positivo separable sobre F. Denominaremos grupo de Galois de $f(X)$ sobre F al grupo de Galois del cuerpo de descomposición de $f(X)$ sobre F. Denotaremos* $\mathrm{Gal}(f/F)$.

Ejemplos 3.8.11. (1) Sea $K = F(\sqrt{D})$ una extensión cuadrática, i.e., $[K : F] = 2$ o, equivalente, $D \in F - F^2$, con $\mathrm{char}\, F \neq 2$. Entonces K/F es de Galois y

$$\mathrm{Gal}(K/F) = \{1, \sigma\} \simeq \mathbb{Z}_2,$$

con $\sigma(a + b\sqrt{D}) = a - b\sqrt{D}$.

(2) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es de Galois.

(3) La extensión $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, de grado $[K : \mathbb{Q}] = 4$, es el cuerpo de descomposición de $(X^2 - 2)(X^2 - 3)$, es, por tanto, una extensión de Galois. Su grupo de Galois tiene orden 4, $G = \mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_3\}$. Cada automorfismo está determinado por $\sigma_i(\sqrt{2}) = \pm\sqrt{2}, \sigma_i(\sqrt{3}) = \pm\sqrt{3}$. Esto es

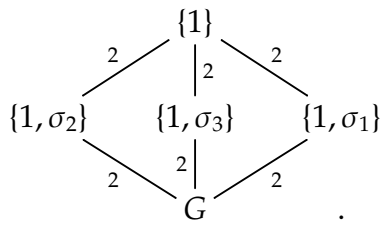
	$\sqrt{2}$	$\sqrt{3}$	$\sqrt{6}$
1	$\sqrt{2}$	$\sqrt{3}$	$\sqrt{6}$
σ_1	$-\sqrt{2}$	$\sqrt{3}$	$-\sqrt{6}$
σ_2	$\sqrt{2}$	$-\sqrt{3}$	$-\sqrt{6}$
σ_3	$-\sqrt{2}$	$-\sqrt{3}$	$\sqrt{6}$

Por tanto, las cuatro opciones combinatorias posibles definen un automorfismo. Es claro que $\sigma_1\sigma_2 = \sigma_2\sigma_1 = \sigma_3$ y que cada σ_i tiene orden 2. Así $\mathrm{Gal}(K/F) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

De forma explícita, en la base $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ de K/F

$$\begin{aligned}
\sigma_1 &: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\
\sigma_2 &: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\
\sigma_3 &: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}
\end{aligned}$$

El retículo de subgrupos de $G = \mathrm{Gal}(K/F) = \{1, \sigma_1, \sigma_2, \sigma_3\}$ es



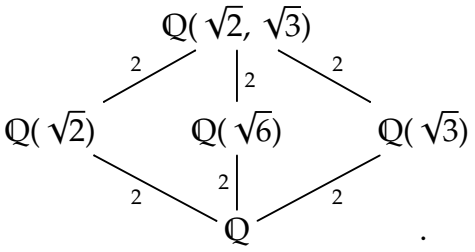
.

Los correspondientes cuerpos fijos:

$$\begin{aligned}\mathrm{Fix}(\{1,\sigma_1\}) &= \mathrm{Fix}(\sigma_1) = \mathbb{Q}(\sqrt{3})\\ \mathrm{Fix}(\{1,\sigma_2\}) &= \mathrm{Fix}(\sigma_2) = \mathbb{Q}(\sqrt{2})\\ \mathrm{Fix}(\{1,\sigma_3\}) &= \mathrm{Fix}(\sigma_3) = \mathbb{Q}(\sqrt{6})\end{aligned}$$

Por ejemplo, $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \in \mathrm{Fix}(\sigma_3)$ si, y sólo si, $a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6} = \sigma_3(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ si, y sólo si, $b=-b, c=-c$ si, y sólo si, $b=c=0$ si, y sólo si, $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} = a+d\sqrt{6} \in \mathbb{Q}(\sqrt{6})$. El argumento puede ser más sencillo: de $\sigma_3(\sqrt{6}) = \sqrt{6}$ se deduce que $\mathbb{Q}(\sqrt{6}) \subset \mathrm{Fix}(\sigma_3)$.Por otra parte, la teoría afirma que $[\mathrm{Fix}(\sigma_3) : \mathbb{Q}] = 2$. En consecuencia se obtiene la igualdad $\mathrm{Fix}(\sigma_3) = \mathbb{Q}(\sqrt{6})$.

El retículo de los subcuerpos que observamos en la extensión $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ es



(4) Las raíces de X^3-2 son $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$, con $\omega = -\frac{1}{2}+\frac{\sqrt{3}}{2}i$, $\omega^2 = -\frac{1}{2}-\frac{\sqrt{3}}{2}i$ las raíces cúbicas primitivas de 1.

El cuerpo de descomposición de X^3-2 es

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

El polinomio mínimo de ω, ω^2 sobre $\mathbb{Q}$ es X^2+X+1 y, es claro que $\omega \notin \mathbb{Q}(\sqrt[3]{2})$. Por tanto $[\mathbb{Q}(\sqrt[3]{2},\omega) : \mathbb{Q}(\sqrt[3]{2})] = 2$. Así

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

Los subcuerpos, $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\omega), \mathbb{Q}(\sqrt[3]{2}\omega^2)$ son distintos. En efecto, si dos de ellos fueran el mismo subcuerpo L de grado 3 sobre $\mathbb{Q}$, entonces, para $0 \le i < j \le 2$, el elemento $\frac{\sqrt[3]{2}\omega^j}{\sqrt[3]{2}\omega^i} = \omega^{j-i} \in L$. Esto no es posible, puesto que $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^2)$ es de grado 2 sobre $\mathbb{Q}$: la ecuación irreducible $X^2+X+1=0$ tiene por raíces ω, ω^2.

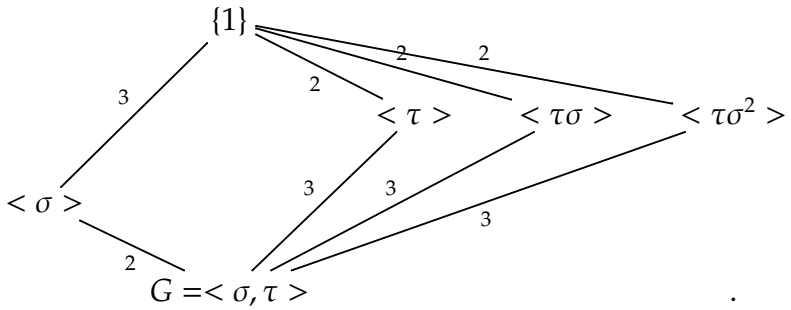
El grupo $G = \mathrm{Gal}(K/F)$ tiene orden 6. Un elemento $\sigma \in \mathrm{Gal}(K/F)$ está determinado por los valores $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2; \sigma(\omega) = \omega, \omega^2$. Por tanto, las 6 opciones combinatorias definen cada uno de los elementos de $\mathrm{Gal}(K/F)$.

	$\sqrt[3]{2}$	ω	ω^2	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
1	$\sqrt[3]{2}$	ω	ω^2	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
σ	$\sqrt[3]{2}\omega$	ω	ω^2	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$
σ^2	$\sqrt[3]{2}\omega^2$	ω	ω^2	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$
τ	$\sqrt[3]{2}$	ω^2	ω	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}\omega$
$\tau\sigma^2$	$\sqrt[3]{2}\omega$	ω^2	ω	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega^2$
$\tau\sigma$	$\sqrt[3]{2}\omega^2$	ω^2	ω	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}$

Definimos σ por $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega, \sigma(\omega) = \omega$ y τ por $\tau(\sqrt[3]{2}) = \sqrt[3]{2}, \tau(\omega) = \omega^2$. Entonces la tabla del grupo es

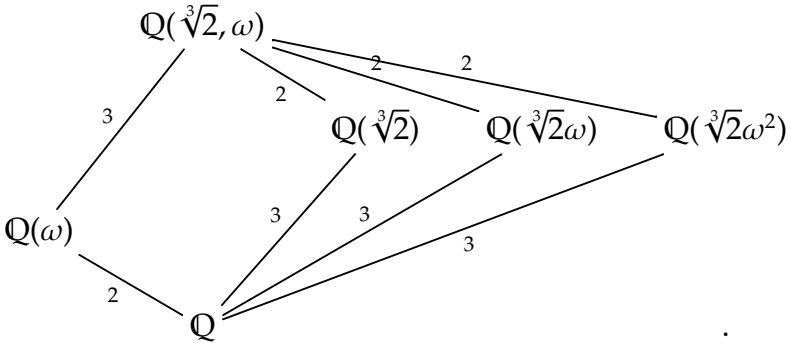
Se verifica $\sigma^3 = \tau^2 = 1, \sigma\tau = \tau\sigma^2$. Por tanto, $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) =< \sigma, \tau > \simeq D_3 \simeq S_3$.

El retículo de los subgrupos de este grupo diedro es



.

Los correspondientes cuerpos fijos aparecen en el retículo de los subcuerpos que observamos en la extensión $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$



.

Calculemos, por ejemplo, Fix(σ).

Una base de $K/\mathbb{Q}$ es $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega\}$, producto de la base $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ de $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ y la base $\{1, \omega\}$ de $K/\mathbb{Q}(\sqrt[3]{2})$. Usando esta base

$$\sigma(a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\sqrt[3]{2}\omega + f\sqrt[3]{4}\omega) = a - e\sqrt[3]{2} + (f - c)\sqrt[3]{4} + d\omega + (b - e)\sqrt[3]{2}\omega - c\sqrt[3]{4}\omega.$$

Así

$$\sigma(a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\sqrt[3]{2}\omega + f\sqrt[3]{4}\omega) = a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\sqrt[3]{2}\omega + f\sqrt[3]{4}\omega,$$

si, y sólo si,

$$a - e\sqrt[3]{2} + (f - c)\sqrt[3]{4} + d\omega + (b - e)\sqrt[3]{2}\omega - c\sqrt[3]{4}\omega = a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\sqrt[3]{2}\omega + f\sqrt[3]{4}\omega,$$

si, y sólo si,

$$-e = b, f - c = c, b - e = e, -c = f,$$

si, y sólo si,

$$b = c = f = e = 0,$$

si, y sólo si,

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\sqrt[3]{2}\omega + f\sqrt[3]{4}\omega = a + d\omega,$$

si, y sólo si,

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\omega + e\sqrt[3]{2}\omega + f\sqrt[3]{4}\omega \in \mathbb{Q}(\omega).$$

Por tanto,

$$\mathrm{Fix}(\sigma) = \mathbb{Q}(\omega).$$

Observemos que el único subgrupo normal de G es $< \sigma >$ y el cuerpo fijo correspondiente $\mathbb{Q}(\omega)/\mathbb{Q}$ es el único cuerpo intermedio, de los observados, que es una extensión normal de $\mathbb{Q}$.

(5) La extensión $\mathbb{F}_{p^n}/\mathbb{F}_p$ es de Galois, puesto que es el cuerpo descomposición del polinomio separable $X^{p^n} - X$. El grupo $G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ es, por tanto, de orden n. Consideremos el automorfismo de Frobenius

$$\begin{aligned} \sigma_p : \mathbb{F}_{p^n} &\to \mathbb{F}_{p^n} \\ \alpha &\mapsto \alpha^p. \end{aligned}$$

Sus potencias $i = 0, 1, \ldots, n - 1$

$$\begin{aligned} \sigma_p^i : \mathbb{F}_{p^n} &\to \mathbb{F}_{p^n} \\ \alpha &\mapsto \alpha^{p^i}. \end{aligned}$$

Puesto que $\alpha^{p^n} = \alpha$, para cada $\alpha \in \mathbb{F}_{p^n}$, es $\sigma_p^{p^n} = 1$. Esto no ocurre para $i < n$. Por tanto, el grupo es cíclico, generado por el automorfismo de Frobenius

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = < \sigma_p > .$$

El Teorema Fundamental demuestra que la relación observada entre los retículos de subgrupos y de cuerpos intermedios es, de hecho, una biyección para toda extensión de Galois, en la que subgrupos normales corresponden a cuerpos intermedios extensión normal de la base.

Teorema 3.8.12 (Fundamental de la Teoría de Galois)**.** *Sean K/F una extensión finita de Galois y $G = \mathrm{Gal}(K/F)$. Existe una biyección*

$$\left\{\begin{array}{cc} & K \\ \text{Subcuerpos } E & | \\ \text{de } K & E \\ \text{que contienen a } F & | \\ & F \end{array}\right\} \longleftrightarrow \left\{\begin{array}{cc} & \{1\} \\ \text{Subgrupos } H & | \\ \text{de } G & H \\ & | \\ & G \end{array}\right\}$$

definida por las asignaciones

$$E \mapsto \mathrm{Gal}(K/E) = \{\sigma \in G \,|\, \sigma(\alpha) = \alpha, \text{ para todo } \alpha \in E\}$$

$$\{\alpha \in K \,|\, \sigma(\alpha) = \alpha, \text{ para todo } \sigma \in H\} = \mathrm{Fix}(H) \leftarrow H$$

que son inversas una de la otra.
En estas correspondencias:

(1) Para cada cuerpo intermedio $F \subset E \subset K$, la extensión K/E es de Galois.

(2) (Inversión de las inclusiones) Si E_1, E_2 corresponden, respectivamente, a H_1, H_2, entonces $E_1 \subset E_2$ si, y sólo si, $H_2 \leq H_1$.

(3) Sean E y H que corresponden en la biyección. Esto es, $H = \mathrm{Gal}(K/E)$, $E = \mathrm{Fix}(H)$. Entonces $[K : E] = |H|$ y $[E : F] = [G : H]$ el índice de H en G. De otro modo, $[K : E] = |\mathrm{Gal}(K/E)|$ y $[\mathrm{Fix}(H) : F] = [G : H]$.

(4) El cuerpo intermedio E es normal sobre F y, por tanto, E/F es de Galois si, y sólo si, $H = \mathrm{Gal}(K/E)$ es un subgrupo normal de G. En este caso

$$\mathrm{Gal}(E/F) \simeq G/H = \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E).$$

Más general, las inmersiones de E en un cierre algebraico de F que contiene a K, que son la identidad en F están en biyección con las clases σH de congruencia módulo H en G.

(5) Si E_1, E_2 corresponden, respectivamente, a H_1, H_2, entonces la intersección $E_1 \cap E_2$ corresponde al subgrupo $< H_1, H_2 >$ generado por $H_1 \cup H_2$ y, el subcuerpo compuesto E_1E_2, menor subcuerpo de K que contiene a $E_1 \cup E_2$, corresponde al subgrupo intersección $H_1 \cap H_2$. Por tanto, el retículo de cuerpos intermedios de K/F y el retículo de subgrupos de G son duales.

Resultados preliminares para la demostración del Teorema Fundamental

Independencia lineal de caracteres

Definición 3.8.13. Un carácter (lineal) χ de un grupo G con valores en un cuerpo L es un homomorfismo de $G \xrightarrow{\chi} L^*$ en el grupo multiplicativo de L, i.e. $\chi(gg') = \chi(g)\chi(g')$ y $\chi(g) \neq 0$ para $g, g' \in G$.

Definición 3.8.14. Diremos que los caracteres $\chi_1, \ldots, \chi_n$ de G son linealmente independientes sobre L si de toda relación $a_1\chi_1(g) + \cdots + a_n\chi_n(g) = 0$ para todo $g \in G$, donde $a_i \in L$, se deduce $a_i = 0$.

Teorema 3.8.15. *Cualesquiera caracteres de G distintos $\chi_1, \ldots, \chi_n$ son linealmente independientes sobre L.*

Demostración. Supongamos por el contrario que hay relaciones no triviales. Elegimos una relación con el menor número posible m de coeficientes no nulos. Ha de ser $m \geq 2$. Reordenando, si es preciso, podemos suponer que es la relación

$$a_1\chi_1(g) + \cdots + a_m\chi_m(g) = 0, \tag{3.8.15.1}$$

para todo $g \in G$. Puesto que $\chi_1 \neq \chi_m$, existe $g_0 \in G$ tal que $\chi_1(g_0) \neq \chi_m(g_0)$. La relación (3.8.15.1) expresa, en particular, la igualdad

$$a_1\chi_1(g_0g) + \cdots + a_m\chi_m(g_0g) = 0,$$

i.e.

$$a_1\chi_1(g_0)\chi_1(g) + \cdots + a_m\chi_m(g_0)\chi_m(g) = 0. \tag{3.8.15.2}$$

Ahora $\chi_m(g_0)$ (3.8.15.1)$-$(3.8.15.2) es la relación

$$(\chi_m(g_0) - \chi_1(g_0))a_1\chi_1(g) + \cdots + (\chi_m(g_0) - \chi_{m-1}(g_0))a_{m-1}\chi_{m-1}(g) = 0, \tag{3.8.15.3}$$

para todo $g \in G$. Esta última es una relación no trivial con menos de m coeficientes no nulos. Contradicción. □

Consideremos ahora un homomorfismo $K \xrightarrow{\sigma} L$ de un cuerpo K en L. Puesto que σ es siempre inyectivo, es un homomorfismo de grupos multiplicativos $K^* \xrightarrow{\sigma} L^*$, que podemos ver como un carácter de K^* en L. Este carácter contiene toda la información relativa a σ puesto que $\sigma(0) = 0$.

Corolario 3.8.16. *Cualesquiera diferentes inmersiones $\sigma_1, \ldots, \sigma_n$ de un cuerpo K en un cuerpo L son, como funciones definidas en K, linealmente independientes sobre L.*

Usamos el corolario anterior para probar la relación entre los órdenes de subgrupos de automorfismos de un cuerpo K y los grados de las extensiones sobre sus cuerpos fijos.

Teorema 3.8.17. *Sean $G = \{1 = \sigma_1, \ldots, \sigma_n\}$ un subgrupo finito de automorfismos de un cuerpo K y $F = \mathrm{Fix}\,(G)$ el subcuerpo fijo de G. Entonces K/F es finita y $[K : F] = n = |G|$.*

Demostración. Supongamos primero que $m = [K : F] < n$ y fijemos una base $\omega_1, \ldots, \omega_m$ de K sobre F. Entonces el sistema $\sum_{j=1,\ldots,n} \sigma_j(\omega_i)x_j = 0,\ i = 1, \ldots, m$, de m ecuaciones con n incógnitas $x_1, \ldots, x_n$ tiene solución no trivial $\beta_1, \ldots, \beta_n \in K$.
Sean $a_1, \ldots, a_m \in F$ elementos cualesquiera. Entonces, según la hipótesis, $\sigma_i(a_j) = a_j$. Por

tanto, multiplicando la ecuación i–ésima por a_i obtenemos las identidades $\sum_{j=1,\dots,n} \sigma_j(a_i\omega_i)\beta_j = 0,\ i = 1,\dots,m$. Sumando estas m identidades vemos que existen $\beta_1,\dots,\beta_m \in K$ no todos nulos, que verifican la identidad

$$\sigma_1(a_1\omega_1 + \cdots + a_m\omega_m)\beta_1 + \cdots + \sigma_n(a_1\omega_1 + \cdots + a_m\omega_m)\beta_n = 0,$$

para cualquiera elección $a_1,\dots,a_m \in F$. Puesto que los ω_i forman una base de K sobre F, esto significa que para todo $\alpha \in K$ se tiene la identidad

$$\sigma_1(\alpha)\beta_1 + \cdots + \sigma_n(\alpha)\beta_n = 0.$$

Pero esto significa que los automorfismos distintos $\sigma_1,\dots,\sigma_n$ son linealmente dependientes sobre K, en contra del Corolario 3.8.16.
Por tanto hemos probado que $n \leq [K : F]$. Supongamos ahora que $n < [K : F]$, (pudiera ser $[K : F] = \infty$). Entonces hay más de n elementos F–linealmente independientes en K, digamos $\alpha_1,\dots,\alpha_{n+1} \in K$. El sistema

$$\sum_{j=1,\dots,n+1} \sigma_i(\alpha_j)x_j = 0,\ i = 1,\dots,n, \tag{3.8.17.1}$$

de n ecuaciones con $n+1$ incógnitas tiene solución no trivial $\beta_1,\dots,\beta_{n+1} \in K$. Si todos los $\beta_j \in F$ entonces la primera ecuación (recordemos que $\sigma_1 = 1$) contradiría la independencia lineal sobre F de los α_j. Por tanto, al menos uno de los $\beta_j \notin F$. Entre todas las soluciones no triviales elegimos una con el menor número posible $r(> 0)$ de β_j no nulos. Reordenando podemos suponer $\beta_1,\dots,\beta_r, 0,\dots,0$. Dividiendo por β_r podemos suponer $\beta_r = 1$. Ya hemos visto que alguno de los $\beta_1,\dots,\beta_{r-1}, 1$ no esta en F. Esto prueba que $r > 1$, y podemos suponer $\beta_1 \notin F$. Entonces el sistema (3.8.17.1) dice

$$\begin{array}{ccccccccc} \sigma_1(\alpha_1)\beta_1 & + & \cdots & + & \sigma_1(\alpha_{r-1})\beta_{r-1} & + & \sigma_1(\alpha_r) & = & 0 \\ \vdots & & & & \vdots & & \vdots & & \\ \sigma_n(\alpha_1)\beta_1 & + & \cdots & + & \sigma_n(\alpha_{r-1})\beta_{r-1} & + & \sigma_n(\alpha_r) & = & 0. \end{array} \tag{3.8.17.2}$$

Puesto que $\beta_1 \notin F$, existe σ_{j_0} tal que $\sigma_{j_0}(\beta_1) \neq \beta_1$. Aplicando σ_{j_0} a las identidades (3.8.17.2), obtenemos

$$\begin{array}{ccccccccc} \sigma_{j_0}\sigma_1(\alpha_1)\sigma_{j_0}(\beta_1) & + & \cdots & + & \sigma_{j_0}\sigma_1(\alpha_{r-1})\sigma_{j_0}(\beta_{r-1}) & + & \sigma_{j_0}\sigma_1(\alpha_r) & = & 0 \\ \vdots & & & & \vdots & & \vdots & & \\ \sigma_{j_0}\sigma_n(\alpha_1)\sigma_{j_0}(\beta_1) & + & \cdots & + & \sigma_{j_0}\sigma_n(\alpha_{r-1})\sigma_{j_0}(\beta_{r-1}) & + & \sigma_{j_0}\sigma_n(\alpha_r) & = & 0. \end{array} \tag{3.8.17.3}$$

Ahora bien, los $\sigma_{j_0}\sigma_1,\dots,\sigma_{j_0}\sigma_n$ son los $\sigma_1,\dots,\sigma_n$ en algún orden, puesto que los $\sigma_1,\dots,\sigma_n$ forman un grupo. Por tanto reordenando (3.8.17.3) obtenemos

$$\begin{array}{ccccccccc} \sigma_1(\alpha_1)\sigma_{j_0}(\beta_1) & + & \cdots & + & \sigma_1(\alpha_{r-1})\sigma_{j_0}(\beta_{r-1}) & + & \sigma_1(\alpha_r) & = & 0 \\ \vdots & & & & \vdots & & \vdots & & \\ \sigma_n(\alpha_1)\sigma_{j_0}(\beta_1) & + & \cdots & + & \sigma_n(\alpha_{r-1})\sigma_{j_0}(\beta_{r-1}) & + & \sigma_n(\alpha_r) & = & 0. \end{array} \tag{3.8.17.4}$$

La diferencia (3.8.17.2)−(3.8.17.4) muestra que $0 \neq \beta_1 - \sigma_{j_0}(\beta_1), \ldots, \beta_{r-1} - \sigma_{j_0}(\beta_{r-1}), 0, \ldots, 0$ es una solución no trivial de (3.8.17.1) con menos de r elementos no nulos. Contradicción. □

Corolario 3.8.18. *Sea K/F una extensión finita. Entonces el orden del grupo de automorfismos $|\mathrm{Aut}(K/F)|$ divide al grado $[K : F]$, con igualdad si, y sólo si, F es el cuerpo fijo de $\mathrm{Aut}(K/F)$. Dicho de otra forma K/F es una extensión de Galois si, y sólo si, F es el cuerpo fijo de $\mathrm{Aut}(K/F)$.*

Demostración. Denotemos F_1 el cuerpo fijo de $\mathrm{Aut}(K/F)$, entonces $F \subset F_1 \subset K$. Hemos probado que el grupo $\mathrm{Aut}(K/F)$ es finito. Así, según el Teorema 3.8.17, $|\mathrm{Aut}(K/F)| = [K : F_1]$. Por tanto $[K : F] = |\mathrm{Aut}(K/F)| \cdot [F_1 : F]$. En particular, $|\mathrm{Aut}(K/F)|$ divide a $[K : F]$ y se tiene la igualdad si, y sólo si, $F = F_1$. □

Corolario 3.8.19. *Sean G un subgrupo finito de automorfismos de un cuerpo K y F el cuerpo fijo. Entonces cada automorfismo de K que deja fijo los elementos de F está en G, i.e. $G = \mathrm{Aut}(K/F)$.*

Demostración. Es claro que G es un subgrupo de $\mathrm{Aut}(K/F)$. Por tanto $|G| \mid |\mathrm{Aut}(K/F)1$. Por el Teorema 3.8.17 $|G| = [K : F]$ y, por Corolario 3.8.18 $|\mathrm{Aut}(K/F)| \mid [K : F]$. En consecuencia $|G| = |\mathrm{Aut}(K/F)|$. □

Corolario 3.8.20. *Si $G_1 \neq G_2$ son subgrupos finitos distintos de automorfismos de un cuerpo K entonces sus cuerpos fijos son distintos.*

Demostración del Teorema Fundamental

Proposición 3.8.21. *Sea K/F una extensión finita. Entonces K/F es separable y normal si, y sólo si, $|\mathrm{Aut}(K/F)| = [K : F]$.*

Demostración. La primera implicación está demostrada en Corolario 3.5.6.

Supongamos $|\mathrm{Aut}(K/F)| = [K : F] = n$. Hemos de probar que K/F es separable y normal. Las condiciones separable y normal equivalen a probar que todo polinomio mónico $p(X) \in F[X]$ irreducible sobre F que tiene una raíz en K factoriza en K en producto de factores lineales no repetidos. Denotemos $G = \mathrm{Aut}(K/F) = \{1, \sigma_2, \ldots, \sigma_n\}$. Supongamos que $\alpha \in K$ es raíz de $p(X)$. Denotemos $\alpha, \alpha_2, \ldots, \alpha_r \in K$ los elementos distintos en la serie $\alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha) \in K$.

Para cada $\tau \in G$ la multiplicación $G \to G; \sigma \mapsto \tau\sigma$ es biyectiva, i.e., $G = \{\tau, \tau\sigma_2, \ldots, \tau\sigma_n\}$. Se deduce que la serie $\tau(\alpha), \tau\sigma_2(\alpha), \ldots, \tau\sigma_n(\alpha)$ es una permutación de la serie $\alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$. Por tanto, $\tau(\alpha), \tau(\alpha_2), \ldots, \tau(\alpha_r)$ es una permutación de $\alpha, \alpha_2, \ldots, \alpha_r$. En consecuencia, los coeficientes del polinomio $f(X) = (X - \alpha)(X - \alpha_2) \cdots (X - \alpha_r)$ son fijados por cada elemento de G, puesto que estos coeficientes son funciones simétricas de las raíces. Esto es los coeficientes de $f(X)$ están en el cuerpo fijo de G. Según Corolario 3.8.18, este cuerpo fijo es F. Por tanto, $f(X) \in F[X]$. Puesto que $p(X)$ es mónico irreducible y $p(\alpha) = 0$, es $p(X)$ el polinomio mínimo de α sobre F. Como $f(\alpha) = 0$ y $f(X) \in F[X]$, se deduce que $p(X)$ divide a $f(X)$ en $F[X]$. Por otra parte, es claro que $f(X)$ divide a $p(X)$ (en $K[X]$), ya que $\alpha, \alpha_2, \ldots, \alpha_r \in K$ son F–conjugados distintos de α, esto es raíces distintas de $p(X)$. Así $f(X) = p(X)$. Por tanto, $p(X)$ es producto de factores lineales distintos en $K[X]$. □

Observación 3.8.22. Sean K/F finita de Galois y $\alpha \in K$. La demostración de Proposición 3.8.21 muestra que los F–conjugados de α son los elementos distintos en la serie $\alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$, donde $\mathrm{Gal}(K/F) = \{1, \sigma_2, \ldots, \sigma_n\}$.

Recapitulemos las condiciones que definen el concepto de extensión de Galois.

Teorema 3.8.23. *Sea K/F un extensión. Son condiciones equivalentes.*

(1) El cuerpo K es el cuerpo de descomposición sobre F de un polinomio separable de $F[X]$.

(2) La extensión K/F es finita, separable y normal.

(3) La extensión K/F es finita y $|\mathrm{Aut}(K/F)| = [K : F]$.

(4) La extensión K/F es finita y $F = \mathrm{Fix}(\mathrm{Aut}(K/F))$.

En estas condiciones diremos que K/F es una extensión (finita) de Galois.

Corolario 3.8.24. *Sea K/F una extensión finita de Galois. Entonces para cada cuerpo intermedio $F \subset E \subset K$, la extensión K/E es finita de Galois.*

Demostración. Basta aplicar la caracterización (1) de Teorema 3.8.23. Si K es el cuerpo de descomposición sobre F del polinomio separable $f(X) \in F[X]$, entonces K es el cuerpo de descomposición sobre E del polinomio separable $f(X) \in E[X]$. □

Teorema 3.8.25 (Fundamental de la Teoría de Galois)**.** *Sean K/F una extensión finita de Galois y $G = \mathrm{Gal}(K/F)$. Existe una biyección*

$$\left\{\begin{array}{c} \\ \text{Subcuerpos } E \\ \text{de } K \\ \text{que contienen a } F \\ \\ \end{array}\begin{array}{c} K \\ | \\ E \\ | \\ F \end{array}\right\} \longleftrightarrow \left\{\begin{array}{c} \\ \text{Subgrupos } H \\ \text{de } G \\ \\ \end{array}\begin{array}{c} \{1\} \\ | \\ H \\ | \\ G \end{array}\right\}$$

definida por las asignaciones

$$E \mapsto \mathrm{Gal}(K/E) = \{\sigma \in G \,|\, \sigma(\alpha) = \alpha, \text{ para todo } \alpha \in E\}$$

$$\{\alpha \in K \,|\, \sigma(\alpha) = \alpha, \text{ para todo } \sigma \in H\} = \mathrm{Fix}(H) \leftarrow H$$

que son inversas una de la otra.
En estas correspondencias:

(1) Para cada cuerpo intermedio $F \subset E \subset K$, la extensión K/E es de Galois.

(2) (Inversión de las inclusiones) Si E_1, E_2 corresponden, respectivamente, a H_1, H_2, entonces $E_1 \subset E_2$ si, y sólo si, $H_2 \leq H_1$.

(3) *Sean E y H que corresponden en la biyección. Esto es,* $H = \mathrm{Gal}(K/E)$, $E = \mathrm{Fix}(H)$. *Entonces* $[K : E] = |H|$ *y* $[E : F] = [G : H]$ *el índice de H en G. De otro modo,* $[K : E] = |\mathrm{Gal}(K/E)|$ *y* $[\mathrm{Fix}(H) : F] = [G : H]$.

(4) *El cuerpo intermedio E es normal sobre F y, por tanto, E/F es de Galois si, y sólo si,* $H = \mathrm{Gal}(K/E)$ *es un subgrupo normal de G. En este caso*

$$\mathrm{Gal}(E/F) \simeq G/H = \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E).$$

Más general, las inmersiones de E en un cierre algebraico de F que contiene a K, que son la identidad en F están en biyección con las clases σH *de congruencia módulo H en G.*

(5) *Si* E_1, E_2 *corresponden, respectivamente, a* H_1, H_2, *entonces la intersección* $E_1 \cap E_2$ *corresponde al subgrupo* $< H_1, H_2 >$ *generado por* $H_1 \cup H_2$ *y, el subcuerpo compuesto* E_1E_2, *menor subcuerpo de K que contiene a* $E_1 \cup E_2$, *corresponde al subgrupo intersección* $H_1 \cap H_2$. *Por tanto, el retículo de cuerpos intermedios de K/F y el retículo de subgrupos de G son duales.*

Demostración. Sean $H \leq G$ y $E = \mathrm{Fix}(H)$. Según Corolario 3.8.19 es $\mathrm{Gal}(K/E) = H$. Esto es, la composición $H \mapsto \mathrm{Fix}(H) \mapsto \mathrm{Gal}(K/\mathrm{Fix}(H))$ es la identidad.

Sea $F \subset E \subset K$ un cuerpo intermedio. Según Corolario 3.8.24 la extensión K/E es de Galois. Esto equivale a $E = \mathrm{Fix}(\mathrm{Gal}(K/E))$, según Teorema 3.8.23. Esto es, la composición $E \mapsto \mathrm{Gal}(K/E) \mapsto \mathrm{Fix}(\mathrm{Gal}(K/E))$ es la identidad.

Por tanto, la biyección está establecida.

La inversión de las inclusiones está en Observación 3.8.1.

Las fórmulas de (3) se obtienen de Teorema 3.8.23, la fórmula de los grados y la fórmula de Lagrange para grupos finitos. En efecto, $F \subset E \subset K$, donde K/F y K/E son Galois. Así $[K : F] = |\mathrm{Gal}(K/F)| = |G|$ y $[K : E] = |\mathrm{Gal}(K/E)| = |H|$. La fórmula de los grados $[K : F] = [K : E][E : F]$. Además $|G| = |H| \cdot [G : H]$ (teorema de Lagrange). De aquí, $[E : F] = [G : H]$.

Demostremos (4). Sea $E = \mathrm{Fix}(H)$. Cada $\sigma \in G$ restringido a E es un isomorfismo de E con el subcuerpo $\sigma(E) \subset K$. Recíprocamente, sea $\tau : E \xrightarrow{\sim} \tau(E) \subset \overline{F}$ una inmersión de E en un cierre algebraico $\overline{F}$ de F que contiene a K, tal que τ es la identidad en F. Entonces τ extiende a $\sigma : K \to \overline{F}$ que, por ser K/F normal, verifica $\sigma(K) = K$. Esto es cada inmersión de E en $\overline{F}$ sobre F es la restricción de algún $\sigma \in G$.

Es claro que dos automorfismos $\sigma, \sigma' \in G$ restringen a la misma inmersión de E si, y sólo si, $\sigma^{-1}\sigma'$ es la identidad en E. Esto es, si, y sólo si, $\sigma^{-1}\sigma' \in \mathrm{Gal}(K/E) = H$, o bien, si, y sólo si, $\sigma' H = \sigma H$.

Por tanto, las inmersiones de E están en biyección con las clases σH de congruencia módulo H en G. En particular, esto proporciona la fórmula

$$|\mathrm{Emb}(E/F)| = [G : H] = [E : F],$$

donde $\mathrm{Emb}(E/F)$ es el conjunto de las inmersiones de E en $\overline{F}$ que son la identidad en F.

Recordemos que $\mathrm{Aut}(E/F) \subset \mathrm{Emb}(E/F)$ y que E/F es de Galois si, y sólo si, $\mathrm{Aut}(E/F) = \mathrm{Emb}(E/F)$, esto es , si, y sólo si, para cada $\sigma \in G$ se verifica $\sigma(E) = E$.

Sea $\sigma \in G$, entonces $\sigma(E) = \mathrm{Fix}(\sigma H \sigma^{-1})$. En efecto, sea $\alpha \in E$, entonces para cada $h \in H = \mathrm{Gal}(K/E)$ se verifica $(\sigma h \sigma^{-1})(\sigma(\alpha)) = \sigma(h\alpha) = \sigma(\alpha)$, lo que prueba $\sigma(E) \subset \mathrm{Fix}(\sigma H \sigma^{-1})$ o, de forma equivalente, $\sigma H \sigma^{-1} \leq \mathrm{Gal}(K/\sigma(E))$. Por otra parte, $|\sigma H|\sigma^{-1} = |H|$ y $|\mathrm{Gal}(K/\sigma(E)| = |\mathrm{Gal}(K/E)| = |H|$, puesto que $E \simeq \sigma(E)$. Así $\sigma H \sigma^{-1} = \mathrm{Gal}(K/\sigma(E))$.

En consecuencia, $\sigma(E) = E$ para todo $\sigma \in G$ si, y sólo si, $\sigma H \sigma^{-1} = H$ para todo $\sigma \in G$. Esto es, E/F es de Galois si, y sólo si, H es normal en G.
Además, en este caso, el grupo cociente G/H se identifica con el grupo $\mathrm{Gal}(E/F)$, puesto que la biyección anterior, entre las inmersiones de E y H es claramente, en este caso, un homomorfismo.

Finalmente, sean $H_1 = \mathrm{Gal}(K/E_1)$ y $H_2 = \mathrm{Gal}(K/E_2)$. Cada elemento de $H_1 \cap H_2$ fija ambos E_1 y E_2, por tanto, fija cada elemento del compuesto E_1E_2, puesto que éstos son combinaciones algebraicas de elementos de E_1 y E_2. Recíprocamente si $\sigma \in G$ fija E_1E_2, entonces σ fija E_1 y E_2, por tanto $\sigma \in H_1 \cap H_2$.

De forma similar se prueba $\mathrm{Fix}(< H_1, H_2 >) = E_1 \cap E_2$. □

Extensiones compuestas y extensiones simples

Finalizamos este capítulo con algunos resultados, acerca de extensiones compuestas, que serán usados más adelante. Vemos también que el Teorema del Elemento Primitivo puede ser obtenido como consecuencia del Teorema Fundamental. De hecho, hemos dado (Teorema 3.5.2) una demostración elemental de la versión más general del Teorema del Elemento Primitivo, que permite usar este teorema para simplificar las demostraciones de los resultados previos al Teorema Fundamental. En la prueba de estos resultados previos se pueden obviar el uso del Teorema del Elemento Primitivo, si así se prefiere, obteniendo el Teorema del Elemento Primitivo como corolario del Teorema Fundamental.

Proposición 3.8.26. *Sean K/F de Galois y F'/F una extensión algebraica contenida en $\overline{F}$. Entonces KF'/F' es de Galois, con grupo de Galois*

$$\mathrm{Gal}(KF'/F') \simeq \mathrm{Gal}(K/K \cap F').$$

isomorfo a un subgrupo de $\mathrm{Gal}(K/F)$.

Demostración. Si K/F es de Galois, entonces K es el cuerpo de descomposición sobre F de algún polinomio separable $f(X)$ in $F[X]$. Entonces KF'/F' es el cuerpo de descomposición de $f(X)$ como polinomio en $F'[X]$, así esta extensión es Galois. Puesto que K/F es Galois, cada inmersión de K que es la identidad en F es un automorfismo de K, por tanto la aplicación

$$\begin{aligned} \varphi : \mathrm{Gal}(KF'/F') &\to \mathrm{Gal}(K/F) \\ \sigma &\mapsto \sigma_{|K}, \end{aligned}$$

definida por restricción al subcuerpo K, está bien definida. Es claramente un homomorfismo con núcleo

$$\ker \varphi = \{\sigma \in \mathrm{Gal}(KF'/F') \mid \sigma_{|K} = 1\}.$$

Puesto que todo elemento en $\mathrm{Gal}(KF'/F')$ es trivial en F', los elementos del núcleo son triviales tanto en K como en F' y, por tanto, triviales en su compuesto. Así el núcleo se reduce a la identidad. Esto es, φ es inyectivo.
Denotemos H la imagen de φ en $\mathrm{Gal}(K/F)$ y sea $\mathrm{Fix}(H)$ el correspondiente cuerpo fijo que contiene a F. Puesto que cada elemento en H fija F', el cuerpo fijo $\mathrm{Fix}(H)$ contiene a $K \cap F'$. Por otra parte, el compuesto $\mathrm{Fix}(H)F'$ está fijado por $\mathrm{Gal}(KF'/F')$ (cada $\sigma \in \mathrm{Gal}(KF'/F')$ fija F' y actúa en $\mathrm{Fix}(H) \subset K$ via su restricción $\sigma_{|K} \in H$, que fija $\mathrm{Fix}(H)$ por definición). Por el Teorema Fundamental se deduce que $\mathrm{Fix}(H)F' = F'$, de forma que $\mathrm{Fix}(H) \subset F'$, que proporciona la inclusión opuesta $\mathrm{Fix}(H) \subset K \cap F'$. Por tanto $\mathrm{Fix}(H) = K \cap F'$, así de nuevo por el Teorema Fundamental, $H = \mathrm{Gal}(K/K \cap F')$, lo que completa la demostración. □

Corolario 3.8.27. *Sean K/F de Galois y F'/F una extensión finita. Entonces*

$$[KF' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}.$$

Demostración. Esta fórmula se sigue por la Proposición 3.8.26 de la igualdad $[KF' : F'] = [K : K \cap F']$ dada por los órdenes de los grupos de Galois en la Proposición 3.8.26. □

Ejemplo 3.8.28. Los cuerpos $F = \mathbb{Q}, K = \mathbb{Q}(\sqrt[3]{2}), F' = \mathbb{Q}(\sqrt[3]{2}\omega)$, donde ω es una raíz cúbica primitiva de la unidad, muestran que la fórmula de Corolario 3.8.27 no se verifica, en general, si ninguna de las dos extensiones es Galois.

Proposición 3.8.29. *Sean $K_1/F, K_2/F$ extensiones de Galois contenidas en un cierre algebraico de F.*

(1) La intersección $K_1 \cap K_2$ es de Galois sobre F.

(2) El compuesto K_1K_2 es de Galois sobre F. El grupo de Galois $\mathrm{Gal}(K_1K_2/F)$ es isomorfo al subgrupo

$$H = \{(\sigma, \tau) \mid \sigma_{|K_1 \cap K_2} = \tau_{|K_1 \cap K_2}\}$$

del producto directo $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$ formado por los elementos cuyas restricciones a la intersección $K_1 \cap K_2$ son iguales.

Demostración. (1) El cuerpo $K_1 \cap K_2$ es separable sobre f puesto que es un subcuerpo de una extensión separable. Por otra parte, supongamos $p(X) \in F[X]$ es un polinomio irreducible con una raíz α en $K_1 \cap K_2$. Puesto que $\alpha \in K_i$ y K_i/F es Galois, todas las raíces de $p(X)$ están en K_i, por tanto están en $K_1 \cap K_2$. esto significa que $K_1 \cap K_2$ es normal sobre F.
(2) Si K_i es el cuerpo de descomposición del polinomio separable $f_i(X) \in F[X]$, entonces K_1K_2 es el cuerpo de descomposición sobre F del polinomio separable $f_1(X)f_2(X)$, por tanto K_1K_2 es Galois sobre F.

La aplicación

$$\varphi : \mathrm{Gal}(K_1K_2/F) \to \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$$
$$\sigma \mapsto (\sigma_{|K_1}, \sigma_{|K_2})$$

es un homomorfismo. El núcleo consiste en los elementos que son la identidad tanto en K_1 como en K_2, esto es la identidad en el compuesto K_1K_2, por tanto φ es inyectivo. La imagen está contenida en el subgrupo H, puesto que

$$(\sigma_{|K_1})_{|K_1\cap K_2} = \sigma_{|K_1\cap K_2} = (\sigma_{|K_2})_{|K_1\cap K_2}.$$

El orden de H puede ser calculado observando que para cada $\sigma \in \mathrm{Gal}(K_1/F)$ hay $|\mathrm{Gal}(K_2/K_1 \cap K_2)|$ elementos $\tau \in \mathrm{Gal}(K_2/F)$ cuyas restricciones a $K_1 \cap K_2$ son $\sigma_{|K_1\cap K_2}$. Por tanto

$$\begin{aligned} |H| &= |\mathrm{Gal}(K_1/F)| \cdot |\mathrm{Gal}(K_2/K_1 \cap K_2)| \\ &= |\mathrm{Gal}(K_1/F)| \frac{|\mathrm{Gal}(K_2/F)|}{|\mathrm{Gal}(K_1 \cap K_2/F)|}. \end{aligned} \tag{3.8.29.1}$$

Por Corolario 3.8.27 y la fórmula (3.8.29.1) vemos que los órdenes de H y de $\mathrm{Gal}(K_1K_2/F)$ son ambos iguales a

$$[K_1K_2 : F] = \frac{[K_1 : F][K_2 : F]}{[K_1 \cap K_2 : F]}.$$

Por tanto la imagen de φ es precisamente H, lo que completa la demostración. □

Corolario 3.8.30. *Sean K_1/F y K_2/F extensiones de Galois con $K_1 \cap K_2 = F$. Entonces*

$$\mathrm{Gal}(K_1K_2/F) \simeq \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

Recíprocamente, si K/F es de Galois y $G = \mathrm{Gal}(K/F) = G_1 \times G_2$ es el producto directo de dos subgrupos G_1 y G_2, entonces K es el compuesto de dos extensiones de Galois K_1/F y K_2/F con $K_1 \cap K_2 = F$.

Demostración. La primera parte de deduce inmediatamente de la Proposición 3.8.29. Para la segunda, sea K_1 el cuerpo fijo de $G_1 \leq G$ y sea K_2 el cuerpo fijo de $G_2 \leq G$. Entonces $K_1 \cap K_2$ es el subcuerpo que corresponde al subgrupo G_1G_2, que es todo G en este caso, por tanto $K_1 \cap K_2 = F$. El compuesto K_1K_2 es el cuerpo que corresponde al subgrupo $G_1 \cap G_2$, que es la identidad aquí, por tanto $K_1K_2 = K$, lo que completa la demostración. □

Ejemplo 3.8.31. Sean $K_1 = \mathbb{Q}(\alpha)$, donde α es una raíz de un polinomio irreducible de grado 3 con discriminante un cuadrado en $\mathbb{Q}$, y $K_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Entonces $\mathrm{Gal}(K_1/\mathbb{Q}) = \mathbb{Z}_3$ y $\mathrm{Gal}(K_2/\mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2$. Además $K_1 \cap K_2 = \mathbb{Q}$. Por tanto, $\mathrm{Gal}(K_1K_2/\mathbb{Q}) = \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Otros ejemplos de aplicación del Corolario 3.8.30 aparecen en los ejercicios (10) y (23) del apéndice.

Corolario 3.8.32. *Sea E/F una extensión finita y separable. Entonces E está contenido en una extensión K/F que es Galois y es minimal con esta propiedad, en el sentido de que, en un cierre algebraico fijado, cualquier otra extensión de Galois de F que contiene a E contiene también a K.*

Demostración. Existe una extensión de Galois de F que contiene a E, por ejemplo el compuesto de los cuerpos de descomposición de los polinomios mínimos de un conjunto finito de generadores de E sobre F (que son todos separables puesto que E/F es separable). Entonces la intersección de todas las extensiones de Galois de F que contienen a E es el cuerpo K. □

Definición 3.8.33. La extensión de Galois K/F que contiene a E en Corolario 3.8.32 se denomina la clausura o cierre de Galois de E sobre F.

Recordemos que una extensión K/F se dice simple si $K = F(\alpha)$ para algún $\alpha \in K$, en cuyo caso α se denomina elemento primitivo.

Proposición 3.8.34. *Sea K/F una extensión finita. Entonces K/F es simple si, y sólo si, existe sólo una cantidad finita de subcuerpos de K que contienen a F.*

Demostración. Ver Teorema 3.5.2 (1). □

Teorema 3.8.35 (El Teorema del Elemento Primitivo)**.** *Si K/F es finita y separable, entonces K/F es simple. En particular, toda extensión finita de cuerpos de característica cero es simple.*

Demostración. Sea L/F la clausura de Galois de K/F. Entonces cada subcuerpo de K que contiene a F corresponde a un subgrupo del grupo $\mathrm{Gal}(L/F)$ según el Teorema Fundamental. Puesto que sólo hay una cantidad finita de tales subgrupos, la Proposición 3.8.34 demuestra que K/F es simple. La última afirmación se sigue del hecho de que toda extensión es separable en característica cero. □

3.9. El Teorema Fundamental del Álgebra

Teorema 3.9.1 (Teorema Fundamental del Álgebra)**.** *Sea $p(X) \in \mathbb{C}[X]$ un polinomio de grado positivo con coeficientes complejos. Entonces existe $z \in \mathbb{C}$ tal que $p(z) = 0$.*

Demostración. Recordemos que $\mathbb{C} = \mathbb{R}(i)$, donde $i = \sqrt{-1}$. Puesto que $\mathbb{R}$ tiene característica cero toda extensión finita de $\mathbb{R}$ es separable. En consecuencia, cada extensión finita de $\mathbb{R}(i)$ está contenida en una extensión K que es finita y de Galois sobre $\mathbb{R}$. Hemos de probar que $K = \mathbb{R}(i)$. Sean G el grupo de Galois de K sobre $\mathbb{R}$ y H un 2–subgrupo de Sylow de G. Sea $\mathbb{R} \subset F \subset K$ el cuerpo fijo de H. Puesto que $[G : H]$ es impar (por ser H 2–subgrupo de Sylow de G) y, por el Teorema 3.8.25, $[F : \mathbb{R}] = [G : H]$, vemos que $[F : \mathbb{R}]$ es impar. Por el Teorema 3.8.35, existe $\alpha \in F$ tal que $F = \mathbb{R}(\alpha)$. Entonces α es raíz de un polinomio irreducible en $\mathbb{R}[X]$ de grado impar. Puesto que todo polinomio de grado impar en $\mathbb{R}[X]$ tiene un raíz en $\mathbb{R}$ (en efecto, un polinomio de grado impar en

$\mathbb{R}[X]$ define una función continua en todo $\mathbb{R}$ que, por ser un polinomio de grado impar, toma valores negativos y positivos) el grado del polinomio irreducible de α sobre $\mathbb{R}$ ha de ser 1. Por tanto $G = H$ es un 2–grupo.
Ahora usamos que K es de Galois sobre $\mathbb{R}(i)$. Sea $G_1 = \mathrm{Gal}(K/\mathbb{R}(i)) \leq G$. Por tanto, G_1 es un 2–grupo. Si G_1 no es trivial, entonces G_1 tiene un subgrupo G_2 de índice 2. Sea $\mathbb{R}(i) \subset L \subset K$ el cuerpo fijo de G_2. Entonces $[L : \mathbb{R}(i)] = [G_1 : G_2] = 2$. Pero todo elemento de $\mathbb{R}(i)$ tiene una raíz cuadrada en $\mathbb{R}(i)$. En efecto, sea $a + bi \in \mathbb{R}(i), a, b \in \mathbb{R}$, entonces la raíz cuadrada es $c + di$, donde $c^2 = \frac{a+\sqrt{a^2+b^2}}{2}, d^2 = \frac{-a+\sqrt{a^2+b^2}}{2}$ y el signo de c, d se determina trivialmente para que $(c + di)^2 = a + bi$. Por tanto, $\mathbb{R}(i)$ no tiene extensiones de grado 2. Se deduce que G_1 es el grupo trivial y, por tanto, $K = \mathbb{R}(i)$, como queríamos probar. □

Corolario 3.9.2. *Sea* $p(X) = a_nX^n + a_{n-1}X^{n-1} + \cdot + a_1X + a_0 \in \mathbb{C}[X]$, *donde* $n \geq 1, a_n \neq 0$. *Entonces existen* $z_1, \ldots, z_n \in \mathbb{C}$ *tales que* $p(X) = a_n(X - z_1) \cdots (X - z_n)$.

3.10. Teoría de Galois II

3.10.1. Permutaciones de las raíces

Sea $f(X) \in F[X]$ un polinomio de grado $n \geq 1$ separable (i.e., sin raíces múltiples). Sean $\alpha_1, \ldots, \alpha_n$ sus n raíces distintas en un cierre algebraico $\overline{F}$ de F y $E = F(\alpha_1, \ldots, \alpha_n)$ su cuerpo de descomposición sobre F. La extensión E/F es de Galois y hemos convenido en denotar $\mathrm{Gal}(f/F) = \mathrm{Gal}(E/F)$. Elegimos una ordenación $\alpha_1, \ldots, \alpha_n$ de las raíces. En $E[X]$, el polinomio factoriza $f(X) = c(X - \alpha_1) \cdots (X - \alpha_n)$, con $\alpha_1, \ldots, \alpha_n \in E$ distintos.

3.10.1. Sea $\sigma \in \mathrm{Gal}(f/F)$. Para cada raíz α_i de f, la imagen $\sigma(\alpha_i)$ es también una raíz $\alpha_{\sigma(i)}$ de f. Así, $\sigma : \{\alpha_1, \ldots, \alpha_n\} \to \{\alpha_1, \ldots, \alpha_n\}$ es una aplicación inyectiva de un conjunto de n elementos en el mismo conjunto. Por tanto, $\sigma : \{\alpha_1, \ldots, \alpha_n\} \to \{\alpha_1, \ldots, \alpha_n\}$ es una permutación de n elementos. Esto claramente define un homomorfismo de grupos

$$\mathrm{Gal}(f/F) \to S_n.$$

Además, este homomorfismo $\mathrm{Gal}(f/F) \to S_n$ es inyectivo, puesto que cada $\sigma \in \mathrm{Gal}(f/F)$ queda determinado por su acción en los generadores $\alpha_1, \ldots, \alpha_n$ de E sobre F.

Proposición 3.10.2. *Sea $f(X) \in F[X]$ un polinomio de grado $n \geq 1$ sin raíces múltiples.*

(1) El grupo $G = \mathrm{Gal}(f/F)$ es isomorfo a un subgrupo de S_n. En particular, $|G| \mid n!$

(2) El polinomio $f(X) \in F[X]$ es irreducible si, y sólo si, el subgrupo G de S_n es transitivo. En este caso: $n \mid |G|$.

Demostración. (2) $\Rightarrow$) Sean α_i, α_j dos raíces. Puesto que f es irreducible, el Teorema 3.1.17, asegura que existe un F–isomorfismo $F(\alpha_i) \xrightarrow{\sim} F(\alpha_j)$ que, por Teorema 3.2.5, se puede extender a un F–automorfismo de E. Esto implica que subgrupo imagen en S_n es transitivo.
$\Rightarrow$) Sea h un factor irreducible de f, vamos a probar que $\deg h \geq n = \deg f$ (esto implica que f es irreducible). En efecto, existe α_i tal que $h(\alpha_i) = 0$. La hipótesis asegura que para cada $j = 1, \ldots, n$ existe $\sigma_j \in G$ tal que $\sigma_j(\alpha_i) = \alpha_j$. Entonces $h(\alpha_j) = 0$, para cada $j = 1, \ldots, n$. Puesto que las raíces son distintas $\deg h \geq n$.
En este caso, $n = [F(\alpha_i) : F] \mid [E : F] = |G|$. □

Ejemplos 3.10.3. (1) Sea $f(X) \in F[X]$ separable e irreducible.

a) Si $\deg f = 2$, entonces $G \simeq S_2 \simeq \mathbb{Z}_2$.
Si $f(X) = X^2 + bX + c = (X - \alpha)(X - \beta)$, el discriminante es $b^2 - 4c = (\alpha - \beta)^2$.

b) Si $\deg f = 3$, entonces $3 \mid |G|$. Por tanto, $G = A_3 \simeq \mathbb{Z}_3$ o $G = S_3 \simeq D_3$.
Sea $f(X) = X^3 + bX^2 + cX + d = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$.
El discriminante

$$\Delta = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2,$$

que es una función simétrica en las raíces, está, por tanto, fijado por cada elemento de G. Así $\Delta \in F = \mathrm{Fix}(G)$. Más aun, el Teorema 3.10.12 garantiza que Δ se escribe, de modo único, como polinomio en las funciones simétricas elementales

$$s_1 = \alpha_1 + \alpha_2 + \alpha_3 = -b,\ s_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = c,\ s_3 = \alpha_1\alpha_2\alpha_3 = -d.$$

De hecho

$$\begin{aligned}\Delta &= (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2 = \\ &= b^2c^2 + 18bcd - 4c^3 - 4b^3d - 27d^2.\end{aligned}$$

Veremos que:

1) Si $\sqrt{\Delta} \in F$, entonces $E = F(\alpha)$, donde α es una raíz. Así E es de grado 3 sobre F y $G = A_3 =< (123) >=< (132) >\simeq \mathbb{Z}_3$.
   Por ejemplo, si $f(X) = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$, entonces $\Delta = 49$.
   Si α es una raíz, entonces $f(X) = (X-\alpha)(X-(\alpha^2-2))(X-(1-\alpha-\alpha^2))$. Numerando $\alpha_1 = \alpha, \alpha_2 = \alpha^2 - 2, \alpha_3 = 1 - \alpha - \alpha^2$, el grupo es $G = \{\sigma_1 = 1, \sigma_2, \sigma_3\}$, donde $\sigma_i(\alpha) = \alpha_i$. Entonces $\sigma_2 = (123), \sigma_3 = (132)$.
2) Si $\sqrt{\Delta} \notin F$, entonces $E = F(\alpha, \sqrt{\Delta})$ es de grado 6 sobre F y $G = S_3 \simeq D_3$.
   Por ejemplo, si $f(X) = X^3 - 2 \in \mathbb{Q}[X]$, entonces $\Delta = -27 \cdot 4$. Así $E = \mathbb{Q}(\alpha, \sqrt{\Delta}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$, donde $\omega^2 + \omega + 1 = 0$. El grupo $G =< \sigma, \tau >\simeq D_3$, con $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega, \sigma(\omega) = \omega$; $\tau(\sqrt[3]{2}) = \sqrt[3]{2}, \tau(\omega) = \omega^2$. Numerando las raíces $\alpha_1 = \sqrt[3]{2}, \alpha_2 = \sqrt[3]{2}\omega, \alpha_3 = \sqrt[3]{2}\omega^2$, el grupo $G =< \sigma, \tau >= S_3$, con $\sigma = (123), \tau = (23)$.

(2) Sea $f(X) = (X^2-2)(X^2-3) \in \mathbb{Q}[X]$. Entonces $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y $G = \{1, \sigma, \tau, \sigma\tau\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, donde $\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(\sqrt{3}) = \sqrt{3}$; $\tau(\sqrt{2}) = \sqrt{2}, \tau(\sqrt{3}) = -\sqrt{3}$. Numerando las raíces $\alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}, \alpha_3 = \sqrt{3}, \alpha_4 = -\sqrt{3}$, es $\sigma = (12), \tau = (34), \sigma\tau = (12)(34) \in S_4$ y $G = \{1, (12), (34), (12)(34)\} \leq S_4$.

Ecuación cúbica. Fórmulas de Cardano

3.10.4. Consideremos una ecuación cúbica $ax^3 + bx^2 + cx + d = 0$, con $0 \neq a \in F,\ b, c, d \in F$ (con $\mathbb{Q} \subset F$). Dividiendo por a, podemos suponer que la ecuación corresponde a las raíces de un polinomio cúbico mónico

$$x^3 + bx^2 + cx + d = 0, \qquad b, c, d \in F. \tag{3.10.4.1}$$

A continuación, el cambio de variable $x = y - b/3$ anula el coeficiente de x^2.

$$\begin{aligned}0 &= x^3 + bx^2 + cx + d \\ &= (y^3 - by^2 + \frac{b^2}{3}y - \frac{b^3}{27}) + b(y^2 - \frac{2b}{3}y + \frac{b^2}{9}) + c(y - \frac{b}{3}) + d \\ &= y^3 + (-\frac{b^2}{3} + c)y + (\frac{2b^3}{27} - \frac{bc}{3} + d).\end{aligned}$$

La ecuación cúbica resultante tiene la *forma reducida*

$$y^3 + py + q = 0, \tag{3.10.4.2}$$

where

$$p = -\frac{b^2}{3} + c,$$
$$q = \frac{2b^3}{27} - \frac{bc}{3} + d.$$

Si y_1, y_2, y_3 son las raíces de la cúbica reducida (3.10.4.2), entonces $y_1 - \frac{b}{3}, y_2 - \frac{b}{3}, y_3 - \frac{b}{3}$ son las raíces de (3.10.4.1).

Para resolver $y^3 + py + q = 0$, hacemos el cambio de variable

$$y = z - \frac{p}{3z}.$$

De forma equivalente, $3z^2 - 3yz - p = 0$. Esto es $z = \frac{y}{2} \pm \sqrt{(\frac{y}{2})^2 + \frac{p}{3}}$. Así $z = 0$ si, y sólo si, $p = 0$. En este caso, $y^3 + q = 0$ tiene por solución $y = \sqrt[3]{-q}, \sqrt[3]{-q}\omega, \sqrt[3]{-q}\omega^2$, con ω raíz cúbica primitiva de la unidad.

Con el cambio $y = z - \frac{p}{3z}$ obtenemos la ecuación

$$\begin{aligned} y^3 + py + q &= (z^3 - pz + \frac{p^2}{3z} - \frac{p^3}{27z^3}) + p(z - \frac{p}{3z}) + q \\ &= z^3 - \frac{p^3}{27z^3} + q. \end{aligned}$$

Por tanto, la ecuación (3.10.4.2) es equivalente a

$$z^6 + qz^3 - \frac{p^3}{27} = 0, \tag{3.10.4.3}$$

con $3z^2 - 3yz - p = 0$.

La ecuación (3.10.4.3) es la *resolvente cúbica* de la cúbica reducida $y^3 + py + q = 0$.

Las soluciones de la resolvente cúbica (3.10.4.3) son

$$z = \sqrt[3]{\frac{1}{2}\left(-q \pm \sqrt{q^2 + \frac{4p^3}{27}}\right)}.$$

Denotemos

$$\sqrt{q^2 + \frac{4p^3}{27}},$$

una elección de raíz cuadrada. Con esta elección, sea

$$z_1 = \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right)},$$

una raíz cúbica fijada. Obtenemos las otras dos raíces cúbicas multiplicando por las raíces cúbicas primitivas de la unidad ω, ω^2.

Denotemos

$$z_2 = -\frac{p}{3z_1}.$$

Entonces

$$y_1 = z_1 + z_2 = z_1 - \frac{p^3}{3z_1}$$

es una raíz de la cúbica reducida $y^3 + py + q$.

Para entender z_2, observemos que

$$z_1^3 z_2^3 = -\frac{p^3}{27} = z_1^3 \frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right).$$

Puesto que $z_1 \neq 0$, se deduce que z_2 es una raíz cúbica de $\frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)$, de forma que

(3.10.4.4) $$z_1 = \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right)}, \qquad z_2 = \sqrt[3]{\frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)},$$

son raíces cúbicas con la propiedad de que su producto es $-p/3$.

De (3.10.4), vemos que $y_1 = z_1 + z_2$ es una raíz de $y^3 + py + q$. Para obtener las otras raíces, observemos que (3.10.4) produce una raíz de la cúbica reducida, siempre que las raíces cúbicas se elijan de modo que su producto sea $-p/3$. Por tanto, si usamos la raíz cúbica ωz_1, entonces

$$\omega z_1 \cdot \omega^2 z_2 = -\frac{p}{3},$$

muestra que $y_2 = \omega z_1 + \omega^2 z_2$ es también una raíz. De forma similar, usando $\omega^2 z_1$ vemos que $y_3 = \omega^2 z_1 + \omega z_2$ es la tercera raíz de la cúbica reducida. Así, las tres soluciones de

$y^3 + py + q = 0$ son

$$y_1 = \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right)} + \sqrt[3]{\frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)}$$
$$y_2 = \omega\sqrt[3]{\frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right)} + \omega^2\sqrt[3]{\frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)}$$
$$y_3 = \omega^2\sqrt[3]{\frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right)} + \omega\sqrt[3]{\frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)},$$

siempre que las raíces cúbicas en (3.10.4.4) sean elegidas con producto igual a $-p/3$. estas son las *fórmulas de Cardano* para la cúbica reducida $y^3 + py + q = 0$.

Ejemplo 3.10.5. Para la cúbica reducida y^3+3y+1, consideramos las raíces cúbicas reales

$$\sqrt[3]{\frac{1}{2}\left(-1 + \sqrt{5}\right)}; \qquad \sqrt[3]{\frac{1}{2}\left(-1 - \sqrt{5}\right)}.$$

Su producto es $-1 = -p/3$, por tanto, las raíces de $y^3 + 3y + 1$ son

$$y_1 = \sqrt[3]{\frac{1}{2}\left(-1 + \sqrt{5}\right)} + \sqrt[3]{\frac{1}{2}\left(-1 - \sqrt{5}\right)}$$
$$y_2 = \omega\sqrt[3]{\frac{1}{2}\left(-1 + \sqrt{5}\right)} + \omega^2\sqrt[3]{\frac{1}{2}\left(-1 - \sqrt{5}\right)}$$
$$y_3 = \omega^2\sqrt[3]{\frac{1}{2}\left(-1 + \sqrt{5}\right)} + \omega\sqrt[3]{\frac{1}{2}\left(-1 - \sqrt{5}\right)}.$$

La raíz y_1 es real, las y_2, y_3 son complejos no reales conjugados.

Las soluciones de la cúbica $x^3 + bx^2 + cx + d = 0$, son

$$\begin{aligned} x_1 &= -\frac{b}{3} + z_1 + z_2, \\ x_2 &= -\frac{b}{3} + \omega z_1 + \omega^2 z_2, \\ x_3 &= -\frac{b}{3} + \omega^2 z_1 + \omega z_2, \end{aligned} \tag{3.10.5.1}$$

donde z_1, z_2 de (3.10.4.4), verifican $z_1 z_2 = -p/3$, y

$$p = -\frac{b^2}{3} + c,$$
$$q = \frac{2b^3}{27} - \frac{bc}{3} + d.$$

En la deducción de las fórmulas de Cardano henos supuesto que $p \neq 0$. Sin embargo, estas fórmulas proporcionan también las soluciones correctas si $p = 0$.

Ejemplo 3.10.6. La cúbica $y^3 - 3y = 0$ tiene raíces $y = 0, \pm\sqrt{3}$, todas reales. Si aplicamos las fórmulas de Cardano, comenzamos con

$$z_1 = \sqrt[3]{\frac{1}{2}\left(-0 + \sqrt{0^2 + \frac{4(-3)^3}{27}}\right)} = \sqrt[3]{i}.$$

Podemos elegir $z_1 = -i$. Así $z_2 = -p/3z_1 = i$. Por tanto, las fórmulas de Cardano proporcionan las raíces

$$\begin{aligned} y_1 &= -i + i = 0, \\ y_2 &= \omega(-i) + \omega^2(i) = \sqrt{3}, \\ y_3 &= \omega^2(-i) + \omega(i) = -\sqrt{3}. \end{aligned}$$

Permutaciones de las raíces

3.10.7. Podemos expresar z_1, z_2 en términos de x_1, x_2, x_3. De (3.10.5.1), obtenemos

$$x_1 + \omega^2 x_2 + \omega x_3 = -(1 + \omega^2 + \omega)\frac{b}{3} + 3z_1 + (1 + \omega + \omega^2)z_2 = 3z_1.$$

De forma similar obtenemos que las seis raíces $z_1, z_2, \omega z_1, \omega z_2, \omega^2 z_1, \omega^2 z_2$ de la resolvente (3.10.4.3) se expresan con las permutaciones de x_1, x_2, x_3 en la forma

$$\begin{aligned} z_1 &= \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3), \\ z_2 &= \frac{1}{3}(x_1 + \omega^2 x_3 + \omega x_2), \\ \omega z_1 &= \frac{1}{3}(x_2 + \omega^2 x_3 + \omega x_1), \\ \omega z_2 &= \frac{1}{3}(x_3 + \omega^2 x_2 + \omega x_1), \\ \omega^2 z_1 &= \frac{1}{3}(x_3 + \omega^2 x_1 + \omega x_2), \\ \omega^2 z_2 &= \frac{1}{3}(x_2 + \omega^2 x_1 + \omega x_3). \end{aligned} \tag{3.10.7.1}$$

Esto muestra cómo el grupo simétrico entra en juego en la ecuación cúbica general, y explica por qué el grado de la resolvente es 6.

El discriminante

3.10.8. Denotemos

$$D = q^2 + \frac{4p^3}{27}.$$

Entonces

$$z_1 = \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{D}\right)}, \qquad z_2 = \sqrt[3]{\frac{1}{2}\left(-q - \sqrt{D}\right)}.$$

Así,

$$z_1^3 - z_2^3 = \frac{1}{2}\left(-q + \sqrt{D}\right) - \frac{1}{2}\left(-q - \sqrt{D}\right) = \sqrt{D}.$$

Por otra parte,

$$z_1^3 - z_2^3 = (z_1 - z_2)(z_1 - \omega z_2)(z_1 - \omega^2 z_2). \tag{3.10.8.1}$$

Usando (3.10.7.1), obtenemos

$$\begin{aligned} z_1 - z_2 &= \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3) - \frac{1}{3}(x_1 + \omega^2 x_3 + \omega x_2) \\ &= \frac{1}{3}(\omega^2 - \omega)(x_2 - x_3) \\ &= \frac{-i}{\sqrt{3}}(x_2 - x_3) \qquad (3.10.8.2) \\ z_1 - \omega z_2 &= \frac{i\omega^2}{\sqrt{3}}(x_1 - x_3) \\ z_1 - \omega^2 z_2 &= \frac{-i\omega}{\sqrt{3}}(x_1 - x_2). \end{aligned}$$

Combinando (3.10.8.2), (3.10.8.1) y $z_1^3 - z_2^3 = \sqrt{D}$, obtenemos

$$\sqrt{D} = -\frac{i}{3\sqrt{3}}(x_1 - x_2)(x_1 - x_3)(x_2 - x_3).$$

De donde

$$\begin{aligned} \Delta &= (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 \\ &= \left(-\frac{3\sqrt{3}}{i}\sqrt{D}\right)^2 \\ &= -27D \\ &= -27\left(q^2 + \frac{4p^3}{27}\right) \\ &= -4p^3 - 27q^2 \\ &= b^2c^2 + 18bcd - 4c^3 - 4b^3d - 27d^2. \end{aligned}$$

El discriminante determina el número de raíces reales de un polinomio cúbico con coeficientes reales.

Teorema 3.10.9. *Supongamos que* $y^3 + py + q \in \mathbb{R}[y]$ *tiene discriminante* $\Delta \neq 0$. *Entonces:*

(1) $\Delta > 0$ *si, y sólo si, las raíces de* $y^3 + py + q = 0$ *son todas reales.*

(2) $\Delta < 0$ *si, y sólo si,* $y^3 + py + q = 0$ *tiene una única raíz real y las otras dos complejas no reales conjugadas.*

Demostración. Ver página 15 del libro de Cox, [Cox04]. □

El grupo de Galois de la extensión universal

Polinomios simétricos

Definición 3.10.10. Sea F un cuerpo. Diremos que $x_1, \ldots, x_n$, en algún anillo extensión de F, son algebraicamente independientes sobre F, o que son indeterminadas sobre F, si de cada relación

$$\sum_{i_1+\cdots+i_n \leq k} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n},$$

con $a_{i_1,\ldots,i_n} \in F$ y $k \geq 0$, se deduce que todo $a_{i_1,\ldots,i_n} = 0$.

Definición 3.10.11. Sean $x_1, \ldots, x_n$ indeterminadas sobre un cuerpo F. Un polinomio $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ se dice simétrico si $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n)$, para todo $\sigma \in S_n$. El conjunto $\mathscr{S}$ de los polinomios simétricos es un subanillo de $F[x_1, \ldots, x_n]$.

3.10.12 (Funciones simétricas elementales)**.** Los polinomios simétricos

$$\begin{aligned}
s_1 &= x_1 + \cdots + x_n \\
s_2 &= \sum_{1 \leq i < j \leq n} x_i x_j = x_1 x_2 + \cdots + x_{n-1} x_n \\
&\cdots \\
s_k &= \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} \cdots x_{i_k} \\
&\cdots \\
s_n &= x_1 \cdots x_n,
\end{aligned}$$

son las *funciones simétricas elementales*. El subanillo $F[s_1, \ldots, s_n] \subset \mathscr{S} \subset F[x_1, \ldots, x_n]$.

3.10.13. Sea $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in F[X]$, con factorización

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n = (X - \alpha_1) \cdots (X - \alpha_n),$$

en $E[X]$. Entonces

$$a_k = (-1)^k s_k(\alpha_1, \ldots, \alpha_n).$$

Teorema 3.10.14 (Teorema de las funciones simétricas elementales)**.** *Cada polinomio simétrico en n variables con coeficientes en F se escribe de modo* único *como polinomio en las $s_1, \ldots, s_n$ con coeficientes en F.*

Demostración. Ver página 30 y siguientes de [Cox04], o bien [DuFo04]. □

3.10.15. En otros términos, el Teorema 3.10.14 significa que el homomorfismo $F[x_1, \ldots, x_n] \to F[x_1, \ldots, x_n]$ tal que $x_i \mapsto s_i$, es inyectivo con imagen el subanillo de los polinomios simétricos.

En particular, si $x_1, \ldots, x_n$ son algebraicamente independientes sobre F, entonces los $s_1, \ldots, s_n$ son algebraicamente independientes sobre F. El recíproco es también cierto.

Ejemplos 3.10.16. (1) $(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = s_1^2 - 4s_2$.

(2) $(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 = s_1^2s_2^2 + 18s_1s_2s_3 - 4s_2^3 - 4s_1^3s_3 - 27s_3^2$.

(3) $x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = s_1^2 - 2s_2$.

(4) $x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = s_2^2 - 2s_1s_3$.

(5) $\sum_4 x_1^3x_2^2x_3 := \sum_{\sigma \in S_4} x_{\sigma(1)}^3 x_{\sigma(2)}^2 x_{\sigma(3)}^1 x_{\sigma(4)}^0 = x_1^3x_2^2x_3^1x_4^0 + x_1^3x_2^2x_4^1x_3^0 + x_1^3x_3^2x_2^1x_4^0 + \cdots = s_1s_2s_3 - 3s_1^2s_4 - 3s_3^2 + 4s_2s_4$.

El discriminante

3.10.17. Sean $n \geq 2$ y $x_1, \ldots, x_n$ indeterminadas sobre F. El discriminante

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 = (-1)^{\frac{1}{2}n(n-1)} \prod_{1 \leq i \neq j \leq n} (x_i - x_j) \in F[x_1, \ldots, x_n]$$

es simétrico en $x_1, \ldots, x_n$. Por tanto, según Teorema 3.10.14,

$$\Delta \in F[s_1, \ldots, s_n].$$

Para $n = 3$ conocemos la fórmula

$$\Delta = -4s_2^3 - 27s_3^2 + s_1^2s_2^2 - 4s_1^3s_3 + 18s_1s_2s_3. \tag{3.10.17.1}$$

Una fórmula general para Δ en función de $s_1, \ldots, s_n$ viene expresada por

$$\Delta = (-1)^{n(n-1)/2} \det(M),$$

donde M es la siguiente $(2n-1)\times(2n-1)$ matriz (ver [Cox04] o [DuFo04]):

$$\begin{pmatrix}
1 & & & & n & & & \\
-s_1 & 1 & & & -(n-1)s_1 & n & & \\
s_2 & -s_1 & \ddots & 1 & (n-2)s_2 & -(n-1)s_1 & \ddots & \\
\vdots & s_2 & \ddots & -s_1 & \vdots & (n-2)s_2 & \ddots & n \\
\vdots & \vdots & \ddots & s_2 & \vdots & \vdots & \ddots & -(n-1)s_1 \\
(-1)^{n-1}s_{n-1} & \vdots & & \vdots & (-1)^{n-1}s_{n-1} & \vdots & & (n-2)s_2 \\
(-1)^n s_n & (-1)^{n-1}s_{n-1} & & \vdots & & (-1)^{n-1}s_{n-1} & & \vdots \\
 & (-1)^n s_n & \ddots & (-1)^{n-1}s_{n-1} & & & \ddots & \vdots \\
 & & \ddots & (-1)^n s_n & & & & (-1)^{n-1}s_{n-1}
\end{pmatrix},$$

cuyos puntos suspensivos significan $n-1$ columnas en el bloque de la izquierda y n columnas en el bloque de la derecha.

La definición muestra que Δ tiene una raíz cuadrada en $F[x_1,\dots,x_n]$. Definimos

$$\sqrt{\Delta} = \prod_{1\le i<j\le n}(x_i - x_j) = \det\begin{pmatrix}
x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \\
x_1^{n-2} & x_2^{n-2} & \cdots & x_n^{n-2} \\
\vdots & \vdots & \ddots & \vdots \\
x_1 & x_2 & \cdots & x_n \\
1 & 1 & \cdots & 1
\end{pmatrix}.$$

Proposición 3.10.18. *Sea $\sigma \in S_n$. Entonces*

$$\sigma\cdot\sqrt{\Delta} = \operatorname{sgn}(\sigma)\ \sqrt{\Delta}, \tag{3.10.18.1}$$

donde $\operatorname{sgn}(\sigma)$ *es* ± 1*, según σ sea par o impar y $\sigma\cdot\sqrt{\Delta}$ es el polinomio obtenido de $\sqrt{\Delta}$ permutando las variables $x_1,\dots,x_n$ según σ.*

3.10.19. Sea $f = X^n + a_1X^{n-1} + \cdots + a_iX^{n-i} + \cdots + a_n \in F[X]$ un polinomio mónico de grado $n \ge 2$ que factoriza $f = (X-\alpha_1)\cdots(X-\alpha_n)$ en un cuerpo de descomposición E. El discriminante de f es

$$\Delta(f) = \prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2 = \Delta(-a_1,\dots,(-1)^i a_i,\dots,(-1)^n a_n) \in F.$$

3.10.20. El polinomio f no tiene raíces múltiples si, y sólo si, $\Delta(f)\neq 0$. Definimos

$$\sqrt{\Delta(f)} = \prod_{1\le i<j\le n}(\alpha_i-\alpha_j) \in E.$$

Observemos que la raíz cuadrada elegida depende de la numeración de las raíces fijada.

Si $\Delta(f) \neq 0$, sabemos que $\mathrm{Gal}(f/F)$ se identifica con un subgrupo de S_n. La relación entre $A_n \subset S_n$ y $\mathrm{Gal}(f/F)$ está controlada por $\sqrt{\Delta(f)}$.

Teorema 3.10.21. *Sean F de característica $\neq 2$ y $f \in F[X]$ un polinomio mónico de grado $n \geq 2$ con $\Delta(f) \neq 0$.*

(1) Si $\sigma \in \mathrm{Gal}(f/F) \subset S_n$, entonces

$$\sigma(\sqrt{\Delta(f)}) = \mathrm{sgn}(\sigma)\sqrt{\Delta(f)}. \tag{3.10.21.1}$$

(2) La imagen de $\mathrm{Gal}(f/F)$ está contenida en A_n si, y sólo si, $\sqrt{\Delta(f)} \in F$.

Demostración. (1) La propiedad (3.10.21.1) se obtiene de (3.10.18.1) evaluando $x_i \mapsto \alpha_i$.
(2) La extensión E/F es de Galois. Es decir, $F = \mathrm{Fix}(\mathrm{Gal}(f/F)$. Así

$$\begin{aligned}\sqrt{\Delta(f)} \in F &\Leftrightarrow \sigma(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)} \text{ para todo } \sigma \in \mathrm{Gal}(f/F)\\ &\Leftrightarrow \mathrm{sgn}(\sigma)\sqrt{\Delta(f)} = \sqrt{\Delta(f)} \text{ para todo}\end{aligned}$$

Puesto que $\Delta(f) \neq 0$ y la característica de F es $\neq 2$, la última condición es equivalente a $\mathrm{sgn}(\sigma) = 1$ para todo $\sigma \in \mathrm{Gal}(f/F)$. Esto es si, y sólo si, $\mathrm{Gal}(f/F) \subset A_n$. □

Teorema 3.10.22. *Sea $f \in F[X]$ un polinomio mónico irreducible separable cúbico, donde la característica de F es $\neq 2$. Sean E el cuerpo de descomposición de f sobre F y $\alpha \in E$ una raíz de f. Entonces $\Delta(f) \neq 0$ y*

(1) $E = F(\alpha)$ y $\mathrm{Gal}(f/F) = A_3 \simeq \mathbb{Z}_3$, si $\sqrt{\Delta(f)} \in F$.

(2) $E = F(\alpha, \sqrt{\Delta(f)})$ y $\mathrm{Gal}(f/F) = S_3$, en otro caso.

Demostración. El orden $|\mathrm{Gal}(f/F)|$ es divisible por 3. Por tanto, $\mathrm{Gal}(f/F) = A_3$ o S_3.
De Teorema 3.10.21 (2), se deduce que $\mathrm{Gal}(f/F) = A_3$ si, y sólo si, $\sqrt{\Delta(f)} \in F$. En este caso, $[E : F] = 3$. De donde $E = F(\alpha)$.
Si $\sqrt{\Delta(f)} \notin F$, entonces $[E : F] = 6 = [F(\alpha, \sqrt{\Delta(f)}) : F]$. Así $E = F(\alpha, \sqrt{\Delta(f)})$. □

Ejemplo 3.10.23. Consideremos $f = X^3+X^2-2X-1 \in \mathbb{Q}[X]$. Este polinomio es irreducible sobre $\mathbb{Q}$, puesto que no tiene raíces en $\mathbb{Q}$ y es de grado 3. El discriminante es $\Delta(f) = 49 = 7^2$.

La extensión universal

Definición 3.10.24. El polinomio universal de grado n en $F(s_1, \ldots, s_n)[X]$ es

$$f(X) = (X - x_1)\cdots(X - x_n) = X^n - s_1X^{n-1} + \cdots + (-1)^{n-1}s_{n-1}X + (-1)^n s_n.$$

Teorema 3.10.25. *La extensión $F(x_1,\dots,x_n)/F(s_1,\dots,s_n)$ es el cuerpo del polinomio separable universal de grado n*

$$f(X) = (X-x_1)\cdots(X-x_n) = X^n - s_1X^{n-1} + \cdots + (-1)^{n-1}s_{n-1}X + (-1)^n s_n.$$

La acción del grupo de Galois de la extensión en las raíces del polinomio define un isomorfismo

$$\mathrm{Gal}(F(x_1,\dots,x_n)/F(s_1,\dots,s_n)) = S_n.$$

En particular, el grado $[F(x_1,\dots,x_n) : F(s_1,\dots,s_n)] = n!$.

Demostración. El polinomio es separable puesto que sus raíces $x_1,\dots,x_n$ son distintas. Por tanto, la extensión es de Galois. Además, según 3.10.1, hay un homomorfismo inyectivo $G \hookrightarrow S_n$. Hemos de probar que este homomorfismo es sobreyectivo. En efecto, cada $\tau \in S_n$ define un automorfismo $F[x_1,\dots,x_n] \to F[x_1,\dots,x_n]$ tal que $x_i \mapsto x_{\tau(i)}$. Este automorfismo extiende de manera única a un automorfismo de $F(x_1,\dots,x_n)$ que, claramente, es la identidad en $F(s_1,\dots,s_n)$. □

Definición 3.10.26. *Diremos que $F(x_1,\dots,x_n)/F(s_1,\dots,s_n)$ es la extensión universal de Galois.*

Teorema 3.10.27. *Sea $m \in F(x_1,\dots,x_n)$.*

(1) m es simétrica (i.e., invariante por S_n) si, y sólo si, $m \in F(s_1,\dots,s_n)$.

(2) Supongamos que F es de característica $\neq 2$. Entonces m es invariante por A_n si, y sólo si, $m \in F(s_1,\dots,s_n)(\sqrt{\Delta})$, i.e., si, y sólo si, existen $A, B \in F(s_1,\dots,s_n)$ tales que

$$m = A + B\sqrt{\Delta}.$$

Además, si $m \in F[x_1,\dots,x_n]$, entonces $A, B \in F[s_1,\dots,s_n]$.

Demostración. (1) Según el Teorema 3.10.25, una función racional m en las variables $x_1,\dots,x_n$ es invariante por S_n si, y sólo si, m queda fijada por cada automorfismo de la extensión universal de Galois. Por tanto, si, y sólo si, m está en el cuerpo fijo de la extensión, i.e., $m \in F(s_1,\dots,s_n)$.

(2) Sea $K = \mathrm{Fix}(A_n) \subset F(x_1,\dots,x_n)$. Puesto que A_n es de índice 2 en S_n, el Teorema Fundamental dice que $K/F(s_1,\dots,s_n)$ es una extensión de grado 2. Por otra parte, (3.10.18) muestra que $\sqrt{\Delta} \in K$ y, puesto que la característica $\neq 2$, también muestra que $\sqrt{\Delta} \notin F(s_1,\dots,s_n)$. Por tanto, $K = F(s_1,\dots,x_n)(\sqrt{\Delta})$. □

Ejemplo 3.10.28. El polinomio $f(X) = X^5 - 6X + 3 \in \mathbb{Q}[X]$ tiene grupo de Galois G isomorfo a S_5. En efecto, f es irreducible por Eisenstein. Por tanto, G es un subgrupo de S_5 cuyo orden $|G|$ es divisible por 5. Así G contiene un elemento de orden 5 que, en S_5, ha de ser un 5–ciclo σ. Es elemental comprobar que f tiene exactamente 3 raíces reales $\alpha_1, \alpha_2, \alpha_3$ y, por tanto, 2 raíces complejas no reales conjugadas $\alpha_4, \alpha_5 = \overline{\alpha_4}$. Así, la conjugación compleja define una trasposición $\tau \in G \leq S_5$. Renumerando las raíces, podemos suponer que $\sigma = (12345), \tau = (12)$. Es un resultado clásico que estas dos permutaciones generan S_5.

3.10.2. Extensiones radicales y extensiones resolubles

3.10.29. Recordemos las fórmulas de Cardano para las raíces de la cúbica reducida $X^3 + pX + q = 0$, donde $p, q \in \mathbb{Q}$.

$$
\begin{aligned}
x_1 &= \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right)} + \sqrt[3]{\frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)} \\
x_2 &= \omega\sqrt[3]{\frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right)} + \omega^2\sqrt[3]{\frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)} \\
x_3 &= \omega^2\sqrt[3]{\frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right)} + \omega\sqrt[3]{\frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)}.
\end{aligned}
\tag{3.10.29.1}
$$

Denotemos

$$D = q^2 + \frac{4p^3}{27}, \quad u_1 = \frac{1}{2}\left(-q + \sqrt{D}\right) \quad u_2 = \frac{1}{2}\left(-q - \sqrt{D}\right).$$

Consideremos la serie de extensiones

$$
\begin{aligned}
F_0 = \mathbb{Q} \subset F_1 = F_0(\omega) = F_0(\sqrt{-3}) \subset F_2 = \mathbb{Q}(\sqrt{-3}, \sqrt{D}) = F_1(\sqrt{D}) \subset \\
\subset F_3 = \mathbb{Q}(\sqrt{-3}, \sqrt{D}, \sqrt[3]{u_1}) = F_2(\sqrt[3]{u_1}) \subset F_4 = F(\sqrt{-3}, \sqrt{D}, \sqrt[3]{u_1}, \sqrt[3]{u_2}) = F_3(\sqrt[3]{u_2}) = L,
\end{aligned}
$$

donde $(\sqrt{-3})^2 \in F_0$, $(\sqrt{D})^2 \in F_1$, $(\sqrt[3]{u_1})^3 \in F_2$, $(\sqrt[3]{u_2})^3 \in F_3$. Diremos que L es una extensión radical de F.

Sea E el cuerpo de descomposición de $X^3 + pX + q$ sobre $\mathbb{Q}$. Las fórmulas (3.10.29.1) muestran que $E \subset L$. Esto es, las raíces de $X^3 + pX + q = 0$ están en L. Esto corresponde al hecho de que estas raíces se expresan con fórmulas con radicales encajados a partir de los coeficientes de la ecuación. En otras palabras, diremos que las raíces de la ecuación $X^3 + pX + q = 0$ son *expresables por radicales*, o que el polinomio $X^3 + pX^2 + q$ es *resoluble por radicales*.

Definición 3.10.30. Diremos que la extensión L/F es radical si existe una serie de extensiones

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = L, \tag{3.10.30.1}$$

donde para $i = 1, \ldots, n$ existe $\gamma_i \in F_i$ tal que $F_i = F_{i-1}(\gamma_i)$ y $\gamma_i^{m_i} \in F_{i-1}$, $m_i > 0$. Escribiremos $F_i = F_{i-1}(\sqrt[m_i]{b_i})$, con $b_i = \gamma_i^{m_i} \in F_{i-1}$, $m_i > 0$.

Es decir, una extensión radical se obtiene por sucesivas adjunciones de radicales.

Ejemplos 3.10.31. (1) $\mathbb{Q} \subset \mathbb{Q}(\gamma_1 = \sqrt{2}) \subset \mathbb{Q}(\gamma_1)(\gamma_2 = \sqrt{2 + \sqrt{2}})$.

(2) El polinomio irreducible $f = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$ tiene discriminante $\Delta(f) = 49 = 7^2 > 0$. Por tanto, las tres raíces son reales y el cuerpo de descomposición $E = \mathbb{Q}(\alpha) \subset \mathbb{R}$, donde α es una raíz. El polinomio factoriza

$$f(X) = (X - \alpha)(X - (\alpha^2 - 2))(X - (-\alpha^2 - \alpha + 1)).$$

La extensión $E/\mathbb{Q}$ no es radical. En efecto, si lo fuera, puesto que $[E : \mathbb{Q}] = 3$, se tendría $E = \mathbb{Q}(\gamma)$ con $\gamma^m \in \mathbb{Q}$ y $m \geq 3$. Entonces el polinomio mínimo g de γ sobre $\mathbb{Q}$ es de grado 3 y divide a $X^m - \gamma^m$. Puesto que $E/\mathbb{Q}$ es de Galois, el polinomio g se descompone en producto de factores lineales en $E = \mathbb{Q}(\gamma)$. Así $\gamma, \zeta\gamma, \ldots, \zeta^{m-1}\gamma \in E$, con $\zeta = e^{2\pi i/m}$. Esto es imposible puesto que $\zeta \in \mathbb{R}$ si, y sólo si, $\zeta = \pm 1$.

Esto sugiere la siguiente definición.

Definición 3.10.32. Diremos que la extensión E/F es resoluble (o resoluble por radicales) si existe una extensión radical L/F tal que $E \subset L$.

Compuestos y clausura de Galois

Definición 3.10.33. Sean $K_1, K_2 \subset L$ subcuerpos. El subcuerpo compuesto $K_1K_2 \subset L$ es el menor subcuerpo de L que contiene a K_1 y K_2.
Si $F \subset L$ y $K_1 = F(\alpha_1, \ldots, \alpha_n)$, $K_2 = F(\beta_1, \ldots, \beta_m)$, entonces $K_1K_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$.

Proposición–Definición 3.10.34. *Sea L/F una extensión finita separable. Existe una extensión $L \subset K$ tal que:*

(1) K/F es de Galois.

(2) Si $L \subset K'$ y K'/F es de Galois, entonces existe una inmersión $K \xrightarrow{\varphi} K'$ que es la identidad en L.

Diremos que K/F es el cierre o clausura de Galois de L/F. Es decir, la extensión K/F es la "menor" extensión de L que es de Galois sobre F.

Demostración. (1) Sean $L = F(\alpha_1, \ldots, \alpha_n)$ y $p(X)$ el producto de los polinomios no repetidos entre los polinomios mínimos de los $\alpha_1, \ldots, \alpha_n$ sobre F. Tomamos K un cuerpo de descomposición de $p(X)$ sobre F. Entonces $F \subset K$ y cada $\alpha_i \in K$. Por tanto, $L \subset K$ y K/F es de Galois.
Si K'/F es de Galois el polinomio $p(X)$ es producto de factores lineales en $K'[X]$. Por tanto, K' contiene un cuerpo K'' de descomposición de $p(X)$ sobre F. Puesto que todo $\alpha_i \in K''$ es $L \subset K''$.
Ambos K y K'' son también cuerpos de descomposición de $p(X)$ sobre L. Por tanto, la unicidad del cuerpo de descomposición afirma que existe un isomorfismo $K \to K''$ que es la identidad en L. Este isomorfismo es una inmersión $K \to K'$ que es la identidad en L. □

Proposición 3.10.35. *Sean $F \subset L \subset M$, donde M/F es de Galois. Entonces el compuesto de todos los subcuerpos de M conjugados de L es la clausura de Galois de L/F.*

Demostración. Sea $G = \mathrm{Gal}(M/F) = \{1 = \sigma_1, \ldots, \sigma_r\}$. Los subcuerpos $L_i = \sigma_i(L)$ son los subcuerpos conjugados de L. Puesto que M/F es finita y separable, también L/F es finita y separable. Así, por Teorema 3.5.2, $L = F(\alpha)$, para cierto $\alpha \in L$. Entonces $L_i = \sigma_i(L) = F(\alpha_i)$, donde $\alpha_i = \sigma_i(\alpha)$. El compuesto $K = L_1 \cdots L_r = F(\alpha_1, \ldots, \alpha_r)$ es de Galois sobre F, puesto que $m_{\alpha,F}(X) = (X - \alpha_1) \cdots (X - \alpha_r) \in M[X]$ es el polinomio mínimo de $\alpha = \alpha_1$ sobre F. Es claro que $L \subset K$ y, razonando como antes vemos que K/F es la clausura de Galois de L/F. □

Propiedades de las extensiones radicales y resolubles

Lema 3.10.36. *(1) Si K/L y L/F son extensiones radicales, entonces K/F es radical.*

(2) Sean $F \subset K_1 \subset L$ y $F \subset K_2 \subset L$. Si K_1/F es radical, entonces K_1K_2/K_2 es radical.

(3) Sean $F \subset K_1 \subset L$ y $F \subset K_2 \subset L$. Si K_1/F y K_2/F son radicales, entonces K_1K_2/F es radical.

Demostración. (1) Se tiene

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = L,$$

donde $F_i = F_{i-1}(\sqrt[m_i]{b_i})$, con $b_i \in F_{i-1},\ m_i > 0,\ i = 1, \ldots, n$,

$$L = L_0 \subset L_1 \subset \cdots \subset L_{r-1} \subset L_r = K,$$

donde $L_j = L_{j-1}(\sqrt[n_j]{a_j})$, con $a_j \in L_{j-1},\ n_j > 0,\ j = 1, \ldots, r$.
Entonces

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = L = L_0 \subset L_1 \subset \cdots \subset L_{r-1} \subset L_r = K$$

es una serie que muestra que K/F es radical.

(2) Se tiene

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = K_1,$$

donde $F_i = F_{i-1}(\sqrt[m_i]{b_i})$, con $b_i \in F_{i-1},\ m_i > 0,\ i = 1, \ldots, n$
Entonces la serie de extensiones

$$K_2 = F_0K_2 = F_0' \subset F_1' = F_1K_2 = F_0(\sqrt[m_1]{b_1})K_2 = F_0K_2(\sqrt[m_1]{b_1}) = F_0'(\sqrt[m_1]{b_1}),\ b_1 \in F_0 \subset F_0',$$

$$F_1' = F_1K_2 \subset F_2' = F_2K_2 = F_1(\sqrt[m_2]{b_2})K_2 = F_1K_2(\sqrt[m_2]{b_2}) = F_1'(\sqrt[m_2]{b_2}),\ b_2 \in F_1 \subset F_1',$$

$$\vdots$$

$$F_{i-1}' = F_{i-1}K_2 \subset F_i' = F_iK_2 = F_{i-1}(\sqrt[m_i]{b_i})K_2 = F_{i-1}K_2(\sqrt[m_i]{b_i}) = F_{i-1}'(\sqrt[m_i]{b_i}),\ b_i \in F_{i-1} \subset F_{i-1}',$$

$$\vdots$$

$$F'_{n-1} = F_{n-1}K_2 \subset F'_n = F_nK_2 = K_1K_2 = F_{n-1}(\sqrt[m_n]{b_n})K_2 = F_{n-1}K_2(\sqrt[m_n]{b_n}) = F'_{n-1}(\sqrt[m_n]{b_n}),$$
$$b_n \in F_{n-1} \subset F'_{n-1},$$

muestra que K_1K_2/K_2 es radical.

(3) Según (2), la extensión K_1K_2/K_2 es radical. Ahora se aplica (1). □

Lema 3.10.37. *Sea $F \subset L \subset K$ extensión finita. Si L/F es radical y $\sigma \in \mathrm{Aut}(K/F)$, entonces $\sigma(L)/F$ es radical.*

Demostración. Se tiene

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = L,$$

donde $F_i = F_{i-1}(\gamma_i)$, con $\gamma_i^{m_i} \in F_{i-1},\ m_i > 0,\ i = 1, \ldots, n$.

Entonces la serie

$$F = \sigma(F) = \sigma(F_0) \subset \sigma(F_1) \subset \cdots \subset \sigma(F_{n-1}) \subset \sigma(F_n) = \sigma(L),$$

donde $\sigma(F_i) = \sigma(F_{i-1})(\sigma(\gamma_i))$, con $\sigma(\gamma_i)^{m_i} = \sigma(\gamma_i^{m_i}) \in \sigma(F_{i-1}),\ m_i > 0,\ i = 1, \ldots, n$, muestra que $\sigma(L)/F$ es radical. □

Teorema 3.10.38. *Si L/F es finita separable y radical, entonces su clausura de Galois es también radical.*

Demostración. Sea M/F de Galois tal que $L \subset M$. Para cada $\sigma \in \mathrm{Gal}(M/F)$, es $F \subset \sigma(L) \subset M$ y, según Lema 3.10.37, L/F radical implica que $\sigma(L)/F$ es radical. Si $\mathrm{Gal}(M/F) = \{\sigma_1, \ldots, \sigma_r\}$, entonces la clausura de Galois de L/F es $\sigma_1(L) \cdots \sigma_r(L)$, que es compuesto de extensiones radicales y, por tanto, radical. □

Corolario 3.10.39. *Si E/F es finita y resoluble, donde F es un cuerpo perfecto (e.g. de característica cero), entonces su clausura de Galois es resoluble.*

Demostración. Por definición de resoluble, existe $F \subset E \subset L$, tal que L/F es radical.

Por otra parte, L/F es separable, puesto que suponemos F perfecto. Por tanto, L/F tiene una clausura de Galois $F \subset L \subset M$. Entonces, según Teorema 3.10.38, M/F es radical.

Ahora consideramos $F \subset E \subset M$. Puesto que M/F es de Galois, contiene la clausura de Galois K de E/F. Por tanto, K está contenido en la extensión radical M, de forma que K/F es resoluble, según la definición. □

3.10.3. Extensiones resolubles y grupos resolubles

A partir de ahora suponemos, para simplificar, que la característica de F es 0, o bien que, de ser positiva, la característica de F no divide al índice m de cualquiera de los radicales que aparezcan. Convenimos que la expresión: "sea m un entero que no divide a la característica de F", incluye las dos opciones: F de característica 0, o F de característica positiva que no divide a m.

Raíces de la unidad y resolventes de Lagrange

Consideremos una extensión radical simple $F(\sqrt[m]{b})$, donde $0 \neq b \in F$. Si añadimos una raíz primitiva m–ésima ζ de la unidad, la extensión $F(\sqrt[m]{b}, \zeta)/F$ es de Galois, puesto que es el cuerpo de descomposición sobre F del polinomio separable $X^m - b$. En efecto, el polinomio derivado mX^{m-1} tiene 0 como única raíz, que no es raíz de $X^m - b$, si suponemos $b \neq 0$. En consecuencia, las m raíces $\sqrt[m]{b}\zeta^j,\ j = 0, \ldots, m-1$ de $X^m - b$ son todas distintas, y este polinomio es separable.

En particular, la extensión $F(\zeta)/F$, donde ζ es una raíz primitiva m–ésima de la unidad (i.e., un generador del grupo cíclico formado por las raíces m–ésimas de 1), es una extensión de Galois.

En característica cero, como consecuencia inmediata del Teorema 3.7.11, obtenemos:

Proposición 3.10.40. *Sea ζ una raíz primitiva m–ésima de la unidad sobre $\mathbb{Q}$. La extensión ciclotómica $\mathbb{Q}(\zeta)/\mathbb{Q}$ tiene grupo de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$, isomorfo al grupo conmutativo de las unidades del anillo $\mathbb{Z}/m\mathbb{Z}$. En particular, si m es primo el grupo $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ es cíclico.*

Demostración. El Teorema 3.7.11, dice que los $\mathbb{Q}$–conjugados de ζ son los ζ^a, donde $1 \leq a < m,$ y $\mathrm{mcd}(a, m) = 1$. Por tanto, un automorfismo $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ está determinado por $\sigma(\zeta) = \zeta^a$, para un único $1 \leq a < m,$ con $\mathrm{mcd}(a, m) = 1$. Por otra parte, $(\mathbb{Z}/m\mathbb{Z})^* = \{\bar{a} \mid 1 \leq a < m,$ y $\mathrm{mcd}(a, m) = 1\}$. El isomorfismo está definido por $\sigma \mapsto \bar{a}$. □

En general, podemos asegurar algo más débil.

Proposición 3.10.41. *Sean m un entero positivo que no divide a la característica de F y ζ una raíz primitiva m–ésima sobre F. La extensión $F(\zeta)/F$ es de Galois con grupo de Galois $\mathrm{Gal}(F(\zeta)/F)$ conmutativo.*

Demostración. Cada automorfismo $\sigma \in \mathrm{Gal}(F(\zeta)/F)$ está determinado por $\sigma(\zeta)$ que ha de ser ζ^{i_σ}, para algún $1 \leq i_\sigma \leq m-1$, puesto que el polinomio mínimo de ζ sobre F es un divisor de $X^m - 1$, y las raíces de $X^m - 1$ son los $\zeta^i, 0 \leq 1 \leq m-1$.

Sean $\sigma, \tau \in \mathrm{Gal}(F(\zeta)/F)$ con $\sigma(\zeta) = \zeta^{i_\sigma}, \tau(\zeta) = \zeta^{i_\tau}$. Entonces $\sigma\tau(\zeta) = \sigma(\zeta^{i_\tau}) = (\sigma(\zeta))^{i_\tau} = (\zeta^{i_\sigma})^{i_\tau} = (\zeta^{i_\tau})^{i_\sigma} = (\tau(\zeta))^{i_\sigma} = \tau(\zeta^{i_\sigma}) = \tau\sigma(\zeta)$. Esto es, $\sigma\tau = \tau\sigma$. □

La cuestión que tratamos de responder es, cómo caracterizar la resolubilidad de una extensión finita de Galois L/F en términos de su grupo de Galois $G = \mathrm{Gal}(L/F)$.

Lema 3.10.42. *Sea F un cuerpo de característica nula o característica positiva que no divide a m. Sean L/F finita de Galois y ζ una raíz primitiva m-ésima de la unidad. Entonces $L(\zeta)/F$ y $L(\zeta)/F(\zeta)$ son finitas de Galois, y son equivalentes*

(1) $\mathrm{Gal}(L/F)$ *es resoluble,*

(2) $\mathrm{Gal}(L(\zeta)/F)$ *es resoluble,*

(3) $\mathrm{Gal}(L(\zeta)/F(\zeta))$ *es resoluble.*

Demostración. La extensión L/F es Galois. Por tanto, L es el cuerpo de descomposición sobre F de cierto polinomio (separable) $f(X) \in F[X]$. Por otra parte, $F(\zeta)$ es el cuerpo de descomposición sobre F del polinomio (separable) $X^m - 1$. En consecuencia, $L(\zeta)$ es el cuerpo de descomposición sobre F del polinomio producto de los factores irreducibles no repetidos de $(X^n-1)f(X) \in F[X]$. Esto significa que $L(\zeta)/F$ es Galois. Ahora $F \subset F(\zeta) \subset L(\zeta)$, y $L(\zeta)/F$ es Galois, por tanto, $L(\zeta)/F(\zeta)$ es Galois.

(1) $\Leftrightarrow$ (2) Puesto que $L(\zeta)/L$ y L/F son ambas Galois, el Teorema Fundamental dice que $\mathrm{Gal}(L(\zeta)/L) \trianglelefteq \mathrm{Gal}(L(\zeta)/F)$ y

$$\mathrm{Gal}(L/F) \simeq \mathrm{Gal}(L(\zeta)/F)/\mathrm{Gal}(L(\zeta)/L).$$

Ahora bien $\mathrm{Gal}(L(\zeta)/L)$ es resoluble, puesto que es conmutativo. De aquí, usando Teorema 2.6.14, obtenemos la equivalencia de (1) y (2).

(2) $\Leftrightarrow$ (3) Consideramos $F \subset F(\zeta) \subset L(\zeta)$. Ahora $\mathrm{Gal}(L(\zeta)/F(\zeta)) \trianglelefteq \mathrm{Gal}(L(\zeta)/F)$ y

$$\mathrm{Gal}(F(\zeta)/F) \simeq \mathrm{Gal}(L(\zeta)/F)/\mathrm{Gal}(L(\zeta)/F(\zeta)).$$

Aquí, $\mathrm{Gal}(F(\zeta)/F)$ es resoluble, puesto que es conmutativo. En consecuencia, usando Teorema 2.6.14, se obtiene la equivalencia de (2) y (3). □

Extensiones cíclicas

Definición 3.10.43. *Una extensión K/F se dice cíclica si es de Galois y su grupo de Galois es un grupo cíclico.*

Lema 3.10.44. *Sean p un número primo y K un cuerpo cuya característica no divide a p, que contiene a una raíz primitiva p–ésima de la unidad $\zeta \in K$. Sea $a \in K$. Supongamos que $X^p - a \in K[X]$ es irreducible sobre K. Entonces $M = K(\sqrt[p]{a})$ es el cuerpo de descomposición sobre K de $X^p - a$ y $\mathrm{Gal}(M/K) =< \sigma >$ es cíclico de orden p generado por σ tal que $\sigma(\sqrt[p]{a}) = \sqrt[p]{a}\zeta$.*

Demostración. Puesto que $X^p - a$ es irreducible sobre K los conjugados de $\sqrt[p]{a}$ son los $\sqrt[p]{a}\zeta^j$, con $0 \leq j \leq p-1$. La hipótesis dice que $\zeta^j \in K$, para todo j. Por tanto $M = K(\sqrt[p]{a}, \zeta) = K(\sqrt[p]{a})$ es de Galois sobre K, de grado p y los elementos σ_j de $\mathrm{Gal}(M/K)$ están determinados por $\sigma_j(\sqrt[p]{a}) = \sqrt[p]{a}\zeta^j$ para $0 \leq j \leq p-1$. Es claro que $\sigma_j = (\sigma)^j$. □

Ejemplo 3.10.45. Sean ζ una raíz primitiva 5–ésima, $K = \mathbb{Q}(\zeta)$ y $M = K(\sqrt[5]{3})$. Entonces $X^5 - 3$ es irreducible sobre $\mathbb{Q}(\zeta)$. Así, el grupo $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[5]{3}, \zeta)/\mathbb{Q})$ tiene orden 20. El subgrupo $\mathbb{Z}_5 = \mathrm{Gal}(M/K)$ es normal en G y $G/\mathbb{Z}_5 \simeq \mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}_4$.

El recíproco del Lema anterior, cuya demostración usa una ingeniosa idea debida a Lagrange, será uno de los puntos cruciales en la demostración del Gran Teorema de Galois 3.10.49

Teorema 3.10.46. *Sean p un número primo y K un cuerpo cuya característica no divide a p, que contiene a una raíz primitiva p–ésima de la unidad $\zeta \in K$. Supongamos que M/K es una extensión finita de Galois con grupo* $\mathrm{Gal}(M/K) \simeq \mathbb{Z}/p\mathbb{Z}$. *Entonces existe $\alpha \in M$ tal que $M = K(\alpha)$ y $\alpha^p \in K$. En particular, $X^p - \alpha^p$ es irreducible sobre K.*

Demostración. Sea $\sigma \in \mathrm{Gal}(M/K)$ un generador como grupo. Fijemos $\beta \in M - K$. Para cada $i = 0, \ldots, p-1$, consideramos la *resolvente de Lagrange* definida por

$$\alpha_i = \beta + \zeta^{-i}\sigma(\beta) + \zeta^{-2i}\sigma^2(\beta) + \cdots + \zeta^{-i(p-1)}\sigma^{p-1}(\beta). \tag{3.10.46.1}$$

De (3.10.46.1), usando $\zeta^p = 1, \sigma^p = 1$, se obtiene

$$\begin{aligned}\zeta^{-i}\sigma(\alpha_i) &= \zeta^{-i}\sigma(\beta) + \zeta^{-2i}\sigma^2(\beta) + \cdots + \zeta^{-i(p-1)}\sigma^{p-1}(\beta) + \zeta^{-ip}\sigma^p(\beta)\\ &= \zeta^{-i}\sigma(\beta) + \zeta^{-2i}\sigma^2(\beta) + \cdots + \zeta^{-i(p-1)}\sigma^{p-1}(\beta) + \beta\\ &= \alpha_i.\end{aligned}$$

Por tanto,

$$\sigma(\alpha_i) = \zeta^i\alpha_i. \tag{3.10.46.2}$$

(El polinomio característico del K–endomorfismo $M \xrightarrow{\sigma} M$ es $X^p - 1$, y los α_i son los vectores propios de los autovalores ζ^i). De (3.10.46.2), usando $\zeta^p = 1$, se obtiene para $i = 0, \ldots, p-1$

$$\sigma(\alpha_i^p) = (\zeta^i\alpha_i)^p = \alpha_i^p. \tag{3.10.46.3}$$

Puesto que σ genera el grupo $\mathrm{Gal}(M/K)$, la fórmula (3.10.46.3) significa que

$$\alpha_i^p \in \mathrm{Fix}(\mathrm{Gal}(M/K)) = K,\ i = 0, \ldots, p-1.$$

Para $i = 0$, la fórmula (3.10.46.2) dice que $\sigma(\alpha_0) = \alpha_0$. Esto es

$$\alpha_0 \in K.$$

Supongamos que existe algún $1 \leq i \leq p-1$ tal que

$$\alpha_i \neq 0.$$

En este caso, puesto que $\zeta^i \neq 1$, se deduce

$$\zeta^i\alpha_i \neq \alpha_i.$$

Esto significa, según (3.10.46.2), que

$$\sigma(\alpha_i) \neq \alpha_i,$$

y, por tanto,

$$\alpha_i \notin K.$$

Esto implica

$$M = K(\alpha_i),$$

puesto que $[M : K] = p$ es primo. Entonces, $\alpha = \alpha_i$ tiene las propiedades buscadas puesto que $\alpha_i^p \in K$.

Basta, por tanto, probar que existe $\alpha_i \neq 0$, con $1 \leq i \leq p-1$. Supongamos, por el contrario, que $\alpha_i = 0$ para todo $i = 1, \ldots, p-1$. En este caso, sumando las igualdades de (3.10.46.1) para $i = 0, \ldots, p-1$ se obtiene

$$\begin{aligned}
\alpha_0 &= \alpha_0 + \alpha_1 + \cdots + \alpha_{p-1} \\
&= (\beta + \sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^{p-1}(\beta)) \\
&+ (\beta + \zeta^{-1}\sigma(\beta) + \zeta^{-2}\sigma^2(\beta) + \cdots + \zeta^{-(p-1)}\sigma^{p-1}(\beta)) \\
&\vdots \\
&+ (\beta + \zeta^{-i}\sigma(\beta) + \zeta^{-2i}\sigma^2(\beta) + \cdots + \zeta^{-(p-1)i}\sigma^{p-1}(\beta)) \\
&\vdots \\
&+ (\beta + \zeta^{-(p-1)}\sigma(\beta) + \zeta^{-2(p-1)}\sigma^2(\beta) + \cdots + \zeta^{-(p-1)(p-1)}\sigma^{p-1}(\beta)) \\
&= p\beta \\
&+ (1 + \zeta^{-1} + \zeta^{-2} + \cdots + \zeta^{-(p-1)})\sigma(\beta) \\
&\vdots \\
&+ (1 + \zeta^{-i} + \zeta^{-2i} + \cdots + \zeta^{-(p-1)i})\sigma^i(\beta) \\
&\vdots \\
&+ (1 + \zeta^{-(p-1)} + \zeta^{-2(p-1)} + \cdots + \zeta^{-(p-1)(p-1)})\sigma^{p-1}(\beta).
\end{aligned} \tag{3.10.46.4}$$

Puesto que, para $i = 1, \ldots, p-1$ se verifica

$$1 + \zeta^{-i} + \zeta^{-2i} + \cdots + \zeta^{-(p-1)i} = 0,$$

de (3.10.46.4) se obtiene $\alpha_0 = p\beta$. Puesto que $p \neq 0$ en K se deduce $\beta = p^{-1}\alpha_0 \in K$, en contra de la elección $\beta \notin K$. Contradicción. □

Lema 3.10.47. *Para $i = 1, \ldots, p-1$ se verifica*

$$1 + \zeta^{-i} + \zeta^{-2i} + \cdots + \zeta^{-(p-1)i} = 0,$$

Demostración. De la factorización

$$X^p - 1 = (X-1)(X-\zeta)\cdots(X-\zeta^{p-1}) = X^p - (1+\zeta+\cdots+\zeta^{p-1})X^{p-1} + \cdots,$$

se obtiene la fórmula

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0.$$

Basta ahora observar que, puesto que p es primo, para cada $i = 1, \ldots, p-1$, el grupo cíclico de las raíces de la unidad $\mu_p =< \zeta >$ tiene, también, por generador $\mu_p =< \zeta^{-i} >$. En consecuencia

$$1 + \zeta^{-i} + \zeta^{-2i} + \cdots + \zeta^{-(p-1)i} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1}.$$

□

Usaremos también, en la demostración del Gran Teorema de Galois, un resultado un poco más general que Lema 3.10.44.

Lema 3.10.48. *Sean m un entero positivo y F un cuerpo cuya característica no divide a m, que contiene a una raíz primitiva m–ésima de la unidad $\zeta \in F$. Sea $a \in F$. Entonces $L = F(\sqrt[m]{a})$ es el cuerpo de descomposición sobre F de $X^m - a$ y* $\mathrm{Gal}(L/F)$ *es cíclico.*

Demostración. El cuerpo $L = F(\sqrt[m]{a})$ es el cuerpo de descomposición sobre F del polinomio $X^m - a$, cuyas raíces son simples, puesto que la característica de F no divide a m. Los conjugados de $\sqrt[m]{a}$ son los $\sqrt[m]{a}\zeta^j$, para ciertos $0 \leq j \leq m-1$ (no necesariamente para todo j). Por tanto, cada $\sigma \in \mathrm{Gal}(L/F)$ está determinado por $\sigma(\sqrt[m]{a}) = \sqrt[m]{a}\zeta^{j_\sigma}$ para un único $0 \leq j_\sigma \leq m-1$. Así la aplicación

$$\begin{aligned} \mathrm{Gal}(L/F) &\to \mathbb{Z}/m\mathbb{Z} \\ \sigma &\mapsto j_\sigma, \end{aligned}$$

define un homomorfismo de grupos, puesto que

$$\sigma\tau(\sqrt[m]{a}) = \sigma(\sqrt[m]{a}\zeta^{j_\tau}) = \zeta^{j_\tau}\sigma(\sqrt[m]{a}) = \zeta^{j_\tau}\zeta^{j_\sigma}\sqrt[m]{a},$$

dice que $j_{\sigma\tau} = j_\sigma + j_\tau$.

El núcleo está formado por aquellos automorfismos que dejan fijo $\sqrt[m]{a}$, esto es $\mathrm{Gal}(L/L) = \{1\}$. Por tanto, $\mathrm{Gal}(L/F)$ isomorfo a un subgrupo del grupo cíclico $\mathbb{Z}/m\mathbb{Z}$, es cíclico. □

3.10.4. El gran teorema de Galois

Teorema 3.10.49 (Gran teorema de Galois)**.** *Sean F un cuerpo de característica cero y E/F una extensión finita de Galois. Son equivalentes*

(1) La extensión E/F es resoluble.

(2) El grupo $\mathrm{Gal}(E/F)$ *es resoluble.*

Demostración. (1) $\Rightarrow$ (2) en tres etapas.
Reducción al caso radical.
Por definición de extensión resoluble, existe una extensión radical L/F tal que $E \subset L$. Según Teorema 3.10.38, la clausura de Galois M/F de L/F es una extensión radical. Podemos, por tanto, suponer $F \subset E \subset L$, donde L/F es radical y de Galois. Supongamos que hemos probado que $\mathrm{Gal}(L/F)$ es resoluble. Entonces, puesto que E/F es de Galois, el grupo $\mathrm{Gal}(E/F)$ es un cociente

$$\mathrm{Gal}(E/F) \simeq \mathrm{Gal}(L/F)/\mathrm{Gal}(L/E),$$

del grupo resoluble $\mathrm{Gal}(L/F)$. Por tanto, $\mathrm{Gal}(E/F)$ es resoluble.

Así, basta demostrar (1) $\Rightarrow$ (2) para una extensión L/F radical y de Galois.

Adjunción de raíces de la unidad.
Supongamos L/F radical y de Galois. Si adjuntamos a F y a L una raíz primitiva m–ésima de la unidad ζ obtenemos una extensión de Galois $L(\zeta)/F(\zeta)$ que, según (2) de Lema 3.10.36, es radical, puesto que $L(\zeta)/F(\zeta)$ se obtiene de la extensión radical L/F por cambio de base con $F(\zeta)/F$. Además, según Lema 3.10.42, es equivalente $\mathrm{Gal}(L(\zeta)/F(\zeta)$ resoluble y $\mathrm{Gal}(L/F)$ resoluble. Por tanto, podemos suponer, sin pérdida de generalidad, que F contiene cualquier raíz m–ésima primitiva de la unidad.

Etapa final.
Por definición de extensión radical, existe una serie

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = L, \tag{3.10.49.1}$$

donde $F_i = F_{i-1}(\gamma_i)$ con $\gamma_i^{m_i} \in F_{i-1}$ para $i = 1, \ldots, n$. Puesto que podemos suponer que F contiene una raíz primitiva m_i–ésima de la unidad, para cada m_i, la extensión F_i/F_{i-1} es de Galois y, según Lema 3.10.48, grupo de Galois cíclico.
Ahora demostramos la resolubilidad. En la serie (3.10.49.1), consideramos los subgrupos $G_{n-i} = \mathrm{Gal}(L/F_i) \leq G = \mathrm{Gal}(L/F)$ proporcionan una serie

$$G = \mathrm{Gal}(L/F) = G_n \geq G_{n-1} \geq \cdots \geq G_1 \geq G_0 = \{1\}. \tag{3.10.49.2}$$

Consideremos las extensiones $F_{i-1} \subset F_i \subset L$. Aquí, L/F_{i-1}, L/F_i y F_i/F_{i-1} son de Galois. Por tanto, el Teorema Fundamental dice que $G_{n-i+1} \trianglerighteq G_{n-i}$ y $G_{n-i+1}/G_{n-i} \simeq \mathrm{Gal}(F_i/F_{i-1})$, que es un grupo cíclico, en particular conmutativo. Esto es la serie (3.10.49.2) resuelve el grupo $\mathrm{Gal}(L/F)$.

(2) $\Rightarrow$ (1) en dos etapas.
Un caso especial
Sea L/F de Galois con grupo resoluble. Supongamos que F satisface la hipótesis adicional:

(*) F contiene una raíz p–ésima primitiva de la unidad para cada primo p que divide al orden $|\mathrm{Gal}(L/F)|$.

Demostramos que, en esta situación, L/F es radical. En efecto, puesto que $\mathrm{Gal}(L/F)$ es resoluble y finito, el Teorema 2.6.23, dice que existe una serie normal

$$G = \mathrm{Gal}(L/F) = G_n \triangleright G_{n-1} \triangleright \cdots \triangleright G_1 \triangleright G_0 = \{1\},$$

cuyos factores G_{n-i+1}/G_{n-i} son cíclicos de orden primo.
Consideremos los cuerpos fijos $F_{i-1} = \mathrm{Fix}(G_{n-i+1}) \subset F_i = \mathrm{Fix}(G_{n-i}) \subset L$. Aquí $\mathrm{Gal}(F_i/F_{i-1}) \simeq G_{n-i+1}/G_{n-i}$ es cíclico de orden primo p y, por la hipótesis (∗), podemos suponer que F_{i-1} contiene una raíz p–ésima primitiva de la unidad. Entonces, según Teorema 3.10.46, F_i se obtiene por adjunción a F_{i-1} de la raíz p–ésima de algún elemento de F_{i-1}. Esto demuestra que L/F es radical.

Caso general
Sea ζ una raíz primitiva m–ésima de la unidad, donde $m = |\mathrm{Gal}(L/F)|$.
El Lema 3.10.42, asegura que $\mathrm{Gal}(L(\zeta)/F(\zeta))$ es resoluble, puesto que $\mathrm{Gal}(L/F)$ es resoluble. Relacionamos los órdenes de estos grupos como sigue. Como en la demostración del Lema 3.10.42, se tiene un isomorfismo

$$\mathrm{Gal}(L/F) \simeq \mathrm{Gal}(L(\zeta)/F)/\mathrm{Gal}(L(\zeta)/L).$$

Este isomorfismo proviene del homomorfismo

$$\mathrm{Gal}(L(\zeta)/F) \to \mathrm{Gal}(L/F)$$

dado por restricción de los automorfismos de $L(\zeta)$ a L. Puesto que $\mathrm{Gal}(L(\zeta)/F(\zeta))$ es un subgrupo de $\mathrm{Gal}(L(\zeta)/F)$, se tiene un homomorfismo

$$\mathrm{Gal}(L(\zeta)/F(\zeta)) \to \mathrm{Gal}(L/F) \tag{3.10.49.3}$$

también definido por restricción a L. Pero el núcleo de (3.10.49.3) es la identidad, puesto que los elementos del núcleo son la identidad tanto en L como en $F(\zeta)$. Por tanto, el homomorfismo (3.10.49.3) es inyectivo. Esto implica que el orden

$$m = |\mathrm{Gal}(L/F)| \text{ es múltiplo de } |\mathrm{Gal}(L(\zeta)/F(\zeta))|. \tag{3.10.49.4}$$

Sea ahora p un primo que divide a $|\mathrm{Gal}(L(\zeta)/F(\zeta))|$. Entonces p divide a m, por (3.10.49.4). Puesto que ζ es una raíz primitiva m–ésima de la unidad, $\zeta^{m/p}$ es una raíz primitiva p–ésima de la unidad. Además $\zeta^{m/p} \in F(\zeta)$. Así $L(\zeta)/F(\zeta)$ satisface la hipótesis adicional (∗), con F y L reemplazados por $F(\zeta)$ y $L(\zeta)$ respectivamente. Por tanto $L(\zeta)/F(\zeta)$ es radical por el caso especial. Pero, es claro que $F(\zeta)/F$ es radical ($\zeta^m = 1 \in F$), de forma que $L(\zeta)/F$ es radical por la parte (1) de Lema 3.10.36.
Puesto que $L(\zeta)/F$ es radical, la inclusión $L \subset L(\zeta)$ dice que L/F es resoluble. Esto completa la demostración del Teorema. □

La demostración del Teorema 3.10.49 implica que una extensión de Galois resoluble se convierte en radical por adjunción de una raíz de la unidad adecuada.

Corolario 3.10.50. *Sean L/F de Galois resoluble y ζ una raíz primitiva m–ésima de la unidad, donde $m = [L : F]$. Entonces las extensiones $L(\zeta)/F(\zeta)$ y $L(\zeta)/F$ son de Galois radicales.*

Demostración. Está demostrado en el caso general de (2) $\Rightarrow$ (1) de Teorema 3.10.49. □

Polinomios resolubles por radicales

Sea F un cuerpo de característica cero.

Definición 3.10.51. Sea $f \in F[X]$ separable de grado ≥ 1 con cuerpo de descomposición E/F.

(1) Una raíz $\alpha \in E$ de f es expresable por radicales sobre F si α está en alguna extensión radical de F. De forma equivalente, $F(\alpha)/F$ es resoluble.

(2) El polinomio f es resoluble por radicales sobre F si E/F es una extensión resoluble.

Puesto que el compuesto de extensiones radicales es radical, la condición (2) es equivalente a

(3) El polinomio f es resoluble por radicales si todas sus raíces son expresables por radicales.

Es claro que (2) es independiente del cuerpo de descomposición elegido.

Proposición 3.10.52. *Sea $f \in F[X]$ irreducible. Entonces f es resoluble por radicales si, y sólo si, alguna raíz de f es expresable por radicales.*

Demostración. Supongamos que α es una raíz de f, tal que $F(\alpha)/F$ es resoluble. Según Corolario 3.10.39, su clausura de Galois $F \subset F(\alpha) \subset K$ es también resoluble. Puesto que f es irreducible y tiene una raíz en la extensión de Galois K/F, factoriza en producto de factores lineales sobre K. Por tanto K contiene un cuerpo de descomposición de f sobre F. De hecho K/F es el cuerpo de descomposición de f sobre F. Esto prueba la Proposición, puesto que K/F es resoluble. □

El Teorema 3.10.49 implica el siguiente resultado.

Teorema 3.10.53. *Un polinomio separable $f \in F[X]$ es resoluble por radicales si, y sólo si, el grupo de Galois de f sobre F es un grupo resoluble.*

Proposición 3.10.54. *Todo polinomio separable $f \in F[X]$ de grado ≤ 4 es resoluble por radicales.*

Demostración. El grupo de Galois de f es un subgrupo de S_n, con $n \leq 4$. Puesto que S_n es resoluble para $n \leq 4$, la proposición está demostrada. □

Ejemplo 3.10.55. Hemos probado que $f = X^5 - 6X + 3$ tiene S_5 como grupo de Galois sobre $\mathbb{Q}$. Pero S_5 no es resoluble, de forma que f no es resoluble por radicales sobre $\mathbb{Q}$. Además, puesto que f es irreducible ninguna de sus raíces es expresable por radicales sobre $\mathbb{Q}$.

Este ejemplo requiere que revisemos la forma en que pensamos en las raíces de un polinomio. De forma ingenua, se puede pensar que las raíces de un polinomio $f \in \mathbb{Q}[X]$ son siempre números de la forma $\sqrt{2} + \sqrt{3}$, $\sqrt{2 + \sqrt{2}}$, $\sqrt[7]{12 + 7i}$... Las raíces de un polinomio como $X^5 - 6X + 3 \in \mathbb{Q}[X]$ no se pueden expresar con fórmulas de este tipo. Las raíces de un polinomio irreducible no resoluble por radicales son intrínsecamente más complicadas que las simples expresiones radicales.

Teorema 3.10.56. *Si $n \geq 5$ el polinomio universal de grado n sobre F no es resoluble por radicales, y ninguna de sus raíces es expresable por radicales.*

Demostración. El polinomio universal de grado n es irreducible sobre F con grupo de Galois S_n, que para $n \geq 5$ es no resoluble. □

Esto significa que para $n \geq 5$ no existen fórmulas universales que proporcionen las raíces del polinomio en función de los coeficientes, similares a las fórmulas conocidas para $n = 2, 3, 4$.

Teorema 3.10.57. *Para cada n existen infinitos polinomios $f(X) \in \mathbb{Z}[X]$ de grado n cuyo grupo de Galois sobre $\mathbb{Q}$ es S_n.*

Demostración. [DuFo04, página 642] □

3.10.5. Extensiones ciclotómicas

Sea ζ_n una raíz primitiva n-ésima de la unidad. La extensión $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, que es el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $X^n - 1$, recibe el nombre de cuerpo ciclotómico de las raíces n–ésimas de la unidad.

Proposición 3.10.58. *Sea ζ_n una raíz primitiva n–ésima de la unidad sobre $\mathbb{Q}$. La extensión ciclotómica $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ tiene grupo de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$, isomorfo al grupo conmutativo de las unidades del anillo $\mathbb{Z}/n\mathbb{Z}$. En particular, si n es un primo p el grupo $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ es cíclico.*

Demostración. El Teorema 3.7.11, dice que los $\mathbb{Q}$–conjugados de ζ son los ζ^a, donde $1 \leq a < m$, y $\mathrm{mcd}(a, m) = 1$. Por tanto, un automorfismo $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ está determinado por $\sigma(\zeta) = \zeta^a$, para un único $1 \leq a < m$, con $\mathrm{mcd}(a, m) = 1$. Por otra parte, $(\mathbb{Z}/m\mathbb{Z})^* = \{\bar{a} \mid 1 \leq a < m,$ y $\mathrm{mcd}(a, m) = 1\}$. El isomorfismo está definido por $\sigma \mapsto \bar{a}$. □

Ejemplos 3.10.59. (1) El grupo $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \simeq (\mathbb{Z}/5\mathbb{Z})^* \simeq \mathbb{Z}/4\mathbb{Z}$ es cíclico generado por $\sigma : \zeta_5 \mapsto \zeta_5^2$.

Hay exactamente un cuerpo intermedio, que corresponde al único subgrupo no trivial: $\{1, \sigma^2\}$. Este cuerpo intermedio es una extensión cuadrática de $\mathbb{Q}$, uno de cuyos elementos es:

$$\alpha = \zeta_5 + \zeta_5^4.$$

En efecto: $\sigma^2(\alpha) = \sigma^2(\zeta_5) + \sigma^2(\zeta_5^4) = \sigma(\zeta_5^2) + (\sigma^2(\zeta_5))^4 = (\sigma(\zeta_5))^2 + (\sigma^2(\zeta_5))^4 = (\zeta_5^2)^2 + (\sigma^2(\zeta_5))^4 = \zeta_5^4 + (\zeta_5^4)^4 = \zeta_5^4 + \zeta_5$. Cálculo que muestra que α está en el cuerpo fijo de $\{1, \sigma^2\}$.

Haciendo uso de la igualdad $\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0$, podemos calcular:

$$\alpha^2 + \alpha - 1 = \zeta_5^2 + 2 + \zeta_5^3 + \zeta_5 + \zeta_5^4 - 1 = 0.$$

En consecuencia

$$\alpha = \frac{-1 \pm \sqrt{5}}{2}.$$

Por tanto, el cuerpo cuadrático intermedio de la extensión es

$$\mathbb{Q}(\zeta_5 + \zeta_5^4) = \mathbb{Q}(\sqrt{5}).$$

(2) Se puede demostrar que, si p es un primo impar, el cuerpo ciclotómico $\mathbb{Q}(\zeta_p)$ contiene a $\mathbb{Q}(\sqrt{\pm p})$, donde el signo positivo corresponde a $p \equiv 1 \pmod 4$ y el signo negativo a $p \equiv 3 \pmod 4$.

Correspondencia de Galois en $\mathbb{Q}(\zeta_p)/\mathbb{Q}$

Sean p un primo impar y ζ_p una raíz primitiva de la unidad. Una base de $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$. Puesto que $\zeta_p^{p-1} + \zeta_p^{p-2} + \cdots + \zeta_p + 1 = 0$, también los elementos

$$\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}, \zeta_p^{p-1}\}, \tag{3.10.59.1}$$

forman una base. La razón para elegir la base (3.10.59.1) es que cada $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ permuta los elementos de la base (3.10.59.1), ya que (3.10.59.1) está formada por todas las raíces primitivas p–ésimas de la unidad. Obsérvese que aquí es imprescindible que p sea primo: en general, las raíces n–ésimas primitivas no forman una base de $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.
Sean $H \leq \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ y

$$\alpha_H = \sum_{\sigma \in H} \sigma\zeta_p = \zeta_p + \sum_{\sigma \in H - \{1\}} \sigma\zeta_p. \tag{3.10.59.2}$$

Para cada $\tau \in H$, los elementos $\tau\sigma$ recorren H según σ recorre H. Se deduce que

$$\tau\alpha_H = \alpha_H,$$

de forma que

$$\alpha_H \in \text{Fix}(H).$$

Así

$$\mathbb{Q}(\alpha_H) \subset \text{Fix}(H).$$

Si $\tau \notin H$, entonces $\tau\alpha_H$ es la suma de elementos de la base (3.10.59.1), uno de los cuales es $\tau\zeta_p$. Así, si se verificara $\tau\alpha = \alpha$, entonces se tendría

$$\tau\zeta_p = \sigma\zeta_p, \tag{3.10.59.3}$$

para alguno de los $\sigma \in H - \{1\}$. La igualdad (3.10.59.3) implica $\tau = \sigma$, en contra de $\tau \notin H$. Por tanto, si $\tau \notin H$ es $\tau\alpha_H \neq \alpha_H$. En consecuencia,

$$\mathbb{Q}(\alpha_H) = \text{Fix}(H).$$

Ejemplo 3.10.60. $\mathbb{Q}(\zeta_{13})/\mathbb{Q}$.
Los cuerpos intermedios de esta extensión corresponden a los subgrupos de $(\mathbb{Z}/13\mathbb{Z})^* = \{\bar{1}, \bar{2}, \ldots, \bar{12}\} =< \bar{2} >$. Es decir, $\text{Gal}(\mathbb{Q}(\zeta_{13})/\mathbb{Q}) =< \sigma >$ es cíclico generado por σ definido por $\sigma\zeta_{13} = \zeta_{13}^2$. Los subgrupos no triviales son un único subgrupo para cada orden $2, 3, 4, 6$ divisor de 12; subgrupos cíclicos con generadores $\sigma^6, \sigma^4, \sigma^3, \sigma^2$. Los cuerpos fijos correspondientes tienen grados $6, 4, 3, 2$ sobre $\mathbb{Q}$.
Los correspondientes generadores α_H de estos cuerpos intermedios son:

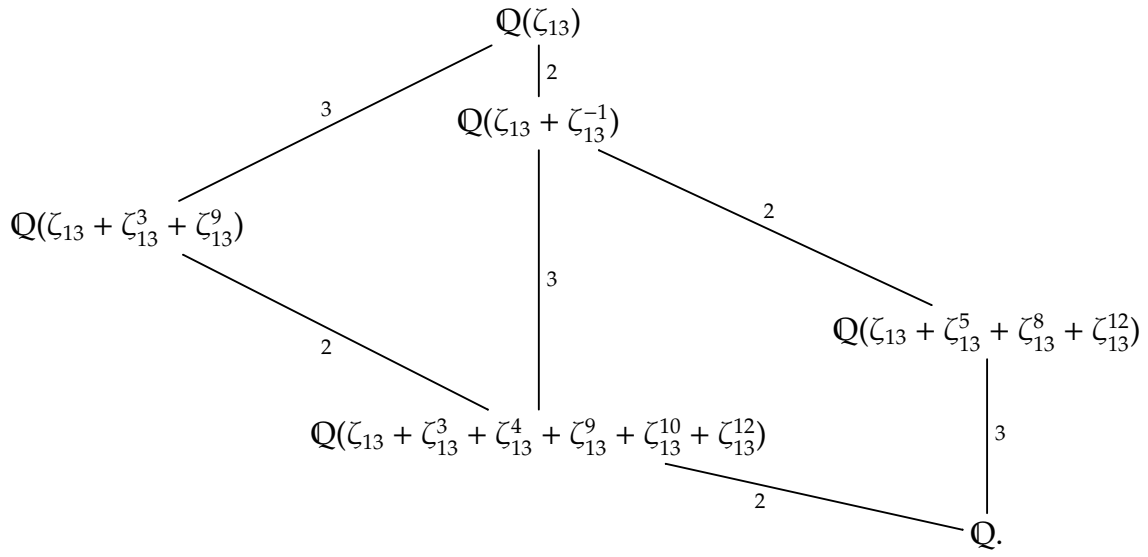
$$\zeta_{13} + \sigma^6\zeta_{13} = \zeta_{13} + \zeta_{13}^{2^6} = \zeta_{13} + \zeta_{13}^{-1},$$

$$\zeta_{13} + \sigma^4\zeta_{13} + \sigma^8\zeta_{13} = \zeta_{13} + \zeta_{13}^{2^4} + \zeta_{13}^{2^8} = \zeta_{13} + \zeta_{13}^3 + \zeta_{13}^9,$$

$$\zeta_{13} + \sigma^3\zeta_{13} + \sigma^6\zeta_{13} + \sigma^9\zeta_{13} = \zeta_{13} + \zeta_{13}^{2^3} + \zeta_{13}^{2^6} + \zeta_{13}^{2^9} = \zeta_{13} + \zeta_{13}^8 + \zeta_{13}^{12} + \zeta_{13}^5,$$

$$\zeta_{13} + \sigma^2\zeta_{13} + \sigma^4\zeta_{13} + \sigma^6\zeta_{13} + \sigma^8\zeta_{13} + \sigma^{10}\zeta_{13} = \zeta_{13} + \zeta_{13}^4 + \zeta_{13}^3 + \zeta_{13}^{12} + \zeta_{13}^9 + \zeta_{13}^{10}.$$

El retículo de subcuerpos de $\mathbb{Q}(\zeta_{13})/\mathbb{Q}$ es:



Los elementos que aparecen en las ecuaciones (3.10.59.2), se denominan periodos de ζ_p. Estos elementos son útiles en el estudio de la aritmética de los cuerpos ciclotómicos. El estudio de su combinatoria se denomina ciclotomía.

3.10.61. Supongamos que $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ es la descomposición de n en producto de potencias de primos distintos. Puesto que $\zeta_n^{p_2^{a_2}\cdots p_k^{a_k}}$ es una raíz primitiva $p_1^{a_1}$–ésima de la unidad, el cuerpo $K_1 = \mathbb{Q}(\zeta_{p_1^{a_1}})$ es un subcuerpo de $\mathbb{Q}(\zeta_n)$. De forma similar, cada uno de los cuerpos $K_i = \mathbb{Q}(\zeta_{p_i^{a_i}}), i = 1, 2, \ldots, k$ es un subcuerpo de $\mathbb{Q}(\zeta_n)$. El compuesto $K_1 \cdots K_k$ contiene el producto $\zeta_{p_1^{a_1}} \cdots \zeta_{p_k^{a_k}}$, que es una raíz primitiva n–ésima de la unidad, por tanto el cuerpo compuesto es $\mathbb{Q}(\zeta_n)$. Puesto que los grados $[K_i : \mathbb{Q}] = \varphi(p_i^{a_i}), i = 1, 2, \cdots, k$ y $\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2})\cdots\varphi(p_k^{a_k})$, el grado del compuesto de los K_i es precisamente el producto de los grados de los K_i. Se deduce que $K_1 \cap \cdots \cap K_k = \mathbb{Q}$, mediante un argumento de inducción, usando la Proposición 3.8.29. Entonces el Corolario 3.8.30 muestra que el grupo de Galois de $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es el producto directo de los grupos de Galois de los subcuerpos $K_i/\mathbb{Q}$. Podemos enunciar el argumento anterior como el siguiente corolario.

Corolario 3.10.62. *Sea $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ la descomposición del entero positivo n en producto de potencias de primos distintos. Entonces los cuerpos ciclotómicos $\mathbb{Q}(\zeta_{p_i^{a_i}}), i = 1, 2, \cdots, k$ intersecan en el cuerpo $\mathbb{Q}$ y su compuesto es el cuerpo ciclotómico $\mathbb{Q}(\zeta_n)$. Se tiene un isomorfismo*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_2^{a_2}})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k^{a_k}})/\mathbb{Q}),$$

que bajo el isomorfismo de Proposición3.10.58 corresponde al isomorfismo del Teorema Chino del Resto:

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \times (\mathbb{Z}/p_2^{a_2}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^*.$$

3.10.63. (1) Para $a \geq 2$

$$(\mathbb{Z}/2^a\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{a-2}\mathbb{Z}).$$

(2) Para p primo impar

$$(\mathbb{Z}/p^a\mathbb{Z})^* \simeq (\mathbb{Z}/p^{a-1}(p-1)\mathbb{Z}).$$

3.10.64. La Proposición 3.10.58 muestra, en particular, que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ es abeliano.

Definición 3.10.65. *La extensión K/F se dice abeliana si es de Galois y su grupo de Galois es un grupo abeliano.*

3.10.66. Puesto que todo subgrupo y todo cociente de un grupo abeliano es abeliano resulta, del Teorema Fundamental, que cada cuerpo intermedio de una extensión abeliana de F es también una extensión abeliana de F. Por los resultados de extensiones compuestas en la Sección 3.8.2, vemos también que el compuesto de dos extensiones abelianas es también una extensión abeliana (puesto que el grupo de Galois del compuesto es isomorfo a un subgrupo del producto directo de los grupos de Galois, por tanto abeliano).

Es un problema abierto determinar que grupos aparecen como grupos de Galois de extensiones de $\mathbb{Q}$. Usando resultados anteriores podemos ver que todo grupo abeliano aparece como grupo de Galois de alguna extensión de $\mathbb{Q}$, de hecho como el grupo de Galois de algún subcuerpo de un cuerpo ciclotómico. En efecto:
Sea $n = p_1 p_2 \cdots p_k$ el producto de primos distintos. Entonces por el Teorema Chino del Resto

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^* &\simeq (\mathbb{Z}/p_1\mathbb{Z})^* \times (\mathbb{Z}/p_2\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^* \\ &\simeq \mathbb{Z}_{p_1-1} \times \mathbb{Z}_{p_2-1} \times \cdots \times \mathbb{Z}_{p_k-1}.\end{aligned} \tag{3.10.66.1}$$

Ahora, supongamos que G es un grupo finito abeliano cualquiera. Por el Teorema de Clasificación de Grupos Abelianos,

$$G \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k},$$

para ciertos enteros $n_1, n_2, \ldots, n_k$. Daremos por conocido que dado un entero m existen infinitos primos p con $p \equiv 1 \pmod{m}$ (se puede encontrar una prueba de este hecho en la página 557 del libro de Dummit y Foote). Asumiendo este resultado, elegimos primos distintos tales que $p_i \equiv 1 \pmod{n_i}$, $i = 1, \ldots, k$ y sea $n = p_1 p_2 \cdots p_k$ como antes.
Por construcción, n_1 divide a $p_i - 1$ para $i = 1, \ldots, k$, de forma que el grupo $\mathbb{Z}_{p_i-1}$ tiene un subgrupo (cíclico) de orden $\frac{p_i-1}{n_i}$ para $i = 1, \ldots, k$, y el cociente por este subgrupo es cíclico de orden n_i. Por tanto el cociente de $(\mathbb{Z}/n\mathbb{Z})^*$ en (3.10.66.1) por $H_1 \times \cdots \times H_k$ es isomorfo al grupo G. Por la Proposición 3.10.58 y el Teorema Fundamental, vemos que existe un subcuerpo de $\mathbb{Q}(\zeta_{p_1 p_2 \cdots p_k})$ que es Galois sobre $\mathbb{Q}$ con G como grupo de Galois. Podemos resumir todo este argumento en el siguiente corolario.

Corolario 3.10.67. *Sea G un grupo finito abeliano. Entonces existe un subcuerpo K de un cuerpo ciclotómico con* $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$.

Existe un recíproco de este resultado (cuya prueba escapa de nuestras posibilidades), el celebrado Teorema de Kronecker–Weber:

Teorema 3.10.68 (Kronecker–Weber)**.** *Sea K un cuerpo extensión finita abeliana de $\mathbb{Q}$. Entonces K está contenido en una extensión ciclotómica de $\mathbb{Q}$.*

Las extensiones abelianas de $\mathbb{Q}$ son las "más sencillas" extensiones de Galois (al menos en lo que concierne a la estructura de sus grupo de Galois) y el resultado previo muestra que pueden ser clasificadas por las extensiones ciclotómicas de $\mathbb{Q}$. Para otras extensiones finitas de $\mathbb{Q}$ como cuerpo base, es más difícil describir sus extensiones abelianas. El estudio de las extensiones abelianas de una extensión finita arbitraria F de $\mathbb{Q}$ es denominado *teoría de cuerpos de clase*. Existe una clasificación de las extensiones abelianas de F por invariantes asociados a F que generaliza los resultados acerca de cuerpos ciclotómicos sobre $\mathbb{Q}$. En general, sin embargo, la construcción de extensiones abelianas es ni mucho menos tan explícita como en el caso de cuerpos ciclotómicos. Un caso donde tal

descripción es posible es para extensiones abelianas de de un cuerpo cuadrático imaginario $\mathbb{Q}(\sqrt{-D})$ para D positivo), donde las extensiones abelianas pueden ser construidas adjuntando valores de ciertas funciones elípticas (esto es el análogo de adjuntar raíces de la unidad, que son valores de la función exponencial e^x para cierto x). El estudio de la aritmética de tales extensiones abelianas y la búsqueda de resultados similares para extensiones no–abelianas son áreas de investigación matemática actual.

3.11. Construcciones con regla y compás

Nuestra idea intuitiva de regla (no marcada) y compás es la de una pareja de instrumentos matemáticos ideales que, en el caso de la regla, permite construir la línea que pasa por dos puntos (previamente construidos) distintos dados y, en el caso del compás, construye la circunferencia de centro un punto (p.c.) dado y radio un segmento (p.c., esto es cuyos extremos han sido construidos) dado. Construcciones con regla y compás son aquellas construcciones geométricas en el plano afín (o bien, en el plano complejo), que pueden ser llevadas a cabo usando únicamente estos dos instrumentos a partir de dos puntos dados que suponemos construidos. De esta forma, es posible, por ejemplo, construir la recta perpendicular a una recta (p.c.) dada por un punto (p.c.) dado en la recta o exterior a la recta, la recta paralela a una dada por un punto dado, la bisectriz de un ángulo dado, y otras tantas construcciones elementales.

3.11.1. El cuerpo de los números constructibles

Para demostrar teoremas acerca de construcciones geométricas necesitamos una descripción algo más cuidadosa de qué entendemos por punto, línea o circunferencia constructibles en el plano complejo.

Los siguiente enunciados pueden ser tomados como "axiomas".

($A1$) La recta (o el segmento) determinado por dos puntos distintos constructibles es constructible.

($A2$) La circunferencia de centro un punto constructible y radio la longitud de un segmento constructible es constructible.

($B1$) El punto de intersección de dos rectas distintas constructibles es constructible.

($B2$) Los puntos de intersección de una recta constructible y una circunferencia constructible son constructibles.

($B3$) Los puntos de intersección de dos circunferencias constructibles son constructibles.

Definición 3.11.1. *Un número complejo $\alpha = a + bi$ (o punto del plano (a, b)) es constructible si existe una sucesión finita de construcciones que usan $(A1), (A2), (B1), (B2), (B3)$ que comienza con 0 y 1 y termina con α.*

Las siguientes afirmaciones son consecuencia inmediata de los axiomas, usando las construcciones elementales con regla y compás adecuadas a cada caso.

Ejemplos 3.11.2. (1) Los enteros son constructibles.

(2) La recta t, paralela a una recta constructible r y que pasa por un punto constructible A exterior a r, es constructible:

Con centro en A y radio constructible trazamos una circunferencia que corta a r en el punto constructible C. Con centro C y radio constructible CA, trazamos la circunferencia constructible $\mathfrak{C}$ que pasa por A y corta a r en los puntos B, D. Con centro en D y radio constructible BA trazamos la circunferencia constructible que corta a $\mathfrak{C}$ en cierto punto A' tal que la recta AA' es la paralela buscada.

(3) La recta t, perpendicular a una recta constructible r y que pasa por un punto constructible A, es constructible:

(4) La bisectriz de un ángulo cuyos lados son rectas constructibles es constructible.

(5) Los racionales son constructibles.

(6) La mediatriz de un segmento de extremos constructibles es constructible.

(7) La circunferencia determinada por tres puntos constructibles no alineados es constructible.

Proposición 3.11.3. *El número $a + bi$ es constructible si, y sólo si, los números reales a, b son constructibles.*

Teorema 3.11.4. *El conjunto de los números complejos constructibles es un subcuerpo de $\mathbb{C}$, que denotaremos $\mathscr{C}$.*

Demostración. Por definición $0, 1 \in \mathscr{C}$. En consecuencia el eje real es constructible. Además $-1 \in \mathscr{C}$, puesto que es la intersección del eje real con la circunferencia de centro 0 y radio 1. La mediatriz del segmento de extremos -1 y 1 es constructible. Por tanto, el eje imaginario es constructible.
Trazando las perpendiculares a los ejes que pasan por el punto (a, b) vemos que $(a, b) \in \mathscr{C}$ si, y sólo si, $(a, 0), (0, b) \in \mathscr{C}$ si, y sólo si, $(a, 0), (b, 0) \in \mathscr{C}$.
En consecuencia, para probar que $\mathscr{C}$ es un subcuerpo de $\mathbb{C}$ basta probar que $\mathbb{R} \cap \mathscr{C}$ es un subcuerpo.
Sean $a < b \in \mathbb{R}$ tales que $(a, 0), (b, 0) \in \mathscr{C}$, entonces $(a + b, 0) \in \mathscr{C}$, puesto que es la intersección del eje real con la circunferencia de centro $(a, 0)$ y radio $|b|$.
Por otra parte, si $(a, 0) \in \mathscr{C}$, es claro que $(-a, 0) \in \mathscr{C}$.
Respecto del producto de $a, b > 0$ tales que $(a, 0), (b, 0)$ son constructibles: el punto D intersección de la circunferencia que pasa por $A = (0, a), B = (0, -b), C = (-1, 0)$ con el eje real tiene coordenadas $D = (ab, 0)$, lo que muestra que $(ab, 0)$ es constructible.
Respecto del inverso de $a > 0$ tal que $(a, 0)$ es constructible, el punto D intersección de la circunferencia que pasa por $A = (0, 1), B = (0, -1), C = (-a, 0)$ con el eje real tiene coordenadas $D = (a^{-1}, 0)$, lo que muestra que $(a^{-1}, 0)$ es constructible. □

Proposición 3.11.5. *$\alpha \in \mathscr{C}$ implica que $\sqrt{\alpha} \in \mathscr{C}$.*

Demostración. podemos suponer $\alpha \neq 0$. Si escribimos $\alpha = re^{i\theta}$, entonces es suficiente probar que $\sqrt{r}e^{i\theta/2}$ es constructible. Para probar esto, observemos que la constructibilidad de α implica:

- Usando el eje real y la linea que pasa por el origen y por α, construimos el ángulo θ que podemos bisecar por la construcción con regla y compás habitual. Por tanto el ángulo $\theta/2$ es constructible.
- El círculo de radio $r = |\alpha|$ con centro en el origen interseca el eje real en $(\pm r, 0)$. Por tanto $(\pm r, 0)$ son constructibles.
- Si probamos que $\sqrt{r}$ es constructible, supuesto $r > 0$ constructible, entonces podemos construir el círculo de radio $\sqrt{r}$ con centro el origen. La intersección de este círculo con el ángulo $\theta/2$ construye $\sqrt{r}e^{i\theta/2}$.

Sólo queda por probar que $\sqrt{r}$ es constructible. Para ello consideramos el segmento de extremos $(1, 0)$ y el punto intersección de la semicircunferencia, en el primer cuadrante, que tiene por diámetro los puntos $(0, 0), (1 + r, 0)$ con la perpendicular por el punto $(1, 0)$. □

Ejemplo 3.11.6. La raíz quinta primitiva de la unidad $\zeta = e^{2\pi i/5} \in \mathscr{C}$. En efecto,

$$\zeta = \frac{-1 + \sqrt{5}}{4} + \frac{i}{2}\sqrt{\frac{5 + \sqrt{5}}{2}}.$$

Esta expresión muestra que el pentágono regular es constructible con regla y compás.

Diremos que $\mathscr{C}$ es el cuerpo de los números constructibles. A continuación estudiamos la estructura de $\mathscr{C}$.

Teorema 3.11.7. *Sea $\alpha \in \mathbb{C}$. Entonces $\alpha \in \mathscr{C}$ si, y sólo si, existen subcuerpos*

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C} \tag{3.11.7.1}$$

tales que $\alpha \in F_n$ y $[F_i, F_{i-1}] = 2$ para $1 \leq i \leq n$.

Demostración. Supongamos primero que tenemos una torre como (3.11.7.1). Entonces $F_i = F_{i-1}(\sqrt{\alpha_i})$ para cierto $\alpha_i \in F_{i-1}$, según Ejemplo 3.1.27 (1). Probaremos que $F_i \subset \mathscr{C}$ por inducción en $0 \leq i \leq n$. El caso $F_0 \subset \mathscr{C}$ está probado. Supongamos $F_{i-1} \subset \mathscr{C}$. Entonces $\alpha_i \in F_{i-1}$ es constructible, que implica $\sqrt{\alpha} \in \mathscr{C}$ por Proposición 3.11.5. Por tanto $F_i = F_{i-1}(\alpha_i) \subset \mathscr{C}$. Esto prueba $F_n \subset \mathscr{C}$.
Recíprocamente, dado $\alpha \in \mathscr{C}$ probaremos que hay extensiones $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$ donde $[F_i, F_{i-1}] = 2$ tales que F_n contiene las partes real e imaginarias de todos los números construidos durante el procesos de construcción de α. El teorema se obtendrá entonces, puesto que $\alpha = a + bi$ implicará que $a, b \in F_n$, de forma que $\alpha \in F_n(i)$.

Probaremos la afirmación anterior por inducción en el número N de veces que usamos los axiomas $(B1)$, $(B2)$, $(B3)$ en la construcción de α.
Si $N = 0$, entonces $\alpha = 0$ o 1, en cuyo caso ponemos $F_n = F_0 = \mathbb{Q}$.
Supongamos ahora α construido en $N > 0$ etapas, donde la última etapa usa $(B1)$, la intersección de dos rectas distintas l_1, l_2 constructibles. La recta habrá sido construida a partir de dos puntos distintos α_1 y β_1 usando $(A1)$ y, de forma similar, l_2 a partir de α_2 y β_2. Por nuestra hipótesis de inducción existen extensiones $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$ donde $[F_i, F_{i-1}] = 2$ tales que F_n contiene las partes real e imaginarias de $\alpha_1, \beta_1, \alpha_2, \beta_2$. Vamos a demostrar que F_n contiene las partes real e imaginaria de α. En efecto, la línea l_1 tiene una ecuación de la forma $a_1x + b_1y = c_1$ y pasa por $\alpha_1 \neq \beta_1$. Puesto que las partes real e imaginaria de α_1, β_1 están en F_n, podemos suponer que los coeficientes a_1, b_1, c_1 están en F_n. De forma similar l_2 tiene una ecuación $a_2x + b_2y = c_2$, donde $a_2, b_2, c_2 \in F_n$. Ahora, la fórmula de Cramer muestra que las partes real e imaginaria de α, que son la única solución del sistema formado por las dos ecuaciones, están en F_n.
Supongamos que la última etapa en la construcción de α usa $(B2)$, la intersección de una línea l y un círculo $\mathfrak{C}$. La línea será l_1 que pasa por los puntos $\alpha_1 \neq \beta_1$ (construcción $(A1)$), y $\mathfrak{C}$ el círculo con centro γ_2 y radio $|\alpha_2 - \beta_2|$ (construcción $(A2)$). Los cinco puntos $\alpha_1, \beta_1, \alpha_2, \beta_2, \gamma_2$ proceden de etapas anteriores de la construcción, de forma que por la hipótesis de inducción, existen extensiones $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$ donde $[F_i, F_{i-1}] = 2$ tales que F_n contiene las partes real e imaginarias de estos cinco puntos. Vamos a probar que las partes real e imaginaria de α están en F_n o en una extensión cuadrática de F_n. Como antes, l_1 tiene una ecuación $a_1x + b_1y = c_1$, donde $a_1, b_1, c_1 \in F_n$. También es sencillo comprobar que $\mathfrak{C}$ tiene una ecuación $x^2 + y^2 + a_2x + b_2y + c_2 = 0$, donde $a_2, b_2, c_2 \in F_n$. Supongamos que $a_1 \neq 0$. Entonces, dividiendo por a_1, podemos suponer que la ecuación de l_1 es $x + b_1y = c_1$. Sustituyendo en la ecuación de $\mathfrak{C}$ y usando la fórmula de las soluciones de la ecuación cuadrática vemos que la solución para y contiene la raíz cuadrada de una expresión en F_n. Si esta raíz cuadrada es un elemento de F_n, entonces y y también $x = -b_1y + c_1$ están en F_n, y se deduce que las partes real e imaginaria de α están en F_n. Por otra parte, si la raíz cuadrada no está en F_n, entonces obtenemos una extensión cuadrática $F_n \subset F_{n+1}$, tal que las soluciones del sistema y, por tanto, las partes real e imaginaria de α están en F_{n+1}.
Si $a_1 = 0$ el argumento es similar.
Finalmente, supongamos que la última etapa en la construcción de α usa $(B3)$, la intersección de dos círculos distintos $\mathfrak{C}_1, \mathfrak{C}_2$. Como antes, existen extensiones $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$ donde $[F_i, F_{i-1}] = 2$ tales que los círculos tienen ecuaciones $x^2 + y^2 + a_ix + b_iy + c_i = 0$ cuyos coeficientes están en F_n. Además, sabemos que las partes real e imaginaria de α dan una solución del sistema formado por estas dos ecuaciones. Puesto que los círculos son distintos y no disjuntos, considerando la diferencia de las ecuaciones, obtenemos la ecuación de una recta con coeficientes en F_n. Cambiando la ecuación de uno de los círculos por la de esta recta, estamos en el caso anterior $(B2)$. Esto completa la demostración. □

Corolario 3.11.8. *El cuerpo $\mathscr{C}$ de los números constructibles es el menor subcuerpo de $\mathbb{C}$ cerrado*

para la operación de tomar raíz cuadrada.

Demostración. La Proposición 3.11.5 afirma que $\mathscr{C}$ es cerrado para la operación de tomar raíz cuadrada. Ahora, sea F un subcuerpo de $\mathbb{C}$ cerrado para la operación de raíz cuadrada. Hemos de probar que $\mathscr{C} \subset F$. Sea $\alpha \in \mathscr{C}$. Elegimos una torre $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$ donde $[F_i, F_{i-1}] = 2$, tal que $\alpha \in F_n$. El primer párrafo de la demostración del Teorema 3.11.7 prueba que $F_n \subset F$. Por tanto $\alpha \in F$. □

El siguiente resultado es una muy útil condición necesaria para que un número sea constructible.

Corolario 3.11.9. *Si $\alpha \in \mathscr{C}$, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ para cierto $m \geq 0$.*

Demostración. Si $\alpha \in \mathscr{C}$ existe una torre $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$ donde $[F_i, F_{i-1}] = 2$, tal que $\alpha \in F_n$. Entonces, la fórmula de los grados muestra que $[F_n : \mathbb{Q}] = 2^n$. Además de $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset F_n]$ se obtiene $[F_n : \mathbb{Q}] = [F_n : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. De aquí resulta lo afirmado. □

La condición necesaria para que un número sea constructible que acabamos de obtener, permite resolver de forma negativa varios famosos problemas de la Geometría de la Grecia Clásica.

Ejemplo 3.11.10. *Trisección del ángulo.* Conocemos la clásica construcción con regla y compás para construir la bisectriz de cualquier ángulo. El problema clásico preguntaba si es posible trisecar cualquier ángulo usando regla y compás. Vamos a probar que el ángulo (constructible) de 60° no puede ser trisecado con regla y compás.
Un ángulo θ es constructible si, y sólo si, el número $\cos\theta$ es constructible. Por tanto, 60° es constructible. Sin embargo, el número $\beta = \cos 20°$ no es constructible. En efecto, de la fórmula

$$\cos\theta = 4\cos^3\frac{\theta}{3} - 3\cos\frac{\theta}{3}$$

obtenemos para $\beta = \cos 20°$

$$4\beta^3 - 3\beta - \frac{1}{2} = 0.$$

O bien

$$\alpha^3 - 3\alpha - 1 = 0,$$

donde $\alpha = 2\beta$. El polinomio $X^3 - 3X - 1 \in \mathbb{Q}[X]$ es irreducible puesto que es de grado 3 y no tiene raíces racionales. Por tanto

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

lo que muestra que $\beta \notin \mathscr{C}$.

Podemos caracterizar los ángulos cuya medida es un número entero de grados, que pueden ser trisecados con regla y compás, como sigue: los ángulos de 1° o 2° no son

constructibles; en caso contrario, por las formulas del ángulo doble, 20° sería constructible. Por otra parte, 3° es constructible (72° es constructible: pentágono regular, 60° es constructible: triángulo equilátero, fórmulas de adición y ángulo mitad). Se deduce que θ cuya medida en grados es un número entero, es constructible si, y sólo si, θ es múltiplo de 3. De hecho

$$\cos 3^\circ = \frac{1}{8}(\sqrt{3}+1)\sqrt{5+\sqrt{5}} + \frac{1}{16}(\sqrt{6}-\sqrt{2})(\sqrt{5}-1),$$
$$\operatorname{sen} 3^\circ = \frac{1}{16}(\sqrt{6}+\sqrt{2})(\sqrt{5}-1) - \frac{1}{8}(\sqrt{3}-1)\sqrt{5+\sqrt{5}}.$$

Ejemplo 3.11.11. *Duplicación del cubo.* Aquí el problema consiste en dado un cubo de arista constructible, construir otro cubo de volumen doble. Es claro que el problema equivale a construir el número $\sqrt[3]{2}$. Puesto que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, la duplicación del cubo no es posible con regla y compás.

Ejemplo 3.11.12. *Cuadratura del círculo.* El problema consiste en construir un cuadrado cuya área sea igual que le área de un círculo constructible dado. El problema equivale a la pregunta: ¿es $\sqrt{\pi}$ un número constructible? Por lo demostrado para $\mathscr{C}$ esta pregunta es equivalente a: ¿es π constructible?
En este caso, sabemos que, de hecho, π no es un número algebraico. Por tanto, $\pi \notin \mathscr{C}$.

La pregunta natural es si el recíproco del Corolario 3.11.9 es cierto. Esto es: ¿si $\alpha \in \overline{\mathbb{Q}}$ y el grado del polinomio mínimo de α sobre $\mathbb{Q}$ es una potencia de 2, entonces $\alpha \in \mathscr{C}$? El siguiente resultado resuelve la cuestión.

Teorema 3.11.13. *Sean $\alpha \in \overline{\mathbb{Q}}$ y $\mathbb{Q} \subset L \subset \overline{\mathbb{Q}}$ el cuerpo de descomposición del polinomio mínimo de α sobre $\mathbb{Q}$. Entonces $\alpha \in \mathscr{C}$ si, y sólo si, $[L : \mathbb{Q}]$ es una potencia de 2.*

Demostración. Supongamos, en primer lugar, que $[L : \mathbb{Q}] = 2^m$. Puesto que $L/\mathbb{Q}$ es Galois se deduce que el orden del grupo de Galois es $|\mathrm{Gal}(L/\mathbb{Q})| = 2^m$. Esto es, $\mathrm{Gal}(L/\mathbb{Q})$ es un 2-grupo y, en consecuencia, es un grupo resoluble. Esto significa que existe una torre de subgrupos

$$\mathrm{Gal}(L/\mathbb{Q}) = G_m \triangleright G_{m-1} \triangleright \cdots \triangleright G_1 \triangleright G_0 = \{1\},$$

tales que $[G_i : G_{i-1}] = 2$ (puesto que $|\mathrm{Gal}(L/\mathbb{Q})| = 2^m$). Esta torre de subgrupos corresponde a una torre de subcuerpos

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{m-1} \subset F_m = L,$$

donde $[F_i : F_{i-1}] = 2$. Por Teorema 3.11.7, α es constructible.
Para el recíproco, demostramos primero que $\mathbb{Q} \subset \mathscr{C}$ es una extensión normal (de grado infinito). En efecto, sean $\alpha \in \mathscr{C}$ y p el polinomio mínimo de α sobre $\mathbb{Q}$. Hemos de probar que p factoriza en producto de factores lineales en $\mathscr{C}$. En efecto, existe

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C},$$

donde $[F_i : F_{i-1}] = 2$ y $\alpha \in F_n$. Sea $M \subset \mathbb{C}$ la clausura de Galois de $F_n/\mathbb{Q}$. Entonces p factoriza en producto de factores lineales en M, puesto que $M/\mathbb{Q}$ es normal y $\alpha \in F_n \subset M$. Ahora, sea $\beta \in M$ una raíz de p. Existe $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$ tal que $\sigma(\alpha) = \beta$. Aplicando σ a la torre anterior obtenemos

$$\mathbb{Q} = \sigma(F_0) \subset \sigma(F_1) \subset \cdots \subset \sigma(F_{n-1}) \subset \sigma(F_n) \subset \mathbb{C},$$

donde $[\sigma(F_i) : \sigma(F_{i-1})] = 2$ y $\beta \in \sigma(F_n)$. Esto muestra que $\beta \in \mathscr{C}$ y, por tanto, p factoriza en producto de factores lineales en $\mathscr{C}$.
Se deduce que $\mathscr{C}$ contiene el cuerpo $L \subset \mathbb{C}$ de descomposición de p sobre $\mathbb{Q}$. Por el Teorema de elemento primitivo $L = \mathbb{Q}(\gamma)$ para algún $\gamma \in L$. Puesto que $\gamma \in \mathscr{C}$, por Corolario 3.11.9, se deduce que $[\mathbb{Q}(\gamma) : \mathbb{Q}] = [L : \mathbb{Q}]$ es una potencia de 2. Esto completa la demostración del Teorema. □

Ejemplo 3.11.14. Sea α una raíz del polinomio

$$f = X^4 - 4X^2 + X + 1 \in \mathbb{Q}[X].$$

Es fácil comprobar que f es irreducible sobre $\mathbb{Q}$, de forma que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Si embargo, se puede probar que el grupo $\mathrm{Gal}(f/\mathbb{Q})$ es el grupo simétrico S_4. Por tanto, el grado del cuerpo L de descomposición del polinomio mínimo de α sobre $\mathbb{Q}$ es $[L : \mathbb{Q}] = 24$, que no es una potencia de 2. Concluimos que α no es constructible, aunque $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es una potencia de 2.

3.11.2. Polígonos regulares y raíces de la unidad

La teoría de la sección anterior permite obtener una condición necesaria y suficiente para que el polígono regular de n lados sea constructible con regla y compás. Para ello usaremos la extensión ciclotómica $\mathbb{Q}(\zeta)/\mathbb{Q}$, donde ζ es una raíz primitiva n–ésima de la unidad.
Antes de enunciar el resultado principal, necesitamos alguna terminología: un primo impar p se dice un *primo de Fermat* si se puede escribir en la forma

$$p = 2^{2^m} + 1$$

para algún entero $m \geq 0$. El siguiente resultado, que caracteriza los polígonos constructibles, se debe a Gauss.

Teorema 3.11.15. *Sea $n \geq 3$ un entero. Entonces el polígono regular de n lados es constructible con regla y compás si, y sólo si,*

$$n = 2^s p_1 \cdots p_r,$$

donde $s \geq 0$ es un entero y $p_1, \ldots, p_r$ son $r \geq 0$ distintos primos de Fermat.

Demostración. Construir con regla y compás el polígono regular de n lados equivale a dividir la circunferencia en n arcos iguales que, a su vez, es equivalente a construir las raíces n–ésimas de la unidad y, por tanto, es equivalente a construir una raíz n–ésima primitiva de la unidad ζ.
Sabemos que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ y que la extensión $\mathbb{Q}(\zeta)/\mathbb{Q}$ es normal. Por tanto, según el Teorema 3.11.13, ζ es constructible si, y sólo si, $\varphi(n)$ es una potencia de 2.
Escribimos $n = q_1^{a_1} \cdots q_t^{a_t}$, donde q_i primos distintos y $a_i \geq 1$. Entonces

$$\varphi(n) = \varphi(q_1^{a_1}) \cdots \varphi(q_t^{a_t}) = q_1^{a_1-1}(q_1 - 1) \cdots q_t^{a_t-1}(q_t - 1).$$

Por tanto, $\varphi(n)$ es una potencia de 2 si, y sólo si,

$$n = 2^s p_1 \cdots p_r$$

donde los p_i son primos impares distintos tales que $p_i - 1$ es una potencia de 2.
Ahora bien, $p_i - 1$ es una potencia de 2 si, y sólo si, $p_i = 2^{s_i} + 1$. Además si $p = 2^t + 1$ es primo, entonces t es una potencia de 2. En efecto, si $t = uv$, donde v es impar entonces $2^t + 1 = (2^u + 1)(2^{u(v-1)} - 2^{u(v-2)} + \cdots - 2^u + 1)$. Esto completa la demostración del teorema. □

3.11.16. Observemos que la potencia de 2 en el teorema anterior tiene sentido, puesto que si el polígono regular de n lados es constructible, entonces trazando la bisectriz de cada ángulo se construye el polígono regular de $2n$ lados.

3.11.17. El *m–ésimo número de Fermat* es $F_m = 2^{2^m} + 1$, y un primo de Fermat es un número de Fermat que es primo. Los cinco primos de Fermat conocidos son

$$\begin{aligned} F_0 &= 3, \\ F_1 &= 5, \\ F_2 &= 17, \\ F_3 &= 257, \\ F_4 &= 65537. \end{aligned}$$

El número $F_5 = 2^{32} + 1$ es divisible por 641. También es conocido que $F_6, \ldots, F_{31}, F_{32}$ son compuestos, pero la condición de F_{33} es todavía incierta (en 2003). Este F_{33} es realmente un número muy grande. También se sabe que F_m es compuesto para ciertos valores diseminados de m. Por ejemplo, en 2003 se probó que $F_{2478782}$ es divisible por $3 \cdot 2^{2478785} + 1$. Estos son números extremadamente grandes. De hecho, mucha gente sospecha que F_0, F_1, F_2, F_3, F_4 son los únicos primos de Fermat.

3.11.18. El número $F_2 = 17$ es primo. Por tanto, el polígono regular de 17 lados es constructible con regla y compás. Gauss sabía que una construcción con regla y compás efectiva del polígono regular de 17 lados no era un asunto sencillo. De hecho, en lugar de dar una construcción explícita, Gauss demuestra que

$$\begin{aligned} \cos(2\pi/17) = &-\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} \\ &+ \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}. \end{aligned}$$

Esta fórmula permite dar una construcción explícita, aunque no es muy eficiente, del polígono de 17 lados. Métodos más elegantes para construir este polígono, junto con el 257 lados, fueron descubiertos hacia 1830. Existe también la historia del Profesor Hermes en Lingen que, a finales del siglo XIX, trabajó 10 años en la construcción del polígono regular de 65537 lados.

3.12. Ejercicios

(1) Consideremos la ecuación $x^3 + x - 2 = 0$, una de cuyas raíces es $x = 1$.

a) Usar las fórmulas de Cardano para obtener la fórmula

$$1 = \sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}} + \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{3}}}.$$

b) Demostrar que $1 + \frac{2}{3}\sqrt{\frac{7}{3}} = \left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{7}{3}}\right)^3$. Usar esta igualdad para explicar el apartado anterior.

(2) (Fórmulas de Newton) Sea $f(X)$ un polinomio mónico de grado n con raíces $\alpha_1, \ldots, \alpha_n$. Sea s_i la función simétrica elemental de grado i en las raíces y definamos $s_i = 0$ para $i > n$. Sea $p_i = \alpha_1^i + \ldots + \alpha_n^i$, $i \geq 0$, la suma de las potencias i–ésimas de las raíces de $f(X)$. Demostrar la fórmulas de Newton:

$$\begin{aligned} p_1 - s_1 &= 0, \\ p_2 - s_1 p_1 + 2s_2 &= 0, \\ p_3 - s_1 p_2 + s_2 p_1 - 3s_3 &= 0, \\ &\vdots \\ p_i - s_1 p_{i-1} + s_2 p_{i-2} - \cdots + (-1)^{i-1} s_{i-1} p_1 + (-1)^i i s_i &= 0. \end{aligned}$$

(3) Sea $f(X)$ un polinomio mónico de grado n con raíces $\alpha_1, \ldots, \alpha_n$.
(a) Demostrar que el discriminante D de $f(X)$ es el cuadrado del determinante de Vandermonde

$$\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{vmatrix} = \prod_{i<j} (\alpha_i - \alpha_j).$$

(b) Demostrar que multiplicando a la izquierda la matriz de Vandermonde anterior por su traspuesta y tomando determinante se obtiene

$$D = \begin{vmatrix} p_0 & p_1 & p_2 & \cdots & p_{n-1} \\ p_1 & p_2 & p_3 & \cdots & p_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_n & p_{n+1} & \cdots & p_{2n-2} \end{vmatrix}$$

donde $p_i = \alpha_1^i + \ldots + \alpha_n^i$, $i \geq 0$, la suma de las potencias i–ésimas de las raíces de $f(X)$, que pueden ser calculadas en términos de los coeficientes de $f(X)$ usando las fórmulas de Newton anteriores. Esto proporciona un procedimiento eficiente para calcular el determinante de un polinomio.

(4) (a) Sea p un primo y denotemos $\epsilon_1, \epsilon_2, \ldots, \epsilon_{p-1}$ las raíces primitivas p–ésimas de la unidad. Definimos $p_n = \epsilon_1^n + \epsilon_2^n + \cdots + \epsilon_{p-1}^n$, la suma de las potencias n–ésimas de los ϵ_i. Demostrar que $p_n = -1$ si p no divide a n y que $p_n = p - 1$ si p divide a n. [Un enfoque: $p_1 = -1$ según $\Phi_p(X)$; demostrar que p_n es un conjugado de p_1 para p que no divide a n, por tanto es también -1.]
(b) Demostrar que el discriminante del polinomio ciclotómico $\Phi_p(X)$ de las raíces p–ésimas de la unidad para un primo impar p es $(-1)^{(p-1)/2}p^{p-2}$.
(c) Demostrar que $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}) \subset \mathbb{Q}(\zeta_p)$ para p un primo impar.

(5) Usar las fórmulas de Cardano para resolver la ecuación cúbica $X^3 + X^2 - 2$. En particular mostrar que la ecuación tiene la raíz real

$$\frac{1}{3}(\sqrt[3]{26 + 15\sqrt{3}} + \sqrt[3]{26 - 15\sqrt{3}} - 1).$$

Mostrar directamente que las raíces de esta cúbica son $1, -1 \pm i$. Explicar esto probando que

$$\sqrt[3]{26 + 15\sqrt{3}} = 2 + \sqrt{3} \qquad \sqrt[3]{26 - 15\sqrt{3}} = 2 - \sqrt{3},$$

de forma que

$$\sqrt[3]{26 + 15\sqrt{3}} + \sqrt[3]{26 - 15\sqrt{3}} = 4.$$

(6) Sean p un primo impar, y ζ una raíz primitiva p–ésima de la unidad en $\mathbb{C}$. Sean $E = \mathbb{Q}(\zeta)$ y $G = Gal(E/\mathbb{Q})$; de forma que $G = (\mathbb{Z}/(p))^*$. Sea H un subgrupo de índice 2 en G. Denotemos $\alpha = \sum_{i \in H} \zeta^i$ y $\beta = \sum_{i \in G/H} \zeta^i$. Demostrar:

a) Ambos α y β son fijados por H;

b) si $\sigma \in G/H$, entonces $\sigma\alpha = \beta, \sigma\beta = \alpha$.

Por tanto α y β son raíces del polinomio $X^2 + X + \alpha\beta \in \mathbb{Q}[X]$. Calcular $\alpha\beta$ y mostrar que el cuerpo fijo de H es $\mathbb{Q}[\sqrt{p}]$ cuando $p \equiv 1 \pmod 4$ y $\mathbb{Q}[\sqrt{-p}]$ cuando $p \equiv 3 \pmod 4$.

(7) Hallar el grado y el polinomio mínimo sobre $\mathbb{Q}$ de $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

(8) Demostrar que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ [una inclusión es trivial, para la otra considerar $(\sqrt{2} + \sqrt{3})^2$, etc.]. Concluir que $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. Obtener el polinomio mínimo sobre $\mathbb{Q}$ de $\sqrt{2} + \sqrt{3}$.

(9) Sea F un cuerpo de característica distinta de 2. Sean D_1 y D_2 elementos de F, ninguno de ellos un cuadrado en F. Demostrar que $F(\sqrt{D_1}, \sqrt{D_2})$ es de grado 4 sobre F si D_1D_2 no es un cuadrado en F y es de grado 2 sobre F en otro caso. En el caso de grado 4 se llama una extensión bicuadrática.

(10) Determinar el grado de la extensión $\mathbb{Q}(\sqrt{3+2\sqrt{2}})$ sobre $\mathbb{Q}$.

(11) Supongamos que $F = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ donde $\alpha_i^2 \in \mathbb{Q}$ para $i = 1, \ldots, n$. Demostrar que $\sqrt[3]{2} \notin F$.

(12) Sea K/F una extensión algebraica y sea R un subanillo de K que contiene a F. Demostrar que R es un subcuerpo de K.

(13) Sea $f(X)$ un polinomio irreducible de grado n sobre un cuerpo F. Sea $g(X)$ un polinomio en $F[X]$. Demostrar que cada factor irreducible del polinomio $f(g(X))$ tiene grado divisible por n.

(14) Sea K/F una extensión de grado n.
(a) Para cada $\alpha \in K$ la acción de α por multiplicación a la izquierda en K es una aplicación F–lineal.
(b) Demostrar que K es isomorfo a un subcuerpo del anillo de matrices $n \times n$ sobre F, de forma que el anillo de matrices $n \times n$ sobre F contiene una copia isomorfa de cada extensión de F de grado n.
(c) Sea A la matriz de la multiplicación por α. Demostrar que α es raíz del polinomio característico de A. Usar este procedimiento para obtener el polinomio mónico de grado 3 una de cuyas raíces es $\sqrt[3]{2}$, ídem. para $1 + \sqrt[3]{2} + \sqrt[3]{4}$.
(d) Sea $K = \mathbb{Q}(\sqrt{D})$ para cierto entero libre de cuadrados. Sea $\alpha = a + b\sqrt{D} \in K$. Usar la base $\{1, \sqrt{D}\}$ para K como $\mathbb{Q}$–espacio vectorial para probar que la matriz de la multiplicación por α en K es $\begin{bmatrix} a & bD \\ b & a \end{bmatrix}$. Demostrar directamente que la aplicación $a+b\sqrt{D} \mapsto \begin{bmatrix} a & bD \\ b & a \end{bmatrix}$ es un isomorfismo de K con un subcuerpo del anillo de matrices 2×2 sobre $\mathbb{Q}$.

(15) Demostrar que si $[F(\alpha) : F]$ es (finito) impar, entonces $F(\alpha^2) = F(\alpha)$.

(16) Sean F un cuerpo y α una raíz del polinomio irreducible $X^n - a \in F[X]$ (e.g. $X^n - 2 \in \mathbb{Q}[X]$). Supongamos que $m|n$. Demostrar que $[F(\alpha^m) : F] = n/m$. ¿Cuál es el polinomio mínimo de α^m sobre F?

(17) Supongamos que $[F(\alpha) : F] = m$ y $[F(\beta) : F] = n$. Demostrar que $[F(\beta)(\alpha) : F(\beta)] = m$ si, y sólo si, $[F(\alpha)(\beta) : F(\alpha)] = n$, y que ambas son ciertas si mcd $(m, n) = 1$ y, entonces $[F(\alpha, \beta) : F] = mn$.

(18) Sean $a \in F$ y mcd $(m, n) = 1$. Demostrar
(a) α es raíz de $X^{mn} - a$ si, y sólo si, α^m es raíz de $X^n - a$.
(b) Si α es raíz de $X^{mn} - a$ y $X^m - a$ y $X^n - a$ son irreducibles sobre F, entonces $[F(\alpha^m) : F] = n$, $[F(\alpha^n) : F] = m$ y $[F(\alpha) : F] = mn$.
(c) $X^{mn} - a$ es irreducible si, y sólo si, $X^m - a$ y $X^n - a$ son irreducibles.

(19) Hallar los polinomios mínimos sobre $\mathbb{Q}$ de los elementos
(a) $\sqrt{5} + \sqrt[4]{5}$.
(b) $\alpha^2 - 1$, si $\alpha^3 - 2\alpha - 2 = 0$.

(20) Calcular $[\mathbb{Q}(\sqrt[3]{2}, \alpha) : \mathbb{Q}]$ si $\alpha^4 + 6\alpha + 2 = 0$.

(21) Determinar cuáles de los polinomios que siguen son irreducibles sobre los cuerpos que se indican.
(a) $X^2 + 3$ sobre $\mathbb{Q}(\sqrt{7})$.
(b) $X^3 + 8X - 2$ sobre $\mathbb{Q}(\sqrt{2})$.
(c) $X^5 + 3X^3 - 9X - 6$ sobre $\mathbb{Q}(\sqrt{7}, \sqrt{5}, 1 + i)$.

(22) Consideramos el polinomio $f(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$.
(a) Probar que $f(X)$ es irreducible.
(b) Sea α una raíz de $f(X)$. Escribir $\beta = \frac{3\alpha-2}{\alpha^2+1} \in \mathbb{Q}(\alpha)$ en función de la base $\{1, \alpha, \alpha^2\}$.
(c) Hallar el polinomio mínimo de $\delta = 5\alpha - 2$ sobre $\mathbb{Q}$.

(23) Sea α una raíz del polinomio $X^4 + 2X^2 + 2 \in \mathbb{Q}[X]$.
(a) Hallar $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ y expresar el inverso de $\alpha + 1$ en $\mathbb{Q}(\alpha)$ en función de una base de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$.
(b) Hallar el polinomio mínimo de $\beta = \frac{1}{2}\alpha$ sobre $\mathbb{Q}$.
(c) Hallar $[\mathbb{Q}(\alpha^2 - 1) : \mathbb{Q}]$.

(24) Sea α una raíz del polinomio $f(X) = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$.
(a) Calcular $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ y una base de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$.
(b) Obtener el polinomio mínimo de $\alpha^2 - 2$ sobre $\mathbb{Q}$.
(c) Demostrar que $\mathbb{Q}(\alpha)$ es un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$.

(25) Sean t un elemento trascendente sobre $\mathbb{F}_3$, $F = \mathbb{F}_3(t)$, $f(X) = X^6 - (t+1)X^3 + (-t^2+1) \in F[X]$ y α una raíz de $f(X)$.
(a) Averiguar si $f(X)$ es separable o inseparable.
(b) Hallar el polinomio mínimo de α^3 sobre F.
(c) Hallar el polinomio mínimo de α sobre $F(\alpha^3)$.

(26) Sean $f(X) = X^3 + 2X + 1 \in \mathbb{F}_5[X]$ y α una raíz de $f(X)$.
(a) Demostrar que $f(X)$ es irreducible.
(b) Demostrar que $\mathbb{F}_5(\alpha)$ es perfecto.
(c) Expresar $\sqrt[5]{\alpha}$ en función de una base de $\mathbb{F}_5(\alpha)$ sobre $\mathbb{F}_5$.

(27) (a) Hallar todos los polinomios irreducibles de grados 1, 2 y 4 sobre $\mathbb{F}_2$. Probar que su producto es $X^{16} - X$.
En general se tiene:
(b) Sea $f(X) \in \mathbb{F}_q[X]$ irreducible. Demostrar que $f(X)$ divide a $X^{q^n} - X$ si, y sólo si,

deg f divide a n. Demostrar la formula

$$X^{q^n} - X = \prod_{d|n} \prod_{f_d} f_d(X),$$

donde el producto interior es sobre todos los polinomios mónicos irreducibles de grado d. Contando los grados, demostrar que

$$q^n = \sum_{d|n} d\psi(d),$$

donde $\psi(d)$ es el número de polinomios mónicos irreducibles de grado d. Invertir esta fórmula usando el siguiente resultado.
(c) Sea $\mathbb{Z}^+$ el conjunto de los enteros positivos, y A un grupo aditivo abeliano. Sean $\mathbb{Z}^+ \xrightarrow{f} A$ y $\mathbb{Z}^+ \xrightarrow{g} A$ aplicaciones. Supongamos que para todo n,

$$f(n) = \sum_{d|n} g(d).$$

Sea μ la función de Mobius definida por $\mu(1) = 1$, $\mu(p_1 \cdots p_r) = (-1)^r$ si $p_1, \ldots, p_r$ son primos distintos, y $\mu(m) = 0$ si m es divisible por p^2 para algún primo p. Demostrar que

$$g(n) = \sum_{d|n} \mu(n/d) f(d).$$

(d) Obtener la fórmula

$$n\psi(n) = \sum_{d|n} \mu(d) q^{n/d}.$$

(28) (a) Para cada primo p y cada elemento no nulo $a \in \mathbb{F}_p$ demostrar que $X^p - X - a$ es irreducible sobre $\mathbb{F}_p$. (Indicación: demostrar que si α es una raíz entonces $\alpha + 1$ es también una raíz).
(b) Estudiar la irreducibilidad y el grupo de Galois de $X^5 - X - u$ sobre $\mathbb{F}_5(u)$, donde u es una raíz de $X^3 + 2X^2 + 2X + 2 \in \mathbb{F}_5[X]$. (Indicación: obtener la descomposición en producto de factores lineales de $X^5 - X - u$ en $\mathbb{F}_5(u)(\alpha)$ con α una raíz de $X^5 - X - u$).

(29) Usando la fórmula

$$X^{p^n - 1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^*} (X - \alpha),$$

obtener la fórmula

$$\prod_{\alpha \in \mathbb{F}_{p^n}^*} \alpha = (-1)^{p^n}.$$

Por tanto, el producto de los elementos no nulos de un cuerpo finito es $+1$ si $p = 2$ y -1 si p es impar. Para p impar y $n = 1$ deducir el Teorema de Wilson:

$$(p-1)! \equiv -1 \pmod{p}.$$

(30) (a) Supongamos que $\mathrm{mcd}(m,n) = 1$. Sean ζ_m y ζ_n raíces primitivas m–ésima y n-ésima de la unidad. Probar que $\zeta_m\zeta_n$ es una raíz primitiva mn-ésima de la unidad.
(b) Probar que si un cuerpo (donde $2 \neq 0$) contiene las raíces n-ésimas de la unidad para n impar entonces también contiene las raíces $2n$-ésimas de la unidad.

(31) Demostrar que, en característica cero, si $n > 1$ es impar, $\Phi_{2n}(X) = \Phi_n(-X)$.

(32) (a) Demostrar que existe $\alpha \in \mathbb{F}_{p^n}$ tal que $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$. (Indicación: el grupo $\mathbb{F}_{p^n}^*$ es cíclico). Concluir que para cada n existen polinomios irreducibles de grado n en $\mathbb{F}_p[X]$.
(b) Construir explícitamente un cuerpo finito de 16 elementos, considerando, por ejemplo, el polinomio $X^4 + X + 1 \in \mathbb{F}_2[X]$.

(33) Hallar los $\mathbb{Q}$–conjugados, estudiar la normalidad y obtener el grupo de Galois de la extensión simple generada por cada uno de los siguientes elementos:
(a) $\sqrt{5}$. (b) $\sqrt[4]{3}$. (c) $\sqrt{2} + \sqrt{3}$. (d) $\sqrt{1 + \sqrt{3}}$.

(34) Dar un ejemplo de cuerpos $F \subset E \subset K$, donde K/E y E/F sean extensiones normales y K/F no sea normal.

(35) Sean $f(X) = X^8 - 8X^4 + 7 \in \mathbb{Q}[X]$ y E_f el cuerpo de descomposición de f sobre $\mathbb{Q}$.
(a) Describir $\mathrm{Gal}(E_f/\mathbb{Q})$.
(b) Hallar un cuerpo intermedio $\mathbb{Q} \subset K \subset E_f$ tal que $\mathrm{Gal}(E_f/K)$ sea un subgrupo normal de orden 2 de $\mathrm{Gal}(E_f/\mathbb{Q})$.

(36) Se considera el polinomio $f(X) = X^6 - 6X^3 + 8 \in \mathbb{Q}[X]$.
(a) Obtener un cuerpo de descomposición, E_f, de f sobre $\mathbb{Q}$. Calcular $[E_f : \mathbb{Q}]$ y hallar $\mathrm{Gal}(E/\mathbb{Q})$.
(b) Determinar si $\mathbb{Q}(\sqrt[3]{4})$, $\mathbb{Q}(\sqrt{3}i)$, $\mathbb{Q}(\sqrt{3}, i)$ son cuerpos intermedios de la extensión $E/\mathbb{Q}$.
(c) Determinar cuáles de los cuerpos del apartado anterior se corresponden con un subgrupo normal de $\mathrm{Gal}(E/\mathbb{Q})$.

(37) (a) Sean F un cuerpo, de característica distinta de 2, y $a, b \in F$ tales que $\sqrt{a}, \sqrt{b} \notin F$. Demostrar que $F(\sqrt{a}) = F(\sqrt{b})$ si, y sólo si, $a = c^2 b$ para algún $c \in F$.
(b) Utilizar el resultado anterior para demostrar que $\mathbb{Q}(\sqrt{3 + \sqrt{2}})$ no es una extensión normal de $\mathbb{Q}$.

(38) Sea α una raíz del polinomio $f(X) = X^3 - 3X + 1$. Demostrar que el cuerpo de descomposición de este polinomio es $\mathbb{Q}(\alpha)$ y que el grupo de Galois es cíclico de orden 3. En particular las otras raíces de este polinomio pueden ser escritas en la forma $a + b\alpha + c\alpha^2$ para ciertos $a, b, c \in \mathbb{Q}$. Hallar las otras raíces de forma explícita en términos de α.

(39) (a) Hallar el polinomio mínimo de $\alpha = \sqrt{1+\sqrt{7}}$ sobre $\mathbb{Q}$.
(b) Averiguar si $\mathbb{Q}(\alpha)$ es una extensión normal de $\mathbb{Q}$.
(c) Hallar $\mathrm{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q})$.
(d) Hallar una extensión E de $\mathbb{Q}(\alpha)$ que sea extensión normal de $\mathbb{Q}$.

(40) Demostrar que el grupo de Galois de $f(X) = X^5 - 6X + 3$ sobre $\mathbb{Q}$ es isomorfo a S_5. En consecuencia la ecuación $X^5 - 6X + 3 = 0$ no es resoluble por radicales.

(41) Sean p un número primo, F un cuerpo que contiene a las raíces p–ésimas de la unidad y $a \in F$ tal que $\sqrt[p]{a} \notin F$. Demostrar que $X^p - a$ es irreducible en $F[X]$.

(42) (a) Hallar el grupo de Galois de $f(X) = X^4 + 2$ sobre $\mathbb{Q}$.
(b) Establecer explícitamente la correspondencia de Galois entre los subgrupos de $\mathrm{Gal}(f/\mathbb{Q})$ y los cuerpos intermedios de la extensión $E_f/\mathbb{Q}$. donde E_f es el cuerpo de descomposición de f sobre $\mathbb{Q}$.

(43) Sean $f(X) = (X^3 - 3)(X^2 + 3) \in \mathbb{Q}[X]$ y E un cuerpo de descomposición de f sobre $\mathbb{Q}$. Se pide:
(a) Hallar $\mathrm{Gal}(E/\mathbb{Q})$.
(b) Establecer la correspondencia de Galois entre los subgrupos de $Gal(E/\mathbb{Q})$ y los cuerpos intermedios entre $\mathbb{Q}$ y E.
(c) Estudiar cuáles de estos cuerpos son extensiones normales de $\mathbb{Q}$.

(44) Sean $p > 2$ y q dos números primos, $f(X) = X^p - q$ y E un cuerpo de descomposición de f sobre $\mathbb{Q}$. Se pide:
(a) Describir $\mathrm{Gal}(E/\mathbb{Q})$.
(b) Obtener todos los cuerpos intermedios $\mathbb{Q} \subset K \subset E$ tales que $[K : \mathbb{Q}] = p - 1$, y estudiar cuáles de ellos son extensiones normales de $\mathbb{Q}$.
(c) En el caso $p = 7$, demostrar que existen cuerpos intermedios de todos los grados posibles en la extensión $E/\mathbb{Q}$.

(45) Se considera el polinomio $f(X) = (X^3 - 5)(X^2 - 3) \in \mathbb{Q}[X]$.
(a) Probar que el grupo de Galois de f sobre $\mathbb{Q}$ es isomorfo a $D_3 \times \mathbb{Z}_2$.
(b) Demostrar que $\mathrm{Gal}(f/\mathbb{Q})$ tiene un único subgrupo normal de orden 3, tres subgrupos no normales de orden 4, y tres subgrupos normales de orden 6.
(c) Sea $\alpha = \sqrt{3} + \omega$. Calcular el polinomio mínimo de α sobre $\mathbb{Q}$.

(46) (a) Obtener el grupo de Galois sobre $\mathbb{Q}$, del polinomio mínimo de $\alpha = \sqrt{1+\sqrt{11}}$ sobre $\mathbb{Q}$.
(b) Obtener los subgrupos normales de orden 2 de dicho grupo y sus correspondientes cuerpos fijos.

(47) Sea $f(X) = (X^{12} - 16)(X^2 - 3) \in \mathbb{Q}[X]$.
(a) Hallar $\mathrm{Gal}(f/\mathbb{Q})$.

(b) Obtener todos los subgrupos de $\mathrm{Gal}(f/\mathbb{Q})$ y sus correspondientes cuerpos fijos.
(c) Averiguar cuáles de los subgrupos de $\mathrm{Gal}(f/\mathbb{Q})$ son normales.

(48) Se considera el polinomio $f(X) = (X^3 - 2)(X^4 - 3) \in \mathbb{Q}[X]$. Se pide:
(a) Describir $\mathrm{Gal}(f/\mathbb{Q})$.
(b) Calcular los subgrupos de Sylow de $\mathrm{Gal}(f/\mathbb{Q})$ y sus correspondientes cuerpos fijos.
(c) Demostrar que $\mathrm{Gal}(f/\mathbb{Q})$ tiene subgrupos de todos los órdenes posibles.

(49) Sean K/F una extensión de Galois y $G = \{\sigma_1, \ldots, \sigma_n\}$ su grupo de Galois. Decidir razonadamente si es cierto que para todo $\alpha \in K$ los elementos $\sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha)$ y $\sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_n(\alpha)$ pertenecen a F.

(50) *a*) Demostrar que $X^3 - \sqrt{3}$ es irreducible sobre $\mathbb{Q}(\sqrt[4]{3})$.

b) Sea E un cuerpo de descomposición del polinomio $f(X) = (X^4 - 3)(X^6 - 3) \in \mathbb{Q}[X]$.

1) Calcular $[E : \mathbb{Q}]$ (indicación: usar el apartado *a*)).
2) Determinar los cuerpos intermedios de la extensión $E/\mathbb{Q}$ que tienen grado 8 sobre $\mathbb{Q}$.
3) Determinar los cuerpos intermedios de la extensión $E/\mathbb{Q}$ que tienen grado 3 sobre $\mathbb{Q}$.

(51) Sea ω una raíz primitiva cúbica de la unidad. Sean $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \omega)$ y $E = \mathbb{Q}(\sqrt{2} + \omega)$.

a) Calcular $[K : \mathbb{Q}]$.

b) Decidir si la extensión $K/\mathbb{Q}$ es de Galois.

c) Describir todos los elementos de $G = \mathrm{Gal}\,(K/\mathbb{Q})$.

d) Determinar los elementos de G que forman $\mathrm{Gal}\,(K/E)$ y halla $[E : \mathbb{Q}]$.

e) Describir todos los elementos de $\mathrm{Gal}\,(E/\mathbb{Q})$.

f) Calcular los coeficientes del polinomio mínimo de $\sqrt{2}+\omega$ sobre $\mathbb{Q}$. (Indicación: los conjugados de $\sqrt{2} + \omega$ están en K).

g) Hallar todos los cuerpos intermedios $\mathbb{Q} \subset F \subset K$ tales que $[F : \mathbb{Q}] = 4$. Justificar que las extensiones que has encontrado son todas las que existen.

(52) Sea $p(X) = (X^3 - 5)(X^2 - 7) \in \mathbb{Q}[X]$.

a) Determinar el cuerpo de descomposición E de $p(X)$ sobre $\mathbb{Q}$ y el grado $[E : \mathbb{Q}]$.

b) Demostrar que $\sqrt{3}\,i \in E$ y hallar el grupo de Galois $\mathrm{Gal}(E/\mathbb{Q}(\sqrt{3}\,i))$.

c) Hallar todos los cuerpos intermedios entre $\mathbb{Q}(\sqrt{3}\,i)$ y E.

(53) Sea α una raíz real del polinomio $f(X) = X^3 - 12X + 8 \in \mathbb{Q}[X]$.

a) Comprobar que $f(X)$ no tiene raíces en $\mathbb{Q}$. Concluir que $f(X)$ es irreducible sobre $\mathbb{Q}$ y obtener $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

b) Comprobar que $\frac{1}{2}\alpha^2 - 4$ es raíz de $f(X)$. Demostrar que $\mathbb{Q}(\alpha)$ es el cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$.

c) Sea E el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $(X^4 - 2)f(X)$.

1) Obtener generadores de E sobre $\mathbb{Q}$ (tres generadores: $E = \mathbb{Q}(?, ?, ?)$). Calcular $[E : \mathbb{Q}]$.
(Indicación: Usar que $\mathbb{Q}(\alpha)$ es el cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$.)

2) Demostrar que $G = \mathrm{Gal}\,(E/\mathbb{Q}) \simeq D_4 \times \mathbb{Z}_3$.

d) Demostrar que en la extensión $E/\mathbb{Q}$ existe un único cuerpo intermedio de grado 3 sobre $\mathbb{Q}$ y un único cuerpo intermedio de grado 8 sobre $\mathbb{Q}$. Obtener ambos cuerpos intermedios.

e) Hallar todos los subgrupos de orden 12 de G.

(54) Consideramos el polinomio $f = X^{12} - 1 \in \mathbb{Q}[X]$.

a) Obtener la descomposición de f en producto de polinomios irreducibles en $\mathbb{Q}[X]$.

b) Hallar un número complejo α tal que $E = \mathbb{Q}(\alpha)$ sea el cuerpo de descomposición de f sobre $\mathbb{Q}$. Hallar el polinomio mínimo de α sobre $\mathbb{Q}$. (Ayuda: $[E : \mathbb{Q}] = 4$).

c) Describir el grupo de Galois $G = \mathrm{Gal}\,(E/\mathbb{Q})$ y describir todos sus subgrupos.

d) Usando la correspondencia de Galois, describir todos los cuerpos intermedios de la extensión $E/\mathbb{Q}$, expresándolos como extensiones simples de $\mathbb{Q}$.

(55) Consideramos el polinomio $f = X^3 + X + 1 \in \mathbb{Q}[X]$.

a) Mostrar, razonadamente, que f es irreducible sobre $\mathbb{Q}$. Decidir, de forma razonada, si f irreducible sobre $\mathbb{Q}(\sqrt[5]{2})$.

b) Sea α una raíz de f. Expresar $(\alpha + 2)^{-1}$ como combinación lineal de una base de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$.

(56) Sean $\zeta = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ y $E = \mathbb{Q}(\sqrt[6]{2}, \zeta)$.

a) Decidir si la extensión $E/\mathbb{Q}$ es de Galois. Hallar, de forma razonada, el grado $[E : \mathbb{Q}]$. Describir los elementos del grupo $G = \mathrm{Gal}\,(E/\mathbb{Q})$.

b) Sea $\alpha = \sqrt[6]{2} + \zeta$. Obtener los elementos de G que fijan α. Decidir, de forma razonada si $E = \mathbb{Q}(\alpha)$.

c) Obtener todos los subgrupos $H \leq G$ cuyo orden sea $|H| = 4$. ¿Son subgrupos normales?

d) Obtener todos los cuerpos intermedios $\mathbb{Q} \subset K \subset E$ tales que $[K : \mathbb{Q}] = 4$. ¿Son extensiones normales de $\mathbb{Q}$?

(57) Sea α una raíz real del polinomio $f(X) = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$.

a) Comprobar que $f(X)$ no tiene raíces en $\mathbb{Q}$. Concluir que $f(X)$ es irreducible sobre $\mathbb{Q}$ y obtener $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Comprobar que $\alpha^2 - 2$ es raíz de $f(X)$. Concluir que $\mathbb{Q}(\alpha)$ es el cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$.

b) Sea E el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $(X^8 - 4) \cdot f(X)$.

1) Obtener generadores de E sobre $\mathbb{Q}$ (tres generadores: $E = \mathbb{Q}(?, ?, ?)$). Demostrar que $[E : \mathbb{Q}] = 24$.
(Indicación: Usar que $\mathbb{Q}(\alpha)$ es el cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$.)
2) Demostrar que $G = \mathrm{Gal}\,(E/\mathbb{Q}) \simeq D_4 \times \mathbb{Z}_3$.

c) Demostrar que en la extensión $E/\mathbb{Q}$ existe un único cuerpo intermedio de grado 3 sobre $\mathbb{Q}$ y un único cuerpo intermedio de grado 8 sobre $\mathbb{Q}$. Obtener ambos cuerpos intermedios.

d) Hallar todos los cuerpos intermedios de la extensión de grado 2 sobre $\mathbb{Q}$.

(58) Sea $f \in \mathbb{Q}[X]$ un polinomio que tiene una raíz en $\mathbb{C}\mathbb{R}$. ¿Se puede asegurar que $\sqrt{-1}$ pertenece al cuerpo de descomposición de f sobre $\mathbb{Q}$?

(59) Demostrar que el polinomio $X^2 - 2 - 2\sqrt{-2}$ es irreducible en $(\mathbb{Z}[\sqrt{-2}])[X]$ y en $(\mathbb{Q}(\sqrt{-2}))[X]$.

(60) Sean $\alpha = \sqrt{1 + \sqrt{3}}, \beta = \sqrt{1 - \sqrt{3}}$ y $L = \mathbb{Q}(\alpha, \beta)$. Se pide:

a) Demostrar que la extensión $\mathbb{Q} \subset L$ es de Galois. Calcular $[L : \mathbb{Q}]$.

b) Demostrar que $\mathrm{Gal}(L/\mathbb{Q})$ es isomorfo a D_4.

c) Demostrar que $\sqrt{3} \in L$ y que $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{3}))$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

d) Hallar, de forma razonada, todos los cuerpos intermedios $\mathbb{Q} \subset K \subset L$ con $[K : \mathbb{Q}] = 2$.

e) Hallar, de forma razonada, todos los cuerpos intermedios $\mathbb{Q} \subset K \subset L$ con $[K : \mathbb{Q}] = 4$. ¿Cuáles de ellos son extensión normal de $\mathbb{Q}$?

(61) Sea $\alpha = a + bi \in \mathbb{C}$ un número algebraico. Mostrar, razonadamente, que a, b son algebraicos sobre $\mathbb{Q}$.

(62) Sea $p(X) = (X^4 - 3)(X^3 - 7) \in \mathbb{Q}[X]$.

a) Determinar el cuerpo de descomposición E de $p(X)$ sobre $\mathbb{Q}$. Demostrar que el grado $[E : \mathbb{Q}] = 24$.

b) Sea G el grupo de Galois de $E/\mathbb{Q}$. Decidir, de forma razonada, cuántos subgrupos de orden 8 tiene G.

c) Obtener, de forma razonada, todos los cuerpos intermedios de grado 8 sobre $\mathbb{Q}$. ¿Son extensiones normales de $\mathbb{Q}$?

(63) Sea f un polinomio en $\mathbb{Q}[X]$ con cuerpo de descomposición E sobre $\mathbb{Q}$ tal que su grupo de Galois $G = \mathrm{Gal}(E/\mathbb{Q})$ es isomorfo al grupo diedro D_5 del pentágono regular. Decidir, de forma razonada, si f es resoluble por radicales.

(64) Sean $\xi = e^{\pi i/10}$, $\eta = \xi^4$, $i = \sqrt{-1}$ y $u = \eta + \frac{1}{\eta}$. Se pide:

a) Demostrar que $\mathbb{Q} \subset \mathbb{Q}(\eta)$ es una extensión cíclica de grado cuatro cuyo único cuerpo intermedio no trivial es $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{5})$.

b) Demostrar que $\mathbb{Q}(\xi) = \mathbb{Q}(i, \eta)$, $[\mathbb{Q}(\xi) : \mathbb{Q}] = 8$ y calcular el polinomio de ξ sobre $\mathbb{Q}$.

c) Demostrar que el polinomio mínimo de $\xi^2 + \frac{1}{\xi^2}$ sobre $\mathbb{Q}$ es $X^2 - X - 1$ y calcular el polinomio mínimo de $\xi + \frac{1}{\xi}$ sobre $\mathbb{Q}$.

d) Probar que el grupo de Galois $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ es abeliano y encontrar generadores sobre $\mathbb{Q}$ de los cuerpos intermedios de la extensión $\mathbb{Q} \subset \mathbb{Q}(\xi)$.

e) Sea E el cuerpo de descomposición sobre $\mathbb{Q}(\xi)$ del polinomio $f(X) = X^4 - 5$. Demostrar que la extensión $[E : \mathbb{Q}]$ es de Galois, calcular su grado y decidir si el grupo de Galois $\mathrm{Gal}(E/\mathbb{Q})$ es o no abeliano.

(65) El cuerpo de descomposición E de cierto polinomio $f \in \mathbb{Q}[X]$, contiene como subcuerpo a $\mathbb{Q}(\sqrt[4]{7}, i)$. El grado $[E : \mathbb{Q}(\sqrt[4]{7}, i)] = 3$. ¿Es f resoluble por radicales?

(66) Sea E el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $(X^4 - 3)(X^3 - 5)$. Se pide:

a) Expresar, de forma razonada, el cuerpo E como extensión finitamente generada de $\mathbb{Q}$ y demostrar que $[E : \mathbb{Q}] = 24$.

b) Decidir, razonadamente, si $X^3 - 5$ es el polinomio mínimo de $\sqrt[3]{5}$ sobre $\mathbb{Q}(i)$. ¿Y sobre $\mathbb{Q}(i, \sqrt[4]{3})$?

c) Decidir, de forma razonada, cuántos subgrupos de orden 8 tiene $\mathrm{Gal}(E/\mathbb{Q})$.

d) Obtener, de forma razonada, todos los cuerpos intermedios de grado 8 sobre $\mathbb{Q}$. ¿Son extensiones normales de $\mathbb{Q}$?

e) Determinar, de forma razonada, el grupo de Galois de E sobre $\mathbb{Q}(\sqrt[4]{3})$.

(67) Sea $p(X) = (X^4 - 3)(X^3 - 11) \in \mathbb{Q}[X]$.

a) Determinar, de forma razonada, el cuerpo de descomposición E de $p(X)$ sobre $\mathbb{Q}$. Demostrar que el grado $[E : \mathbb{Q}] = 24$.

b) Sea G el grupo de Galois de $E/\mathbb{Q}$. Decidir, de forma razonada, cuántos subgrupos de orden 8 tiene G.

c) Obtener, de forma razonada, todos los cuerpos intermedios de grado 8 sobre $\mathbb{Q}$. ¿Son extensiones normales de $\mathbb{Q}$?

(68) Sea ζ una raíz primitiva undécima de la unidad (e.g. $\zeta = e^{2\pi i/11}$). Sea G el grupo de Galois de la extensión $\mathbb{Q}(\zeta)/\mathbb{Q}$.

a) Demostrar que la extensión $\mathbb{Q}(\zeta)/\mathbb{Q}$ es cíclica. ¿Cuál es su grado? Obtener un generador del grupo cíclico G y el orden de cada uno de los elementos de G.

b) Sea $\alpha = \zeta + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^9$. Demostrar que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-11})$.

c) Sea $\beta = \zeta + \zeta^{10}$. Obtener el subgrupo $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\beta))$.

d) Establecer, razonadamente, la correspondencia de Galois en la extensión $\mathbb{Q}(\zeta)/\mathbb{Q}$.

e) Calcular el polinomio mínimo de β sobre $\mathbb{Q}$. ¿Es posible expresar las raíces de este polinomio como combinación lineal con coeficientes en $\mathbb{Q}$ de potencias de β?

Apéndice A

Ejercicios

A.1. Capítulos 1, 2

(1) Sea R un anillo conmutativo unitario. Sea $p(x) = a_0 + a_1X + \cdots + a_nX^n$ un elemento de $R[X]$. Demostrar que

a) $p(X)$ es unidad en $R[X]$ si, y sólo si, a_0 es unidad en R y $a_1, \cdots, a_n$ son nilpotentes.

b) $p(X)$ es nilpotente si, y sólo si, $a_0, a_1, \cdots, a_n$ son nilpotentes.

c) $p(X)$ es un divisor de cero si, y sólo si, existe $0 \neq b \in R$ tal que $bp(X) = 0$.

d) Si R es un dominio de integridad entonces $R[X]$ es un dominio de integridad.

(2) *a)* Sean $R = \mathbb{Z}[X, Y]$ y $M = (X^2 - 3, X^3 - 3X + 7, Y + X^2)R$. Demostrar que el ideal M es maximal en $R = \mathbb{Z}[X, Y]$ identificando el cociente R/M como un cuerpo finito concreto.

Podemos cambiar los generadores de $M = (X^2 - 3, X^3 - 3X + 7 - X(X^2 - 3), Y + X^2 - (X^2 - 3)) = (X^2 - 3, 7, Y + 3)$. Así obtenemos el isomorfismo

$$\frac{\mathbb{Z}[X,Y]}{M} = \frac{\mathbb{Z}[X,Y]}{7\mathbb{Z}[X,Y] + (X^2 - 3, Y + 3)\mathbb{Z}[X,Y]} \simeq$$
$$\simeq \frac{\frac{\mathbb{Z}[X,Y]}{7\mathbb{Z}[X,Y]}}{\frac{7\mathbb{Z}[X,Y] + (X^2-3, Y+3)\mathbb{Z}[X,Y]}{7\mathbb{Z}[X,Y]}} \simeq \frac{\mathbb{F}_7[X,Y]}{(X^3 - \overline{3}, Y + \overline{3})\mathbb{F}_7[X,Y]},$$

donde $\mathbb{F}_7$ es el cuerpo de 7 elementos.

Comprobamos que el polinomio $X^3 - \overline{3}$ no tiene raíces en $\mathbb{F}_7$ sustituyendo los elementos de $\mathbb{F}_7$ en el polinomio. Esto muestra que $X^2 - \overline{3}$ es irreducible sobre $\mathbb{F}_7$. Sea α una raíz de $X^2 - \overline{3}$ sobre $\mathbb{F}_7$. Puesto que $X^2 - \overline{3}$ es irreducible sobre $\mathbb{F}_7$,

la extensión $\mathbb{F}_7(\alpha) = \mathbb{F}_{49}$ es el cuerpo de 49 elementos. Consideramos ahora el homomorfismo de sustitución

$$\begin{aligned} \mathbb{F}_7[X,Y] &\xrightarrow{\varphi} \mathbb{F}_7(\alpha) \\ X &\mapsto \alpha \\ Y &\mapsto \overline{4}. \end{aligned}$$

El homomorfismo φ es sobreyectivo, puesto que los elementos de $\mathbb{F}_7(\alpha)$ son de la forma $\overline{a}+\overline{b}\alpha$ y el elemento $\overline{a}+\overline{b}\alpha$ es la imagen por φ del polinomio $\overline{a}+\overline{b}X$. Si probamos que $(X^3-\overline{3}, Y+\overline{3})\mathbb{F}_7[X,Y] = \ker\varphi$, por el teorema de isomorfismo obtenemos $\mathbb{F}_7[X,Y]/(X^3-\overline{3}, Y+\overline{3})\mathbb{F}_7[X,Y] \simeq \mathbb{F}_7(\alpha)$ y, en consecuencia, M es maximal en $\mathbb{Z}[X,Y]$. Es claro que $(X^3-\overline{3}, Y+\overline{3})\mathbb{F}_7[X,Y] \subset \ker\varphi$. Para probar que $\ker\varphi \subset (X^3-\overline{3}, Y+\overline{3})\mathbb{F}_7[X,Y]$, sea $f(X,Y) \in \ker\varphi$; dividimos

$$f(X,Y) = (Y+\overline{3})q(X,Y) + (X^2-\overline{3})q_1(X) + \overline{a}X + \overline{b},$$

en $\mathbb{F}_7[X,Y]$. Aplicando φ obtenemos $0 = \overline{a}\alpha + \overline{b}$. Puesto que $\{1,\alpha\}$ son linealmente independientes sobre $\mathbb{F}_7$, obtenemos $\overline{a} = \overline{b} = 0$. Por tanto $f \in (X^3-\overline{3}, Y+\overline{3})\mathbb{F}_7[X,Y]$, como queríamos probar.

b) ¿Qué podemos decir del ideal $I = (X^2-3, X^3-3X+7, Y+X^2)\mathbb{Q}[X,Y]$?

En este caso $I = (X^2-3, 7, Y+3)$. Puesto que 7 es una unidad en $\mathbb{Q}[X,Y]$, vemos que $I = \mathbb{Q}[X,Y]$.

(3) En el anillo $\mathbb{Z}[\sqrt{-6}] = \{a+b\sqrt{-6} \mid a,b \in \mathbb{Z}\}$, consideramos la norma $N(a+b\sqrt{-6}) = a^2+6b^2$.

a) Estudiar, de forma razonada, si el elemento 3 es irreducible en $\mathbb{Z}[\sqrt{-6}]$, y si el ideal $(3)\mathbb{Z}[\sqrt{-6}] = \{3(a+b\sqrt{-6}) \mid a,b \in \mathbb{Z}\}$ es un ideal primo en $\mathbb{Z}[\sqrt{-6}]$.

Para ver que 3 es irreducible en $\mathbb{Z}[\sqrt{-6}]$, hemos de probar que si $3 = (a+b\sqrt{-6})(c+d\sqrt{-6})$, en $\mathbb{Z}[\sqrt{-6}]$, entonces $a+b\sqrt{-6}$ ó $c+d\sqrt{-6}$ es unidad en $\mathbb{Z}[\sqrt{-6}]$. Es decir, que $a^2+6b^2 = 1$ o $c^2+6d^2 = 1$. Tomando normas $9 = (a^2+6b^2)(c^2+6d^2)$. De sta ecuación en $\mathbb{Z}$ deducimos: (1) $a^2+6b^2 = 1, c^2+6d^2 = 9$, (2) $a^2+6b^2 = 3, c^2+6d^2 = 3$, (3) $a^2+6b^2 = 9, c^2+6d^2 = 1$. En el caso (1) $a+b\sqrt{-6}$ es unidad. En el caso (3) $c+d\sqrt{-6}$ es unidad. El caso (2) no ocurre, puesto que $a^2+6b^2 = 3$ no tiene soluciones en $\mathbb{Z}$.

El elemento 3 no es primo en $\mathbb{Z}[\sqrt{-6}]$, Por ejemplo, $\sqrt{-6}\sqrt{-6} = (-2)\cdot 3$, esto es 3 divide a $\sqrt{-6}\sqrt{-6}$ en $\mathbb{Z}[\sqrt{-6}]$; sin embargo, 3 no divide a $\sqrt{-6}$ en $\mathbb{Z}[\sqrt{-6}]$.

b) Demostrar que un elemento $\alpha = a + b\sqrt{-6}$ es unidad en $\mathbb{Z}[\sqrt{-6}]$ si, sólo si, $N(\alpha) = 1$.

Lema 1.2.3: Por definición, $\alpha \in \mathbb{Z}[\sqrt{-6}]$ es unidad si existe $\beta \in \mathbb{Z}[\sqrt{-6}]$ tal que $\alpha\beta = 1$. Supongamos que $\alpha\beta = 1$ entonces $N(\alpha)N(\beta) = 1$ y, por tanto, $N(\alpha) = \pm 1$.
Recíprocamente, si $N(\alpha) = \pm 1$, entonces $\alpha\bar{\alpha} = N(\alpha) = \pm 1$. De aquí $\alpha^{-1} = \pm\bar{\alpha} \in \mathbb{Z}[\sqrt{-6}]$.
En este caso, $N(\alpha) = a^2 + 6b^2$ es siempre positivo. Por tanto, $\alpha \in \mathbb{Z}[\sqrt{-6}]$ es unidad si, y sólo si, $N(\alpha) = 1$.

¿Cuáles son las unidades de $\mathbb{Z}[\sqrt{-6}]$?

Hay que resolver la ecuación $a^2 + 6b^2 = 1$ en $\mathbb{Z}$. Ha de ser $a^2 = 1, b^2 = 0$. Esto es, $a = \pm 1, b = 0$. Por tanto, $\mathbb{Z}[\sqrt{-6}]^* = \{\pm 1\}$.

(4) Consideramos el ideal $I = (X^2 + X + 1,\ Y + X + Z + 1)$ en el anillo $R = \mathbb{Q}[X, Y, Z]$.

a) Estudiar, de forma razonada, si I es primo o maximal en R.

Sea $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Consideramos el homomorfismo de sustitución

$$\begin{aligned} \mathbb{Q}[X, Y, Z] &\xrightarrow{\varphi} \mathbb{Q}(\omega)[Z] \\ f(X, Y, Z) &\mapsto f(\omega, -Z - \omega - 1, Z). \end{aligned}$$

Este homomorfismo es sobreyectivo: $(a_0+b_0X)+(a_1+b_1X)Z+\cdots+(a_n+b_nX)Z^n \mapsto (a_0 + b_0\omega) + (a_1 + b_1\omega)Z + \cdots + (a_n + b_n\omega)Z^n$, donde $(a_0 + b_0\omega) + (a_1 + b_1\omega)Z + \cdots + (a_n + b_n\omega)Z^n$, con $a_i, b_i \in \mathbb{Q}$, representa un elemento cualquiera de $\mathbb{Q}(\omega)[Z]$.

Veamos que $I = \ker\varphi$.

$I \subset \ker\varphi$: un elemento cualquiera de I se escribe $(X^2 + X + 1)f(X, Y, Z) + (Y + X + Z + 1)g(X, Y, Z)$. Así $\varphi((X^2 + X + 1)f(X, Y, Z) + (Y + X + Z + 1)g(X, Y, Z)) = \varphi(X^2 + X + 1)\varphi(f) + \varphi(Y + X + Z + 1)\varphi(g) = 0 \cdot \varphi(f) + 0 \cdot \varphi(g) = 0$.

$\ker\varphi \subset I$: Sea $f \in \ker\varphi$. Dividimos en la variable Y, $f(X, Y, Z) = (Y + X + Z + 1)q(X, Y, Z) + r(X, Z)$. Dividimos en la variable X, $r(X, Z) = (X^2 + X + 1)q_1(X, Z) + (a(Z)X + b(Z))$. Así $f(X, Y, Z) = (Y + X + Z + 1)q(X, Y, Z) + (X^2 + X + 1)q_1(X, Z) + (a_0 + a_1Z + \cdots + a_nZ^n)X + (b_0 + b_1Z + \cdots + b_nZ^n)$. Aplicando φ obtenemos $0 = (a_0 + a_1Z + \cdots + a_nZ^n)\omega + (b_0 + b_1Z + \cdots + b_nZ^n) = (a_0 + b_0\omega) + (a_1 + b_1\omega)Z + \cdots + (a_n + b_n\omega)Z^n$. Por tanto $a_i + b_i\omega = 0$, para cada i. Puesto que $\{1, \omega\}$ son linealmente independientes sobre $\mathbb{Q}$ y $a_i, b_i \in \mathbb{Q}$ se deduce $a_i = b_i = 0$ para todo i. Esto es $a(Z) = b(Z) = 0$. Así $f(X, Y, Z) = (Y + X + Z + 1)q(X, Y, Z) + (X^2 + X + 1)q_1(X, Z) \in I$.

Aplicando el primer teorema de isomorfismo obtenemos

$$\mathbb{Q}[X, Y, Z]/I = \mathbb{Q}[X, Y, Z]/\ker\varphi \simeq \operatorname{im}\varphi = \mathbb{Q}(\omega)[Z].$$

El anillo $\mathbb{Q}(\omega)[Z]$ es un anillo de polinomios en una variable con coeficientes en el cuerpo $\mathbb{Q}(\omega)$. Es, por tanto, un DI que no es cuerpo. Deducimos que I es primo no maximal.

b) Determinar, de forma razonada, un ideal maximal M de R tal que $I \subset M$. ¿Cuál es el grado sobre $\mathbb{Q}$ del cuerpo R/M?

Consideramos $I \subset M = (X^2+X+1, Y+X+Z+1, Z) = (X^2+X+1, Y+X+1, Z)$. Veamos que M es maximal.

Sea $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Consideramos el homomorfismo de sustitución

$$\begin{aligned} \mathbb{Q}[X,Y,Z] &\xrightarrow{\psi} \mathbb{Q}(\omega) \\ f(X,Y,Z) &\mapsto f(\omega, -\omega - 1, 0). \end{aligned}$$

Este homomorfismo es sobreyectivo: $a + bX \mapsto a + b\omega$, donde $a + b\omega$, con $a, b \in \mathbb{Q}$, representa un elemento cualquiera de $\mathbb{Q}(\omega)$.

que $M = \ker\psi$.

$I \subset \ker\psi$: un elemento cualquiera de M se escribe $(X^2+X+1)f(X,Y,Z) + (Y+X+1)g(X,Y,Z) + Zh(X,Y,Z)$. Así $\psi((X^2+X+1)f(X,Y,Z) + (Y+X+1)g(X,Y,Z) + Zh(X,Y,Z)) = \psi(X^2+X+1)\psi(f) + \psi(Y+X+1)\psi(g) + \psi(Z)\psi(h) = 0 \cdot \psi(f) + 0 \cdot \psi(g) + 0 \cdot \psi(h) = 0$.

$\ker\psi \subset M$: Sea $h \in \ker\psi$. Dividimos en la variable Z, $h(X,Y,Z) = Zt(X,Y,Z) + f(X,Y)$. Dividimos en la variable Y, $f(X,Y) = (Y+X+1)q(X,Y) + r(X)$. Dividimos en la variable X, $r(X) = (X^2+X+1)q_1(X) + (aX+b), a, b \in \mathbb{Q}$. Así $h(X,Y,Z) = Zt(X,Y,Z) + (Y+X+1)q(X,Y) + (X^2+X+1)q_1(X) + (a+bX)$. Aplicando ψ obtenemos $0 = a + b\omega$. Puesto que $\{1, \omega\}$ son linealmente independientes sobre $\mathbb{Q}$ y $a, b \in \mathbb{Q}$ se deduce $a = b = 0$. Así $h(X,Y,Z) = Zt(X,Y,Z) + (Y+X+1)q(X,Y) + (X^2+X+1)q_1(X) \in M$.

Aplicando el primer teorema de isomorfismo obtenemos

$$\mathbb{Q}[X,Y,Z]/M = \mathbb{Q}[X,Y,Z]/\ker\psi \simeq \mathrm{im}\varphi = \mathbb{Q}(\omega).$$

Puesto que $\mathbb{Q}(\omega)$ es un cuerpo deducimos que M es maximal.

$[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. El polinomio mínimo de ω sobre $\mathbb{Q}$ es $X^2 + X + 1$.

(5) Consideramos el ideal $\mathfrak{a} = (6, x^2+5)\mathbb{Z}[X]$. Se pide

a) Probar que hay un isomorfismo de anillos

$$\mathbb{Z}[X]/\mathfrak{a} \simeq \mathbb{Z}[X]/(3, x^2+5) \times \mathbb{Z}[X]/(2, x^2+5).$$

b) Probar que hay un isomorfismo de anillos

$$\mathbb{Z}[X]/\mathfrak{a} \simeq \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_2[X]/(x^2+1).$$

Si $\mathbb{Z}[X]/\mathfrak{a}$ es un conjunto finito, ¿cuántos elementos tiene?

c) Probar que hay un ideal primo $\mathfrak{p}$ de $\mathbb{F}_2[X]$ tal que $(x^2+5)\mathbb{F}_2[X] \subset \mathfrak{p}$.

d) Probar que hay un ideal primo $\mathfrak{q}$ de $\mathbb{Z}[X]$ tal que $\mathfrak{a} \subset \mathfrak{q}$. ¿Es posible encontrar un ideal maximal $\mathfrak{m}$ de $\mathbb{Z}[X]$ tal que $\mathfrak{a} \subset \mathfrak{m}$?

(6) Sean $\alpha \in \mathbb{C}$ tal que $\alpha^3 = 5$ y $\mathfrak{a} = (\alpha+1)\mathbb{Z}[\alpha]$ Consideramos el homomorfismo $\varphi : \mathbb{Z} \to \mathbb{Z}[\alpha]/\mathfrak{a}, x \mapsto x + \mathfrak{a}$

a) Demostrar que cada elemento de $\mathbb{Z}[\alpha]$ se escribe, de modo único, como $a\alpha^2 + b\alpha + c$ para ciertos $a, b, c \in \mathbb{Z}$.

Sea $\zeta \in \mathbb{Z}[\alpha]$. Existe un polinomio $P \in \mathbb{Z}[T]$ tal que $P(\alpha) = \zeta$. Como el polinomio $D(T) = T^3 - 5$ es mónico, existen $Q, R \in \mathbb{Z}[T]$ tales que

$$P(T) = D(T)Q(T) + R(T), \deg R \leq 2.$$

Evaluando en $T = \alpha$, y puesto que $D(\alpha) = 0$, resulta

$$\zeta = P(\alpha) = D(\alpha)Q(\alpha) + R(\alpha) = R(\alpha) = a\alpha^2 + b\alpha + c,\ a, b, c \in \mathbb{Z}.$$

En cuanto a la unicidad, supongamos que los números enteros $a_1, b_1, c_1, a_2, b_2, c_2$ verifican

$$a_1\alpha^2 + b_1\alpha + c_1 = a_2\alpha^2 + b_2\alpha + c_2.$$

Denotando $a = a_2 - a_1, b = b_2 - b_1, c = c_2 - c_1$, resulta que α es raíz del polinomio $F(T) = aT^2 + bT + c \in \mathbb{Z}[T]$ y tenemos que demostrar que el polinomio $F(T)$ es nulo. Como, por el criterio de Eisenstein, $D(T) = T^3 - 5$ es ireducible en $\mathbb{Z}[T]$, si suponemos $F(T) \neq 0$, resulta que mcd $(F(T), T^3 - 5) = 1$, y por la identidad de Bezout en $\mathbb{Q}[T]$ existen polinomios $G, H \in \mathbb{Q}[T]$ tales que

$$1 = D(T)G(T) + F(T)H(T).$$

Evaluando en $T = \alpha$ la identidad anterior llegamos a la contradicción

$$1 = D(\alpha)G(\alpha) + F(\alpha)H(\alpha) = 0.$$

b) Demostrar que φ es sobreyectivo.

Para demostrar la sobreyectividad de φ tenemos que identificar, para cada elemento $\zeta = a\alpha^2 + b\alpha + c \in \mathbb{Z}[\alpha]$, la clase $\zeta + \mathfrak{a}$ como $x + \mathfrak{a}$ para un entero

adecuado x. De forma equivalente, buscamos $x \in \mathbb{Z}$ tal que $\zeta - x \in \mathfrak{a}$, es decir $a\alpha^2 + b\alpha + c - x \in \mathfrak{a}$. Ahora bien,

$$\alpha^2 = (\alpha + 1 - 1)^2 = (\alpha + 1)^2 - 2(\alpha + 1) + 1.$$

Así, $a\alpha^2 + \mathfrak{a} = a + \mathfrak{a}$. Por otro lado, $b\alpha = b(\alpha + 1) - b$, así que

$$a\alpha^2 + b\alpha + c - x \in \mathfrak{a} \Leftrightarrow a - b + c - x \in \mathfrak{a},$$

y esta última condición se cumple trivialmente eligiendo $x = a - b + c \in \mathbb{Z}$, lo que prueba la sobreyetividad de φ.

c) Demostar que $\ker \varphi = 6\mathbb{Z}$

Para cada $x \in \ker \varphi = (\alpha + 1)\mathbb{Z}[\alpha] \cap \mathbb{Z}$, existe $\zeta = a\alpha^2 + b\alpha + c \in \mathbb{Z}[\alpha]$ tales que

$$x = (\alpha+1)(a\alpha^2+b\alpha+c) = a\alpha^3+(a+b)\alpha^2+(b+c)\alpha+c = (a+b)\alpha^2+(b+c)\alpha+(5a+c).$$

Como $x \in \mathbb{Z}$ esto equivale a

$$(*)\begin{cases} a + b = 0 \\ b + c = 0 \\ 5a + c = x. \end{cases}$$

Sumando las ecuaciones primera y tercera y restando la segunda obtenemos $x = 6a \in 6\mathbb{Z}$.
Para probar la inclusión recíproca $6\mathbb{Z} \subset \ker \varphi$ hemos de comprobar que $\varphi(6) = 0$, es decir, $6 \in \mathfrak{a}$. Para esto es suficiente resolver el sistema $(*)$ con $x = 6$. De las dos primeras ecuaciones se deduce que $a = c$, lo que sustituido en la tercera proporciona $6a = 6$, es decir, $a = c = 1, b = -1$. Esto significa que

$$6 = (\alpha + 1)(\alpha^2 - \alpha + 1) \in \mathfrak{a}.$$

(7) En $\mathbb{Z}[i]$.

a) Demostrar que cada unidad de $\mathbb{Z}[i]$ es el cubo de una unidad de $\mathbb{Z}[i]$.

Como $\mathbb{Z}[i]$ es un DE para la norma $N : \mathbb{Z}[i] \to \mathbb{N}, z = a + bi \mapsto z\bar{z} = a^2 + b^2$, las unidades son los elementos de norma 1, esto es, $a^2 + b^2 = 1$. Como $a, b \in \mathbb{Z}$, es claro que las soluciones de la última ecuación son $a = \pm 1, b = 0$ o $a = 0, b = \pm 1$. Por tanto, las unidades son

$$1 = 1^3, -1 = (-1)^3, i = (-i)^3, -i = i^3.$$

Esto muestra que cada unidad es el cubo de una unidad.

b) Dado un entero impar $x \in \mathbb{Z}$, calcular $d = \mathrm{mcd}(x+i, x-i)$ en $\mathbb{Z}[i]$. Demostrar que $d\bar{d} = 2$.

Sea $d = \mathrm{mcd}(x+i, x-i)$. Restando se deduce que d divide a $2i$ y, como i es unidad, d divide a $2 = (1+i)(1-i)$. Ahora bien, 2 no divide a $x+i$ ni a $x-i$; en caso contrario $x \pm i = 2(a+bi)$ para ciertos $a, b \in \mathbb{Z}$, de donde se deduce $\pm 1 = 2b$, que es imposible.

En consecuencia, bien $d = 1$, bien $d = 1+i$, o bien $d = 1-i$. Las dos últimas afirmaciones son idénticas puesto que $1+i, 1-i$ son asociados, ya que $1+i = (1-i)i$. Además por ser x impar,

$$\frac{x+i}{1+i} = \frac{(x+i)(1-i)}{2} = \frac{x+1}{2} + \frac{1-x}{2}i \in \mathbb{Z}[i],$$

luego $1+i$ divide a $x+i$ en $\mathbb{Z}[i]$ y, del mismo modo,

$$\frac{x-i}{1+i} = \frac{(x-i)(1-i)}{2} = \frac{x-1}{2} - \frac{1+x}{2}i \in \mathbb{Z}[i],$$

es decir $1+i$ divide a $x-i$ en $\mathbb{Z}[i]$. En conclusión, $\mathrm{mcd}(x+i, x-i) = 1+i$. Por supuesto,

$$d\bar{d} = (1+i)(1-i) = 2.$$

c) Demostrar que si $\alpha, \beta \in \mathbb{Z}[i]$ son primos entre sí y existe $\gamma \in \mathbb{Z}[i]$ tal que $\alpha\beta = \gamma$, entonces existen $\alpha_1, \beta_1 \in \mathbb{Z}[i]$ tales que $\alpha = \alpha_1^3$ y $\beta = \beta_1^3$.

Como $\mathbb{Z}[i]$ es un DFU y α, β son primos entre sí, existen elementos irreducibles $p_1, \ldots, p_r, q_i, \ldots, q_s \in \mathbb{Z}[i]$, no asociados dos a dos, y unidades u, v tales que

$$\alpha = up_1^{n_1} \cdots p_r^{n_r}, \quad \beta = vq_1^{m_1} \cdots q_s^{m_s}$$

para ciertos enteros positivos $n_1, \ldots, n_r, m_1, \ldots, m_s$. Por otro lado, si $\gamma = w\pi_1^{k_1} \cdots \pi_t^{k_t}$ donde w es unidad y $p_i, \ldots, p_t \in \mathbb{Z}[i]$ son irreducibles no asociados dos a dos y $k_1, \ldots, k_t$ enteros positivos, se tiene

$$uvp_1^{n_1} \cdots p_r^{n_r} q_1^{m_1} \cdots q_s^{m_s} = w^3 \pi_1^{3k_1} \cdots \pi_t^{3k_t}$$

Cada factor irreducible del término de la derecha aparece elevado a un exponente múltiplo de 3 y, por ser $\mathbb{Z}[i]$ DFU, lo mismo ha de suceder a los factores irreducibles del término de la izquierda. Esto implica, al ser los factores no asociados dos a dos, que cada n_i, m_j es múltiplo de 3. Escribimos $n_i = 3e_i, m_j = 3f_j$ y las unidades $u = u_1^3, v = v_1^3$. De este modo, $\alpha = \alpha_1^3, \beta = \beta_1^3$ donde

$$\alpha_1 = u_1 p_1^{e_1} \cdots p_r^{e_r}, \beta_1 = v_1 q_1^{f_1} \cdots q_s^{f_s}.$$

d) Encontrar todas las soluciones enteras de la ecuación $1 + X^2 = 2Y^3$.

Sean $x, y \in \mathbb{Z}$ tales que $1 + x^2 = 2y^3$. Es claro que x es impar y, por *b*) $1 + i$ divide a $x + i$. Por tanto $x + i = (1 + i)(a + bi)$, $a, b \in \mathbb{Z}$. Conjugando se tiene $x - i = (1 - i)(a - bi)$. Puesto que $\text{mcd}(x + i, x - i) = 1 + i$ y $1 + i, 1 - i$ son asociados, concluimos que $\text{mcd}(a + bi, a - bi) = 1$. Además,

$$2y^3 = 1 + x^2 = (x + i)(x - i) = (1 + i)(a + bi)(1 - i)(a - bi) = 2(a + bi)(a - bi),$$

es decir,

$$y^3 = (a + bi)(a - bi).$$

En virtud de *c*) existen $m, n \in \mathbb{Z}$ tales que

$$a + bi = (m + ni)^3.$$

Ahora bien,

$$x + i = (1 + i)(a + bi) = (a - b) + (a + b)i,$$

y por tanto

$$a + b = 1.$$

Entonces, de la igualdad

$$a + bi = (m + ni)^3 = m^3 + 3m^2ni - 3mn^2 - n^3i = (m^3 - 3mn^2) + (3m^2n - n^3)i,$$

se deduce que

$$\begin{aligned} 1 = a + b &= (m^3 - 3mn^2) + (3m^2n - n^3 = (m^3 - n^3) + 3mn(m - n) \\ &= (m - n)(m^2 + mn + n^2) + 3mn(m - n) = (m - n)(m^2 + 4mn + n^2), \end{aligned}$$

lo que nos lleva a distinguir dos casos.

Caso 1. $m - n = m^2 + 4mn + n^2 = 1$. Entonces,

$$1 = m^2 + 4mn + n^2 = (m - n)^2 + 6mn = 1 + 6mn \Rightarrow mn = 0 \Rightarrow$$

$$m = 1, n = 0 \text{ o } m = 0, n = -1.$$

Si $m = 1, n = 0$ resulta

$$a + bi = (m + ni)^3 = 1 \Rightarrow x + i = (1 + i)(a + bi) = 1 + i \Rightarrow x = 1 \Rightarrow y = 1.$$

Si $m = 0, n = -1$ tenemos

$$a + bi = (m + ni)^3 = i \Rightarrow x + i = (1 + i)(a + bi) = -1 + i \Rightarrow x = -1 \Rightarrow y = 1.$$

Caso 2. $m - n = m^2 + 4mn + n^2 = -1$. Entonces,

$$-1 = m^2 + 4mn + n^2 = (m - n)^2 + 6mn = 1 + 6mn \Rightarrow mn = 0, ,$$

es decir, $mn = -\frac{1}{3}$, y esto es imposible.

En consecuencia, las dos soluciones de la ecuación del enunciado son $x = 1, y = 1$ y $x = -1, y = 1$.

(8) En $\mathbb{Z}[i]$:

a) Hallar el máximo común de divisor de $1+i, 1-i$.

b) Factorizar $15-15i$ en producto de irreducibles.

c) Demostrar que $X^{3264}+2X^2+(15-15i)X+(1+i)$ es irreducible.

d) determinar todos los homomorfismos de anillos unitarios de $\mathbb{Z}[i] \to \mathbb{C}$.

(9) Sean $f = X^4+3X^3+X^2+X+1 \in \mathbb{Z}[X]$ e $I = (f, X-1) \subset \mathbb{Z}[X]$.

a) demostrar que f es irreducible en $\mathbb{Z}[X]$.

b) Hallar el inverso de la clase de X^3+1 en el anillo $\mathbb{Q}[X]/(f)$.

c) Hallar un entero k tal que se verifique la igualdad de ideales $I = (k, X-1)$. Deducir que $\mathbb{Z}[X]/I \simeq \mathbb{Z}_k$.

d) ¿Es I un ideal primo de $\mathbb{Z}[X]$? ¿Es primo el ideal $(f, X-1)\mathbb{Q}[X]$?

(10) Consideramos el homomorfismo de sustitución

$$\begin{aligned} \psi : \mathbb{Z}[X] &\to \mathbb{C} \\ f(X) &\mapsto f(\sqrt{-5}). \end{aligned}$$

a) Hallar un generador de $\ker\psi$.

b) Denotemos por R la imagen de ψ. estudiar si R es un DFU.

c) Hallar un generador del ideal $(X^2+5, X^4+10X^2+X+29)\mathbb{Q}[X]$.

d) Sea $I = (X^2+5, X^4+10X^2+X+29)\mathbb{Z}[X]$. Hallar dos polinomios del menor grado posible que generen I.

e) Demostrar que $\psi(I)$ es un ideal de R. Estudiar si el anillo $R/\psi(I)$ es un DI.

(11) Decir cuántos tipos de grupo conmutativo, salvo isomorfismo, hay para el orden 8100. dar un modelo de cada tipo.

(12) Se considera el conjunto $G = \{\sigma \in S_5 \mid \sigma(\{1,2\}) = \{1,2\} \text{ y } \sigma(\{3,4,5\}) = \{3,4,5\}\}$ (es decir, permutaciones que envían los conjuntos $\{1,2\}, \{3,4,5\}$ a ellos mismos). Se pide:

a) Demostrar que G es un subgrupo de S_5 de orden 12.

b) Hallar los órdenes de los elementos de G.

c) Demostrar que existe un único isomorfismo de G en D_6 que envía $(1\,2)(3\,4\,5)$ a σ y $(3\,4)$ a τ (donde σ es el giro de amplitud $\frac{\pi}{3}$ y τ es una simetría fijada del hexágono).

d) Para cada primo p, deducir razonadamente cuántos p–subgrupos de Sylow tiene G.

(13) ¿Puede existir un homomorfismo inyectivo $\mathbb{Z}_6$ en A_5? ¿Y un homomorfismo sobreyectivo de D_4 en $\mathbb{Z}_8$.

(14) Sean $\sigma = (1\,2)$ y $\tau = (4\,3\,2\,5)(1\,6)$ en S_7. Halla la descomposición de la permutación $\sigma\tau$ en producto de ciclos disjuntos y calcula su signatura.

(15) Sean G un grupo, H, K subgrupos de G de índice finito y $M = H \cap K$. Demostrar

a) Para todo $a \in G$ se tiene $aH \cap aK = aM$.

b) M tiene índice finito en G.

(16) Sea G un grupo de orden $13 \cdot 27$ tal que existe un elemento $a \in G$ de orden 27.

a) Demostrar que G tiene un único subgrupo de Sylow normal.

b) ¿Cuántos elementos tiene la clase de conjugación de a?

(17) Sean $f = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Z}_2[X]$ y $\mathbb{K} = \mathbb{Z}_2[X]/(f)$. Denotemos por α la clase de X en $\mathbb{K}$.

a) Estudiar si $\mathbb{K}$ es un cuerpo.

b) Hallar el inverso en $\mathbb{K}$ de $\alpha^3 + \alpha + 1$.

c) ¿Cuál es el orden de α en el grupo de unidades $\mathbb{K}^*$.

d) ¿Cuáles son los divisores elementales del grupo $\mathbb{K}^*$? ¿Y los de $(\mathbb{K}, +)$?

(18) hallar un homorfismo sobreyectivo $D_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$.

(19) Sea G un grupo de orden $n \geq 2$. Supongamos que $f : A_5 \to G$ es un homomorfismo de grupos sobreyectivo. Demostrar que f ha de ser un ismorfismo.

(20) Sea G un grupo de orden p^2 con p primo tal que G no es cíclico. ¿Cuántos subgrupos de orden p tienen G?

(21) Hallar los factores invariantes del grupo de unidades del anillo $\mathbb{Z}_{36}$.

(22) Sean g un grupo y $a \in G$ un elemento de orden $n \geq 2$. Supongamos que a es el único elemento de orden n en G. Demostrar que a está en el centro de G y que $n = 2$.

(23) Sea G un grupo finito generado por dos elementos a, b tales a tiene orden 4, $a^2 = b^2$ y $ab = ba^3$.

a) Hallar el orden de b. Demostrar que b está en el centro de G.

b) Demostrar que $G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$. ¿Es G ismorfo al grupo diédrico D_4?

(24) Sea G un grupo de orden $4563 = 13^2 \cdot 3^3$ tal que G no tiene ningún subgrupo de Sylow normal.

a) ¿Qué dicen los teoremas de Sylow sobre G?

b) Demostrar que existen dos 13–subgrupos de Sylow distintos H, K tales $|H \cap K| = 13$.

c) Demostrar que $H \cap K$ es un subgrupo normal de G.

(25) Estudiar si son ciertas las afirmaciones:

a) Existe sólo un homomorfismo de grupos $A_5 \to \mathbb{Z}_{25}$.

b) Sean R un anillo y $f \in R[X]$ un polinomio de grado $n \geq 1$. Entonces f tiene a lo sumo n raíces en R.

A.2. Capítulo 3

(1) Consideramos el polinomio $f(X) = X^3 + X^2 - X + 1 \in \mathbb{Q}[X]$. Demostrar que f es irreducible sobre $\mathbb{Q}$. ¿Es f irreducible sobre $\mathbb{Q}(\sqrt[4]{2})$?

Un polinomio de grado 3 es irreducible sobre un cuerpo F si, y sólo si, no tiene raíces en F. Los únicos candidatos a raíz racional de f son ± 1. Puesto que $f(\pm 1) \neq 0$, vemos que f no tiene raíces racionales y, por tanto, f es irreducible sobre $\mathbb{Q}$. Por otra parte, si $\alpha \in \mathbb{Q}(\sqrt[4]{2})$ y $f(\alpha) = 0$, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, puesto que f es irreducible sobre $\mathbb{Q}$ y se tiene $4 = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$, lo que es imposible. Así f es irreducible sobre $\mathbb{Q}(\sqrt[4]{2})$.

(2) Consideramos el polinomio $f(X) = (X^4 - 3)(X^3 - 7) \in \mathbb{Q}[X]$.

a) Determinar el cuerpo de descomposición E de $f(X)$ sobre $\mathbb{Q}$. Calcular el grado $[E : \mathbb{Q}]$.

Las raíces de p son $\pm\sqrt[4]{3}, \pm\sqrt[4]{3}i, \sqrt[3]{7}, \sqrt[3]{7}\omega, \sqrt[3]{7}\omega^2$. Por tanto,

$$E = \mathbb{Q}(\pm\sqrt[4]{3}, \pm\sqrt[4]{3}i, \sqrt[3]{7}, \sqrt[3]{7}\omega, \sqrt[3]{7}\omega^2).$$

Puesto que $i = \sqrt[4]{3}i/\sqrt[4]{3} \in E$ y $\omega = \sqrt[3]{7}\omega/\sqrt[3]{7} \in E$. Deducimos $E = \mathbb{Q}(\sqrt[4]{3}, i, \sqrt[3]{7}, \omega)$. Por otra parte, $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ y $\sqrt{3} = (\sqrt[4]{3})^2 \in E$. Deducimos que $E = \mathbb{Q}(\sqrt[4]{3}, i, \sqrt[3]{7})$.

Puesto que, por el criterio de Eisenstein, $X^4 - 3$ y $X^3 - 7$ son irreducibles sobre $\mathbb{Q}$ deducimos que $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$ y $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 3$. De estas dos igualdades, puesto que $\mathrm{mcd}(3, 4) = 1$, deducimos que $[\mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7}) : \mathbb{Q}] = 12$. Por otra parte, puesto que $i \notin \mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7}) \subset \mathbb{R}$ y $i^2 + 1 = 0$ se deduce que $[\mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7})(i) : \mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7})] = 2$. Finalmente, $[E : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7})(i) : \mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7})][\mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7}) : \mathbb{Q}] = 24$.

b) Decidir, de forma razonada, si $X^3 - 7$ es el polinomio mínimo de $\sqrt[3]{7}$ sobre $\mathbb{Q}(i)$.

Hay que estudiar si $X^3 - 7$ es irreducible sobre $\mathbb{Q}(i)$. Puesto que es un polinomio de grado 3, ser irreducible sobre un cuerpo equivale a no tener raíces en dicho cuerpo. Sea α una raíz de $X^3 - 7$. Puesto que $X^3 - 7$ es irreducible sobre $\mathbb{Q}$ el grado $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Si $\alpha \in \mathbb{Q}(i)$ podemos escribir la fórmula $2 = [\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. Esto es imposible. Por tanto $X^3 - 7$ es irreducible sobre $\mathbb{Q}(i)$.

(3) Sean α una raíz de f y $\beta = \alpha^2$. Calcular, de forma razonada, el polinomio mínimo de β sobre $\mathbb{Q}$.

Con la fórmula $\alpha^3 = -\alpha^2 + \alpha - 1$, calculamos las potencias de β.

$$\beta^2 = \alpha^4 = \alpha(-\alpha^2 + \alpha - 1) = -\alpha^3 + \alpha^2 - \alpha = 2\alpha^2 - 2\alpha + 1.$$

$$\beta^3 = \alpha^6 = \alpha^4 \cdot \alpha^2 = \alpha^2(2\alpha^2 - 2\alpha + 1) = 7\alpha^2 - 6\alpha + 4.$$

La ecuación $a + b\beta + c\beta^2 + \beta^3 = 0$ tiene solución única $a, b, c \in \mathbb{Q}$. Sustituyendo los valores anteriores, obtenemos

$$a + b\alpha^2 + c(2\alpha^2 - 2\alpha + 1) + 7\alpha^2 - 6\alpha + 4 = 0.$$

Así $-4 = a + c; 6 = -2c; -7 = b + 2c$. Cuya solución es $a = -1, b = -1, c = -3$. Por tanto, el polinomio mínimo es

$$X^3 - 3X^2 - X - 1.$$

(4) Sea $\alpha = \sqrt{14 + 3\sqrt{3}}$.

a) Obtener, de forma razonada, el polinomio mínimo y los conjugados de α sobre $\mathbb{Q}$.

b) Sea E el cuerpo de descomposición del polinomio mínimo de α sobre $\mathbb{Q}$.

1) Describir el grupo de Galois $G = \mathrm{Gal}(E/\mathbb{Q})$.

2) Obtener, de forma razonada, todos los cuerpos intermedios de la extensión $E/\mathbb{Q}$.

El número $\alpha = \sqrt{14 + 3\sqrt{3}}$ verifica $(\alpha^2 - 14)^2 = 27$, esto es $\alpha^4 - 28\alpha^2 + 169 = 0$. Las raíces de $m(X) = X^4 - 28X^2 + 169$ son $\pm\alpha, \pm\beta$, donde $\beta = \sqrt{14 - 3\sqrt{3}}$. Estos son los conjugados de α y $m(x)$ su polinomio mínimo sobre $\mathbb{Q}$ si demostramos que $m(X)$ es irreducible sobre $\mathbb{Q}$. Puesto que sus raíces $\pm\alpha, \pm\beta$ no son racionales y $m(X)$ tiene coeficientes enteros y coeficiente principal 1, basta probar que no se puede descomponer, con $a, b, c, d \in \mathbb{Z}$, en la forma

$$\begin{aligned} X^4 - 28X^2 + 169 &= (X^2 + aX + b)(X^2 + cX + d) \\ &= X^4 + (a + c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd. \end{aligned}$$

Obtenemos $a + c = 0; b + d + ac = -28; ad + bc = 0; bd = 169$. Un sencillo argumento (¡hacedlo!) muestra que las soluciones no son enteras.

El cuerpo de descomposición de $m(X)$ sobre $\mathbb{Q}$ es $E = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \alpha\beta) = \mathbb{Q}(\alpha)$. La última igualdad se obtiene de la identidad $\alpha\beta = \sqrt{196 - 27} = 13$. Esto es $\beta = \frac{13}{\alpha}$.

	α	β	α^2	β^2	$\alpha+\beta$	$\alpha-\beta$
1	α	β	α^2	β^2	$\alpha+\beta$	$\alpha-\beta$
σ	$-\alpha$	$-\beta$	α^2	β^2	$-(\alpha+\beta)$	$-\alpha+\beta$
τ	β	α	β^2	α^2	$\beta+\alpha$	$\beta-\alpha$
$\sigma\tau$	$-\beta$	$-\alpha$	β^2	α^2	$-(\beta+\alpha)$	$-\beta+\alpha$

Así $[E:\mathbb{Q}]=4$. El grupo de Galois es $G=\{1,\sigma,\tau,\sigma\tau\}\simeq\mathbb{Z}_2\oplus\mathbb{Z}_2$, donde σ,τ están descritos por su acción en α según la tabla

Es claro que $\sigma\tau=\tau\sigma$ está descrito por $\alpha\mapsto-\beta$ puesto que $\alpha\overset{\sigma}{\mapsto}-\alpha\overset{\tau}{\mapsto}-\beta$ y $\alpha\overset{\tau}{\mapsto}\beta=\frac{13}{\alpha}\overset{\sigma}{\mapsto}\frac{13}{-\alpha}=-\beta$. También $\sigma^2=\tau^2=1$, puesto que $\alpha\overset{\sigma}{\mapsto}-\alpha\overset{\sigma}{\mapsto}-(-\alpha)$ y $\alpha\overset{\tau}{\mapsto}\beta=\frac{13}{\alpha}\overset{\tau}{\mapsto}\frac{13}{\beta}=\alpha$.

Los subgrupos de G son $\{1,\sigma\};\{1,\tau\};\{1,\sigma\tau\}$. Los cuerpos intermedios que les corresponden son de grado 2 sobre $\mathbb{Q}$. Veamos que cuerpos intermedios les corresponden. Según la tabla vemos que $\mathbb{Q}(\sqrt{3})=\mathbb{Q}(\alpha^2)=\mathbb{Q}(\beta^2)\subset\mathrm{Fix}(\sigma)$. De aquí la igualdad puesto que ambos cuerpos intermedios tienen grado 2 sobre $\mathbb{Q}$. De forma similar $\mathbb{Q}(\sqrt{6})=\mathbb{Q}(\alpha+\beta)\subset\mathrm{Fix}(\tau)$. De donde se obtiene la igualdad. Finalmente $\mathbb{Q}(\sqrt{2})=\mathbb{Q}(\alpha-\beta)=\mathrm{Fix}(\sigma\tau)$. Las dos últimas igualdades usan las fórmulas $(\alpha\pm\beta)^2=\alpha^2+\beta^2\pm2\alpha\beta=14+3\sqrt{3}+14-3\sqrt{3}\pm26=28\pm26$.

(5) Sean $\zeta=e^{\frac{2\pi i}{23}}$ una raíz primitiva vigesimotercera de la unidad y $E=\mathbb{Q}(\zeta)$.

a) Obtener de forma explícita un automorfismo generador del grupo cíclico $G=\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

b) Demostrar que la extensión $E/\mathbb{Q}$ tiene un único cuerpo intermedio K_{11} tal que $[K_{11}:\mathbb{Q}]=11$ y un único cuerpo intermedio K_2 tal que $[K_2:\mathbb{Q}]=2$.

c) Sea K_{11} el cuerpo del apartado anterior. Determinar, de forma explícita, un elemento $\alpha\in K_{11}$ tal que $K_{11}=\mathbb{Q}(\alpha)$.

Según la teoría, el grupo de Galois $G=\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})=<\sigma>\simeq(\mathbb{Z}_{23})^*$, es el grupo cíclico de orden 22 generado por el automorfismo σ descrito por $\zeta\overset{\sigma}{\mapsto}\zeta^5$. La última afirmación equivale a la igualdad $(\mathbb{Z}_{23})^*=<5>$, que muestran las identidades en $\mathbb{Z}_{23}$, $5^2=2,5^3=10,5^4=4,5^5=20,5^6=8,5^7=17,5^8=16,5^9=11,5^{10}=9,5^{11}=22,5^{12}=18,5^{13}=21,5^{14}=13,5^{15}=19,5^{16}=3,5^{17}=15,5^{18}=6,5^{19}=7,5^{20}=12,5^{21}=14,5^{22}=1$.

Un grupo cíclico tiene un único subgrupo para cada divisor del orden del grupo, que también es cíclico. Por tanto, G contiene un único subgrupo $H_2=<\sigma^{11}>$ de orden 2 y un único subgrupo $H_{11}=<\sigma^2>$ de orden 11, ambos son normales en G, puesto que G es conmutativo. Estos subgrupos corresponden, según el Teorema

Fundamental, respectivamente, a un único cuerpo intermedio K_{11} de grado 11 sobre $\mathbb{Q}$ y a un único cuerpo intermedio K_2 de grado 2 sobre $\mathbb{Q}$ que resultan ser un extensiones normales de $\mathbb{Q}$.

Por el Teorema Fundamental, el grupo de Galois $\mathrm{Gal}(K_{11}/\mathbb{Q}) \simeq G/H_2 \simeq \mathbb{Z}_{11}$ es el grupo cíclico de orden 11. En efecto, la afirmación sobre el grado es clara. Respecto a ser cíclico, basta observar que de $G =< \sigma >$ se obtiene $G/H_2 =< \sigma H_2 >$ (esto es, todo cociente de un grupo cíclico es cíclico)(en este caso también resulta de la primalidad de 11).

Para la última cuestión, consideramos el elemento $\alpha = \zeta + \overline{\zeta} = 2\cos(\frac{2\pi}{23}) \in \mathbb{R}$ y el cuerpo intermedio $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta)$.

Se verifica, $\zeta\alpha = \zeta^2 + 1$, esto es $\zeta^2 - \alpha\zeta + 1 = 0$. Por tanto, $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)] \leq 2$. Puesto que $\alpha \in \mathbb{R}$, es claro que $\zeta \notin \mathbb{Q}(\alpha)$. En consecuencia $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)] = 2$. Por tanto $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 11$. La unicidad de K_{11} prueba que $K_{11} = \mathbb{Q}(\alpha)$.

(6) Consideramos el polinomio $f(X) = X^3 + X + 1 \in \mathbb{Q}[X]$.

a) Demostrar que f es irreducible sobre $\mathbb{Q}$. Estudiar si f es irreducible sobre $\mathbb{Q}(\sqrt{5})$.
Un polinomio de grado 3 es irreducible sobre un cuerpo F si, y sólo si, no tiene raíces en F (puesto que si es reducible ha de tener un factor de grado 1). Una condición necesaria para que una fracción $\frac{a}{b} \in \mathbb{Q}$, donde $\mathrm{mcd}(a, b) = 1$, sea raíz de un polinomio con coeficientes enteros $a_n X^n + \cdots + a_o \in \mathbb{Z}[X]$ es $a|a_0$ y $b|a_n$. Por tanto, las únicas posibles raíces racionales de $f(X) = X^3 + X + 1$ son ± 1. Puesto que $f(\pm 1) \neq 0$, concluimos que $f(X)$ es irreducible sobre $\mathbb{Q}$.
Supongamos que $f(X)$ tiene una raíz α en $\mathbb{Q}(\sqrt{5})$. Entonces $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{5})$, y entonces, por la fórmula de los grados, $2 = [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$. Puesto que hemos probado que f es irreducible sobre $\mathbb{Q}$ es $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Esto muestra que f no tiene raíces en $\mathbb{Q}(\sqrt{5})$. Por tanto, f es irreducible sobre $\mathbb{Q}(\sqrt{5})$.

b) Sean α una raíz de f y $\beta = \alpha^2 + \alpha$. Calcular, de forma razonada, el polinomio mínimo de β sobre $\mathbb{Q}$.
Puesto que $\{1, \alpha, \alpha^2\}$ son linealmente independientes sobre $\mathbb{Q}$, vemos que $\beta \notin \mathbb{Q}$. Por tanto, de la fórmula de los grados, $3 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]$ se deduce $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$ (y $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$). En consecuencia, el polinomio mínimo de β sobre $\mathbb{Q}$ es de grado 3. Es decir, la ecuación $\beta^3 + a\beta^2 + b\beta + c = 0$ tiene solución única para números $a, b, c \in \mathbb{Q}$. Para calcular a, b, c, expresamos las potencias de β en función de potencias de α.

$$\alpha^3 = -\alpha - 1.$$

$$\beta^2 = \alpha^4 + \alpha^2 + 2\alpha^3 = -\alpha^2 - \alpha + \alpha^2 - 2\alpha - 2 = -3\alpha - 2.$$

$$\beta^3 = (\alpha^2+\alpha)(-3\alpha-2) = -3\alpha^3 - 2\alpha^2 - 3\alpha^2 - 2\alpha =$$
$$= -3(-\alpha-1) - 2\alpha^2 - 3\alpha^2 - 2\alpha = -5\alpha^2 + \alpha + 3.$$

Entonces, $\beta^3 + a\beta^2 + b\beta + c = 0$ es equivalente, por la independencia lineal de $\{1, \alpha, \alpha^2\}$, a $-5 + b = 0, 1 - 3a + b = 0, 3 - 2a + c = 0$. Por tanto

$$\beta^3 + 2\beta^2 + 5\beta + 1 = 0.$$

(7) Sea E el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $X^{17} - 2 \in \mathbb{Q}[X]$.

Sea $\zeta = e^{2\pi i/17}$. Consultar apuntes para: $E = \mathbb{Q}(\sqrt[17]{2}, \zeta)$ y $[E : \mathbb{Q}] = 17 \cdot 16$. Sea $G = \mathrm{Gal}(E/\mathbb{Q})$, el orden de G es $2^4 \cdot 17$.

a) Obtener, de forma razonada, todos los cuerpos intermedios $\mathbb{Q} \subset K \subset E$ tales que $[K : \mathbb{Q}] = 16$. Estudiar si son extensiones normales de $\mathbb{Q}$.

El cuerpo intermedio $K = \mathbb{Q}(\zeta)$ tiene grado 16 sobre $\mathbb{Q}$ y es una extensión normal de $\mathbb{Q}$ (es el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $X^{17} - 1$). Por el teorema fundamental, corresponde a un subgrupo normal $H \lhd G$ de orden 17. El subgrupo H es un 17–subgrupo de Sylow de G y es normal, por tanto, es el único subgrupo de orden 17 de G y, en consecuencia, $K = \mathbb{Q}(\zeta)$ es el único cuerpo intermedio de $E/\mathbb{Q}$, de grado 16 sobre $\mathbb{Q}$.

b) Obtener, de forma razonada, todos los cuerpos intermedios $\mathbb{Q} \subset L \subset E$ tales que $[L : \mathbb{Q}] = 17$. Estudiar si son extensiones normales de $\mathbb{Q}$.

Los cuerpos intermedios $L_i = \mathbb{Q}(\sqrt[17]{2}\zeta^i)$ para $i = 0, \ldots, 16$ tienen grado 17 sobre $\mathbb{Q}$ y son 17 cuerpos intermedios distintos dos a dos (consultar apuntes). Ninguno de ellos es normal sobre $\mathbb{Q}$, puesto que los elementos $\sqrt[17]{2}\zeta^i$ son conjugados sobre $\mathbb{Q}$ (son las raíces del polinomio irreducible sobre $\mathbb{Q}$, $X^{17} - 2$). Corresponden, por tanto, a 17 subgrupos distintos de G de orden 2^4. Éstos son 2–subgrupos de Sylow de G. El número posible de ellos, s_2, verifica $s_2 = 1 + 2k | 17$. Por tanto, $s_2 = 17$ y los L_i son todos los cuerpos intermedios de orden 17.

c) Decidir, de forma razonada, cuántos cuerpos intermedios de grado 2 sobre $\mathbb{Q}$, cuántos cuerpos intermedios de grado 4 sobre $\mathbb{Q}$ y cuántos cuerpos intermedios de grado 8 sobre $\mathbb{Q}$ hay en la extensión $E/\mathbb{Q}$. Estudiar si son extensiones normales de $\mathbb{Q}$.

Un cuerpo intermedio $\mathbb{Q} \subset K \subset E$ de grado $2, 4, 8$ corresponde a un subgrupo H de orden $2^3 \cdot 17, 2^2 \cdot 17, 2 \cdot 17$. Este subgrupo ha de contener un subgrupo de orden 17. Por tanto, contiene el único subgrupo de H de orden 17 de G. En consecuencia, K está contenido el cuerpo intermedio $\mathbb{Q}(\zeta)$ que corresponde a H. El grupo de Galois de $\mathbb{Q}(\zeta)/\mathbb{Q}$ es el grupo cíclico de orden 16. Un grupo cíclico contiene un único subgrupo de orden d para cada divisor d del orden

del grupo (subgrupos normales, puesto que es un grupo conmutativo). Por tanto, en $\mathbb{Q}(\zeta)/\mathbb{Q}$ hay un único cuerpo intermedio de cada orden $2, 4, 8$, cada uno de ellos normal sobre $\mathbb{Q}$.

d) Sea $f(X) \in \mathbb{Q}[X]$ un polinomio separable cuyo grupo de Galois sobre $\mathbb{Q}$ es isomorfo al grupo de Galois de $E/\mathbb{Q}$. Estudiar si $f(X)$ es resoluble por radicales.

Por el gran teorema de Galois, f es resoluble por radicales si, y sólo si, su grupo de Galois G es resoluble. Para probar que el grupo G, del apartado anterior, es resoluble usamos la caracterización: G resoluble si, y sólo si, tiene subgrupo normal resoluble con cociente resoluble. En este caso, tenemos el subgrupo normal $H \lhd G$ de orden 17 (un subgrupo de orden primo es cíclico, en particular conmutativo y, por tanto, resoluble) con cociente G/H de orden 2^4. Un resultado teórico afirma que todo grupo cuyo orden es potencia de un primo es resoluble.

(8) Sea ζ una raíz decimonovena primitiva de la unidad sobre $\mathbb{Q}$ (e.g.: $\zeta = e^{2\pi i/19}$).

a) Demostrar que la extensión $\mathbb{Q}(\zeta)/\mathbb{Q}$ tiene un único cuerpo intermedio K de grado $[K : \mathbb{Q}] = 3$.

El grupo de Galois G de $\mathbb{Q}(\zeta)/\mathbb{Q}$ es el grupo cíclico de orden 18 (consultar apuntes). Un grupo cíclico de orden 18 tiene un único subgrupo de orden 6, (además todos sus subgrupos son normales). Por tanto hay un único cuerpo intermedio K de grado 3 sobre $\mathbb{Q}$ y es una extensión normal de $\mathbb{Q}$.

b) Obtener, de forma razonada, un elemento η expresado como suma de potencias de ζ tal que $K = \mathbb{Q}(\eta)$.

Un generador de G es el automorfismo definido por la asignación

$$\sigma : \zeta \mapsto \zeta^2.$$

El subgrupo de orden 6 es

$$H =< \sigma^3 >= \{1, \sigma^3, \sigma^6, \sigma^9, \sigma^{12}, \sigma^{15}\}.$$

Esto sugiere que el candidato es

$$\eta = \zeta + \zeta^8 + \zeta^7 + \zeta^{18} + \zeta^{11} + \zeta^{12}.$$

Comprobamos que, en efecto,

$$\sigma^3(\eta) = \eta.$$

Así

$$\mathbb{Q}(\eta) \subset K.$$

Puesto que el grado es 3, un número primo, para tener la igualdad basta comprobar que $\eta \notin \mathbb{Q}$. Puesto que la ecuación mínima de ζ es

$$1 + \zeta + \cdots + \zeta^{18} = 0,$$

deducimos que

$$\zeta + \zeta^8 + \zeta^7 + \zeta^{18} + \zeta^{11} + \zeta^{12} + a \neq 0$$

para todo $a \in \mathbb{Q}$, esto es $\eta \notin \mathbb{Q}$.

(9) Sea $p(X) = (X^4 - 3)(X^3 - 7) \in \mathbb{Q}[X]$.

a) Determinar el cuerpo de descomposición E de $p(X)$ sobre $\mathbb{Q}$. Demostrar que el grado $[E : \mathbb{Q}] = 24$.

Las raíces de p son $\pm\sqrt[4]{3}, \pm\sqrt[4]{3}i, \sqrt[3]{7}, \sqrt[3]{7}\omega, \sqrt[3]{7}\omega^2$. Por tanto,

$$E = \mathbb{Q}(\pm\sqrt[4]{3}, \pm\sqrt[4]{3}i, \sqrt[3]{7}, \sqrt[3]{7}\omega, \sqrt[3]{7}\omega^2).$$

Puesto que $i = \sqrt[4]{3}i/\sqrt[4]{3} \in E$ y $\omega = \sqrt[3]{7}\omega/\sqrt[3]{7} \in E$. Deducimos $E = \mathbb{Q}(\sqrt[4]{3}, i, \sqrt[3]{7}, \omega)$. Por otra parte, $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ y $\sqrt{3} = (\sqrt[4]{3})^2 \in E$. Deducimos que $E = \mathbb{Q}(\sqrt[4]{3}, i, \sqrt[3]{7})$.

Puesto que, por el criterio de Eisenstein, $X^4 - 3$ y $X^3 - 7$ son irreducibles sobre $\mathbb{Q}$ deducimos que $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$ y $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 3$. De estas dos igualdades, puesto que $\mathrm{mcd}(3, 4) = 1$, deducimos que $[\mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7}) : \mathbb{Q}] = 12$. Por otra parte, puesto que $i \notin \mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7}) \subset \mathbb{R}$ y $i^2 + 1 = 0$ se deduce que $[\mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7})(i) : \mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7})] = 2$. Finalmente, $[E : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7})(i) : \mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7})][\mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{7}) : \mathbb{Q}] = 24$.

b) Sea G el grupo de Galois de $E/\mathbb{Q}$. Decidir, de forma razonada, cuántos subgrupos de orden 8 tiene G.

Los subgrupos $H_8 < G$ de orden 8 son los 2–subgrupos de Sylow de G. El número posible de estos subgrupos es $s_2 = 1 + 2k|3$, por tanto, $s_2 = 1, 3$. Los subgrupos de orden 8 corresponden con cuerpos intermedios $K_3 \subset E$ de grado $[K_3 : \mathbb{Q}] = 3$. En la extensión $E/\mathbb{Q}$ vemos, al menos, tres cuerpos intermedios distintos de grado tres: $\mathbb{Q}(\sqrt[3]{7}), \mathbb{Q}(\sqrt[3]{7}\omega), \mathbb{Q}(\sqrt[3]{7}\omega^2)$. Por tanto hay exactamente 3 subgrupos de orden 8 (y exactamente 3 cuerpos intermedios de grado 8).

c) Obtener, de forma razonada, todos los cuerpos intermedios de grado 8 sobre $\mathbb{Q}$. ¿Son extensiones normales de $\mathbb{Q}$?

Los cuerpos intermedios $K_8 \subset E$ de grado $[K_8 : \mathbb{Q}] = 8$, corresponden con los subgrupos $H_3 < G$ de orden 3. Estos subgrupos son los 3–subgrupos de Sylow de G. Por tanto, hay un único subgrupo H_3 si, y sólo si, hay un $H_3 \lhd G$ normal en G. Además, si $H_3 < G$ corresponde con $K_8 \subset E$, entonces H_3 es normal en G si, y sólo si, $K_8/\mathbb{Q}$ es una extensión normal. Así, hay un único cuerpo intermedio $K_8 \subset E$ si, y sólo si, hay un cuerpo intermedio K_8 que es normal sobre $\mathbb{Q}$. En nuestro caso $K_8 = \mathbb{Q}(\sqrt[4]{3}, i) \subset E$ es un cuerpo intermedio de grado 8 sobre $\mathbb{Q}$, que es normal sobre $\mathbb{Q}$, puesto que es el cuerpo de descomposición

sobre $\mathbb{Q}$ del polinomio X^4-3. Em consecuencia, $\mathbb{Q}(\sqrt[4]{3}, i) \subset E$ es el único cuerpo intermedio de grado 8 sobre $\mathbb{Q}$ y es una extensión normal de $\mathbb{Q}$ (además, G tiene un único subgrupo de orden 3, y este subgrupo es normal en G).

(10) Sea f un polinomio en $\mathbb{Q}[X]$ con cuerpo de descomposición E sobre $\mathbb{Q}$ tal que su grupo de Galois $G = \mathrm{Gal}(E/\mathbb{Q})$ es isomorfo al grupo diedro D_5 del pentágono regular. Decidir, de forma razonada, si f es resoluble por radicales.

Según el Gran Teorema de Galois, f es resoluble por radicales si, y sólo si, el grupo G es un grupo resoluble. El grupo D_5 es resoluble, puesto que $D_5 \rhd\!< \sigma >\!\lhd \{1\}$ es una serie normal con cociente cíclicos de orden primo.

(11) Consideramos el polinomio $f(X) = X^3 + X^2 - X + 1 \in \mathbb{Q}[X]$.

a) Demostrar que f es irreducible sobre $\mathbb{Q}$. ¿Es f irreducible sobre $\mathbb{Q}(\sqrt[4]{2})$?

Un polinomio de grado 3 es irreducible sobre un cuerpo F si, y sólo si, no tiene raíces en F. Los únicos candidatos a raíz racional de f son ± 1. Puesto que $f(\pm 1) \neq 0$, vemos que f no tiene raíces racionales y, por tanto, f es irreducible sobre $\mathbb{Q}$. Por otra parte, si $\alpha \in \mathbb{Q}(\sqrt[4]{2})$ y $f(\alpha) = 0$, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, puesto que f es irreducible sobre $\mathbb{Q}$ y se tiene $4 = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$, lo que es imposible. Así f es irreducible sobre $\mathbb{Q}(\sqrt[4]{2})$.

b) Sean α una raíz de f y $\beta = \frac{\alpha^2+1}{\alpha+2}$. Calcular, de forma razonada, la expresión de β como combinación lineal de elementos de una base de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$.

Con la fórmula $\alpha^3 = -\alpha^2 + \alpha - 1$, podemos simplificar la ecuación

$$\frac{\alpha^2+1}{\alpha+2} = a + b\alpha + c\alpha^2,$$

que tiene solución única $a, b, c \in \mathbb{Q}$.

$$\begin{aligned}\alpha^2 + 1 &= (\alpha+2)(a + b\alpha + c\alpha^2)\\ &= a\alpha + b\alpha^2 + c(-\alpha^2 + \alpha - 1) + 2a + 2b\alpha + 2c\alpha^2\\ &= (b+c)\alpha^2 + (a + c + 2b)\alpha - c + 2a.\end{aligned}$$

Así $1 = b + c; 0 = a + c + 2b; 1 = -c + 2a$. Cuya solución es $a = 3, b = -4, c = 5$. Por tanto

$$\frac{\alpha^2+1}{\alpha+2} = 3 - 4\alpha + 5\alpha^2.$$

(12) Sea E/F una extensión de Galois cuyo grupo de Galois $G = \mathrm{Gal}(E/F)$ tiene orden $3^2 \cdot 13 \cdot 29$ y que contiene un cuerpo intermedio $F \subset K \subset E$ de grado $[K : F] = 3^2 \cdot 29$ y tal que K/F es una extensión normal. Demostrar que E/F es resoluble por radicales. ¿Cuántos cuerpos intermedios de grado $3^2 \cdot 29$ hay en la extensión E/F?

Por el Teorema Fundamental, al cuerpo intermedio K tal que K/F es normal le corresponde un subgrupo H normal en G. Este subgrupo H tiene orden 13 y, por tanto, es un 13–subgrupo de Sylow de G que, por ser normal, resulta ser único y, en correspondencia, el cuerpo intermedio K es el único de su grado. El grupo cociente $\overline{G} = G/H$ tiene orden $3^2 \cdot 29$. El número de subgrupos de orden 29 en $\overline{G}$ verifica $\bar{s}_{29} = 1 + 29k | 3^2$. De aquí $\bar{s}_{29} = 1$ y, por tanto, hay un único 29–subgrupo de Sylow $\overline{H}_{29}$ en $\overline{G}$ que resulta ser normal por ser único subgrupo de Sylow de su orden. El cociente $\overline{G}/\overline{H}$ tiene orden 3^2. Este último grupo es resoluble por ser su orden una potencia de número primo. El subgrupo $\overline{H}$ es resoluble, puesto que es cíclico. Por tanto, $\overline{G}$ es resoluble. Puesto que H es también resoluble, el mismo argumento muestra que G es resoluble.

(13) Sea $\alpha = \sqrt{11 + \sqrt{21}}$.

a) Obtener, de forma razonada, el polinomio mínimo y los conjugados de α sobre $\mathbb{Q}$.

b) Sea E el cuerpo de descomposición del polinomio mínimo de α sobre $\mathbb{Q}$.

1) Describir el grupo de Galois $G = \mathrm{Gal}(E/\mathbb{Q})$.
2) Obtener, de forma razonada, todos los cuerpos intermedios de la extensión $E/\mathbb{Q}$.

El número $\alpha = \sqrt{11 + \sqrt{21}}$ verifica $(\alpha^2 - 11)^2 = 21$, esto es $\alpha^4 - 22\alpha + 100 = 0$. Las raíces de $m(X) = X^4 - 22X^2 + 100$ son $\pm\alpha, \pm\beta$, donde $\beta = \sqrt{11 - \sqrt{21}}$. Estos son los conjugados de α y $m(x)$ su polinomio mínimo sobre $\mathbb{Q}$ si demostramos que $m(X)$ es irreducible sobre $\mathbb{Q}$. Puesto que sus raíces $\pm\alpha, \pm\beta$ no son racionales y $m(X)$ tiene coeficientes enteros y coeficiente principal 1, basta probar que no se puede descomponer, con $a, b, c, d \in \mathbb{Z}$, en la forma

$$\begin{aligned} X^4 - 22X^2 + 100 &= (X^2 + aX + b)(X^2 + cX + d) \\ &= X^4 + (a + c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd. \end{aligned}$$

Obtenemos $a + c = 0; b + d + ac = -22; ad + bc = 0; bd = 100$. Un sencillo argumento (¡hacedlo!) muestra que las soluciones no son enteras.

El cuerpo de descomposición de $m(X)$ sobre $\mathbb{Q}$ es $E = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \alpha\beta) = \mathbb{Q}(\alpha)$. La última igualdad se obtiene de la identidad $\alpha\beta = \sqrt{121 - 21} = 10$. Esto es $\beta = \frac{10}{\alpha}$.

Así $[E:\mathbb{Q}]=4$. El grupo de Galois es $G=\{1,\sigma,\tau,\sigma\tau\}\simeq\mathbb{Z}_2\oplus\mathbb{Z}_2$, donde σ,τ están descritos por su acción en α según la tabla

	α	β	α^2	β^2	$\alpha+\beta$	$\alpha-\beta$
1	α	β	α^2	β^2	$\alpha+\beta$	$\alpha-\beta$
σ	$-\alpha$	$-\beta$	α^2	β^2	$-(\alpha+\beta)$	$-\alpha+\beta$
τ	β	α	β^2	α^2	$\beta+\alpha$	$\beta-\alpha$
$\sigma\tau$	$-\beta$	$-\alpha$	β^2	α^2	$-(\beta+\alpha)$	$-\beta+\alpha$

Es claro que $\sigma\tau=\tau\sigma$ está descrito por $\alpha\mapsto-\beta$ puesto que $\alpha\overset{\sigma}{\mapsto}-\alpha\overset{\tau}{\mapsto}-\beta$ y $\alpha\overset{\tau}{\mapsto}\beta=\frac{10}{\alpha}\overset{\sigma}{\mapsto}\frac{10}{-\alpha}=-\beta$. También $\sigma^2=\tau^2=1$, puesto que $\alpha\overset{\sigma}{\mapsto}-\alpha\overset{\sigma}{\mapsto}-(-\alpha)$ y $\alpha\overset{\tau}{\mapsto}\beta=\frac{10}{\alpha}\overset{\tau}{\mapsto}\frac{10}{\beta}=\alpha$.

Los subgrupos de G son $\{1,\sigma\};\{1,\tau\};\{1,\sigma\tau\}$. Los cuerpos intermedios que les corresponden son de grado 2 sobre $\mathbb{Q}$. Veamos que cuerpos intermedios les corresponden. Según la tabla vemos que $\mathbb{Q}(\sqrt{21})=\mathbb{Q}(\alpha^2)=\mathbb{Q}(\beta^2)\subset\mathrm{Fix}(\sigma)$. De aquí la igualdad puesto que ambos cuerpos intermedios tienen grado 2 sobre $\mathbb{Q}$. De forma similar $\mathbb{Q}(\sqrt{42})=\mathbb{Q}(\alpha+\beta)\subset\mathrm{Fix}(\tau)$. De donde se obtiene la igualdad. Finalmente $\mathbb{Q}(\sqrt{2})=\mathbb{Q}(\alpha-\beta)=\mathrm{Fix}(\sigma\tau)$. Las dos últimas igualdades usan las fórmulas $(\alpha\pm\beta)^2=\alpha^2+\beta^2\pm2\alpha\beta=11+\sqrt{21}+11-\sqrt{21}\pm20=22\pm20$.

(14) Sean $\zeta=e^{\frac{2\pi i}{17}}$ una raíz primitiva decimoséptima de la unidad y $E=\mathbb{Q}(\zeta)$.

a) Demostrar que la extensión $E/\mathbb{Q}$ tiene un único cuerpo intermedio K tal que $[K:\mathbb{Q}]=8$.

b) Sea K el cuerpo del apartado anterior. Demostrar que $K/\mathbb{Q}$ es una extensión de Galois y que el grupo $G=\mathrm{Gal}(K/\mathbb{Q})$ es el grupo cíclico de orden 8. Determinar, de forma explícita, un elemento $\alpha\in K$ tal que $K=\mathbb{Q}(\alpha)$.

Según la teoría, el grupo de Galois $G=\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})=<\sigma>\simeq(\mathbb{Z}_{17})^*$, es el grupo cíclico de orden 16 generado por el automorfismo σ descrito por $\zeta\overset{\sigma}{\mapsto}\zeta^3$. La última afirmación equivale a la igualdad $(\mathbb{Z}_{17})^*=<3>$, que muestran las identidades en $\mathbb{Z}_{17}$, $3^2=9,3^3=10,3^4=13,3^5=5,3^6=15,3^7=11,3^8=16,3^9=14,3^{10}=8,3^{11}=7,3^{12}=4,3^{13}=12,3^{14}=2,3^{15}=6,3^{16}=1$.

Un grupo cíclico tiene un único subgrupo para cada divisor del orden del grupo, que también es cíclico. Por tanto, G contiene un único subgrupo de orden $H_2=<\sigma^8>$ de orden 2, que es normal en G, puesto que G es conmutativo. Este subgrupo corresponde, según el Teorema Fundamental, a un único cuerpo intermedio de grado K_8 de grado 8 sobre $\mathbb{Q}$ que resulta ser una extensión normal de $\mathbb{Q}$.

Por el Teorema Fundamental, el grupo de Galois $\mathrm{Gal}(K_8/\mathbb{Q}) \simeq G/H_2 \simeq \mathbb{Z}_8$ es el grupo cíclico de orden 8. En efecto, la afirmación sobre el grado es clara. Respecto a ser cíclico, basta observar que de $G =< \sigma >$ se obtiene $G/H_2 =< \sigma H_2 >$ (esto es, todo cociente de un grupo cíclico es cíclico).

Para la última cuestión, consideramos el elemento $\alpha = \zeta + \overline{\zeta} = 2\cos(\frac{2\pi}{17}) \in \mathbb{R}$ y el cuerpo intermedio $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta)$.

Se verifica, $\zeta\alpha = \zeta^2 + 1$, esto es $\zeta^2 - \alpha\zeta + 1 = 0$. Por tanto, $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)] \leq 2$. Puesto que $\alpha \in \mathbb{R}$, es claro que $\zeta \notin \mathbb{Q}(\alpha)$. En consecuencia $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)] = 2$. Por tanto $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$. La unicidad de K_8 prueba que $K_8 = \mathbb{Q}(\alpha)$.

(15) Sean $f(X) = X^{11} - 7 \in \mathbb{Q}[X]$, L el cuerpo de descomposición de f sobre $\mathbb{Q}$ y $G = \mathrm{Gal}(L/\mathbb{Q})$. Sean $\alpha = \sqrt[11]{7}$ y ζ una raíz undécima primitiva de 1. Se pide:

a) Hallar los polinomios mínimos de α y ζ sobre $\mathbb{Q}$. Demostrar que $L = \mathbb{Q}(\alpha, \zeta)$ y que $[L, \mathbb{Q}] = 110$.

b) Demostrar que G tiene algún subgrupo normal no trivial. Probar que hay un subgrupo normal H de G tal que H y G/H son cíclicos.

c) Describir los grupos de $\mathbb{Q}$–automonorfismos de las extensiones $\mathbb{Q}(\alpha)/\mathbb{Q}$ y $\mathbb{Q}(\zeta)/\mathbb{Q}$.

d) Demostrar que la extensión $L/\mathbb{Q}$ tiene cuerpos intermedios de todos los geados posibles sobre $\mathbb{Q}$. ¿Cuántos hay de grados 10, 22 y 55?

e) Escribir un cuerpo intermedio $\mathbb{Q} \subset K \subset L$ de grado $[K : \mathbb{Q}] = 2$ como extensión simple de $\mathbb{Q}$ y encontrar el polinomio mínimo de su generador. ¿Es única?

(16) Sea $\alpha \in \mathbb{C}$ una raíz del polinomio $f(X) = X^3 - X^2 - 4X - 1$.

a) Probar que f es irreducible sobre $\mathbb{Q}$.

b) Probar que $-(1 + \alpha)^{-1}$ es también raíz de f.

c) ¿Es $\mathbb{Q}(\alpha)/\mathbb{Q}$ una extensión de Galois?

d) Sea $\epsilon = \exp(2\pi i/3)$. ¿Es f irreducible sobre $\mathbb{Q}(\epsilon)$?

(17) Sean $\eta = \exp(2\pi i/7) \in \mathbb{C}$, $\alpha = \eta + \eta^6, \beta = \eta^2 + \eta^5$ y $\gamma = \eta^3 + \eta^4$. Se pide:

a) Probar que $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\eta)$ y que $[\mathbb{Q}(\eta) : \mathbb{Q}(\alpha)] \in \{1, 2\}$ y deducir que α tiene grado 3 o 6 sobre $\mathbb{Q}$.

b) Demostrar que $f = (X - \alpha)(X - \beta)(X - \gamma) \in \mathbb{Z}[X]$ y que α tiene grado 3 sobre $\mathbb{Q}$.

c) Hallar un polinomio $r(X) \in \mathbb{Z}[X]$ tal que $r(\alpha) = \beta$.

d) ¿Es $\mathbb{Q}(\alpha)/\mathbb{Q}$ una extension de Galois?

e) Hallar el grupo de Galois de la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$.

f) Describir el grupo $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ como cociente del grupo $\mathrm{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})$.

(18) Sean $p \in \mathbb{Z}$ un entero primo impar, n un entero positivo libre de cuadrados, $R = \mathbb{Z}[\sqrt{n}]$ y K el cuerpo de fracciones de R.

a) Demostrar que el ideal $I = 2R$ no es primo. (Pista: $(n+\sqrt{n})(n-\sqrt{n}) = n(n-1)$)

Como $n(n-1)$ es un entero par, se tiene $(n+\sqrt{n})(n-\sqrt{n}) \in I$ y todo se reduce a probar que $n+\sqrt{n}, n-\sqrt{n} \notin I$. Supongamos lo contrario. Entonces, para $\epsilon = +1$ o -1 existen $a, b \in \mathbb{Z}$ tales que

$$n + \epsilon\sqrt{n} = 2(a + b\sqrt{n}) \Rightarrow \epsilon = 2b,$$

y esto es absurdo.

b) Demostrar que si n es un resto cuadrático módulo p, entonces el ideal $J = pR$ no es primo.

Por hipótesis, existe $x \in \mathbb{Z}$ tal que $x^2 - n \in pR = J$. Por tanto,

$$(x-\sqrt{n})(x+\sqrt{n}) \in J,$$

y si J fuese primo, para $\epsilon = +1$ o -1 se tendría $x + \epsilon\sqrt{n} \in J$. Esto implica que existen $u, v \in \mathbb{Z}$ tales que

$$x + \epsilon\sqrt{n} = p(u + v\sqrt{n}) \Rightarrow \epsilon = pv \in p\mathbb{Z},$$

contradicción.

c) Demostrar que el polinomio $f(X) = X^3 - pX + p$ es irreducible sobre K.

Por el criterio de Eisenstein f es irreducible sobre $\mathbb{Q}$. Supongamos que fuese reducible sobre K. Como $\deg f = 3$ existe una raíz $\alpha \in K$ de f. Entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 3$. Así

$$2 = [\mathbb{Q}(\sqrt{n}) : \mathbb{Q})] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \in 3\mathbb{Z},$$

y esto es imposible. Concluimos que f es irreducible sobre $K = \mathbb{Q}(\sqrt{n})$.

d) Demostrar que si el grupo de Galois de f sobre $\mathbb{Q}$ es cíclico, entonces $p \equiv 1 \pmod 3$.

Ya hemos visto que f es irreducible sobre $\mathbb{Q}$, luego si denotamos Δ_f el discriminante de f, se sabe que $\mathrm{Gal}(f/\mathbb{Q}) = \mathbb{Z}_3$ si Δ_f es un cuadrado en $\mathbb{Q}$ y $\mathrm{Gal}(f/\mathbb{Q}) = S_3$ si Δ_f no es un cuadrado en $\mathbb{Q}$.

Como estamos suponiendo que $\mathrm{Gal}(f/\mathbb{Q})$ es cíclico deducimos que

$$\Delta_f = 4p^3 - 27p^2 = p^2(4p - 27)$$

es el cuadrado de un número racional, luego $4p-27$ también lo es. Como $4p-27$ es un entero ha de ser $4p-27=m^2$ paaar $m\in\mathbb{Z}$. Dividimos $m=3s+t$ con $s,t\in\mathbb{Z}$ y $o\le t\le 2$. De hecho $t\neq 0$, porque en caso contrario $4p=27+m^2=9(3+s^2)\in 3\mathbb{Z}$, así que $p=3$ y $m^2=4p-27=-15$, absurdo. En consecuencia $m=3s+t$ con $s\in\mathbb{Z}$ y $t=1,2$. Por ser $3p-27\in 3\mathbb{Z}$ resulta

$$p\equiv p+(3p-27)=4p-27=m^2=(3s+t)^2=9s^2+6st+t^2\equiv t^2\equiv 1\ (\mathrm{mod}\ 3).$$

(19) *a*) Demostrar que $a=\tan(2\pi/7)$ es algebraico sobre $\mathbb{Q}$ y que el polinomio mínimo de a sobre $\mathbb{Q}$ es $f(T)=T^6-21T^4+35T^2-7$.

Denotamos $\theta=2\pi/7$. Por la fórmula de Moivre, se tiene

$$(\cos\theta+i\sin\theta)^7=\cos 7\theta+i\sin 7\theta=\cos 2\pi+i\sin 2\pi=1.$$

Por la fórmula del binomio,

$$\begin{aligned}1=(\cos\theta+i\sin\theta)^7=\cos^7\theta+7i\cos^6\theta\sin\theta-21\cos^5\theta\sin^2\theta-35i\cos^4\theta\sin^3\theta\\+35\cos^3\theta\sin^4\theta+21i\cos^2\theta\sin^5\theta-7\cos\theta\sin^6\theta-i\sin^7\theta.\end{aligned}$$

Por tanto, la parte imaginaria

$$7\cos^6\sin\theta-35\cos^4\theta\sin^3\theta+21\cos^2\theta\sin^5\theta-\sin^7\theta=0.$$

Diviendo por $\cos^7\theta$ obtenemos

$$7\tan\theta-35\tan^3\theta+21\tan^5\theta-\tan^7\theta=0.$$

Por tanto, $a=\tan\theta\neq 0$ es raíz del polinomio $f(X)=T^6-21T^4+35T^2-7$. Observese que, por el criterio de Eisnestein, f es irreducible sobre $\mathbb{Q}$. Así que $f=m_{a,\mathbb{Q}}$.

b) Demostrar que las raíces de f en $\mathbb{C}$ son $\pm\tan(2\pi/7)$, $\pm\tan(4\pi/7)$ y $\pm\tan(6\pi/7)$.

El argumento empleado para el ángulo θ es válido también para los ángulos $-\theta$, $\pm 2\theta=\pm 4\pi/7$ y $\pm 3\theta=\pm 6\pi/7$, es decir, otras raíces de f son $-\tan\theta$, $\pm\tan 2\theta$ y $\pm\tan 3\theta$. Como f tiene grado 6, si probamos que los números anteriores son todos distintos tendremos todas las raíces de f. Veremos en el apartado siguiente que estos números son distintos.

c) Demostrar que la extensión $\mathbb{Q}(a)/\mathbb{Q}$ es de Galois.

Usando la fórmula de la tangente de la suma deducimos

$$\tan 2\theta=\frac{2\tan\theta}{1-\tan^2\theta}=\frac{2a}{1-a^2},\quad \tan 3\theta=\frac{\tan\theta+\tan 2\theta}{1-\tan\theta\tan 2\theta}=\frac{a+\frac{2a}{1-a^2}}{1-\frac{2a^2}{1-a^2}=\frac{3a-a^3}{1-3a^2}}.$$

Se comprueba directamente que si $\tan k\theta = \tan m\theta$ para $-3 \leq k, m \leq 3, k \neq n, k, m \neq 0$ entonces a satisfaría una ecuación polinómica de grado menor que 6, lo que no es posible por la irreducibilidad de f.

Como consecuencia de lo anterior y de c), las raíces de f son

$$\pm a, \pm\frac{2a}{1-a^2}, \pm\frac{3a-a^3}{1-3a^2} \in \mathbb{Q}(a),$$

luego $\mathbb{Q}(a)$ es el cuerpo de descomposición de f sobre $\mathbb{Q}$, por lo que la extensión $\mathbb{Q}(a)/\mathbb{Q}$ es de Galois.

d) Comprobar que el grupo $\mathrm{Gal}(f/\mathbb{Q})$ tiene orden 6 y calcularlo.

Por ser $\mathbb{Q}(a)/\mathbb{Q}$ de Galois

$$|\mathrm{Gal}(f/\mathbb{Q})| = [\mathbb{Q}(a) : \mathbb{Q}] = \deg f = 6,$$

y se trata de decidir si $\mathrm{Gal}(f/\mathbb{Q})$ es cíclico o D_3. Es claro que

$$\mathrm{Gal}(f/\mathbb{Q}) = \{1, \tau, \varphi, \tau\varphi, \psi, \tau\psi\}$$

donde τ, φ, ψ son los automorfismos de $\mathbb{Q}(a)$ determinados por la condición:

$$\tau(a) = -a, \varphi(a) = \frac{2a}{1-a^2}, \psi(a) = \frac{3a-a^3}{1-3a^2}.$$

Es inmediato que τ pertenece al centro de $\mathrm{Gal}(f/\mathbb{Q})$, y como el centro de D_3 es trivial concluimos que $\mathrm{Gal}(f/\mathbb{Q})$ es el grupo cíclico de orden 6.

e) ¿Cuántos cuerpos intermedios propios posee la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$? Hallar un elemento primitivo de cada una de ellas.

Como $\mathrm{Gal}(f/\mathbb{Q})$ tiene un único subgrupo de orden 2 y un único subgrupo de orden 3. La Extensión $\mathbb{Q}(a)/\mathbb{Q}$ tiene sólo dos cuerpos intermedios K, L, con grados $[K : \mathbb{Q}] = 2, [L : \mathbb{Q}] = 3$.

Es sencillo identificar un elemento primitivo de L. Para ello observamos que el polinomio

$$g(T) = T^3 - 21T^2 + 35T - 7$$

es irreducible por el criterio de Eisenstein y $g(a^2) = 0$. En consecuencia, $g = m_{a^2,\mathbb{Q}}$ y $[\mathbb{Q}(a^2) : \mathbb{Q}] = 3$. Así, $L = \mathbb{Q}(a^2)$.

Por otra parte, las raíces de f se pueden escribir como $\pm a, \pm b, \pm c$ y, por tanto,

$$T^6 - 21T^4 + 35T^2 - 7 = f(T) = (T-a)(T+a)(T-b)(T+b)(T-c)(T+c)$$

por lo que $-7 = -(abc)^2$, es decir $\sqrt{7} = abc \in \mathbb{Q}(a)$. En consecuencia, $K = \mathbb{Q}(\sqrt{7})$.

Podríamos haber llegado a este resultado por otro procedimiento. El cuerpo K es el cuerpo fijo del único subgrupo H de orden 3. Comprobamos que H está generado por φ. Basta operar

$$\varphi^2(a) = \varphi(\frac{2a}{1-a^2}) = \frac{2\varphi(a)}{1-\varphi(a)^2} = \frac{\frac{4a}{1-a^2}}{1-\frac{4a^2}{(1-a^2)^2}} = \frac{4a(1-a^2)}{a^4-6a^2+1}.$$

Comprobemos la igualdad

$$\frac{4a(1-a^2)}{a^4-6a^2+1} = -\tan 3\theta = \frac{a(a^2-3)}{1-3a^2},$$

que equivale a

$$4(1-a^2)(1-3a^2) = (a^2-3)(a^4-6a^2+1) \Leftrightarrow a^6-21a^4+35a^2-7 = 0,$$

y ya sabemos que esta última es cierta. Ahora, utilizando la anterior igualdad

$$\varphi^3(a) = \varphi(\frac{a(a^2-3)}{1-3a^2}) = \frac{\frac{2a}{1-a^2}(\frac{4a^2}{(1-a^2)^3}-3)}{1-\frac{12a^2}{(1-a^2)^2}} = \frac{a(-6a^4+20a^2-6)}{-a^6+15a^4-15a^2+1} = a$$

lo que demuestra que φ tiene orden 3. En consecuencia, $K = \mathrm{Fix}(\varphi)$. Además hemos demostrado que

$$\varphi(a) = b = \frac{2a}{1-a^2}, \varphi^2(a) = c = \frac{a(a^2-3)}{1-3a^2}$$

y por tanto, $\delta = abc$ queda fijo por φ, puesto que

$$\varphi(\delta) = \varphi(a\varphi(a)\varphi^2(a)) = \varphi(a)\varphi^2(a)\varphi^3(a) = \varphi(a)\varphi^2(a)\,a = \delta.$$

Ya vimos que $\delta = \sqrt{7} \notin \mathbb{Q}$, luego $K = \mathbb{Q}(\delta)$.

(20) *a*) Calcular el polinomio mínimo de $\zeta = \exp(\pi i/5)$ sobre $\mathbb{Q}$

Puesto que $\zeta^5 = \exp(\pi i) = -1$ se tiene

$$0 = \zeta^5 + 1 = (\zeta+1)(\zeta^4-\zeta^3+\zeta^2-\zeta+1)$$

y, como $\zeta \neq -1$, se deduce que ζ es raíz del polinomio

$$p(X) = X^4 - X^3 + X^2 - X + 1.$$

El polinomio p es irreducible sobre $\mathbb{Q}$, puesto que $p(-X)$ es el quinto polinomio ciclotómico que sabemos es irreducible sobre $\mathbb{Q}$.

b) Probar que el polinomio mínimo sobre $\mathbb{Q}$ de $\eta = \zeta + \zeta^{-1}$ es $X^2 - X - 1$.

Dividimos entre ζ^2 la igualdad $\zeta^4 - \zeta^3 + \zeta^2 - \zeta + 1 = 0$ para obtener

$$0 = \zeta^2 - \zeta + 1 - \zeta^{-1} + \zeta^{-2} = \zeta^2 + \zeta^{-2} + 1 - (\zeta + \zeta^{-1}) = (\zeta + \zeta^{-1})^2 - 1 - (\zeta + \zeta^{-1}),$$

es decir,

$$\eta^2 - \eta - 1 = 0.$$

Por tanto η es raíz del polinomio $X^2 - X - 1$ que es irreducible sobre $\mathbb{Q}$ puesto que sus raíces $\frac{1 \pm \sqrt{5}}{2} \notin \mathbb{Q}$. Por tanto $X^2 - X - 1$ es el polinomio mínimo de η sobre $\mathbb{Q}$.

c) Probar que el grupo de Galois de la extensión $\mathbb{Q}(\zeta)/\mathbb{Q}$ es cíclico de orden 4.

Para probar que $p(\zeta) = 0$ sólo hemos usado $\zeta^5 = 1$ y $\zeta \neq 1$. Por tanto $\zeta^2, \zeta^3, \zeta^4$ también son raíces de $p(X)$. En consecuencia $\mathbb{Q}(\zeta)/\mathbb{Q}$ es una extensión de Galois de grado 4. Su grupo de Galois es, por tanto,

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})) = \{\varphi_i \mid \varphi_i(\zeta) = \zeta^i,\ i = 1, 2, 3, 4\}.$$

Ahora bien,

$$\varphi_2^2(\zeta) = \varphi_2(\zeta^2) = (\varphi_2(\zeta)) = \zeta^4 \neq \zeta,$$

luego φ_2 no tiene orden 2 ni es la identidad. En consecuencia $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}))$ es cíclico de orden 4 generado por φ_2.

d) Calcular el número de cuerpos intermedios propios de la extensión $\mathbb{Q}(\zeta)/\mathbb{Q}$. encontrar un elemento primitivo de cada una de ellas.

El grupo cíclico de orden 4 tiene un único subgrupo propio de orden 2. Por tanto, en $\mathbb{Q}(\zeta)/\mathbb{Q}$ hay un único cuerpo intermedio propio de grado 2 sobre $\mathbb{Q}$. Puesto que $\eta \in \mathbb{Q}(\zeta)$ tiene grado 2 sobre $\mathbb{Q}$, el único cuerpo intermedio es $\mathbb{Q}(\eta) = \mathbb{Q}(\sqrt{5})$.

e) Calcular el polinomio mínimo de ζ sobre $K = \mathbb{Q}(\sqrt{3})$.

Puesto que $\sqrt{3} \notin \mathbb{Q}(\zeta)$ el grado

$$[K(\zeta) : \mathbb{Q}(\zeta)] = 2.$$

Así que,

$$[K(\zeta) : K] = \frac{[K(\zeta) : \mathbb{Q}]}{[K : \mathbb{Q}]} = \frac{[K(\zeta) : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}]}{2} = 4.$$

En consecuencia, $p(X)$ es el polinomio mínimo de ζ sobre K.

(21) *a*) Probar que el grupo de Galois sobre $\mathbb{Q}$ del polinomio

$$f = 1 + \sum_{j=1}^{10} X^j$$

es cíclico de orden 10 y que la suma de sus raíces es -1.

Observemos que $(X-1)f(X) = X^{11} - 1$, luego las raíces de f son $\{\zeta^k : k = 1, \ldots, 10\}$, donde $\zeta = \exp(2\pi i/11)$. El polinomio f es irreducible sobre $\mathbb{Q}$, puesto que es el undécimo polinomio ciclotómico. Por tanto, f es el polinomio mínimo de ζ sobre $\mathbb{Q}$ y su cuerpo de descomposición es $\mathbb{Q}(\zeta)/\mathbb{Q}$. En consecuencia $G = \mathrm{Gal}(f/\mathbb{Q})$ tiene orden 10. El único grupo conmutativo de orden 10 es el cíclico, por tanto, para ver que G es cíclico basta probar que es conmutativo. En efecto, los elementos de G son los φ_k definidos por $\varphi_k : \zeta \mapsto \zeta^k, k = 1, \ldots, 10$. Es claro que los φ_k conmutan:

$$\varphi_k(\varphi_l(\zeta)) = \varphi_k(\zeta^l) = (\zeta^k)^l = (\zeta^l)^k = \varphi_l(\zeta^k) = \varphi_l(\varphi_k(\zeta)).$$

b) Probar que existe un polinomio $g \in \mathbb{Q}[X]$ irreducible y de grado 5 cuyo grupo de Galois sobre $\mathbb{Q}$ es cíclico de orden 5. (Pista: buscar un subcuerpo K adecuado del cuerpo L de descomposición de f sobre $\mathbb{Q}$.))

El grupo G posee un único subgrupo H de orden 2. Por tanto, su cuerpo fijo K es el único cuerpo intermedio de $\mathbb{Q}(\zeta)/\mathbb{Q}$ de grado 5 sobre $\mathbb{Q}$. Además $K/\mathbb{Q}$ es de Galois, puesto que G es conmutativo y, en consecuencia, todo subgrupo de G es normal. El grupo $\mathrm{Gal}(K/\mathbb{Q})$ es de orden 5, por tanto, es cíclico. Puesto que $K/\mathbb{Q}$ admite un elemento primitivo, su polinomio mínimo sobre $\mathbb{Q}$ es el polinomio g pedido.

c) Encontrar un polinomio $g \in \mathbb{Q}[X]$ en las condiciones del apartado anterior.

Buscamos $\alpha \in \mathbb{Q}(\zeta)$ tal que $K = \mathbb{Q}(\alpha)$. Puesto que $\zeta^{10} = \zeta^{-1}$, el automorfismo φ_{10} tiene orden 2. En efecto,

$$\varphi_{10}^2(\zeta) = \varphi_{10}(\zeta^{10}) = \varphi_{10}(\zeta^{-1}) = (\varphi_{10}(\zeta))^{-1} = (\zeta^{10})^{-1} = \zeta.$$

Por tanto, $H = \{1, \varphi_{10}\}$ y $K = \{x \in \mathbb{Q}(\zeta) \mid \varphi_{10}(x) = x\}$. Sabemos que cada $x \in \mathbb{Q}(\zeta)$ se escribe, de modo único, como combinación lineal con coeficientes $a_0, \ldots, a_9 \in \mathbb{Q}$

$$x = a_0 + a_1\zeta + \cdots + a_9\zeta^9.$$

Ahora, $x \in K$ si, y sólo si,

$$\sum_{k=0}^{9} a_k\zeta^k = \varphi_{10}(\sum_{k=0}^{9} a_k\zeta^k) = \sum_{k=0}^{9} a_k\zeta^{11-k} = \sum_{k=2}^{9} a_{11-k}\zeta^k + a_1\zeta^{10} + a_0\zeta^{11}.$$

Sabemos que $\zeta^{11} = 1$ y $\zeta^{10} = -\sum_{k=0}^{9} \zeta^k$, lo que sustituido en la fórmula anterior proporciona

$$\sum_{k=0}^{9} a_k \zeta^k = (a_0 - a_1) - a_1\zeta + \sum_{k=2}^{9} (a_{11-k} - a_1)\zeta^k.$$

La última fórmula es equivalente a

$$\begin{cases} a_0 = a_0 - a_1 \\ a_1 = -a_1 \\ a_k = a_{11-k} - a_1, \quad 2 \le k \le 9 \end{cases}$$

$$\Leftrightarrow \begin{cases} a_1 = 0 \\ a_k = a_{11-k}, \quad 2 \le k \le 9. \end{cases}$$

Por tanto,

$$K = \{a_0 + \sum_{k=2}^{5} a_k(\zeta^k + \zeta^{11-k}) : a_k \in \mathbb{Q}\}.$$

Un elemento de K candidato a elemento primitivo es

$$\alpha = \zeta^2 + \zeta^9 \in K.$$

Comprobemos que $\zeta^k + \zeta^{11-k} \in \mathbb{Q}(\alpha)$ para $k = 3, 4, 5$, calculando potencias de α:

$$\alpha^2 = \zeta^4 + \zeta^{18} + 2 = \zeta^4 + \zeta^7 + 2 \Rightarrow \zeta^4 + \zeta^7 = \alpha^2 - 2.$$

$$\alpha^3 = (\zeta^4+\zeta^7+2)(\zeta^2+\zeta^9) = \zeta^6+\zeta^2+\zeta^9+\zeta^5+2\zeta^2+2\zeta^9 = \zeta^6+\zeta^5+3\alpha \Rightarrow \zeta^5+\zeta^6 = \alpha^3-3\alpha.$$

$$\alpha^4 = (\zeta^4+\zeta^7+2)^2 = \zeta^8+\zeta^3+4+2+4\zeta^4+4\zeta^7 = \zeta^3+\zeta^8+6+4(\alpha^2-2) \Rightarrow \zeta^3+\zeta^8 = \alpha^4-4\alpha^2+2.$$

Esto prueba que $K = \mathbb{Q}(\alpha)$. Calculamos también

$$\begin{aligned} \alpha^5 &= (\zeta^3 + \zeta^8 + 6 + 4\zeta^4 + 4\zeta^7))(\zeta^2 + \zeta^9) \\ &= \zeta^5 + \zeta + \zeta^{10} + \zeta^6 + 6\zeta^2 + 6\zeta^9 + 4\zeta^6 + 4\zeta^2 + 4\zeta^9 + 4\zeta^5 \\ &= \zeta^{10} + 5(\zeta^5 + \zeta^6) + 10(\zeta^2 + \zeta^9) + \zeta \Rightarrow \\ \zeta + \zeta^{10} &= \alpha^5 - 5(\alpha^3 - 3\alpha) - 10\alpha = \alpha^5 - 5\alpha^3 + 5\alpha. \end{aligned}$$

Coleccionamos las igualdades que hemos obtenido:

$$\begin{aligned} \zeta + \zeta^{10} &= \alpha^5 - 5\alpha^3 + 5\alpha \\ \zeta^2 + \zeta^9 &= \alpha \\ \zeta^3 + \zeta^8 &= \alpha^4 - 4\alpha^2 + 2 \\ \zeta^4 + \zeta^7 &= \alpha^2 - 2 \\ \zeta^5 + \zeta^6 &= \alpha^3 - 3\alpha. \end{aligned}$$

y al sumarlas resulta

$$-1 = \sum_{k=1}^{10} \zeta^k = \alpha^5 + \alpha^4 - 4\alpha^3 - 3\alpha^2 + 3\alpha.$$

Así, finalmente, el polinomio mínimo de $\alpha = \zeta^2 + \zeta^9$ sobre $\mathbb{Q}$ es

$$g(X) = X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1.$$

Bibliografía

[DuFo04] D.S. Dummit, R.M. Foote, *Abstract Algebra, third edition*, Wiley, 2004.

[AdWe93] W. A. Adkins, S.H. Weintraub, *Algebra. An Approach via Module Theory*, Graduate Texts in Mathematics, 136, Springer, 1992.

[Hun74] T.W. Hungerford, *Algebra*, Graduate Texts in Mathematics 73, Springer–Verlag, 1974.

[BEG89] E. Bujalance, J.J. Etayo, J.M. Gamboa, *Teoría elemental de grupos, 3ª edición*, Cuadernos de la UNED, 1989.

[DFX00] F. Delgado, C. Fuertes, S. Xambó, *Introducción al Álgebra, vol. 1,2 y 3*, Univ. de Valladolid, 2000.

[Rot98] J. Rotman, *Galois Theory, second edition*, Springer, 1998.

[Cox04] D.A. Cox, *Galois Theory*, Wiley. 2004.

[GaRu00] J.M. Gamboa, J.M Ruiz, *Anillos y cuerpos conmutativos, 3ª edición*, Cuadernos de la UNED, 2000.

[Ste89] I. Stewart, *Galois Theory, second edition*, Chapman & Hall, 1989.