Apuntes de Estructuras Algebraicas

por Enrique Arrondo(*)

Versión del 17 de Mayo de 2011

(*) Departamento de Álgebra, Facultad de Ciencias Matemáticas, Universidad Complutense de Madrid, 28040 Madrid, arrondo@mat.ucm.es

1. Teoría básica de grupos, anillos y cuerpos

Definición. Un *grupo* es un conjunto G con una operación interna $\cdot$ que verifica las siguientes propiedades:

(i) $g \cdot (h \cdot k) = (g \cdot h) \cdot k$ para cualesquiera $a, b, c \in G$ (propiedad asociativa).

(ii) Existe $1 \in G$ (elemento neutro) tal que $1 \cdot g = g \cdot 1 = g$ para cualquier $g \in G$.

(iii) Para cada $g \in G$ existe $g^{-1} \in G$ (elemento inverso) tal que $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

Si además

(iv) $gh = hg$ para cualesquiera $g, h \in G$ (propiedad conmutativa) entonces se dice que G es un *grupo abeliano*.

Normalmente, se omite el signo $\cdot$ si ello no da lugar a confusión. Es también habitual denotar a la operación con $+$ cuando el grupo es abeliano (como veremos, por ejemplo, en los anillos), en cuyo caso el elemento neutro se denota con 0 y el inverso de g con $-g$. El cardinal de un grupo se llama *orden del grupo* y se denota por $|G|$.

Ejemplo 1.1. El ejemplo de grupo que más usaremos es el del *grupo de permutaciones de n elementos*, denotado por S_n, y que consiste en el conjunto de biyecciones $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ con la composición (indicaremos simplemente $\sigma\tau$ para designar a la composición $\sigma \circ \tau$). El orden de S_n es $n!$. Llamaremos *r-ciclo* a la permutación, que denotaremos por $(i_1\ i_2 \ldots i_r)$ (con $i_1, \ldots, i_r$ elementos distintos de $\{1, 2, \ldots, n\}$) que manda i_1 a i_2, i_2 a i_3,..., i_{r-1} a i_r, i_r a i_1 y deja fijos todos los demás elementos de $\{1, 2, \ldots, n\}$. Un 2-ciclo $(i\ j)$ se llama *transposición* (ya que lo único que hace es intercambiar entre sí los números i y j). Dos ciclos $(i_1\ i_2 \ldots i_r)$, $(j_1\ j_2 \ldots j_s)$ conmutan si y sólo si $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots, j_s\} = \emptyset$ (en cuyo caso se dice que son *ciclos disjuntos*). Toda permutación se puede poner de forma única (salvo el orden) como producto de ciclos disjuntos dos a dos.

Definición. Un *subgrupo* de un grupo G es un subconjunto $H \subset G$ tal que, para cualesquiera $g, h \in H$ se tiene que $gh^{-1} \in H$; en otras palabras, H tiene estructura de grupo con la misma operación que G. Para indicar que un subconjunto $H \subset G$ es un subgrupo, escribiremos normalmente $H < G$.

Definición. Dado un subconjunto cualquiera $S \subset G$, se llama *subgrupo generado por el subconjunto S* al mínimo subgrupo de G que contiene a los elementos de S, y lo denotaremos normalmente por $< S >$. Si $G =< g >$, diremos que G es un *grupo cíclico*. En este caso, todos los elementos de G son de la forma g^n, donde

$$g^n = \begin{cases} \overbrace{g \ldots g}^{n)} & \text{si } n \geq 0 \\ \overbrace{(g^{-1}) \ldots (g^{-1})}^{-n)} & \text{si } n \leq 0 \end{cases}$$

Ejercicio 1.2. Demostrar que cada uno de los siguientes conjuntos genera el grupo S_n:

(i) Las transposiciones.

(ii) Las transposición $(1\ 2)$ y el n-ciclo $(1\ 2\ \ldots\ n)$.

(iii) Cualquier transposición y cualquier n-ciclo, si n es un número primo.

Dado un subgrupo $H < G$, se definen las relaciones de equivalencia:

$$g \sim_H g' \Leftrightarrow g^{-1}g' \in H \Leftrightarrow gH = g'H$$

$$g_H \sim g' \Leftrightarrow gg'^{-1} \in H \Leftrightarrow Hg = Hg'$$

(donde $gH = \{gh \mid h \in H\}$ y $Hg = \{hg \mid h \in H\}$). Los conjuntos de clases de equivalencia están en biyección, y su cardinal común se llama *índice de H en G*, y se denota por $[G : H]$.

Teorema de Lagrange. *Si H es un subgrupo de un grupo finito, entonces se tiene la igualdad $|G| = [G : H]|H|$. En particular, el orden de un subgrupo divide siempre al orden del grupo.*

Los cocientes $G/\sim_H$ y $G/_H\sim$ se pueden ver respectivamente como el conjunto de subconjuntos de la forma gH y el conjunto de subconjuntos de la forma Hg. Ninguno de estos cocientes tiene en general estructura de grupo definiendo el producto de gH con $g'H$ como $(gg')H$, o el producto de Hg con Hg' como $H(gg')$. De hecho, cualquiera de ellos tiene estructura de grupo si y sólo si H es un *subgrupo normal* de G, es decir, que para cada $g \in G, h \in H$, se tiene $ghg^{-1} \in H$. En tal caso, las dos relaciones de equivalencia coinciden (ya que $gH = Hg$ para cualquier $g \in G$) y el cociente se denota por G/H. Indicaremos que H es normal en G mediante el símbolo $H \lhd G$.

Ejercicio 1.3. Demostrar que el subconjunto $\{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ de S_4 es un subgrupo normal.

Definición. Un *homomorfismo de grupos* es una aplicación $\varphi : G \to G'$ entre dos grupos tal que $\varphi(gh) = \varphi(g)\varphi(h)$ para cualesquiera $g, h \in G$. Si φ es inyectiva, se dice que es un *monomorfismo*; si es suprayectiva, es un *epimorfismo*, y si es biyectiva, es un *isomorfismo* (y en este caso, su inversa es también un homomorfismo).

Definición. Dado un homomorfismo de grupos $\varphi : G \to G'$, se llama *núcleo del homomorfismo* al subgrupo (normal) $\ker\varphi := \{g \in G \mid \varphi(g) = 1\}$ y se llama *imagen del homomorfismo* al subgrupo $\mathrm{Im}\,\varphi := \varphi(G) < G'$.

Ejemplo 1.4. Consideramos $\{1, -1\}$ con la estructura de grupo dada por el producto y definimos la aplicación $\mathrm{sgn} : S_n \to \{1, -1\}$ definida por

$$\mathrm{sgn}(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Obsérvese que los factores que aparecen en el numerador son los mismos que los que aparecen en el denominador, aunque cambiados de orden y quizá de signo, por lo que, en efecto, el valor total es 1 o -1, en concreto -1 elevado al número de veces que $i < j$ pero $\sigma(i > \sigma(j)$. Si σ, τ son dos permutaciones, se tendrá

$$\operatorname{sgn}(\sigma\tau) = \prod_{1\leq i<j\leq n} \frac{\sigma\tau(i) - \sigma\tau(j)}{i-j}$$

$$= \prod_{1\leq i<j\leq n} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \prod_{1\leq i<j\leq n} \frac{\tau(i) - \tau(j)}{i-j} = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

La última igualdad se debe a que el conjunto de pares (no ordenados) $\{i, j\}$ coincide con el conjunto de pares $\{\tau(i), \tau(j)\}$ y el conjunto de cocientes $\frac{\sigma(i)-\sigma(j)}{i-j}$ coincide con el conjunto de cocientes $\frac{\sigma\tau(i)-\sigma\tau(j)}{\tau(i)-\tau(j)}$ (con la única salvedad de que, si $i < j$ pero $\tau(i) > \tau(j)$ entonces hay que cambiar de signo numerador y denominador). Por tanto, tenemos que sgn es un homomorfismo de grupos. El valor $\operatorname{sgn}(\sigma)$ se llama *signo de la permutación* σ. Una *permutación par* es una permutación con signo $+1$, y una *permutación impar* es una permutacion de signo -1. El conjunto de permutaciones pares es el núcleo de sgn, por lo que es un subgrupo normal, llamado *subgrupo alternado* A_n. El motivo del nombre par o impar para una permutación es el siguiente. Supongamos que tenemos una transposición $\sigma = (a\ b)$. Como $(a\ b) = (b\ a)$, podemos suponer $a < b$. Entonces los factores negativos en la definición de $\operatorname{sgn}(a\ b)$ son exactamente (recuérdese que $i < j$)

$$\frac{\sigma(i) - \sigma(j)}{i-j} = \begin{cases} \frac{b-j}{a-j} & \text{si } i = a < j < b \\ \frac{i-a}{i-b} & \text{si } a < i < j = b \\ \frac{b-a}{a-b} = -1 & \text{si } i = a < j = b \end{cases}$$

luego en total hay $(b-a-1)+(b-a-1)+1$ (que es un números par) factores negativos, con lo que $\operatorname{sgn}(a\ b) = -1$. Dado que cualquier permutación es producto de transposiciones, esto demuestra que una permutación es par si y sólo si se se puede escribir como producto de un número par de transposiciones, e impar si y sólo si se escribe como producto de un número impar (y por supuesto, ninguna se puede escribir simultáneamente como producto de un número par y un número impar de transposiciones).

Ejercicio 1.5. Demostrar que el grupo A_n está generado por los 3-ciclos.

Primer teorema de isomorfía. *Sea $\varphi : G \to G'$ un homomorfismo de grupos. Entonces la aplicación natural $\bar{\varphi} : G/\ker\varphi \to \operatorname{Im}\varphi$ definida por $\bar{\varphi}(gH) = \varphi(g)$ es un isomorfismo.*

Ejemplo 1.6. Dado un grupo G y un elemento G, consideramos el homomorfismo de grupos $\varphi_g : \mathbb{Z} \to G$) (donde en $\mathbb{Z}$ tomamos la adición) definido por $\varphi(n) = g^n$. Entonces $\operatorname{Im}\varphi_g =< g >$. Como cualquier subgrupo de $\mathbb{Z}$ es cíclico $< n >$, se tiene que $< g > \cong \mathbb{Z}/ < n >= \mathbb{Z}_n$. Si $n > 0$, se dice que n es el *orden del elemento* g. Como $| < g > | = n$, el teorema de Lagrange implica que, si G es finito, el orden de cualquier elemento divide al orden del grupo. Obsérvese que el orden n es el menor entero n tal que $g^n = 1$.

Ejercicio 1.7. Sea G es un grupo cíclico de orden n generado por un elemento g. Demostrar que para cada divisor m de n existe un único subgrupo de G de orden m, y que es el subgrupo cíclico generado por $g^{\frac{n}{m}}$.

Segundo teorema de isomorfía. *Sea G un grupo y sea $N \lhd G$. Entonces la proyección natural $\pi : G \to G/N$ induce una biyección entre el conjunto de los subgrupos de G que contienen a N y los subgrupos de G/N; es decir, los subgrupos de G/N se pueden escribir de forma única como H/N, donde $N < H < G$. Además, $H/N \lhd G/N$ si y sólo si $H \lhd G$, y en este caso $(G/N)/(H/N) \cong G/H$ (mediante la aplicación natural).*

Tercer teorema de isomorfía. *Sea G un grupo y sean $H < G$, $N \lhd G$. Entonces:*

(i) $H \cap N \lhd H$.

(ii) El conjunto $HN = \{hn \mid h \in H, n \in N\}$ *es un subgrupo de* G.

(iii) La aplicación natural $H/(H \cap N) \to HN/N$ *es un isomorfismo.*

Teorema de estructura de los grupos abelianos finitos. *Sea G un grupo abeliano finito. Entonces existen $n_1, n_2, \ldots, n_r \in \mathbb{N}$ únicos tales que $n_1|n_2|\ldots|n_r$ y con $G \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$.*

Ejercicio 1.8. Demostrar, a partir del teorema de estructura, que todo grupo abeliano finito G posee subgrupos de orden cualquier divisor de $|G|$.

Definición. Un *anillo* es un conjunto A con dos operaciones internas, $+$ y $\cdot$, tales que $(A, +)$ es un grupo abeliano y se verifican las propiedades:

(i) $(a+b)\cdot c = a\cdot c+b\cdot c$ y $a\cdot(b+c) = a\cdot b+a\cdot c$ para cualesquiera $a, b, c \in A$ (distributividad del producto respecto de la suma).

(ii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para cualesquiera $a, b, c \in A$ (asociatividad del producto).

El anillo se dice *conmutativo* si además se verifica

(iii) $a \cdot b = b \cdot a$ para cualesquiera $a, b \in A$ (conmutatividad del producto).

Y se dice *con unidad* si se verifica

(iv) Existe $1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a$ para cualquier $a \in A$ (existencia de elemento neutro para el producto).

Supondremos que todos nuestros anillos son conmutativos y con unidad. Al elemento neutro para la suma lo denotaremos por 0, y al inverso para la suma de a por $-a$. Omitiremos también sistemáticamente el punto $\cdot$ en el producto de dos elementos.

Definición. *Una unidad* en un anillo A es un elemento $a \in A$ que tiene inverso para el producto, es decir, que existe $a^{-1} \in A$ tal que $aa^{-1} = a^{-1}a = 1$. Un anillo en el que todos los elementos $a \neq 0$ son unidades es un *cuerpo*.

Definición. Un anillo se dice que es un *dominio de integridad* (que abreviaremos con D.I.) si, dados $a, b \in A$ tales que $ab = 0$, entonces necesariamente $a = 0$ ó $b = 0$.

Definición. Un *subanillo* de un anillo A es un subconjunto $B \subset A$ tal que, para cualesquiera $a, b, c, d \in B$ se tiene que $ab + cd \in B$; en otras palabras, B tiene estructura de anillo con las mismas operaciones que A.

Sin embargo, los subconjuntos buenos de los anillos no son los subanillos, ya que el cociente de un anillo por un subanillo no tiene estructura de anillo. Para ello, hay que pedir una condición más, llegando a la siguiente:

Definición. Un *ideal* en un anillo I es un subconjunto $I \subset A$ tal que, para cualesquiera elementos $a, b \in A$, $c, d \in I$ se tiene $ac + bd \in I$. La relación

$$a \equiv b \Leftrightarrow a + I = b + I \Leftrightarrow a - b \in I$$

(donde $a + I = \{a + a' \mid a' \in I\}$) es una relación de equivalencia. El correspondiente conjunto cociente A/I tiene, con las operaciones naturales, estructura de anillo, y se llama *anillo cociente*. Puede considerarse como el conjunto formado por los subconjuntos de A de la forma $a + I$.

Definición. Un *ideal maximal* es un ideal propio de A (i.e. $I \subsetneq A$) que no está contenido en otro ideal propio de A. Equivalentemente, A/I es un cuerpo.

Definición. Un *ideal primo* es un ideal propio I de A tal que, dados $a, b \in A$ tales que $ab \in I$, entonces necesariamente $a \in I$ ó $b \in I$. Equivalentemente, A/I es un D.I. (y del mismo modo, un D.I. está caracterizado por el hecho de que el ideal trivial (0) sea primo).

Definición. Se llama *ideal generado por los elementos* $b_1, \ldots, b_r$ de un anillo A al conjunto $(b_1, \ldots, b_r) := \{a_1b_1 + \ldots + a_rb_r \mid a_1, \ldots, a_r \in A\}$. Este conjunto es el ideal de A más pequeño que contiene a los elementos $b_1, \ldots, b_r$. En particular, el ideal generado por dos ideales I, J es el conjunto $I + J = \{a + b \mid a \in I, b \in J\}$, que se llama *ideal suma*. Se llama *ideal principal* a un ideal generado por un solo elemento $b \in A$, es decir, de la forma $(b) = \{ab \mid a \in A\}$. Un anillo en el que todos los ideales son principales se llama *dominio de ideales principales* (D.I.P. para abreviar).

Ejemplo 1.9. $\mathbb{Z}$ y $K[X]$ (donde K es un cuerpo) son D.I.P.

Ejercicio 1.10. Demostrar que dos elementos $, a, b \in A$ de un D.I. generan el mismo ideal si y sólo si existe una unidad $u \in A$ tal que $a = ub$.

Definición. Un *homomorfismo de anillos* es una aplicación $\varphi : A \to A'$ entre dos anillos tal que $\varphi(ab + cd) = \varphi(a)\varphi(b) + \varphi(c)\varphi(d)$ para cualesquiera $a, b, c, d \in A$. Como estamos considerando anillos con unidad, pediremos también la condición $\varphi(1_A) = 1_{A'}$ (donde 1_A y $1_{A'}$ son, respectivamente, los elementos unidad para el producto de A y A'). Si φ es inyectiva, se dice que es un *monomorfismo*; si es suprayectiva, es un *epimorfismo*, y si es biyectiva, es un *isomorfismo* (y en este caso, su inversa es también un homomorfismo).

Ejercicio 1.11. Demostrar que, si A' es un D.I., entonces la condición $\varphi(1_A) = 1_{A'}$ en la definición de homomorfismo se deduce de la otra siempre que φ no sea nula. Dar en cambio un ejemplo de aplicación no nula $\varphi : A \to A'$ que verifique $\varphi(ab+cd) = \varphi(a)\varphi(b)+\varphi(c)\varphi(d)$ pero $\varphi(1_A) \neq 1_{A'}$.

Observación 1.12. Conviene observar que, mientras que la imagen inversa de un ideal por un homomorfismo es un ideal, la imagen de un ideal no es en general un ideal (salvo que el homomorfismo sea suprayectivo). Lo único que se puede afirmar es que la imagen de un subanillo es un subanillo.

Definición. Dado un homomorfismo de anillos $\varphi : A \to A'$, se llama *núcleo del homomorfismo* al ideal $\ker \varphi := \{a \in A \mid \varphi(a) = 0\}$ y se llama *imagen del homomorfismo* al subanillo $\operatorname{Im} \varphi := \varphi(A) \subset A'$.

Primer teorema de isomorfía. *Sea $\varphi : A \to A'$ un homomorfismo de anillos. Entonces la aplicación natural $\bar{\varphi} : A/\ker \varphi \to \operatorname{Im} \varphi$ definida por $\bar{\varphi}(a + I) = \varphi(a)$ es un isomorfismo.*

Definición. Se llama *característica de un anillo* A al único generador no negativo del núcleo del homomorfismo $\mathbb{Z} \to A$ definido por

$$n \mapsto \begin{cases} 1 + \overset{n)}{\ldots} + 1 & \text{si } n \geq 0 \\ (-1) + \overset{-n)}{\ldots} + (-1) & \text{si } n \leq 0 \end{cases}$$

En otras palabras, A tiene *característica cero* si ninguna suma positiva de unos es nula, mientras que tiene *característica positiva* n si n es el menor número de veces que sumado el uno obtenemos cero. Por el primer teorema de isomorfía, $\mathbb{Z}_n$ es isomorfo a un subanillo de A, por lo que si A es un D.I. (por ejemplo, si es un cuerpo) su característica (si no es cero) es un número primo.

Ejercicio 1.13. Sea A un anillo con característica un número primo p. Demostrar que $(a+b)^p = a^p + b^p$ para cualesquiera $a, b \in A$. Más en general, $(a+b)^{p^k} = a^{p^k} + b^{p^k}$ para cualquier $k \in \mathbb{N}$.

Segundo teorema de isomorfía. *Sea A un grupo y sea $I \subset A$ un ideal. Entonces la proyección natural $\pi : A \to A/I$ induce una biyección entre el conjunto de los ideales de A que contienen a I y los ideales de A/I; es decir, los subgrupos de A/I se pueden escribir de forma única como J/I, donde $I \subset J \subset A$. Además, $(A/I)/(J/I) \cong A/J$ (mediante la aplicación natural). En particular, J/I es primo en A/I si y sólo si I es primo en A.*

Tercer teorema de isomorfía. *Sea A un grupo y sean I, J, ideales de A. Entonces la aplicación natural $I/I \cap J \to (I+J)/I$ es un isomorfismo.*

Dedicamos el resto de este capítulo a los anillos más importantes que vamos a utilizar: los anillos de polinomios.

Definición. Dado un anillo A, se llama *anillo de polinomios con coeficientes en A en la indeterminada X* al conjunto $A[X]$ de expresiones formales $f = a_0 + a_1X + a_2X^2 + \ldots$ en que $a_i \in A$ y existe $d \in \mathbb{N}$ tal que $a_i = 0$ si $i > d$, en cuyo caso se escribe normalmente $f = a_0 + a_1X + \ldots + a_dX^d$. Es fácil (aunque lioso) ver que el conjunto $A[X]$ tiene estructura de anillo con las operaciones

$$(a_0 + a_1X + \ldots + a_dX^d) + (b_0 + b_1X + \ldots + b_dX^d) = (a_0 + b_0) + (a_1 + b_1)X + \ldots + (a_d + b_d)X^d$$

$$(a_0 + a_1X + \ldots + a_dX^d)(b_0 + b_1X + \ldots + b_eX^e) = (a_0b_0) + (a_0b_1 + a_1b_0)X + \ldots + (a_db_e)X^{d+e}$$

(nótese que dos polinomios arbitrarios los podemos escribir con el mismo d, ya que basta tomar el más grande de ambos).

Ejercicio 1.14. Dado un anillo A, el *grado de un polinomio no nulo* $f \in A[X]$ (que denotaremos por ∂f) es el mayor exponente de X que tiene coeficiente no nulo en f. Es decir, que f tenga grado d quiere decir que f se puede escribir $f = a_0 + a_1X + \ldots + a_dX^d$ con $a_n \neq 0$. Por comodidad, se suele escribir convenir que el grado de cero es $-\infty$.

(i) Demostrar que A, identificado con el conjunto de polinomios de grado menor o igual que cero, es un subanillo de $A[X]$.

(ii) Demostrar que, dados $f, g \in A[X]$, entonces $\partial(f+g) \leq \max\{\partial f, \partial g\}$, y que si no se da la igualdad entonces $\partial f = \partial g$.

(iii) Si A es un D.I., demostrar que $\partial(fg) = \partial f + \partial g$ para cualesquiera $f, g \in A[X]$. Concluir entonces que $A[X]$ es un D.I. y que sus unidades son las unidades de A (en particular, en $K[X]$, con K cuerpo, sus unidades son las constantes no nulas de K).

(iv) Dar un contraejemplo a la propiedad de los grados del apartado anterior si no se supone que A sea un D.I.

Si queremos trabajar con varias indeterminadas, repetir todo lo anterior (en concreto describir el producto de dos polinomios) es especialmente engorroso, por lo que daremos la definición por recurrencia:

Definición. Dado un anillo A, se llama *anillo de polinomios con coeficientes en A en las indeterminadas $X_1, \ldots, X_n$* al conjunto $A[X_1, \ldots, X_n]$ definido como $(A[X_1, \ldots, X_{n-1}])[X_n]$. Obsérvese que existe un monomorfismo natural de anillos $i : A \to A[X_1, \ldots, X_n]$.

La definición anterior no es completamente satisfactoria, ya que parece depender del orden en que se introducen las indetermiadas. Para solucionar esto, utilizaremos una técnica frecuente en matemáticas, que consiste en caracterizar (salvo isomorfismo) ciertos objetos por medio de lo que se llama una *propiedad universal*. Ilustramos este hecho con la correspondiente propiedad universal para anillos de polinomios:

Proposición 1.15. *Sea A un anillo y $R = A[X_1, \ldots, X_n]$ el anillo de polinomios en las indeterminadas $X_1, \ldots, X_n$ con coeficientes en A. Entonces la inclusión natural $i : A \hookrightarrow A[X_1, \ldots, X_n]$ verifica la siguiente propiedad universal:*

(*) Para cada anillo A', homomorfismo $\varphi : A \to A'$ y elementos $a'_1, \ldots, a'_n \in A'$, existe un único homomorfismo de anillos $\bar{\varphi} : R \to A'$ tal que $\varphi = \bar{\varphi} \circ i$ y $\bar{\varphi}(X_j) = a'_j$ para $j = 1, \ldots, n$.

$$\begin{array}{ccc} A & & \\ \downarrow{\scriptstyle i} & \searrow^{\varphi} & \\ R & \xrightarrow[\bar{\varphi}]{} & A' \end{array}$$

Además, cualquier otro anillo R' con elementos $X'_1, \ldots, X'_n$ y con un monomorfismo $i' : A \to R'$ que verifique la propiedad (*) es isomorfo a $A[X_1, \ldots, X_n]$.

Demostración: Demostremos primero, por inducción sobre n, que $A[X_1, \ldots, X_n]$ verifica (*). Obviamente, el caso $n = 0$ es trivial, así que supondremos $n \geq 1$ y que la inclusión $i' : A \to A[X_1, \ldots, X_{n-1}]$ verifica la propiedad universal. Por tanto, dado un homomorfismo de anillos $\varphi : A \to A'$ y elementos $a'_1, \ldots, a'_n \in A'$ podemos asegurar por hipótesis de inducción que existe un único homomorfismo de anillos $\psi : A[X_1, \ldots, X_{n-1}$ tal que $\varphi = \psi \circ i'$ y $\psi(X_i) = a'_1$ para $i = 1, \ldots, n-1$. Queremos construir ahora un homomorfismo $\bar{\varphi} : A[X_1, \ldots, X_n] \to A'$ tal que $\bar{\varphi}(X_n) = a'_n$ y el diagrama

$$\begin{array}{ccc} A & & \\ \downarrow{\scriptstyle i'} & \searrow^{\varphi} & \\ A[X_1, \ldots, X_{n-1}] & \xrightarrow{\psi} & A' \\ \downarrow{\scriptstyle j} & \nearrow_{\bar{\varphi}} & \\ A[X_1, \ldots, X_n] & & \end{array}$$

sea conmutativo (donde j es el monomorfismo natural). Recordando que los elementos de $A[X_1, \ldots, X_n]$ son polinomios en la indeterminada X_n con coeficientes en $A[X_1, \ldots, X_{n-1}]$, debe ser por tanto

$$\bar{\varphi}(f_0 + f_1 X_n + \ldots + f_d X_n^d) = \bar{\varphi}(f_0) + \bar{\varphi}(f_1)\bar{\varphi}(X_n) + \ldots + \bar{\varphi}(f_n)\bar{\varphi}(X_n)^d =$$

$$\bar{\varphi}(j(f_0)) + \bar{\varphi}(j(f_1))\bar{\varphi}(X_n) + \ldots + \bar{\varphi}(j(f_n))\bar{\varphi}(X_n)^d = \psi(f_0) + \psi(f_1)a'_n + \ldots + \psi(f_d){a'_n}^d$$

con lo que $\bar{\varphi}$ es único en esas condiciones. Además es claro que tal $\bar{\varphi}$ es un homomorfismo de grupos y que verifica las condiciones de (*). Hay que ver que es el único que verifica las dos condiciones de (*). Supongamos que otro $\bar{\varphi}'$ las verificara. En particular, tendríamos que $\bar{\varphi}' \circ j$ verifica

$$(\bar{\varphi}' \circ j) \circ i' = \bar{\varphi}' \circ i = \varphi$$

$$\bar{\varphi}' \circ j(X_i) = \bar{\varphi}'(X_i) = a'_i \quad \text{si} \quad i = 1, \ldots, n-1.$$

Como ψ era el único homomorfismo que verificaba esas dos condiciones (por la unicidad en la hipótesis de inducción) se tiene $\bar{\varphi}' \circ j = \psi$. Como se tiene además $\bar{\varphi}'(X_n) = a'_n$, y estas dos propiedades caracterizan a $\bar{\varphi}$, se sigue la igualdad $\bar{\varphi}' = \bar{\varphi}$. Esto termina la demostración de que $R = A[X_1, \ldots, X_n]$ verifica la propiedad (*).

Para ver que la propiedad (*) caracteriza a R salvo isomorfismo, supongamos que tenemos otro $i' : A \to R'$ con $X'_1, \ldots, X'_n \in R'$ que verifica (*) . Aplicando la propiedad (*) a $i : A \to R$ tomando $\varphi = i'$ (y $a'_j = X'_j$ para $j = 1, \ldots, n$) tendremos (ver diagrama de abajo a la izquierda) que existe $\psi : R \to R'$ tal que $i' = \psi \circ i$ y con cada $\psi(X_j) = X'_j$. Aplicando de forma simétrica (*) a i', tendremos (diagrama de abajo a la derecha) $\psi' : R' \to R$ tal que $i = \psi' \circ i$ con $\psi'(X'_j) = X_j$.

$$\begin{array}{ccc} A & & \\ \downarrow{\scriptstyle i} & \searrow^{i'} & \\ R & \xrightarrow[\psi]{} & R' \end{array} \qquad\qquad \begin{array}{ccc} A' & & \\ \downarrow{\scriptstyle i'} & \searrow^{i} & \\ R' & \xrightarrow[\psi']{} & R \end{array}$$

El truco está ahora en volver a aplicar ahora (*) pero a los siguientes diagramas:

$$\begin{array}{ccc} A & & \\ \downarrow{\scriptstyle i} & \searrow^{i} & \\ R & \xrightarrow[\psi' \circ \psi, id_R]{} & R \end{array} \qquad\qquad \begin{array}{ccc} A & & \\ \downarrow{\scriptstyle i'} & \searrow^{i'} & \\ R' & \xrightarrow[\psi \circ \psi', id_{R'}]{} & R' \end{array}$$

Como en ambos la flecha punteada debe ser única, se tiene $\psi' \circ \psi = id_R$, $\psi \circ \psi' = id_{R'}$, con lo que ψ y ψ' son inversas una de la otra, luego isomorfismos. $\square$

Ejercicio 1.16. Usando la propiedad universal de anillos de polinomios, demostrar que, si A es un anillo, entonces $(A[X_1, \ldots, X_n])[Y_1, \ldots, Y_m]$ es canónicamente isomorfo a $A[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$.

La propiedad universal para anillos de polinomios viene a decir que, en cierto modo, las indeterminadas forman una especie de base, en el sentido de que sus imágenes determinan de forma única cualquier homomorfismo de anillos. Ilustremos este hecho con algunas definiciones más (que serán especialmente útiles a la hora de estudiar la teoría de Galois):

Definición. Sea A un subanillo de un anillo B, y sean, $b_1, \ldots, b_n \in B$. Entonces llamaremos *subanillo generado por los elementos* $b_1, \ldots, b_n$ al mínimo subanillo de B que contiene a A y a $b_1, \ldots, b_n$. Es fácil ver que dicho subanillo consiste en las expresiones polinomiales, con coeficientes en A, de $b_1, \ldots, b_n$, por lo que lo denotaremos $A[b_1, \ldots, b_n]$. En otras palabras, tenemos definido el homomorfismo

$$ev_{b_1,\ldots,b_n} : A[X_1, \ldots, X_n] \to B$$

$$f(X_1, \ldots, X_n) \mapsto f(b_1, \ldots, b_n)$$

y $A[b_1, \ldots, b_n]$ es precisamente la imagen.

Definición. En las condiciones anteriores, los elementos $b_1, \ldots, b_n$ se dice que son *algebraicamente independientes sobre el anillo* A si la aplicación $ev_{b_1,\ldots,b_n}$ es inyectiva (y por tanto $A[b_1, \ldots, b_n] \cong A[X_1, \ldots, X_n]$), es decir, si no existe ninguna relación polinomial con coeficientes en A entre los elementos $b_1, \ldots, b_n$. En caso contrario, se dice que los elementos $b_1, \ldots, b_n$ son *algebraicamente dependientes sobre el anillo* A.

Ejemplo 1.17. Consideremos $\mathbb{Z}$ como subanillo de $\mathbb{C}$ y el elemento $i = \sqrt{-1}$. El subanillo $\mathbb{Z}[i]$ generado por i se llama *anillo de los enteros de Gauss*. La aplicación $ev_i : \mathbb{Z}[X] \to \mathbb{C}$ no es inyectiva, ya que $ev_i(X^2+1) = i^2+1 = 0$. Es decir, i es algebraicamente dependiente sobre $\mathbb{Z}$ (cuando se trata de un solo elemento, en teoría de cuerpos abreviaremos diciendo que i es algebraico sobre $\mathbb{Z}$). Obsérvese también que, en virtud de esa relación, cualquier elemento de $\mathbb{Z}[i]$ se puede escribir (de forma única) como $a + bi$, con $a, b \in \mathbb{Z}$. Observamos finalmente que la inclusión natural $j : \mathbb{Z} \hookrightarrow \mathbb{Z}[i]$ no verifica la propiedad universal (*) de los anillos de polinomios. En efecto, si consideramos la inclusión $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Z}[X]$ y el elemento $X \in \mathbb{Z}[X]$ no podemos encontrar $\bar{\varphi} : \mathbb{Z}[i] \to \mathbb{Z}[X]$ tal que $\varphi = \bar{\varphi} \circ j$ y $\bar{\varphi}(i) = X$; dicha aplicación debería verificar $X^2 + 1 = \bar{\varphi}(1 + i^2) = \bar{\varphi}(0) = 0$, lo que es una contradicción.

Ejercicio 1.18. Sea $d \in \mathbb{Z}$ un entero que no sea un cuadrado perfecto.

(i) Demostrar que cualquier elemento del subanillo $\mathbb{Z}[\sqrt{d}] \subset \mathbb{C}$ se escribe de forma única como $a + b\sqrt{d}$, con $a, b \in \mathbb{Z}$.

(ii) Demostrar que la aplicación $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ definida por $N(a + b\sqrt{d}) = a^2 - db^2$ verifica $N(\alpha\beta) = N(\alpha)N(\beta)$ para cualesquiera $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$.

(iii) Demostrar que $\alpha \in \mathbb{Z}[\sqrt{d}]$ es una unidad si y sólo si $N(\alpha) = \pm 1$.

Una consecuencia inmediata de la propiedad universal (que puede verse también directamente a mano) es que un homomorfismo de anillos $\varphi : A \to B$ induce automáticamente otro homomorfismo de anillos $\varphi[X] : A[X] \to B[X]$ definido por $a_0 + a_1X + \ldots + a_dX^d \mapsto \varphi(a_0) + \varphi(a_1)X + \ldots + \varphi(a_d)X^d$. Claramente $\varphi[X]$ es inyectiva o suprayectiva si φ lo es. Vamos a aplicar esto a dos caso concretos. Para el primero de ellos necesitamos una definición previa (que es la generalización de la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$, i.e. de cómo construir un cuerpo que contenga a un anillo).

Definición. Se llama *cuerpo de fracciones* de un D.I. A al conjunto de expresiones $\frac{a}{b}$, con $a, b \in A$ y $b \neq 0$, donde $\frac{a}{b} = \frac{c}{d}$ si y sólo si $ad = bc$. El cuerpo de fracciones de $A[X_1, \ldots, X_n]$ (donde A es un D.I.) se suele denotar por $A(X_1, \ldots, X_n)$. El cuerpo de fracciones tiene estructura de cuerpo (del que A es un subanillo) con las operaciones:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Ejercicio 1.19. Demostrar que la inclusión $i : A \hookrightarrow K$ de un D.I. en su cuerpo de fracciones verifica la siguiente propiedad universal que lo caracteriza salvo isomorfismo: para cada monomorfismo $\varphi : A \to A'$ en un anillo A' tal que los elementos de $\varphi(A \setminus \{0\})$ son unidades existe un único homomorfismo de anillos $\bar{\varphi} : K \to A'$ tal que $\varphi = \bar{\varphi} \circ i$.

Observación 1.20. Obsérvese que un cuerpo está caracterizado por el hecho de que sus ideales son el cero y el total. Por tanto, cualquier homomorfismo de anillos $K \to A$ en el que K sea un cuerpo es un monomorfismo (usaremos este hecho repetidamente); en efecto, el núcleo, que es un ideal, no puede ser el total, porque 1_K debe ir a 1_A, luego el núcleo es cero. En particular, el homomorfismo $\bar{\varphi}$ del ejercicio anterior es siempre inyectivo. Por ejemplo, si un cuerpo K tiene característica cero, entonces existe un monomorfismo $\mathbb{Z} \to K$. Por la propiedad universal del cuerpo de fracciones de $\mathbb{Z}$ (que es $\mathbb{Q}$), este monomorfismo se extenderá a un monomorfismo $\mathbb{Q} \to K$.

La generalización del cuerpo de fracciones (y de hecho su definición precisa) es la siguiente:

Ejercicio 1.21. Sea A un anillo y $S \subset A \setminus \{0\}$ un *subconjunto multiplicativamente cerrado* (i.e. que $\forall s, t \in S$, $st \in S$) tal que $1 \in S$. Se define $S^{-1}A$ como el conjunto de fracciones $\frac{a}{s}$ ($a \in A$, $s \in S$), donde $\frac{a}{s} = \frac{b}{t}$ si y sólo si existe $u \in S$ tal que $uat = ubs$.

(i) Demostrar las operaciones $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ y $\frac{a}{s}\frac{b}{t} = \frac{ab}{st}$ están bien definidas y dotan a $S^{-1}A$ de estructura de anillo (conmutativo y con unidad).

(ii) Demostrar que la aplicación $i_S : A \to S^{-1}A$ definida por $a \mapsto \frac{a}{1}$ es un homomorfismo de anillos, que la imagen de cada elemento de S es una unidad, y que esta propiedad caracteriza a $S^{-1}A$ mediante una propiedad universal.

(iii) Demostrar que i_S es inyectivo si y sólo si S no contiene divisores de cero (i.e. elementos $a \in A$ tales que $ab = 0$ para algún $b \neq 0$.

(iv) Si P es un ideal primo, comprobar que $S = A \setminus P$ es es un subconjunto multiplicativamente cerrado (en este caso, $S^{-1}A$ se denota por A_P y se llama *localización de A en P*).

(v) Demostrar que $S = \{s \in A \mid s \text{ no es un divisor de cero}\}$ es un subconjunto multiplicativamente cerrado de A (en este caso, $S^{-1}A$ se llama *anillo total de fracciones* de A). Si A es un dominio de integridad, comprobar que $S = A \setminus \{0\}$ y $S^{-1}A$ es el cuerpo de fracciones de A.

(vi) Demostrar que i_S^{-1} define una biyección entre los ideales de $S^{-1}A$ y los ideales de A que no cortan a S. Demostrar que tal biyección restringe a una biyección entre los ideales primos de $S^{-1}A$ y los ideales primos de A que no cortan a S. En particular, A_P contiene un único ideal maximal, que es el que corresponde al ideal primo P de A.

Ejemplo 1.22. Si $i : A \hookrightarrow K$ es la inclusión de un D.I. en su cuerpo de fracciones, consideramos el monomorfismo $i[X] : A[X] \to K[X]$. Esta inclusión nos permitirá ver polinomios con coeficientes en un anillo como polinomios con coeficientes en un cuerpo, que en principio tienen propiedades mejores (por ejemplo $K[X]$ es un D.I.P. y tiene una división).

Ejemplo 1.23. Consideramos ahora un anillo A cualquiera y un ideal suyo I, y la proyección canónica $\pi : A \to A/I$. Tenemos entonces el epimorfismo $\pi[X] : A[X] \to (A/I)[X]$. La imagen de un polinomio de $A[X]$ es lo que se llama la *reducción módulo I del polinomio*. El núcleo de $\pi[X]$ es claramente $I[X] = \{a_0 + a_1X + \ldots + a_dX^d \in A[X] \mid a_i \in I \text{ para } i = 0, \ldots, d\}$, por lo que el primer teorema de isomorfía tenemos que $A[X]/I[X]$ es canónicamente isomorfo a $(A/I)[X]$. En particular, si I es primo, entonces A/I es un D.I., por lo que (ver el Ejercicio 1.14) $(A/I)[X]$ y $A[X]/I[X]$ son D.I., es decir, $I[X]$ es un ideal primo. Si I es un ideal maximal, de nuevo $\pi[X]$ permite pasar de polinomios con coeficientes en un anillo a polinomios con coeficientes en un cuerpo.

2. Divisibilidad y factorización en anillos

Definición. Dado un anillo A, y elementos $a, b \in A$, diremos que a *divide a* b (y lo denotaremos por $a|b$ si existe $c \in A$ tal que $b = ac$, es decir, si $b \in (a)$.

La mejor forma de ver si un elemento divide a otro sería el que, como ocurre para los números enteros o los polinomios (en una indeterminada sobre un cuerpo), existiera un algoritmo de división. La definición general es:

Definición. Un anillo A es un *dominio euclídeo (D.E.)* si es un D.I. y existe una aplicación $\delta : A \setminus \{0\} \to \mathbb{N}$ tal que, dados $a, b \in A$ con $b \neq 0$, existe una descomposición (no necesariamente única) $a = qb + r$ con $r = 0$ o bien $\delta(r) < \delta(b)$.

Ejemplo 2.1. El anillo $\mathbb{Z}$ es un D.E. con la división euclídea usual; basta tomar como δ el valor absoluto.

Ejemplo 2.2. El anillo de polinomios $K[X]$ en una indeterminada sobre un cuerpo es un D.E., tomando como δ el grado.

Cuando el anillo de coeficientes del anillo de polinomios no es un cuerpo (pensando por ejemplo en anillos de polinomios en varias indeterminadas), no siempre existe la división. Lo máximo que se puede decir es lo siguiente (que cuando A es un cuerpo en realidad es la demostración de que existe la división):

Proposición 2.3. *Sea A un anillo y sean $f, g \in A[X]$, donde $g = b_0 + b_1X + \ldots + b_mX^m$ con $b_m \neq 0$ (i.e. el grado de g es m). Entonces existe $l \in \mathbb{N}$ y polinomios $q, r \in A[X]$ (con $r = 0$ o de grado menor que m) tales que $b_m^l f = qg + r$. Además, si A es un D.I., se tiene que para cada l los polinomios q y r son únicos.*

Demostración: Demostraremos la existencia de q y r por inducción sobre el grado de f. Si tiene grado menor que m, basta tomar $l = 0$, $q = 0$ y $r = f$. Así que suponemos que f tiene grado $n \geq m$ y que el resultado está demostrado para polinomios de grado menor que n. Escribimos $f = a_0 + a_1X + \ldots + a_nX^n$. Definimos entonces el polinomio $\bar{f} = b_m f - a_n g X^{n-m}$. Claramente, $\bar{f}$ tiene grado menor que n, por lo que por hipótesis de inducción podemos encontrar $l \in \mathbb{N}$ y $\bar{q}, \bar{r} \in A[X]$ (con $\bar{r} = 0$ o de grado menor que m) tales que $b_m^l \bar{f} = \bar{q}g + \bar{r}$. Por tanto, $b_m^{l+1} f = (a_nX^{n-m} + b_m\bar{q})g + b_m\bar{r}$. Tomando $q = a_nX^{n-m} + b_m\bar{q}$ y $r = b_m\bar{r}$ se concluye el resultado de existencia.

Para la unicidad, supongamos que tenemos $b_m^l f = qg + r = q'g + r'$, con r, r' o bien cero o de grado menor que m. Entonces $(q - q')g = r' - r$. Como A es un D.I., si $q - q' \neq 0$, entonces $(q - q')g$ tendría grado al menos m (ver el Ejercicio 1.14), lo que es absurdo, ya que $r - r'$ es cero o tiene grado menor que m. Por tanto, $q = q'$, lo que implica también $r = r'$. □

El resultado anterior implica que sí que existe una buena división cuando dividimos entre polinomios mónicos (es decir, aquéllos en que el coeficiente del término de grado mayor es 1). En concreto, para polinomios de grado uno se tiene que la regla de Ruffini sigue siendo cierta para polinomios con coeficientes en un anillo arbitrario:

Corolario 2.4. *Sea A un anillo y sea $a \in A$. Entonces un polinomio $f \in A[X]$ es divisible por $X - a$ si y sólo si $f(a) = 0$.*

Demostración: Es evidente que si f es divisible por $X - a$ entonces $f(a) = 0$. Recíprocamente, si $f(a) = 0$, por la Proposición 2.3 podemos escribir $f = (X - a)q + r$, con $q, r \in A[X]$ y $r = 0$ o de grado menor que el grado de $X - a$, es decir, $r \in A$. De esa igualdad obtenemos $r = f(a)$, y por tanto $f(a) = 0$ si y sólo si f es divisible por $X - a$. □

Definición. Dado un anillo A, una *raíz de un polinomio* $f \in A[X]$ es un elemento $a \in A$ tal que $f(a) = 0$.

Ejemplo 2.5. Veamos que $\mathbb{Z}[i]$ es un D.E. si tomamos $\delta(a + bi) = N(a + bi) = a^2 + b^2 = ||a+bi||^2$ (ver el Ejercicio 1.18). En efecto, sean $\alpha, \beta \in Z[i]$ con $\beta \neq 0$. Escribimos entonces el número complejo $\frac{\alpha}{\beta}$ como $u + vi$, con $u, v \in \mathbb{Q}$ y claramente podemos escribir $u = p + \epsilon_1$, $v = q + \epsilon_2$, con $p, q \in \mathbb{Z}$ y $|\epsilon_1|, |\epsilon_2| \leq 1/2$. Por tanto $\alpha = \beta(p + qi) + \beta(\epsilon_1 + \epsilon_2 i)$. Obsérvese que $r = \beta(\epsilon_1 + \epsilon_2 i)$ está necesariamente en $\mathbb{Z}[i]$ por ser diferencia de elementos de $\mathbb{Z}[i]$. Además,

$$N(r) = ||r||^2 = ||\beta||^2 ||\epsilon_1 + \epsilon_2 i||^2 = N(\beta)(\epsilon_1^2 + \epsilon_2^2) < N(\beta).$$

Este ejemplo muestra también que la división no es necesariamente única (desde luego, el algoritmo permite hallar distintos cocientes y restos si $\epsilon_1 = 1/2$ o $\epsilon_2 = 1/2$). Por ejemplo, si dividimos $1 + 2i$ entre $1 + i$ tenemos cuatro divisiones distintas:

$$1 + 2i = 2(1 + i) + 1$$

$$1 + 2i = 1(1 + i) + i$$

$$1 + 2i = (2 + i)(1 + i) - i$$

$$1 + 2i = (1 + i)(1 + i) - 1.$$

Ejercicio 2.6. Demostrar, de la misma forma que en el ejemplo anterior, que $\mathbb{Z}[\sqrt{2}]$ y $\mathbb{Z}[\sqrt{-2}]$ son D.E.

Teorema 2.7. *Todo D.E. es un D.I.P.*

Demostración: Sea I un ideal no nulo (si fuera nulo, sería principal generado por 0). Tomamos entonces $b \in I$ no nulo tal que $\delta(b)$ sea mínimo y veamos que b genera I. En efecto, sea a un elemento cualquiera de I. Por ser A D.E., existirán $q, r \in A$ tales que $a = qb + r$, con $r = 0$ o $\delta(r) < \delta(b)$. Como $r = a - qb$, necesariamente está en I, no puede ser $\delta(r) < \delta(b)$, por la elección de b. Por tanto, $r = 0$, luego $a = qb$ y hemos visto por tanto que todo elemento de I es múltiplo de b. □

El resultado anterior indica que ser D.E. es una condición muy fuerte. Por ejemplo, $K[X, Y]$ no puede ser un D.E., ya que no es un D.I.P. (por ejemplo, es un ejercicio sencillo ver que el ideal (X, Y) no es principal). Para estudiar entonces la divisibilidad, intentaremos entonces generalizar el hecho de que cualquier número entero se factoriza en factores primos. Hay dos alternativas (en general no equivalentes, como veremos enseguida) para generalizar la noción de número primo:

Definición. Dado un anillo A, un elemento $a \in A$ que no es ni cero ni unidad diremos que es:

(i) *irreducible* si la única forma de escribir $a = a_1 a_2$ es con a_1 o a_2 unidades;

(ii) *primo* si genera un ideal primo (a), o dicho en el lenguaje de la divisibilidad, si $a|bc$ implica que $a|b$ o $a|c$.

Obsérvese que, por ejemplo en $\mathbb{Z}$, tanto un número primo p como su opuesto $-p$ son elementos primos. En realidad, lo importante es que generen el mismo ideal $(p) = (-p)$. De hecho (ver el Ejercicio 1.10), en un D.I. dos elementos a, b generan el mismo ideal si y sólo si existe una unidad u tal que $a = ub$. A partir de ahora, hablaremos de elementos (primos, irreducibles,...) "salvo multiplicación por una unidad" para indicar que nos da lo mismo trabajar con un elemento a o con su producto por una unidad del anillo.

Ejemplo 2.10. Obsérvese que no es tan inmediato decidir si dos elementos difieren o no por una unidad. Por ejemplo, en $\mathbb{Z}[\sqrt{2}]$ podemos considerar las factorizaciones

$$22 + 19\sqrt{2} = (3 + \sqrt{2})(4 + 5\sqrt{2})$$

$$22 + 19\sqrt{2} = (14 + 9\sqrt{2})(-1 + 2\sqrt{2})$$

que parecen ser distintas. Sin embargo, $14 + 9\sqrt{2} = (4 + 5\sqrt{2})(1 + \sqrt{2})$ y $-1 + 2\sqrt{2} = (3 + \sqrt{2})(-1 + \sqrt{2})$, los elementos $1 + \sqrt{2}, -1 + \sqrt{2}$ son unidades de $\mathbb{Z}[\sqrt{2}]$ (una inversa de la otra), por lo que las segunda factorización se obtiene a partir de la primera cambiando el orden de los factores y multiplicándolos por unidades, con lo que las consideraremos equivalentes. Tenemos además el problema de que hay infinitas unidades en $\mathbb{Z}[\sqrt{2}]$. Por el

Ejercicio 1.18, $a+b\sqrt{2}$ es una unidad si y sólo si $a^2-2b^2=\pm 1$, que es la famosa *ecuación de Pell* de Teoría Elemental de Números, cuya resolución dista mucho de ser trivial. Ni siquiera es fácil caracterizar los elementos irreducibles. En nuestro ejemplo, $3+\sqrt{2}$ es irreducible, ya que $N(3+\sqrt{2})=7$, que es un número primo, luego si $3+\sqrt{2}=\alpha\beta$, entonces, como $N(\alpha)N(\beta)=7$, luego $N(\alpha)$ o $N(\beta)$ son necesariamente ± 1, con lo que α o β es una unidad. Sin embargo, $N(4+5\sqrt{2})=-34$, y como posibles factores no triviales de $4+5\sqrt{2}$ habría que estudiar todos los elementos $a+b\sqrt{2}$ tales que $a^2-2b^2=\pm 2, \pm 17$, lo que no es a priori fácil. En nuestro caso, puede comprobarse que se tiene $4+5\sqrt{2}=\sqrt{2}(5+2\sqrt{2})$, y los factores son ya irreducibles, ya que $N(\sqrt{2})=-2$ y $N(5+2\sqrt{2})=17$ son, salvo el signo, números primos. Vale la pena observar que, sin embargo, en $\mathbb{Z}\sqrt{d}$ con $d<0$, el número de soluciones de cada $a^2-db^2=c$ es finito para cada $c\in\mathbb{Z}$, con lo que este tipo de problemas no se presenta.

Lema 2.8. *Si A es un D.I. entonces cualquier elemento primo es irreducible.*

Demostración: Sea a un elemento primo, y supongamos que podemos escribir $a=bc$. En particular, $a|bc$, con lo que $a|b$ o $a|c$. Sin pérdida de generalidad, podemos suponer $a|b$, es decir, $b=ad$ para algún $d\in A$. Por tanto, $a=adc$, luego (por ser A un D.I.) $dc=1$, con lo que c es una unidad. Esto demuestra que a es irreducible. □

Observación 2.9. La implicación opuesta no es cierta. Si a es irreducible, para ver que es primo tendríamos que ver que $a|bc$ implica que $a|b$ o $a|c$. Sin embargo, de $a|bc$ sólo se deduce que existe un d en A tal que $ad=bc$, pero esto no implica que a divida a b o a c. Teniendo en mente lo que pasa para números enteros, nos haría falta ver que, descomponiendo b y c en factores irreducibles, como $a|bc$, entonces a aparece en alguna de estas dos descomposiciones. En otras palabras, necesitamos una descomposición (única) de elementos en factores irreducibles.

Definición. Un *dominio de factorización única (D.F.U.)* es un anillo A que es un D.I. tal que cada elemento que no es cero ni unidad se puede descomponer de forma única (salvo orden y multiplicación por unidades) como producto finito de elementos irreducibles.

Observación 2.11. Una forma de evitar las unidades en la definición anterior es usar el producto de ideales (se llama *producto de los ideales* $I_1,\dots,I_r$ de un anillo al ideal generado por los productos de la forma $a_1\dots a_r$, con $a_i\in I_i$ para $i=1,\dots,r$). En este lenguaje, un D.F.U. es un D.I. en el que cada ideal principal (a) se escribe de forma única, salvo el orden, como producto de ideales primos principales. Obsérvese por otra parte que en un D.F.U. tiene sentido hablar de mínimo común múltiplo y máximo común divisor de dos o más elementos (siempre definidos salvo multiplicación por constante o definidos como

ideales principales). El modo de calcularlos es como en el caso de los números naturales: factorizando los elementos en factores irreducibles, el m.c.m es el producto de cada uno de los factores elevados al mayor exponente y el M.C.D. es el producto de los factores comunes elevados al menor exponente.

Ejercicio 2.12. Dado un anillo A arbitrario, y dados elementos $a_1, \ldots, a_r \in A$, se dice que a es un máximo común divisor de $a_1, \ldots, a_r$ si a divide a cada a_i y para cada b que divide a cada a_i entonces a divide a b. Si A no es un D.F.U. se pueden dar diversas patologías:

(i) Demostrar que en $\mathbb{Z}[\sqrt{-5}]$ los elementos 6 y $2 + 2\sqrt{-5}$ no tienen máximo común divisor.

(ii) Demostrar que en $\mathbb{Z}[\sqrt{-5}]$ los elementos 3 y $2 + \sqrt{-5}$ tienen máximo común divisor igual a 1, pero el ideal $I = (3, 2 + \sqrt{-5})$ no es el total. Concluir que I no es principal.

Ejercicio 2.13. Demostrar que en un D.F.U. cada elemento irreducible es primo.

Lema 2.14. *Sean A un D.I.P. y $a \in A$ un elemento que no es ni cero ni unidad. Entonces son equivalentes:*

(i) a es primo

(ii) a es irreducible

(iii) El ideal (a) es maximal

Demostración:

$(i) \Rightarrow (ii)$: Inmediato por el Lema 2.8.

$(i) \Rightarrow (ii)$: Supongamos que (a) está contenido en otro ideal, que al ser A un D.I.P. será de la forma (b) para algún $b \in A$. Por tanto, al estar a en (b) existirá $c \in A$ tal que $a = bc$. Como a es irreducible, entonces b o c es una unidad. Si b es una unidad, entonces (b) es el total, mientras que si c es una unidad, entonces la igualdad $a = bc$ implica $(a) = (b)$. En resumen, hemos demostrado que los únicos ideales que contienen a (a) son él mismo y el total, con lo que (a) es maximal.

$(iii) \Rightarrow (i)$: Si (a) es un ideal maximal, en particular es primo, que es lo mismo que decir que el elemento a es primo. □

Teorema 2.15. *Todo D.I.P. es un D.F.U.*

Demostración: Veamos primero que todo elemento que no es cero ni unidad es producto finito de elementos irreducibles. Si no fuera así, existiría un elemento $a_0 \in A$ que no es cero, ni unidad ni expresable como producto finito de elementos irreducibles. En particular a_0 no sería irreducible, luego se podrá escribir $a_0 = a_1 a_1'$, donde ni a_1 ni a_1' son unidades

(y por tanto se tienen contenidos estrictos $(a_0) \subsetneq (a_1)$ y $(a_0) \subsetneq (a_1')$. No puede ocurrir que tanto a_1 como a_1' se puedan escribir como producto finito de elementos irreducibles (porque entonces a_0 también sería producto finito de elementos irreducibles). Sin pérdida de generalidad, podemos suponer que a_1 no es producto finito de elementos irreducibles. Repitiendo el proceso, encontramos una cadena $(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$. La unión $I = (a_0) \cup (a_1) \cup (a_2) \cup \ldots$ es un ideal de A, luego está generada por un elemento a. Como a está en I, existirá in n tal que $a \in (a_n)$, es decir, $a = ba_n$ para algún $b \in A$. Por otra parte, a_{n+1} está en I, por lo que se podrá escribir $a_{n+1} = ca$ para algún $c \in A$. Por tanto, $a_{n+1} = cba_n$, lo que demuestra que (a_{n+1}) está contenido en (a_n), con lo que ambos ideales serían iguales, lo que es absurdo por construcción. Esto demuestra la descomposición de elementos en producto finito de elementos irreducibles.

Veamos finalmente que tal descomposición es única. Sean $a = b_1 \ldots b_n = c_1 \ldots c_m$, con $b_1, \ldots, b_n, c_1, c_m$ irreducibles (y por tanto primos, por el lema anterior), dos descomposiciones de a. Como b_1 divide a $c_1 \ldots c_m$, divide a algún c_j, que podemos suponer reordenando los factores que sea c_1. Por tanto, $c_1 = u_1 b_1$, y como c_1 es irreducible u_1 es necesariamente una unidad (ya que b_1 no lo es por ser un elemento irreducible). Podemos escribir entonces $b_2 \ldots b_n = u_1 c_2 \ldots c_m$, y reiterando lo anterior para $b_2, \ldots, b_n$, se llega a que, salvo unidades, la descomposición es única. □

Obsérvese que la parte final de la demostración anterior en realidad muestra que, si A es un D.I. en que todo elemento es producto de irreducibles, entonces A es un D.F.U. si y sólo si todo elemento irreducible de A es primo (ver el Ejercicio 2.13).

Ejemplo 2.16. Veamos una aplicación de todo lo visto hasta ahora a teoría de números. En concreto, veamos cuándo un número $n \in \mathbb{N}$ se puede escribir como suma de dos cuadrados. Para ello, lo descomponemos en producto de números primos. De hecho, los únicos primos relevantes serán los que aparezcan con potencia impar ya que, agrupando potencias pares de primos, podemos escribir $n = m^2 p_1 \ldots p_r$, con $p_1, \ldots, p_r$ primos distintos (precisamente los que aparecen con exponente impar). Por tanto, la pregunta es cuándo $p_1 \ldots p_r$ es una suma de cuadrados (ya que en tal caso n lo sería también).

Una primera condición es bastante fácil. Supongamos que un primo p divide a una suma $a^2 + b^2$ pero p^2 no la divide. Es claro entonces que p no puede dividir ni a a ni a b. Tomando clases en $\mathbb{Z}_p$ (que denotaremos con una barra), tendremos que $(\frac{\bar{a}}{\bar{b}})^2 = -\bar{1}$. Si $p \neq 2$ (si $p = 2$, claramente podemos escribir $2 = 1^2 + 1^2$, con lo que no hace falta estudiar este caso) tenemos entonces que $(\frac{\bar{a}}{\bar{b}})^4 = \bar{1}$ y $(\frac{\bar{a}}{\bar{b}})^2 \neq \bar{1}$, por lo que $\frac{\bar{a}}{\bar{b}}$ tiene orden 4 en el grupo $\mathbb{Z}_p \setminus \{\bar{0}\}$. Como este grupo tiene orden $p - 1$, se sigue que 4 es un divisor de $p - 1$, es decir que $p \equiv 1 (\text{mod } 4)$.

Recíprocamente, si $p \equiv 1 (\text{mod } 4)$, entonces 4 es un divisor del orden del grupo $\mathbb{Z}_p \setminus$

$\{\bar{0}\}$. Dicho grupo es cíclico (es un resultado de Álgebra Básica, que de todas formas redemostraremos en el Corolario 3.3), por lo que tiene un elemento $\bar{c}$ de orden 4. Esto quiere decir que $\bar{c}^4 = \bar{1}$ y $\bar{c}^2 \neq \bar{1}$. Como $\bar{0} = \bar{c}^4 - \bar{1} = (\bar{c}^2+1)(\bar{c}^2-1)$, se sigue que $\bar{c}^2 = -\bar{1}$, luego $p|c^2+1$. Escrito en $\mathbb{Z}[i]$ (que por los Teoremas 2.7 y 2.15 se tiene que es un D.F.U.), tenemos entonces $p|(c+i)(c-i)$. Como evidentemente p no divide ni a $c+i$ ni a $c-i$, se sigue que p no es primo en $\mathbb{Z}[i]$, luego tampoco es irreducible. Sea $a+bi$ un divisor no trivial de p. Como $N(p) = p^2$ y $N(a+bi)$ tiene que ser un divisor no trivial de $N(p)$, se sigue que $N(a+bi) = p$, es decir, $p = a^2+b^2$.

Para terminar de resolver el problema, observamos que el producto de dos sumas de cuadrados es una suma de cuadrados, ya que se tiene $(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2$. Por tanto, *un número natural es suma de cuadrados si y sólo si sus factores primos p con exponente impar son o bien $p = 2$ o bien $p \equiv 1 (\mathrm{mod}\ 4)$.*

Vamos a centrarnos ahora en la factorialidad de los anillos que más nos van a interesar: los anillos de polinomios en varias indeterminadas o con coeficientes en un anillo. La idea es bien simple: podemos ver todos estos anillos como anillos de polinomios en una indeterminada y con coeficientes en un anillo A (por ejemplo, $k[X_1,\ldots,X_n]$ lo podemos ver como el anillo de polinomios en la indeterminada X_n y coeficientes en el $A = k[X_1,\ldots,X_{n-1}]$, lo que nos permitirá un estudio por recurrencia). Entonces, consideraremos los elementos de $A[X]$ como elementos de $K[X]$, donde K es el cuerpo de fracciones de A (suponiendo que A sea un D.I.), y ya podemos usar que $K[X]$ es un D.F.U. El problema que tendremos que resolver es que la factorización en $K[X]$ tendrá los ceoficientes en K, y tendremos que saber quitar los denominadores para pasar a una factorización en $A[X]$.

Empezamos con la siguiente construcción, que usaremos constantementem y que lo que hace es prescindir de factores comunes redundantes: Dado un polinomio $f = a_0 + a_1X + \ldots + a_nX^n \in A[X]$, donde A es un D.F.U., podemos descomponer cada a_i en factores irreducibles y tomar a su máximo común divisor. Es decir, podemos escribir cada a_i como $a_i = aa_i'$, con $a_0',\ldots,a_n' \in A$ sin factores comunes. Si llamamos $f_0 = a_0' + a_1'X + \ldots + a_n'X^n$, entonces tendremos $f = af_0$.

Definición. Se llama *polinomio primitivo* a un polinomio $f = a_0 + a_1X + \ldots + a_nX^n \in A[X]$ con coeficientes en un D.F.U. tal que $a_0,\ldots,a_n$ no tienen factores comunes.

Theorem 2.17 (Lema de Gauss)**.** *Sea A un D.F.U. y $f,g \in A[X]$ un par de polinomios. Entonces f y g son primitivos si y sólo si fg es primitivo.*

Demostración: Es claro que si fg es primitivo entonces lo son f y g, ya que si, por ejemplo, los coeficientes de f tuvieran un factor común (no unidad) $a \in A$, entonces a sería también un factor común de fg, contra la hipótesis de que es primitivo.

Recíprocamente, supongamos que f y g son primitivos. Si fg no fuera primitivo, existiría algun factor irreducible $p \in A$ común a todos sus coeficientes. Entonces, considerando el ideal $I = (p)$ de A (que es primo de A por el Ejercicio 2.13), se tendría que $fg \in I[X]$. Por el Ejemplo 1.23, $I[X]$ es un ideal primo de $A[X]$, por lo que f o g deberían estar en I. Pero esto es lo mismo que decir que p dividiría a todos los coeficientes de f o de g, con lo que no serían primitivos, en contra de nuestra hipótesis. □

El siguiente es el resultado que andábamos buscando, que relaciona la irreducibilidad de un polinomio con coeficientes en un D.F.U. con la del polinomio visto con ceoficientes en el cuerpo de fracciones.

Proposición 2.18. *Sea A un D.F.U. con cuerpo de fracciones K y sea $f \in A[X]$ un polinomio. Entonces:*

(i) Si f es primitivo y $f = gh$ con $g, h \in K[X]$, entonces existen $r \in K$ y $g_0, h_0 \in A[X]$ polinomios primitivos tales que $g = rg_0, h = \frac{1}{r}h_0$ y por tanto $f = g_0h_0$.

(ii) f es irreducible como polinomio en $A[X]$ si y sólo si o bien es un elemento irreducible de A o bien es de grado positivo, primitivo e irreducible como polinomio en $K[X]$.

Demostración: Para demostrar (i), observamos primero que, tomando común denominador en los respectivos coeficientes, tanto g como h se pueden escribir de la forma $g = \frac{g_1}{b_1}$ y $h = \frac{h_1}{c_1}$, con $b_1, c_1 \in A$ y $g_1, h_1 \in A[X]$. Escribimos ahora $g_1 = b_0g_0$ y $h_1 = c_0h_0$, con $b_0, c_0 \in A$ y $g_0, h_0 \in A[X]$ polinomios primitivos. Tendremos por tanto $f = gh = \frac{b_0c_0}{b_1c_1}g_0h_0$ o equivalentemente, $b_1c_1f = b_0c_0g_0h_0$. De aquí se obtiene que b_0c_0 divide a todos los coeficientes de b_1c_1f. Como los coeficientes de f no tienen ningún factor común (porque por hipótesis f es primitivo), se deduce que b_0c_0 divide a b_1c_1. De modo simétrico, como g_0h_0 es primitivo (por el lema de Gauss) se sigue que b_1c_1 también divide a b_0c_0. Por tanto (ver el Ejercicio 1.10), existe una unidad $u \in A$ tal que $b_0c_0 = ub_1c_1$. Escribimos por tanto $f = (ug_0)h_0$, y tenemos que ug_0, h_0 son los polinomios primitivos buscados (y $r = \frac{b_0}{ub_1} = \frac{c_1}{c_0}$).

Para demostrar (ii), observamos primero que si f es irreducible como polinomio en $A[X]$, entonces es claro que, si es constante, debe ser un elemento irreducible de A, y si tiene grado positivo, debe ser primitivo. Veamos que, en este último caso, (i) implica que f es irreducible como polinomio en $K[X]$. En efecto, si f se descompone de forma no trivial en $K[X]$, necesariamente lo hace como producto de polinomios de grado positivo (ya que los polinomios de grado cero son las constantes no nulas, que son las unidades, según el Ejercicio 1.14(iii)). Pero (i) implica que cualquier descomposición de f en $K[X]$ induce una descomposición en $A[X]$ con factores del mismo grado, lo que implicaría que f sería reducible en $A[X]$.

Recíprocamente, cualquier elemento irreducible de A es un elemento irreducible en $A[X]$. Supongamos entonces que f es de grado positivo, primitivo e irreducible como polinomio en $K[X]$, y consideremos una posible descomposición $f = gh$ con $g, h \in A[X]$. Como g, h también están en $K[X]$, se tendrá que uno de ellos, por ejemplo g, es una unidad en $K[X]$, es decir una constante no nula. Por tanto, g sería un elemento de A, pero como $f = gh$ es primitivo, necesariamente g es una unidad en A. □

Teorema 2.19. *Si A es un D.F.U., entonces $A[X]$ también es un D.F.U.*

Demostración: Dado un polinomio $f \in A[X]$, lo escribimos como af_0, con $a \in A$ y $f_0 \in A[X]$ un polinomio primitivo. Por una parte, si $a = p_1 \dots p_s$ es una descomposición de a en factores irreducibles en A, cada p_i es también irreducible en $A[X]$ (por la Proposición 2.18). Basta por tanto encontrar una descomposición de f_0 para encontrar una de f.

Sea K el cuerpo de fracciones de A. Como $K[X]$ es un D.F.U. podemos escribir $f_0 = f_1 \dots f_r$, con $f_1, \dots, f_r$ polinomios irreducibles de grado positivo en $K[X]$. Por la Proposición 2.18, obtenemos una factorización $f_0 = f_1' \dots f_r'$ con $f_1', \dots, f_r'$ polinomios irreducibles en $A[X]$.

Basta ver que las factorizaciones en $A[X]$ son únicas. Supongamos que tenemos dos factorizaciones distintas $p_1 \dots p_s f_1 \dots f_r = p_1' \dots p_t' f_1' \dots f_l'$ donde $p_1, \dots, p_s, p_1', \dots, p_t'$ son los factores de grado cero (es decir, los elementos de A, que serán irreducibles) y $f_1, \dots, f_r, f_1', \dots, f_l'$ los factores de grado positivo (luego necesariamente polinomios primitivos, e irreducibles tanto en $A[X]$ como en $K[X]$).

Entonces es claro que tanto $f_1, \dots, f_r$ como $f_1', \dots, f_l'$ son los factores irreducibles de f en $K[X]$. Por tanto, los $f_1, \dots, f_r$ coinciden con los $f_1', \dots, f_l'$ salvo multiplicación por una constante de K. Supongamos por ejemplo que cada $f_i = \frac{a_i}{b_i} f_i'$ con $a_i, b_i \in A$ sin factores comunes. Como f_i, f_i' son primitivos, se deduce que a_i, b_i son unidades en A, y en particular $f_1 \dots f_r = u f_1' \dots f_l'$, donde u es una unidad en A. Por tanto, $p_1 \dots p_s = u p_1' \dots p_t'$, y por ser A un D.F.U., se sigue que los $p_1, \dots, p_s$ coinciden con los $p_1', \dots, p_t'$ salvo multiplicación por una unidad de A. □

Corolario 2.20. *Si K es un cuerpo, $K[X_1, \dots, X_n]$ es un D.F.U.*

Demostración: Basta usar inducción sobre n. Si $n = 1$, entonces $K[X_1]$ es un D.I.P., luego un D.F.U. Si $n > 1$, entonces $K[X_1, \dots, X_{n-1}]$ es un D.F.U. por hipótesis de inducción, luego por el Teorema 2.19 también lo es $(K[X_1, \dots, X_{n-1}])[X_n] = K[X_1, \dots, X_n]$. □

Ahora que sabemos que los anillo de polinomios que nos interesarán son D.F.U, veamos criterios para saber si un polinomio es irreducible.

Teorema 2.21 (Criterio de Eisenstein)**.** *Sea A un D.F.U. con cuerpo de fracciones K y sea $f = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + a_nX^n \in A[X]$. Si existe un elemento irreducible $p \in A$ tal que $p|a_0, a_1, \ldots, a_{n-1}$, $p \not| a_n$ y $p^2 \not| a_0$, entonces f es irreducible como polinomio en $K[X]$. Por tanto, si f es además primitivo, es también irreducible como polinomio en $A[X]$.*

Demostración: Basta demostrar el criterio cuando f es primitivo (escribiendo $f = af_0$, con $a \in A$ y f_0 primitivo, como claramente $p \not| a$ (ya que $p \not| a_n$) se sigue que f_0 verifica las hipótesis del criterio, luego sería irreducible en $K[X]$, y por tanto también en $A[X]$). Supongamos entonces que f es primitivo y reducible en $K[X]$ y busquemos un absurdo. Como f es primitivo, será reducible también en $A[X]$, se podrá escribir $f = gh$, con $g = b_0 + b_1X + \ldots, \quad h = c_0 + c_1X + \ldots \in A[X]$ y ambos de grado positivo. Dado que $a_0 = b_0c_0$ es divisible por p pero no por p^2, ese sigue que por ejemplo b_0 no es divisible por p, mientras que c_0 lo es. Sea c_r el primer coeficiente de h que no es divisible por p (que existe, ya que en caso contrario todos los coeficientes de f serían divisibles por p). Se tiene entonces que $a_r = b_0c_r + b_1c_{r-1} + \ldots + b_rc_0$ es, por una parte divisible por p (ya que lo es a_r por hipótesis, puesto que claramente $r \leq \partial h < \partial f = n$), mientras que por otra parte no lo es, ya que p divide a $c_{r-1}, \ldots, c_0$ pero no a b_0c_r. Esto proporciona el absurdo que buscábamos. □

Ejemplo 2.22. Sea $\Phi_p = \frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Z}[X]$. Claramente, $\Phi_p(X)$ será irreducible si y sólo si lo es $\Phi_p(X+1)$. Como

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

y $p|\binom{p}{i}$ para $i = 1, \ldots, p-1$, el criterio de Eisenstein implica que $\Phi_p(X)$ es irreducible.

Ejercicio 2.23. Sea K un cuerpo y $K(t)$ el cuerpo de fracciones del anillo de polinomios con coeficientes en K en la indeterminada t. Demostrar que, para cada $n \in \mathbb{N}$, el polinomio $X^n - t$ es irreducible en $K(t)[X]$.

Observación 2.24. Si A es un D.I. y $f \in A[X]$ es un polinomio mónico, entonces cualquier factor de f es mónico (salvo multiplicación por una unidad). En efecto, si $f = gh$ con $g = b_0 + b_1X + \ldots + b_rX^r$ y $h = c_0 + c_1X + \ldots + c_sX^s$ (con $b_r, c_s \neq 0$), entonces $b_rc_s = 1$ (como A es D.I., $b_rc_s \neq 0$, luego es el coeficiente del término de mayor grado de f); basta entonces escribir $f = (c_sg)(b_rh)$, donde ahora los dos factores son mónicos. Esto implica que cualquier factorización no trivial de f (es decir, en que los factores no sean unidades) es necesariamente en factores de grado positivo. Por supuesto, si el coeficiente del término

de mayor grado de f es una unidad (por ejemplo si A es un cuerpo), multiplicando por el inverso de esta unidad obtendríamos un polinomio mónico y valdría lo anterior.

Observación 2.25. Por la observación anterior y la regla de Ruffini (Corolario 2.4), un polinomio mónico de grado dos o tres en $A[X]$ (donde A es un D.I.) será irreducible si y sólo si no tiene raíces en A (si fuera reducible, tendría algún factor mónico de grado uno, y por tanto una raíz. El Ejemplo 2.27 nos dará también otro método para estudiar la irreducibilidad de polinomios (esta vez de grado arbitrario) a partir de sus raíces.

Observación 2.26. Si A es un D.I. y un polinomio mónico $f \in A[X]$ fuera reducible, por la Observación 2.24 se descompone como $f = gh$, con g, h mónicos de grado positivo. Por tanto, para cualquier ideal primo $I \subset A$, la reducción de f módulo I (ver el Ejemplo 1.23) también descompondrá en factores de grado positivo, luego no sería irreducible. Podemos usar esto para demostrar la irreducibilidad de polinomios. Por ejemplo, el polinomio $X^3 - X + 1 \in \mathbb{Z}[X]$ es irreducible, ya que el polinomio correspondiente $X^3 - X + 1 \in \mathbb{Z}_3[X]$ es irreducible por no tener raíces (de hecho, cualquier elemento de $\mathbb{Z}_3$ es raíz de $X^3 - X$). La hipótesis de que f sea mónico es necesaria para que se conserve el grado de los polinomios. Por ejemplo, el polinomio $(3X + 1)X \in \mathbb{Z}[X]$ es obviamente reducible, pero su reducción módulo 3 es el polinomio irreducible $X \in \mathbb{Z}_3[X]$.

Ejemplo 2.27. Un método bastante útil para ver si un polinomio con coeficientes en un cuerpo es irreducible es encontrar todas sus raíces en un cuerpo más grande (ya veremos en la sección 4 qué quiere decir esto con precisión) y ver si se pueden agrupar. Ilustremos esto con un ejemplo. Consideremos $f = X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$. Sus raíces son $\pm\sqrt{2} \pm \sqrt{3}$, así que en $\mathbb{R}[X]$ se puede factorizar como

$$f = (X - \sqrt{2} - \sqrt{3})(X - \sqrt{2} + \sqrt{3})(X + \sqrt{2} - \sqrt{3})(X + \sqrt{2} + \sqrt{3}).$$

Como f no tiene raíces en $\mathbb{Q}$, si factoriza en $\mathbb{Q}[X]$ sólo puede ser como producto $f = gh$, con $g, h \in \mathbb{Q}[X]$ de grado dos, que claramente se pueden tomar mónicos. Pero si factorizamos g y h en $\mathbb{R}[X]$, por la unicidad de la factorización, tanto g como h tienen que ser el producto de dos de los cuatro factores anteriores. Pero eso es imposible, porque agrupando de dos en dos los factores, las posibles factorizaciones son:

$$f = (X^2 - 2\sqrt{2}X - 1)(X^2 + 2\sqrt{2}X - 1)$$

$$f = (X^2 - 2\sqrt{3}X + 1)(X^2 + 2\sqrt{3}X + 1)$$

$$f = (X^2 - 2\sqrt{6} - 5)(X^2 + 2\sqrt{6} - 5)$$

y ninguna de ellas es una factorización en $\mathbb{Q}[X]$. Esto demuestra que f es irreducible en $\mathbb{Q}[X]$, y por tanto también en $\mathbb{Z}[X]$. Este ejemplo es especialmente interesante porque,

considerando $f \in \mathbb{Z}[X]$ para cada primo p, el polinomio $\bar{f} \in \mathbb{Z}_p[X]$ obtenido tomando cada coeficiente módulo p es en cambio reducible (lo que muestra que el método explicado en la Observación 2.26 no es un si y sólo si, ni siquiera tomando todos los ideales maximales I). En efecto, si 2 es un cuadrado en $\mathbb{Z}_p$, la primera de las tres factorizaciones anteriores da una factorización en $\mathbb{Z}_p$; si es 3 un cuadrado en $\mathbb{Z}_p$, la segunda es la factorización buscada, mientras que si 6 es un cuadrado vale la tercera factorización. Un resultado básico de Teoría Elemental de Números implica que, para cada primo p, si 2 y 3 no son cuadrados en $\mathbb{Z}_p$, entonces 6 lo es (usando símbolos de Legendre, $\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$). De todas formas, este hecho es fácil verlo directamente (supondremos $p \neq 2, 3$, porque para $p = 2, 3$ es todo trivial):

En efecto, el conjunto de cuadrados módulo p distintos de cero es el conjunto Σ imagen de la aplicación $\varphi : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ dada por $\varphi(\alpha) = \alpha^2$. Como $\alpha^2 = \beta^2$ si y sólo si $\alpha = \pm\beta$, para $p \neq 2$ cada elemento de Σ es imagen por φ de exactamente dos elementos de $\mathbb{Z}_p^*$, luego Σ tiene cardinal $\frac{p-1}{2}$, la mitad del cardinal de $\mathbb{Z}_p^*$. Por tanto el conjunto Σ' de los elementos de $\mathbb{Z}_p^*$ que no son cuadrados perfectos también tiene cardinal $\frac{p-1}{2}$. Si suponemos que la clase de 2 no es un cuadrado perfecto, es claro que $\bar{2}\alpha^2$ tampoco es un cuadrado perfecto para cualquier $\alpha^2 \in \Sigma$ (ya que si $\bar{2}\alpha^2 = \beta^2$, entonces $2 = (\frac{\beta}{\alpha})^2$, en contra de la hipótesis). Por tanto, la biyección $\psi : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ dada por $\psi(\alpha) = \bar{2}\alpha$ manda Σ dentro de Σ', y por tener ambas el mismo cardinal se tiene que $\psi(\Sigma) = \Sigma'$. Como $\mathbb{Z}_p^*$ es la unión disjunta de Σ y Σ', se tendrá también que $\psi(\Sigma') = \Sigma$. En particular, $\psi(\bar{3}) = \bar{6}$ es un cuadrado perfecto. Otra demostración independiente de este hecho se verá en el Ejercicio 3.4.

Terminamos la sección dando un criterio para buscar raíces de un polinomio con coeficientes en un D.F.U.

Proposición 2.28. *Sea A un D.F.U. y sea K su cuerpo de fracciones. Supongamos que un polinomio $f = a_0 + a_1X + \ldots + a_nX^n \in A[X]$ tiene una raíz $\frac{p}{q} \in K$, donde $p, q \in A$ son primos entre sí. Entonces $p|a_0$ y $q|a_n$.*

Demostración: Como $\frac{p}{q}$ es una raíz de f, tenemos la siguiente igualdad en K:

$$a_0 + a_1\frac{p}{q} + \ldots + a_n(\frac{p}{q})^n = 0.$$

Multiplicando por q^n tenemos la siguiente igualdad en A:

$$a_0q^n + a_1pq^{n-1} + \ldots + a_{n-1}p^{n-1}q + a_np^n = 0.$$

Como p divide a $a_1pq^{n-1} + \ldots + a_{n-1}p^{n-1}q + a_np^n$, se deduce de esa igualdad que también divide a a_0q^n; pero como p y q no tienen factores comunes, se concluye que p divide a a_0. Análogamente, q divide a $a_0q^n + a_1pq^{n-1} + \ldots + a_{n-1}p^{n-1}q$, luego se deduce de la misma igualdad que también divide a a_np^n; y, como antes, esto implica que q divide a a_n. □

3. Raíces de polinomios

En esta sección vamos a estudiar el comportamiento de las raíces de polinomios en una indeterminada con coeficientes en un anillo. En general, daremos por descontado que las raíces se encuentran en el anillo, dejando para la siguiente sección el ver que todo D.I. se puede ampliar hasta un cuerpo en el que vivan todas las raíces de cualquier polinomio fijado de antemano.

Empezamos con la siguiente definición, motivada por el Corolario 2.4:

Definición. Se llama *multiplicidad de una raíz a de un polinomio $f \in A[X]$* al máximo exponente r tal que $(X-a)^r$ divide a f, es decir, $f = (X-a)^r g$ con $g(a) \neq 0$. Si la multiplicidad de a es al menos dos, se dice que a es una *raíz múltiple* de f.

Lema 3.1. *Si A es un D.F.U. o un cuerpo, todo polinomio no nulo de $A[X]$ tiene a lo más tantas raíces (contadas cada una con su multiplicidad) como su grado.*

Demostración: Sea $f \in A[X]$ no nulo y sean $a_1, \ldots, a_m$ sus raíces distintas, con multiplicidades respectivas $r_1, \ldots, r_m$. Por definición de multiplicidad, cada $(X-a_i)^{r_i}$ divide a f. Como $A[X]$ es un D.F.U. (por el Teorema 2.19) y $X-a_i$ y $X-a_j$ son irreducibles (ya que $A[X]/(X-a_i)$ es isomorfo a A, que es un D.I.) y primos entre sí si $i \neq j$ (por el Corolario 2.4), se tiene que $(X-a_1)^{r_1} \ldots (X-a_m)^{r_m}$ divide a f, por lo que $r_1 + \ldots + r_m$ es como mucho el grado de f. □

Ejemplo 3.2. Si A es un anillo arbitrario, el resultado anterior no es cierto. Por ejemplo, el polinomio $2X \in \mathbb{Z}_4$ tiene dos raíces (las clases de 0 y 2), a pesar de tener grado uno. Obsérvese que, de todas formas, vale la regla de Ruffini (Corolario 2.4) ya que $2X = 2(X-2)$.

Corolario 3.3. *Sea K un cuerpo y sea $G < K \setminus \{0\}$ un subgrupo finito del grupo multiplicativo correspondiente. Entonces G es cíclico. En particular, si K es finito, el grupo $K \setminus \{0\}$ es cíclico.*

Demostración: Por el teorema de estructura de grupos abeliano finitos, G es isomorfo a un producto $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$, con $n_1 | n_2 | \ldots | n_r$. En particular, $|G| = n_1 \ldots n_r$ y cualquier elemento de G tiene orden un divisor de n_r. Esto último quiere decir que el polinomio $X^{n_r} - 1 \in K[X]$ se anula para todos los elementos de G, es decir, tiene $n_1 \ldots n_r$ raíces distintas. Por el Lema 3.1, $n_1 \ldots n_r \leq n_r$, y por tanto $r = 1$ y G es isomorfo a $\mathbb{Z}_{n_1}$, por lo que es cíclico. □

Ejercicio 3.4. Sea p un número primo impar.

(i) Demostrar que para cada $a \in \mathbb{Z}$ coprimo con p, se tiene que $a^{\frac{p-1}{2}}$ es congruente con 1 o -1 módulo p y que es 1 si y sólo si a es un cuadrado en $\mathbb{Z}_p$ [Indicación: escribir la clase de los elementos de $\mathbb{Z}_p$ como potencias de un generador del grupo cíclico $\mathbb{Z}_p \setminus \{0\}$].

(ii) Concluir que, si a_1, a_2 no son cuadrados módulo p, entonces lo es $a_1 a_2$.

Definición. Dado un anillo A, de llama *derivada del polinomio* $f = a_0 + a_1 X + \ldots + a_n X^n$ al polinomio $f' = a_1 + \ldots + n a_n X^{n-1}$. Al coincidir la definición con la del análisis, es fácil ver que se verifican las reglas usuales $(f+g)' = f' + g'$ y $(fg)' = f'g + fg'$.

Proposición 3.5. *Sean A un D.I, $f \in A[X]$ y a una raíz de f. Entonces a es una raíz múltiple de f si y sólo si $f'(a) = 0$.*

Demostración: Como a es una raíz de f, por el Corolario 2.4 podemos escribir $f = (X-a)g$. Por definición, a es una raíz múltiple de f si y sólo si $(X-a)^2$ divide a $f = (X-a)g$. Como A es D.I. (y por tanto también lo es $A[X]$ por el Ejercicio 1.14(iii)), se tiene que entonces $(X-a)^2$ divide a $f = (X-a)g$ si y sólo si $X - a$ divide a g. Aplicando de nuevo el Corolario 2.4 tendremos que a es una raíz múltiple de f si y sólo si $g(a) = 0$. Derivando la igualdad $f = (X-a)g$, tenemos $f' = (X-a)g' + g$, luego $f'(a) = g(a)$, lo que demuestra el resultado. □

Dado que debemos reconocer cuándo f y f' tienen raíces comunes, damos el siguiente resultado que dice al menos cuándo dos polinomios tienen factores comunes. La idea es que, en la siguiente sección, construiremos (al menos para los cuerpos) un cuerpo en el que un polinomio dado tenga todas sus raíces (y por tanto, compartir factores quiere decir compartir raíces).

Teorema 3.6. *Sea A un D.F.U. o un cuerpo y sean $f = a_0 + a_1 X + \ldots + a_n X^n$, $g = b_0 + b_1 X + \ldots + b_m X^m$ dos polinomios en $A[X]$ de grados respectivos n y m (es decir, $a_n, b_m \neq 0$). Entonces f y g tienen un factor común de grado positivo si y sólo si $R(f,g) = 0$, donde*

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \ldots & a_n & 0 & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & a_{n-1} & a_n & 0 & \ldots & 0 \\ & & \ddots & & & & & \\ 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_{n-1} & a_n \\ b_0 & b_1 & \ldots & b_{m-1} & b_m & 0 & \ldots & 0 \\ 0 & b_0 & \ldots & b_{m-2} & b_{m-1} & b_m & 0\ldots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \ldots & 0 & b_0 & b_1 & \ldots & b_{m-1} & b_m \end{vmatrix} \begin{matrix} \\ \\ \\ \left.\begin{matrix} \\ \\ \end{matrix}\right\} m \text{ filas} \\ \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} n \text{ filas} \\ \\ \end{matrix} \tag{3.7}$$

Demostración: Como $A[X]$ es un D.F.U., que en la descomposición de f y g haya un factor común de grado positivo es equivalente a decir que existen polinomios no nulos $p, q \in A[X]$

de grados respectivamente menores a m y n tales que $fp = gq$. Dicho de otra forma, existen $c_0, c_1, \ldots, c_{m-1}, d_0, d_1, \ldots, d_{n-1} \in A$ no todos nulos tales que

$$(a_0 + a_1X + \ldots + a_nX^n)(c_0 + c_1X + \ldots + c_{m-1}X^{m-1})$$

$$= (b_0 + b_1X + \ldots + b_mX^m)(d_0 + d_1X + \ldots + d_{n-1}X^{n-1}).$$

Igualando coeficientes tenemos (suponiendo por ejemplo $n \geq m$):

$$\begin{array}{cccccccccc}
a_0c_0 & & & & & -b_0d_0 & & & & = 0 \\
a_1c_0 & +a_0c_1 & & & & -b_1d_0 & -b_0d_1 & & & = 0 \\
\vdots & & & & & & & & & \\
a_{m-1}c_0 & +a_{m-2}c_1 & \ldots & +a_0c_{m-1} & & -b_{m-1}d_0 & -b_{m-2}d_1 & \ldots & & = 0 \\
a_mc_0 & +a_{m-1}c_1 & \ldots & +a_1c_{m-1} & & -b_md_0 & -b_{m-1}d_1 & \ldots & & = 0 \\
a_{m+1}c_0 & +a_mc_1 & \ldots & +a_2c_{m-1} & & & -b_md_1 & \ldots & & = 0 \\
\vdots & & & & & & & & & \\
a_{n-1}c_0 & +a_{n-2}c_1 & \ldots & +a_{n-m}c_{m-1} & & & & \ldots & -b_0d_{n-1} & = 0 \\
a_nc_0 & +a_{n-1}c_1 & \ldots & +a_{n-m+1}c_{m-1} & & & & \ldots & -b_1d_{n-1} & = 0 \\
 & +a_nc_1 & \ldots & +a_{n-m+2}c_{m-1} & & & & \ldots & -b_2d_{n-1} & = 0 \\
\vdots & & & & & & & & & \\
 & & & a_nc_{m-1} & & & & & -b_md_{n-1} & = 0
\end{array}$$

Podemos ver estas igualdades como un sistema homogéneo de $n+m$ ecuaciones en las $n+m$ incógnitas $c_0, c_1, \ldots, c_{m-1}, d_0, d_1, \ldots, d_{n-1}$ que tiene solución no trivial en A^{n+m}. Si K es el cuerpo de fracciones de A, es claro que el sistema tiene solución no trivial en A^{n+m} si y sólo si la tiene en K^{n+m}, luego la condición necesaria y suficiente es que la matriz de coeficientes del sistema tenga determinante cero. Pero dicha matriz de coeficientes, cambiando de signo las últimas columnas y transponiendo, es exactamente la matriz cuyo determinante es $R(f, g)$. Por tanto, f y g tienen un factor común de grado positivo si y sólo si $R(f, g) = 0$. □

Definición. Dado un anillo A, se llama *resultante de los polinomios* $f, g \in A[X]$ al elemento $R(f, g) \in A$ definido en el teorema anterior por la expresión (3.7).

Ejemplo 3.8. En el caso de un polinomio $f(X) = aX^2 + bX + c$ de grado dos, se reobtiene enseguida el resultado de cuándo tiene una raíz múltiple. En efecto, podemos aplicar la Proposición 3.5, y tendremos $f' = 2aX + b$, que tendrá su única raíz común con f si y sólo si se anula

$$R(f, f') = \begin{vmatrix} c & b & a \\ b & 2a & 0 \\ 0 & b & 2a \end{vmatrix} = 4a^2c - ab = a(4ac - b^2)$$

de donde obtenemos el resultado conocido de que f tiene una raíz doble si y sólo si $b^2-4ac=0$. En realidad, en este caso se podía evitar la resultante para ver si f y f' comparten raíz, ya que f' tiene una sola raíz, precisamente $X=\frac{-b}{2a}$. Por tanto, f y f' comparten raíz si y sólo si $f(\frac{-b}{2a})=0$, es decir

$$0=a\big(\frac{-b}{2a}\big)^2+b\frac{-b}{2a}+c=\frac{-b^2+4ac}{4a}$$

Queremos ahora generalizar las ideas del ejemplo anterior, y expresar la resultante en términos de las raíces del polinomio. Por comodidad, trabajaremos sólo con polinomios mónicos, dejando al lector los cambios oportunos para polinomios arbitrarios. Empezamos con la siguiente observación elemental:

Lema 3.9. *Sea A un D.F.U. o un cuerpo y sea $f=a_0+a_1X+\ldots+a_{n-1}X^{n-1}+X^n\in A[X]$ un polinomio mónico con n raíces $\alpha_1,\ldots,\alpha_n\in A$ (cada una repetida tantas veces como su multiplicidad). Entonces*

$$a_0=(-1)^n\alpha_1\ldots\alpha_n$$

$$a_1=(-1)^{n-1}(\alpha_1\alpha_2\ldots\alpha_{n-1}+\ldots+\alpha_2\ldots\alpha_n)$$
$$\vdots$$
$$a_{n-1}=-(\alpha_1+\alpha_2+\ldots+\alpha_n)$$

es decir, para $j=0,\ldots,n-1$ se tiene $a_j=(-1)^{n-j}e_{n-j}(\alpha_1,\ldots,\alpha_n)$, donde

$$e_k:=\sum_{1\le i_1<\ldots<i_k\le n}X_{i_1}\ldots X_{i_k}\in A[X_1,\ldots,X_n].$$

Demostración: Es una consecuencia inmediata de que, por el Corolario 2.4, f se puede escribir como $f=(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$. □

Definición. Llamaremos *polinomio simétrico elemental* k-ésimo ($k=1,\ldots,n$) en las variables $X_1,\ldots,X_n$ al polinomio

$$e_k:=\sum_{1\le i_1<\ldots<i_k\le n}X_{i_1}\ldots X_{i_k}.$$

Proposición 3.10. *Sea A un D.F.U., sea $A'=A[X_1',\ldots,X_n',X_1'',\ldots,X_m'']$ y sean los polinomios $f=(X-X_1')\ldots(X-X_n')$ y $g=(X-X_1'')\ldots(X-X_m'')$ de $A'[X]$. Entonces*

$$R(f,g)=\prod_{\substack{i=1,\ldots,n\\ j=1,\ldots,m}}(X_j''-X_i').$$

Demostración: Tenemos

$$R(f,g)=\begin{vmatrix}
(-1)^n e'_n & (-1)^{n-1}e'_{n-1} & \dots & 1 & 0 & 0 & \dots & 0\\
0 & (-1)^n e'_n & \dots & -e'_1 & 1 & 0 & \dots & 0\\
 & & \ddots & & & & & \\
0 & \dots & 0 & (-1)^n e'_n & (-1)^{n-1}e'_{n-1} & \dots & -e'_1 & 1\\
(-1)^m e''_m & (-1)^{m-1}e''_{m-1} & \dots & -e''_1 & 1 & 0 & \dots & 0\\
0 & (-1)^m e''_m & \dots & e''_2 & -e''_1 & 1 & 0\dots & 0\\
 & & \ddots & & & & \ddots & \\
0 & \dots & 0 & (-1)^m e''_m & (-1)^{m-1}e''_{m-1} & \dots & -e''_1 & 1
\end{vmatrix}$$

donde $e'_1,\dots,e'_n$ son los polinomios simétricos elementales en $X'_1,\dots,X'_n$, y $e''_1,\dots,e''_m$ los polinomios simétricos elementales en $X''_1,\dots,X''_m$. De aquí se deduce fácilmente que $R(f,g)$, como polinomio en las variables $X'_1,\dots,X'_n$, tiene grado nm y que el término de mayor grado (que viene de la diagonal principal) es $(-1)^{nm}{X'_1}^m\dots{X'_n}^m$. Por otra parte, para cada $i=1,\dots,n$ y $j=1,\dots,m$, se tiene que X'_i es una raíz del polinomio $R(f,g)$ visto como polinomio en la variable X''_j (ya que sustituyendo X''_j por X'_i en $R(f,g)$ queda la resultante de f y el polinomio que resulta al sustituir en g la variable X''_j por X'_i, y dicha resultante es cero por el Teorema 3.6, al compartir ambos polinomios el factor $X-X'_i$, de grado positivo en X). Por el Corolario 2.4, se obtiene entonces que $R(f,g)$ es divisible por $X''_j-X'_i$. Como los polinomios $X''_j-X'_i$ son primos dos a dos, se deduce entonces que su producto $\Pi_{i,j}(X''_j-X'_i)$ divide a $R(f,g)$ en A'. Pero ambos polinomios, como polinomios en $X'_1,\dots,X'_n$, tienen grado nm, siendo el término de mayor grado en ambos $(-1)^{nm}{X'_1}^m\dots{X'_n}^m$, con lo que son necesariamente iguales. □

Corolario 3.11. *Sea A un D.F.U. y $f,g\in A[X]$ de grados respectivos n y m. Supongamos que g es mónico y tiene raíces $\beta_1,\dots,\beta_m$ (cada una repetida tantas veces como su multiplicidad) y que también f tiene n raíces contadas con multiplicidad. Entonces $R(f,g)=f(\beta_1)\dots f(\beta_m)$.*

Demostración: Si f es también mónico, podemos escribir $f=(X-\alpha_1)\dots(X-\alpha_n)$ y $g=(X-\beta_1)\dots(X-\beta_m)$. Como $R(f,g)$ consiste en sustituir, en la expresión de la demostración de la Proposición 3.10, $X'_1,\dots,X'_n,X''_1,\dots,X''_m$ por $\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_m$, tendremos

$$R(f,g)=\prod_{i,j}(\beta_j-\alpha_i)=\prod_j\big((\beta_j-\alpha_1)\dots(\beta_j-\alpha_n)\big)=\prod_j f(\beta_j).$$

Si f no es necesariamente mónico, si $\alpha_1\dots,\alpha_n$ son sus raíces, sabemos que $\bar f:=(X-\alpha_1)\dots(X-\alpha_n)$ divide a f. Como $\bar f$ y f tienen el mismo grado, podemos escribir $f=a\bar f$,

con $a \in A$. De la expresión (3.7) se deduce $R(f,g) = a^m R(\bar{f}, g)$, luego

$$R(f,g) = a^m \prod_j \bar{f}(\beta_j) = (a\bar{f}(\beta_1)) \dots (a\bar{f}(\beta_m)) = f(\beta_1) \dots f(\beta_m).$$

□

Observación 3.12. En realidad, en el Corolario anterior no haría falta pedir que f tuviera todas sus raíces en A (y de hecho a partir de ahora no lo pondremos como hipótesis), ya que en la sección próxima demostraremos (Teorema 4.12) que podremos extender el cuerpo de fracciones de A a un cuerpo en el que ya están todas las raíces de f. De hecho, el Corolario 3.11 demuestra mucho más (usando también que en una extensión oportuna g tiene también todas sus raíces): Si $g = g_1 g_2$ entonces $R(f, g_1 g_2) = R(f, g_1) R(f, g_2)$. El lector que no esté de acuerdo con el hecho de usar algo que veremos más adelante puede tranquilizar su conciencia resolviendo el siguiente:

Ejercicio 3.13. Demostrar la igualdad $R(f, (X-\alpha)g) = f(\alpha)R(f,g)$ [Indicación: En el determinante de orden $(m+1)+n$ que da la resultante de f y $(X-\alpha)g$ efectuar dos series de operaciones elementales; en primer lugar, empezando desde la penúltima columna hasta la primera, ir sumando a cada columna la siguiente multiplicada por α; en segundo lugar, desde la fila segunda hasta la $(m+1)$-ésima de la matriz obtenida, restar a cada fila la anterior multiplicada por α]. Concluir, por inducción sobre m, que en el Corolario 3.11 no hace falta suponer que f tenga n raíces contadas con multiplicidad.

Corolario 3.14. *Sea A un D.F.U., $f \in A[X]$ un polinomio mónico de grado n con raíces $\alpha_1, \dots, \alpha_n$ contadas con multiplicidad. Entonces*

$$R(f', f) = \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Además, si escribimos $\Delta := \prod_{i<j}(\alpha_i - \alpha_j)$, se tiene $R(f', f) = R(f, f') = (-1)^{\frac{n(n+1)}{2}} \Delta^2$.

Demostración: Escribimos $f = (X-\alpha_1)\dots(X-\alpha_n)$, y por el Corolario 3.11 sabemos que $R(f', f) = f'(\alpha_1)\dots f'(\alpha_n)$. Por otra parte, derivando, se obtiene

$$f' = (X-\alpha_2)\dots(X-\alpha_n) + \dots + (X-\alpha_1)\dots(X-\alpha_{n-1})$$

por lo que, para cada $i = 1, \dots, n$, se tiene $f'(\alpha_i) = \prod_{j \neq i}(\alpha_i - \alpha_j)$, que es la primera igualdad que buscábamos.

Para la segunda igualdad, basta observar dos cosas. La primera, que si en (3.7) cambiamos el orden de los polinomios f y f' estamos subiendo $n-1$ filas cada una de

las últimas n filas; como cada permutación de filas cambia el signo, tendremos $R(f,f') = (-1)^{n(n-1)}R(f',f) = R(f',f)$, ya que $n(n-1)$ es siempre par. La segunda observación es que el cociente de $\prod_{j\neq i}(\alpha_i - \alpha_j)$ entre el cuadrado de $\prod_{i<j}(\alpha_i - \alpha_j)$ es el cociente entre $\prod_{i>j}(\alpha_i - \alpha_j)$ y $\prod_{i<j}(\alpha_i - \alpha_j)$; los factores en el numerador y denominador son entonces los mismos, pero todos cambiados de signo, luego como hay $n(n-1)/2$ factores, dicho cociente queda $(-1)^{\frac{n(n+1)}{2}}$ □

Definición. Dado un polinomio $f \in A[X]$ de grado n y con raíces $\alpha_1, \ldots, \alpha_n$ (repetida cada una tantas veces como su multiplicidad), llamaremos *discriminante del polinomio* f a $D := \Delta^2$ (con las notaciones del corolario anterior).

Observación 3.15. Evidentemente, Δ está definido a partir de un orden prefijado de las raíces, y puede cambiar de signo al permutar las raíces (por eso, lo que tiene sentido es definir $D = \Delta^2$). Concretamente, si $\sigma \in S_n$ es una permutación de $\{1, \ldots, n\}$, el nuevo valor del discriminante al ordenar las raíces de la forma $\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}$ será $\Delta' = \prod_{i<j}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$. Entonces tenemos la igualdad

$$\prod_{i<j} \frac{\alpha_{\sigma(i)} - \alpha_{\sigma(j)}}{\sigma(i) - \sigma(j)} = \prod_{i<j} \frac{\alpha_i - \alpha_j}{i-j}$$

ya que en ambos productos tenemos los mismos factores, aunque cambiados de orden (obsérvese que si un numerador de la izquierda cambia de signo respecto del mismo numerador de la derecha entonces los correspondientes denominadores también cambian de signo). Tenemos por tanto

$$\frac{\Delta'}{\Delta} = \frac{\prod_{i<j}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})}{\prod_{i<j}(\alpha_i - \alpha_j)} = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i-j}$$

que es el signo de σ, según vimos en el Ejemplo 1.4. Por tanto, $\Delta' = \operatorname{sgn}(\sigma)\Delta$.

La definición concreta de discriminante varía según los autores. Hay quien llama discriminante a Δ, o a $R(f,f')$, o más generalemente, una constante por D. Por ejemplo, si $f = aX^2 + bX + c$, sabemos que las raíces de f son $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$, con lo que, con nuestra definición, $D = \frac{b^2-4ac}{a^2}$, mientras que se suele llamar discriminante de una ecuación de segundo grado a $b^2 - 4ac$ o a su raíz cuadrada (comparar con el Ejemplo 3.8 otras posibles definiciones naturales para el discriminante de f). Es claro que un polinomio de grado dos (con coeficientes en cualquier cuerpo K) tiene sus raíces en el cuerpo si y sólo si D tiene una raíz cuadrada en K. Cuando el grado es superior, es evidente que, si un polinomio con coeficientes en un anillo A tiene sus raíces en A entonces D tiene una raíz cuadrada en A,

pero el recíproco no es cierto (ni aunque supongamos que A es un cuerpo). La siguiente observación muestra cuál es la situación sobre $\mathbb{R}$.

Observación 3.16. Sea $f \in \mathbb{R}[X]$ de grado n y sin componentes múltiples. Demos de momento por bueno el teorema fundamental del álgebra (que demostraremos en el Teorema 6.9). Entonces las raíces $\alpha_1, \ldots, \alpha_n$ de f son todas distintas, y son o bien reales o bien por cada raíz imaginaria tenemos también su conjugada. Sea entonces σ la permutación de $\{1, \ldots, n\}$ que consiste en dejar fijos los elementos i tales que α_i es una raíz real y transponer i, j si α_i y α_j son raíces imaginarias conjugadas. Por tanto, para cada $i = 1, \ldots, n$, se tendrá $\bar{\alpha}_i = \alpha_{\sigma(i)}$. Por tanto, $\bar{\Delta} = \prod_{i<j}(\bar{\alpha}_i - \bar{\alpha}_j) = \prod_{i<j}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$, luego por la Observación 3.15 será $\bar{\Delta} = \operatorname{sgn}(\sigma)\Delta$. Como σ es el producto de tantas transposiciones como pares de raíces conjugadas tiene f, se concluye que $\bar{\Delta} = \Delta$ (es decir, Δ es real) si y sólo si el número de pares de raíces imaginarias conjugadas de f es par, mientras que en caso contrario Δ es imaginario puro. En otras palabras:

$D > 0$ si y sólo si f tiene una cantidad par de pares de raíces imaginarias conjugadas;

$D < 0$ si y sólo si el número de pares de raíces imaginarias conjugadas es impar.

En particular, si f tiene grado dos se reobtiene que f tiene sus raíces reales si y sólo si su discriminante es positivo. Si f tiene grado tres, obtenemos que $D > 0$ si y sólo si las tres raíces de f son reales y distintas y $D < 0$ si y sólo si una raíz es real y las otras dos imaginarias conjugadas. Para grado superior, la información no es tan precisa; por ejemplo, para grado cuatro, $D < 0$ quiere decir que hay exactamente un par de raíces imaginarias conjugadas, pero si $D > 0$ puede ocurrir que todas las raíces sean reales o todas imaginarias.

Por el Corolario 3.14, D se puede expresar como polinomio en los coeficientes de f. El método clásico de hacer esto, más que calculando resultantes, era observar que D es invariante al permutar las raíces; esta propiedad se da también en los polinomios simétricos elementales (que son los que determinan los coeficientes de f), lo que demostrará (como veremos enseguida) que D se puede poner también en función de los polinomios simétricos elementales, y por tanto de los coeficientes de f. Empecemos con la definición precisa:

Definición. Un polinomio $s \in A[X_1, \ldots, X_n]$ se dice que es un *polinomio simétrico* si, para toda permutación $\sigma \in S_n$ se tiene que $s(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = s$. En otras palabras, cada vez que en s aparece un monomio $X_1^{i_1} \ldots X_n^{i_n}$, entonces aparecen todos los monomios $X_{\sigma(1)}^{i_1} \ldots X_{\sigma(n)}^{i_n}$ y con el mismo coeficiente.

Ejemplo 3.17. Veamos en un ejemplo cómo funciona escribir un polinomio simétrico en función de los elementales. Consideremos el polinomio que corresponderá al discriminante

de una cúbica, es decir,

$$s(X_1, X_2, X_3) = (X_1 - X_2)^2(X_1 - X_3)^2(X_2 - X_3)^2$$

o, desarrollado y agrupado en bloques simétricos,

$$s(X_1, X_2, X_3) = (X_1^4X_2^2 + X_1^4X_3^2 + X_1^2X_2^4 + X_1^2X_3^4 + X_2^4X_3^2 + X_2^2X_3^4)$$

$$+(-2X_1^4X_2X_3 - 2X_1X_2^4X_3 - 2X_1X_2X_3^4) + (-2X_1^3X_2^3 - 2X_1^3X_3^3 - 2X_2^3X_3^3)$$

$$+(2X_1^3X_2^2X_3+2X_1^3X_2X_3^2+2X_1^2X_2^3X_3+2X_1^2X_2X_3^3+2X_1X_2^3X_3^2+2X_1X_2^2X_3^3)-6X_1^2X_2^2X_3^2.$$

Los bloques simétricos están ordenados lexicográficamente respecto a los exponentes (ordenados éstos de mayor a menor): concretamente, los exponentes de cada bloque son: (4,2,0), (4,1,1), (3,3,0), (3,2,1) y (2,2,2). Para eliminar los exponentes (4,2,0), restamos $e_1^2e_2^2$ y obtenemos

$$s - e_1^2e_2^2 = (-4X_1^4X_2X_3 - 4X_1X_2^4X_3 - 4X_1X_2X_3^4) + (-4X_1^3X_2^3 - 4X_1^3X_3^3 - 4X_2^3X_3^3)$$

$$+(-6X_1^3X_2^2X_3-6X_1^3X_2X_3^2-6X_1^2X_2^3X_3-6X_1^2X_2X_3^3-6X_1X_2^3X_3^2-6X_1X_2^2X_3^3)-21X_1^2X_2^2X_3^2$$

Obsérvese que los exponentes no han aumentado (el lector debe averiguar por qué), y ahora los exponentes máximos son (4,1,1) (con coeficiente -4), por lo que ahora sumamos $4e_1^3e_3$, y obtenemos

$$s - e_1^2e_2^2 + 4e_1^3e_3 = (-4X_1^3X_2^3 - 4X_1^3X_3^3 - 4X_2^3X_3^3)$$

$$+(6X_1^3X_2^2X_3+6X_1^3X_2X_3^2+6X_1^2X_2^3X_3+6X_1^2X_2X_3^3+6X_1X_2^3X_3^2+6X_1X_2^2X_3^3)+3X_1^2X_2^2X_3^2$$

Repitiendo el proceso, el lector habrá adivinado que ahora toca:

$$s - e_1^2e_2^2 + 4e_1^3e_3 + 4e_2^3 =$$

$$18(X_1^3X_2^2X_3 + X_1^3X_2X_3^2 + X_1^2X_2^3X_3 + X_1^2X_2X_3^3 + X_1X_2^3X_3^2 + X_1X_2^2X_3^3) + 27X_1^2X_2^2X_3^2$$

y finalmente

$$s - e_1^2e_2^2 + 4e_1^3e_3 + 4e_2^3 - 18e_1e_2e_3 = -27X_1^2X_2^2X_3^2 = -27e_3^2$$

con lo que podemos escribir $s = e_1^2e_2^2 - 4e_1^3e_3 - 4e_2^3 + 18e_1e_2e_3 - 27e_3^2$. De aquí se obtiene que si $f = X^3 + aX^2 + bX + c$, entonces $D = a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2$.

Teorema 3.18. *Sea $s \in A[X_1, \ldots, X_n]$ un polinomio simétrico. Entonces existe $p \in A[Y_1, \ldots, Y_n]$ tal que $s = p(e_1, \ldots, e_n)$.*

Demostración: Basta seguir las ideas del ejemplo anterior. En primer lugar, está claro que cada componente homogénea de s es también simétrica, luego podemos suponer que s es un polinomio homogéneo. Sea $(i_1, \ldots, i_n)$ la sucesión de exponentes máxima respecto al orden lexicográfico tal que $X_1^{i_1} \ldots X_n^{i_n}$ tenga coeficiente $c \neq 0$ en s (claramente, por la simetría de s, se tiene $i_1 \geq \ldots \geq i_n$). Observamos que el polinomio $e_1^{i_1 - i_2} \ldots e_{n-1}^{i_{n-1} - i_n} e_n^{i_n}$ tiene como monomio con sucesión de exponentes máxima respecto al orden lexicográfico a

$$X_1^{i_1 - i_2} (X_1 X_2)^{i_2 - i_3} \ldots (X_1 \ldots X_{n-1})^{i_{n-1} - i_n} (X_1 \ldots X_n)^{i_n} = X_1^{i_1} \ldots X_n^{i_n}.$$

Por tanto, el nuevo polinomio homogéneo simétrico $s - c e_1^{i_1 - i_2} \ldots e_{n-1}^{i_{n-1} - i_n} e_n^{i_n}$ tiene sus sucesiones de exponentes todas estrictamente menores que $(i_1, \ldots, i_n)$. Por recurrencia, y restando siempre polinomios en $e_1, \ldots, e_n$, se llega al polinomio cero (el último caso posible sería la sucesión de exponentes todos iguales, pero esto es una potencia de $e_1 \ldots e_n$, con lo que se llega a cero). □

Ejemplo 3.19. Veamos cómo resolver con las ideas anteriores una ecuación cúbica. La primera observación es que calcular las raceís del polimonio $g(X) = X^3 + aX^2 + bX + c$ es equivalente a calcular las raíces de $g(X - a/3)$, que tiene el aspecto $f(X) = X^3 + pX + q$. Tendremos entonces por el Ejemplo 3.17 que $D = -4p^3 - 27q^2$. Si $\alpha_1, \alpha_2, \alpha_3$ son las raíces de f, tendremos las relaciones

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p$$

$$\alpha_1\alpha_2\alpha_3 = -q$$

$$\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$$

y despejando α_3 en la primera ecuación podemos expresarlo todo en función sólo de α_1 y α_2:

$$p = -\alpha_1^2 - \alpha_1\alpha_2 - \alpha_2^2$$

$$q = \alpha_1^2\alpha_2 + \alpha_1\alpha_2^2$$

$$\Delta = 2\alpha_1^3 + 3\alpha_1^2\alpha_2 - 3\alpha_1\alpha_2^2 - 2\alpha_2^3$$

La idea mágica ahora es que una combinacion lineal (¡con coeficientes imaginarios!) de q y Δ da un cubo perfecto. De hecho, observando que en $\frac{\Delta}{2}$ tenemos los monomios α_1^3 y $-\alpha_2^3$ (que no aparecen en q), es natural comprobar si sumando a $\frac{\Delta}{2}$ algún múltiplo de q se

obtiene $(\alpha_1 - \omega\alpha_2)^3$, donde ω es una raíz cúbica de 1. Se comprueba inmediatamente que para $\omega = 1$ no funciona, mientras que para los otros dos valores de ω se tiene:

$$(\alpha_1 + (\frac{1}{2} \pm \frac{\sqrt{3}}{2}i)\alpha_2)^3 = \alpha_1^3 + (\frac{3}{2} \pm \frac{3\sqrt{3}}{2}i)\alpha_1^2\alpha_2 + (\frac{-3}{2} \pm \frac{3\sqrt{3}}{2}i)\alpha_1\alpha_2^2 - \alpha_2^3 = \frac{\Delta}{2} \pm \frac{3\sqrt{3}}{2}iq$$

Antes de tomar raceís cúbicas, como querremos despejar α_2 al restar las dos expresiones conjugadas de la izquierda, dividimos por $(\sqrt{3}i)^3 = -\sqrt{27}i$ y obtenemos:

$$(\frac{1}{\sqrt{3}i}\alpha_1 + (\frac{1}{2\sqrt{3}i} + \frac{1}{2})\alpha_2)^3 = -\frac{\Delta}{2\sqrt{27}i} - \frac{q}{2} = -\frac{q}{2} + \frac{1}{2}\sqrt{\frac{-D}{27}}$$

$$(\frac{1}{\sqrt{3}i}\alpha_1 + (\frac{1}{2\sqrt{3}i} - \frac{1}{2})\alpha_2)^3 = -\frac{\Delta}{2\sqrt{27}i} + \frac{q}{2} = \frac{q}{2} + \frac{1}{2}\sqrt{\frac{-D}{27}}$$

que, tomando raíces cúbicas (y cambiando primero el signo de la segunda igualdad) queda:

$$\frac{1}{\sqrt{3}i}\alpha_1 + (\frac{1}{2\sqrt{3}i} + \frac{1}{2})\alpha_2 = \sqrt[3]{-\frac{q}{2} + \frac{1}{2}\sqrt{\frac{-D}{27}}} \tag{3.20}$$

$$-\frac{1}{\sqrt{3}i}\alpha_1 + (-\frac{1}{2\sqrt{3}i} + \frac{1}{2})\alpha_2 = \sqrt[3]{-\frac{q}{2} - \frac{1}{2}\sqrt{\frac{-D}{27}}}. \tag{3.21}$$

Sumando y teniendo en cuenta que $D = -4p^3 - 27q^2$ se obtiene la fórmula de Cardano-Tartaglia para el cálculo de las raíces:

$$\alpha_2 = \sqrt[3]{-\frac{q}{2} + \frac{1}{2}\sqrt{\frac{4p^3 + 27q^2}{27}}} + \sqrt[3]{-\frac{q}{2} - \frac{1}{2}\sqrt{\frac{4p^3 + 27q^2}{27}}}. \tag{3.22}$$

A la hora de interpretar la fórmula hay que tener cuidado, ya que cada número tiene dos raíces cuadradas y tres complejas, luego en principio hay muchas posibilidades de elección. Respecto a las raíces cuadradas en la fórmula, está claro que lo que hacemos es tomar las dos, una en cada sumando. El problema está luego en ver qué raíces cúbicas hay que tomar en cada sumando para obtener una raíz de f. La clave está en (3.20) y (3.21). Dichas expresiones dicen que las raíces cúbicas hay que tomarlas de forma que su producto sea $\big(\frac{1}{\sqrt{3}i}\alpha_1 + (\frac{1}{2\sqrt{3}i} + \frac{1}{2})\alpha_2\big)\big(-\frac{1}{\sqrt{3}i}\alpha_1 + (-\frac{1}{2\sqrt{3}i} + \frac{1}{2})\alpha_2\big) = 1/3\alpha_1^2 + 1/3\alpha_1\alpha_2 + 1/3\alpha_2^2 = -\frac{p}{3}$. Por tanto, la fórmula puede escribirse también como

$$\alpha = \sqrt[3]{-\frac{q}{2} + \frac{1}{2}\sqrt{\frac{4p^3 + 27q^2}{27}}} - \frac{p}{3\sqrt[3]{-\frac{q}{2} + \frac{1}{2}\sqrt{\frac{4p^3+27q^2}{27}}}} \tag{3.23}$$

La observación sorprendente es que, en el caso en que las tres raíces son reales y distintas sabemos que $D = -4p^3 - 27q^2$ es positivo (Observación 3.16), mientras que al usar la fórmula (3.22) debemos pasar necesariamente por el número imaginario $\sqrt{\frac{4p^3+27q^2}{27}}$. Este hecho llevó a los matemáticos del siglo XVI a buscar una fórmula alternativa, hasta que se demostró más tarde que cualquier fórmula pasa necesariamente por los números imaginarios.

Ejemplo 3.24. Tomemos $f = X^3 - X$. En este caso $p = -1$, $q = 0$, luego $D = 4$ y la fórmula para las raíces queda

$$\sqrt[3]{-\frac{1}{2}\sqrt{-\frac{4}{27}}} + \sqrt[3]{\frac{1}{2}\sqrt{-\frac{4}{27}}}$$

donde el producto de las raíces cúbicas debe ser $-1/3$. El primer sumando se puede poner como $\frac{\sqrt{3}}{3}\sqrt[3]{i}$, que toma los valores

$$\beta_1 = -\frac{\sqrt{3}}{3}i, \quad \beta_2 = \frac{1}{2} + \frac{\sqrt{3}}{6}i, \quad \beta_3 = -\frac{1}{2} + \frac{\sqrt{3}}{6}i.$$

mientras que el segundo sumando es $\frac{\sqrt{3}}{3}\sqrt[3]{-i}$ y toma los valores

$$\gamma_1 = \frac{\sqrt{3}}{3}i, \quad \gamma_2 = -\frac{1}{2} - \frac{\sqrt{3}}{6}i, \quad \gamma_3 = \frac{1}{2} - \frac{\sqrt{3}}{6}i$$

La condición de que el producto de los dos sumandos debe ser $-\frac{p}{3} = \frac{1}{3}$ implica que las sumas que dan las raíces son

$$\beta_1 + \gamma_1 = 0 \quad \beta_2 + \gamma_3 = -1 \quad \beta_3 + \gamma_2 = 1.$$

Ejercicio 3.25. Repetir todo el ejemplo anterior para el polinomio $f = X^3 + X$.

Ejemplo 3.26. Veamos ahora el método para resolver ecuaciones cuárticas. Resolver $f = X^4 + aX^3 + bX^2 + cX + d = 0$ es equivalente a calcular la intersección de las cónicas $Y^2 + aXY + bY + cX + d = 0$ y $X^2 - Y = 0$. Evidentemente, la intersección de las cónicas es la misma que la de las cónicas $Y^2 + aXY + bY + cX + d + \lambda(X^2 - Y) = 0$ y $X^2 - Y = 0$ para cualquier λ. La idea es entonces escoger λ de forma que la primera cónica sea un par de rectas, lo que permite calcular inmediatamente la intersección. La primera cónica tiene por matriz asociada

$$M = \begin{pmatrix} d & c/2 & b/2 - \lambda/2 \\ c/2 & \lambda & a/2 \\ b/2 - \lambda/2 & a/2 & 1 \end{pmatrix}$$

y por tanto será degenerada si y sólo si $\det M = 0$, es decir, si y sólo si

$$\lambda^3 - 2b\lambda^2 + (ac + b^2 - 4d)\lambda - abc + c^2 + a^2 d.$$

Por tanto, basta resolver esta ecuación cúbica (que ya sabemos resolver), y tomando un valor cualquiera de λ basta escribir la cónica $Y^2 + aXY + bY + cX + d + \lambda(X^2 - Y) = 0$ como unión de dos rectas y cortar cada una de ellas con $Y = X^2$ (para lo cual basta resolver una ecuación cuadrática).

4. Extensiones de cuerpos

Dado un polinomio en una indeterminada con coeficientes reales, se habla siempre de sus raíces aunque éstas no sean siempre reales, sino imaginarias. En realidad, lo que se hace es ampliar el cuerpo $\mathbb{R}$ a un cuerpo más grande, el cuerpo $\mathbb{C}$ de los números complejos, donde viven en realidad las raíces. Cuando el cuerpo de partida no es $\mathbb{R}$, sino un cuerpo arbitrario, no es fácil (aunque se puede) construir un cuerpo más grande en el que todos los polinomios tengan sus raíces (es lo que se llama la *clausura algebraica del cuerpo*). Sin embargo, para cada polinomio concreto sí que es fácil construir un cuerpo en el que vivan las raíces del polinomio, y eso es lo que vamos a hacer en este capítulo.

Definición. Una *extensión de cuerpos* es una inclusión de cuerpos $K \subset L$. Dada una extensión $K \subset L$ y un elemento $\alpha \in L$, se dice que α es *algebraico sobre* K si existe $f \in K[X]$ no nulo tal que $f(\alpha) = 0$. En caso contrario, se dice que α es *transcendente sobre* K. Si todos los elementos de L son algebraicos sobre K se dice que $K \subset L$ es una *extensión algebraica*; en caso contrario, se dice que es una *extensión transcendente*.

Una observación básica es que cualquier homomorfismo de cuerpos $K \to L$ es inyectivo (luego proporciona una extensión del cuerpo K), ya que, visto como homomorfismo de anillos, su núcleo es un ideal, por tanto el cero o el total; y como el 1 de K va a parar al 1 de L, el núcleo no es el total.

Observación 4.1. A nosotros nos interesarán especialmente las extensiones algebraicas, ya que lo que queremos es añadir raíces de polinomios. Sin embargo, debe notarse que hay muchas más extensiones transcendentes que algebraicas. Por ejemplo, consideremos la extensión $\mathbb{Q} \subset \mathbb{C}$ y definamos el conjunto $\bar{\mathbb{Q}}$ de los números complejos que son algebraicos sobre $\mathbb{Q}$. Si llamamos Σ_n al conjunto de los números complejos que son raíces de algún polinomio en $\mathbb{Q}[X]$ de grado menor o igual que n, es claro que Σ_n es numerable (ya que el conjunto de polinomios de grado menor o igual que n está en biyección con el conjunto numerable $\mathbb{Q}^{n+1}$ de sus coeficientes, y cada polinomio tiene un número finito de finito de raíces, de hecho como mucho son n). Como claramente $\bar{\mathbb{Q}} = \cup_{n\in\mathbb{N}}\Sigma_n$, se sigue que $\bar{\mathbb{Q}}$ es numerable, y por tanto un subconjunto muy pequeño dentro de $\mathbb{C}$, que es no numerable. Sin embargo, demostrar la transcendencia de un elemento concreto no es nada fácil. Se sabe, por ejemplo, que números como e y π son transcendentes, pero la demostración dista mucho de ser trivial (ya el demostrar que son irracionales no es precisamente fácil).

Una primera observación sobre extensiones de cuerpos es que no se trata de algo esencialmente nuevo, sino que es básicamente una cuestión de Álgebra Lineal:

Lema 4.2. *Sea $K \subset L$ una extensión de cuerpos. Entonces L tiene una estructura de espacio vectorial sobre K, donde la suma es la propia de L, y el producto de un elemento*

de K con otro de L es el producto de ambos como elementos de L. Con esta estructura, dadas dos extensiones $K \subset L_1$ y $K \subset L_2$, un homomorfismo de cuerpos $\varphi : L_1 \to L_2$ es un homomorfismo de espacios vectoriales sobre K si y sólo si $\varphi_{|K} = id_K$.

Demostración: Es un simple ejercicio el ver que las propiedades de L como cuerpo implican las propiedades de L como espacio vectorial sobre K. Sea ahora $\varphi : L_1 \to L_2$ un homomorfismo de cuerpos entre dos extensiones de K. Si $\varphi_{|K} = id_K$, entonces para cada $\lambda \in K$ y cada $\alpha \in L_1$ se tiene que $\varphi(\lambda\alpha) = \varphi(\lambda)\varphi(\alpha)$ por ser φ un homomorfismo de cuerpos. Pero por ser $\varphi_{|K} = id_K$ se tiene $\varphi(\lambda) = \lambda$, con lo que $\varphi(\lambda\alpha) = \lambda\varphi(\alpha)$, lo que implica que φ es un homomorfismo de espacios vectoriales sobre K (sumas van a sumas por tratarse de un homomorfismo de cuerpos).

Recíprocamente, si $\varphi : L_1 \to L_2$ es un homomorfismo de espacios vectoriales sobre K, entonces para cada $\lambda \in K$ se tiene $\varphi(\lambda) = \varphi(\lambda \cdot 1_{L_1}) = \lambda\varphi(1_{L_1}) = \lambda 1_{L_2} = \lambda$, con lo que $\varphi_{|K} = id_K$. □

Podemos aprovechar este lema para demostrar un resultado sobre cuerpos finitos:

Corolario 4.3. *Si K es un cuerpo finito, entonces su cardinal es una potencia de un número primo p (más precisamente, p es la característica del cuerpo).*

Demostración: Recordemos que la característica es el generador no negativo del núcleo del homomorfismo $\mathbb{Z} \to K$ que manda n a la suma n veces del 1. Si K es finito, el homomorfismo no puede ser inyectivo, luego su núcleo será el conjunto de múltiplos de un primo p. Por el Primer Teorema de isomorfía, podemos ver $\mathbb{Z}_p$ como subcuerpo de K. Por el Lema 4.2, K tendrá estructura de espacio vectorial sobre $\mathbb{Z}_p$. Como K es finito, su dimensión como espacio vectorial será un número finito $n \in \mathbb{N}$, y se tendrá que, como espacio vectorial, K es isomorfo a $(\mathbb{Z}_p)^n$, por lo que tendrá p^n elementos. □

En nuestro plan de extender un cuerpo K hasta que un polinomio dado tenga sus raíces, empecemos por encontrar una primera extensión donde viva al menos una raíz del polinomio. El siguiente resultado nos indica que esencialmente sólo hay una forma de construir tal cuerpo, y que si el polinomio es irreducible las raíces son indistinguibles. Además, cada elemento es raíz de un único polinomio irreducible (luego dos polinomios irreducibles distintos no pueden compartir raíces).

Lema 4.4. *Sea $K \subset L$ una extensión y sea $\alpha \in L$ un elemento algebraico sobre K. Entonces:*

(i) Existe un único polinomio mónico irreducible $f \in K[X]$ tal que α es raíz de f.

(ii) Existe un isomorfismo $K[\alpha] \cong K[X]/(f)$ en que la imagen de α es la clase de X (y en particular $K[\alpha]$ es un cuerpo).

(iii) Para cualquier polinomio $g \in K[X]$ tal que $g(\alpha) = 0$, se tiene que f divide a g.

Demostración: Consideramos el homomorfismo $ev_\alpha : K[X] \to L$ definido por $ev_\alpha(f) = f(\alpha)$. Por hipótesis, el núcleo de ev_α es no nulo y su imagen es $K[\alpha]$ por definición. Como $K[X]$ es un D.I.P., el núcleo está generado por un polinomio $f \in K[X]$, que podemos tomar mónico, y por el primer teorema de isomorfía $K[X]/(f) \cong K[\alpha]$, siendo la imagen de la clase de X el elemento α. Como $K[\alpha]$ es un D.I. (por estar contenido en un cuerpo) (f) es un ideal primo, y por tanto f es irreducible y $K[X]/(f)$ es un cuerpo (por el Lema 2.14), lo que probaría (ii). La parte (iii) es clara, ya que si un polinomio g se anula en α, entonces está en el núcleo de ev_α, luego es divisible por f. La unicidad de f (y por tanto (i)) es consecuencia de que, si α es raíz de otro polinomio mónico irreducible f', por (iii) se tiene que f divide a f', y como ambos son mónicos e irreducibles entonces $f' = f$. □

Definición. Sea $K \subset L$ una extensión de cuerpos y sea $\alpha \in L$ un elemento algebraico sobre K. En las condiciones del lema anterior, se llama *polinomio mínimo de α sobre K* al único polinomio irreducible mónico $f \in K[X]$ tal que $f(\alpha) = 0$. Equivalentemente, f es el polinomio mónico en $K[X]$ de menor grado tal que $f(\alpha) = 0$. Como hemos visto, f divide a todos los demás polinomios de $K[X]$ que se anulan en α. Las otras raíces de f se llaman *conjugados de α respecto de K*.

Observación 4.5. La situación que se produce en el Lema 4.4 es radicalmente distinta si $\alpha \in L$ es un elemento transcendente. En efecto, por definición, el homomorfismo $ev_\alpha : K[X] \to L$ será en tal caso inyectivo. Por tanto, $K[\alpha]$ será isomorfo a $K[X]$, por lo que no será un cuerpo.

Ejemplo 4.6. Según el Lema 4.4, un anillo como por ejemplo $\mathbb{Q}[\sqrt[3]{2}]$ es un cuerpo, es decir, que todos sus elementos distintos de cero tienen inverso. En algunos casos concretos, es fácil encontrarlo directamente. Por ejemplo, usando la fórmula $a^3+b^3 = (a+b)(a^2-ab+b^2)$, se calcula inmediatamente

$$\frac{1}{3+5\sqrt[3]{2}} = \frac{3^2 - 3\cdot 5\sqrt[3]{2} + (5\sqrt[3]{2})^2}{(3+5\sqrt[3]{2})(3^2 - 3\cdot 5\sqrt[3]{2} + (5\sqrt[3]{2})^2)} =$$
$$= \frac{9 - 15\sqrt[3]{2} + 25\sqrt[3]{4}}{3^3 + (5\sqrt[3]{2})^3} = \frac{9}{277} - \frac{15}{277}\sqrt[3]{2} + \frac{25}{277}\sqrt[3]{4}$$

(este proceso recibe el nombre de *racionalizar* la expresión). Sin embargo no es tan evidente cómo calcular el inverso de un elemento como $2 - 3\sqrt[3]{2} + 7\sqrt[3]{4}$. Un método seguro, aunque bastante laborioso, sería el usar el isomorfismo $\mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[X]/(X^3 - 2)$ dado por el Lema 4.4, identificando entonces $2 - 3\sqrt[3]{2} + 7\sqrt[3]{4}$ con la clase del polinomio $2 - 3X + 7X^2$. Como $2 - 3X + 7X^2$ y $X^3 - 2$ son primos entre sí (como $X^3 - 2$ es irreducible, la condición

necesaria y suficiente es que $2 - 3X + 7X^2$ no sea múltiplo suyo), el teorema de Bézout afirma que existen polinomios $p, q \in \mathbb{Q}[X]$ tales que $(2 - 3X + 7X^2)p + (X^3 - 2)q = 1$ (aunque el modo de encontrar p y q no sea especialmente rápido). Evaluando en $\sqrt[3]{2}$, tendríamos entonces que el inverso de $2 - 3\sqrt[3]{2} + 7\sqrt[3]{4}$ sería $p(\alpha)$. No haremos las cuentas porque en el Ejemplo 4.9 daremos un método más efectivo.

Basándonos en el Lema 4.4, construimos ahora una extensión que contenga una raíz de un polinomio irreducible.

Lema 4.7. *Sea $f \in K[X]$ un polinomio irreducible. Entonces:*

(i) $L := K[X]/(f)$ es un cuerpo en el que K está incluido mediante la composición de aplicaciones naturales $i : K \subset K[X] \to K[X]/(f)$, y si α es la clase de X módulo (f), entonces α es una raíz de f

(ii) L tiene una estructura de espacio vectorial sobre K de dimensión igual al grado de f.

(iii) Si L' es otro cuerpo que contiene una raíz α' de f, entonces existe un único monomorfismo $\varphi : L \to L'$ tal que $\varphi_{|K} = id_K$ y $\varphi(\alpha) = \alpha'$.

Demostración: Que L es un cuerpo es una consecuencia del Lema 2.14, ya que (f) es un ideal maximal de $K[X]$. Que la aplicación $i : K \to K[X]/(f)$ es inyectiva se puede ver directamente, ya que el ideal (f) no contiene constantes no nulas, aunque por supuesto es consecuencia de que cualquier homomorfismo de cuerpos es inyectivo. Que la clase de X es una raíz de f es una pura tautología (aunque suele hacer falta reflexionar un poco para darse cuenta de ello): Si escribimos $f = a_0 + a_1X + \ldots + a_nX^n$, con $a_0, \ldots, a_n \in K$, tenemos que su clase módulo (f) es obviamente cero, luego (denotando con una barra las clases módulo (f)) se tiene $\bar{0} = \bar{a}_0 + \bar{a}_1\alpha + \ldots + \bar{a}_n\alpha^n = 0$; como $i(a_j) = \bar{a}_j$, viendo K como contenido en L, esta relación está diciendo precisamente $f(\alpha) = 0$. Esto demuestra (i).

Para la demostración de (ii), veamos que los vectores $1, \alpha, \ldots, \alpha^{n-1}$ (donde n es el grado de f) forman una base de L como espacio vectorial sobre K:

–En primer lugar, son linealmente independientes, porque en caso contrario existiría una combinación lineal $\lambda_0 \cdot 1 + \lambda_1\alpha + \ldots + \lambda_{n-1}\alpha^{n-1} = 0$ con $\lambda_i \in K$ y no todos nulos. Pero esto querría decir que el polinomio $\lambda_0 + \lambda_1X + \ldots + \lambda_{n-1}X^{n-1} \in K[X]$ es no nulo y es divisible por f, lo que es absurdo porque tiene grado menor que el grado de f.

–Por otra parte, forman un sistema de generadores, porque dado un elemento cualquiera de L, será la clase de un polinomio $g \in K[X]$ módulo f. Entonces, haciendo la división euclídea de g entre f tendremos $g = qf + r$, donde $r \in K[X]$ es cero o de grado menor que n. Podremos entonces escribir $r = b_0 + b_1X + \ldots + b_{n-1}X^{n-1}$, con

$b_0, b_1, \ldots, b_{n-1} \in K$. Tomando clases módulo f se tendrá entonces

$$\bar{g} = \bar{r} = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$$

luego cualquier $\bar{g} \in K[X]$ es combinación lineal de $1, \alpha, \ldots, \alpha^{n-1}$.

El apartado (iii) es el Lema 4.4. □

Definición. Se dice que $K \subset L$ es una *extensión finita* si L es un espacio vectorial de dimensión finita sobre K; la dimensión de dicho espacio vectorial se llama *grado de la extensión* y se denota por $[L : K]$.

Podría surgir la duda de si, ampliando el cuerpo K como en el lema anterior, estamos introduciendo elementos que no sean algebraicos. El siguiente resultado nos dice que no es así.

Lema 4.8. *Toda extensión finita es algebraica.*

Demostración: Sea $K \subset L$ una extensión finita y sea $\alpha \in L$ un elemento cualquiera. Si n es la dimensión de L como espacio vectorial sobre K, entonces, los $n+1$ vectores $1, \alpha, \ldots, \alpha^n$ deben ser linealmente dependientes sobre K. Por tanto, existen elementos $a_0, a_1, \ldots, a_n \in K$ no todos nulos tales que $a_0 1 + a_1\alpha + \ldots + a_n\alpha^n = 0$. Entonces el polinomio no nulo $f(X) := a_0 + a_1 X + \ldots + a_n X^n \in K[X]$ verifica $f(\alpha) = 0$, con lo que α es algebraico sobre K. □

Ejemplo 4.9. El resultado anterior nos plantea un nuevo problema (que sin embargo va a ser una solución al problema planteado en el Ejemplo 4.6 de calcular inversos). Si todos los elementos de un $K[\alpha]$ (con α algebraico sobre K) son algebraicos, según el Lema 4.8, entonces tendrán sus correspondientes polinomios mínimos. Como en el Ejemplo 4.6, en algunos casos se pueden calcular directamente a ojo. Por ejemplo, en $\mathbb{Q}[\sqrt[3]{2}]$, es evidente que un polinomio que anula a $\beta = 3 + 5\sqrt[3]{2}$ es $(\frac{X-3}{5})^3 - 2$, con lo que un polinomio mónico que tenga a β como raíz es $X^3 - 9X^2 + 27X - 277$, y no es complicado ver que es irreducible (por ejemplo, observando que no tiene raíces en $\mathbb{Q}$), luego es el polinomio mínimo. Obsérvese que el término independiente de este polinomio mínimo es el denominador que salía al calcular el inverso de β. Por supuesto, no es casualidad, ya que de la relación $\beta^3 - 9\beta^2 + 27\beta - 277 = 0$ se obtiene $\beta(\beta^2 - 9\beta + 27) = 277$, de donde sigue que el inverso de β es $\frac{\beta^2 - 9\beta + 27}{277}$, que, despejando el valor de β y desarrollando nos da el valor $\frac{9}{277} - \frac{15}{277}\sqrt[3]{2} + \frac{25}{277}\sqrt[3]{4}$ obtenido en el Ejemplo 4.6.

Podemos intentar lo mismo para el elemento $\gamma = 2 - 3\sqrt[3]{2} + 7\sqrt[3]{4}$ del que no supimos calcular su inverso de forma sencilla. Tampoco parece evidente cómo calcular su polinomio mínimo

a base de elevar expresiones al cubo y ver si desaparecen las raíces cúbicas. Seguiremos entonces los pasos de la demostración del Lema 4.8. En otras palabras, consideramos la base $B = \{1, \sqrt[3]{2}, \sqrt[3]{4}, \}$ de $\mathbb{Q}[\sqrt[3]{2}]$ como espacio vectorial sobre $\mathbb{Q}$. Calculamos entonces las coordenadas respecto de B de las primeras potencias de γ:

$$\begin{aligned}\gamma^0 &= 1 = (1,0,0)_B\\ \gamma^1 &= 2 - 3\sqrt[3]{2} + 7\sqrt[3]{4} = (2,-3,7)_B\\ \gamma^2 &= -80 + 86\sqrt[3]{2} + 37\sqrt[3]{4} = (-80,86,37)_B\\ \gamma^3 &= 822 + 930\sqrt[3]{2} - 744\sqrt[3]{4} = (822,930,-744)_B\end{aligned}.$$

Como $\begin{vmatrix} 1 & 0 & 0\\ 2 & -3 & 7\\ -80 & 86 & 37\end{vmatrix} \neq 0$, se sigue que $1, \gamma, \gamma^2$ son linealmente independientes, lo que quiere decir que γ no es raíz de un polinomio no nulo de grado menor o igual que dos con coeficientes en $\mathbb{Q}$. Del mismo modo, se obtiene la relación de dependencia lineal:

$$\gamma^3 = 1578 \cdot 1 - 138\gamma + 6\gamma^2$$

de donde se deduce que γ es raíz del polinomio $f(X) = X^3 - 6X^2 + 138X - 1578$. Como no es raíz de un polinomio de grado menor, $f(X)$ es el polinomio mínimo de γ sobre $\mathbb{Q}$ (lo que implica directamente que es irreducible en $\mathbb{Q}[X]$, aunque en este caso se puede obtener por rápidamente por el criterio de Eisenstein). Haciendo igual que para β, llegamos entonces a que el inverso de γ es $\frac{\gamma^2 - 6\gamma^2 + 138}{1578} = \frac{23}{789} + \frac{52}{789}\sqrt[3]{2} - \frac{5}{1578}\sqrt[3]{4}$. Existe otro modo, esencialmente equivalente pero computacionalmente más sencillo, para calcular el inverso. Consideramos la aplicación $\varphi : \mathbb{Q}[\sqrt[3]{2}] \to \mathbb{Q}[\sqrt[3]{2}]$ que consiste en la multiplicación por γ. Esta aplicación no es un homomorfismo de cuerpos, pero es un endomorfismo de espacios vectoriales. Los elementos de la base B se transforman mediante φ de la siguiente forma:

$$\begin{aligned}1 &\mapsto \gamma = (2,-3,7)_B\\ \sqrt[3]{2} &\mapsto \sqrt[3]{2}(2 - 3\sqrt[3]{2} + 7\sqrt[3]{4}) = 2\sqrt[3]{2} - 3\sqrt[3]{4} + 14 = (14,2,-3)_B\\ \sqrt[3]{4} &\mapsto \sqrt[3]{2}(14 + 2\sqrt[3]{2} - 3\sqrt[3]{4}) = 14\sqrt[3]{2} + 2\sqrt[3]{4} - 6 = (-6,14,2)_B\end{aligned}$$

por lo que la matriz de φ respecto de la base B es

$$M = \begin{pmatrix} 2 & 14 & -6\\ -3 & 2 & 14\\ 7 & -3 & 2\end{pmatrix}.$$

Por tanto, la matriz de la multiplicación por γ^{-1} respecto de la base B será:

$$M^{-1} = \begin{pmatrix} \frac{23}{789} & \frac{-5}{789} & \frac{104}{789}\\ \frac{52}{789} & \frac{23}{789} & \frac{-5}{789}\\ \frac{-5}{1578} & \frac{52}{789} & \frac{23}{789}\end{pmatrix}.$$

Como γ^{-1} es la imagen de 1 (primer vector de la base B, se tiene

$$\gamma^{-1} = (\frac{23}{789}, \frac{52}{789}, -\frac{5}{1578})_B = \frac{23}{789} + \frac{52}{789}\sqrt[3]{2} - \frac{5}{1578}\sqrt[3]{4}$$

con lo que reobtenemos el resultado anterior (obsérvese que para este cálculo bastaba sólo con calcular la primera columna de M^{-1}). Finalizamos este ejemplo observando que se puede usar también el Álgebra Lineal para calcular el polinomio mínimo de γ (en general se obtendrá un polinomio que se anule en la raíz que queramos, no necesariamente el mínimo). Parece claro (en realidad no lo es tanto) que γ debe ser un autovalor de φ, por lo que es una raíz del polinomio característico de M, que en efecto resulta ser $-\lambda^3 + 6\lambda^2 - 138\lambda + 1578$.

Ejemplo 4.10. Ya vimos en el Corolario 3.3 que, si K es un cuerpo finito, $K \setminus \{0\}$ es un grupo cíclico con el producto. Sea α un generador del grupo. Entonces, al ser cada elemento de $K\setminus\{0\}$ de la forma α^k para algún k (que podemos suponer positivo), y teniendo en cuenta que $\mathbb{Z}_p \subset K$ (donde p es la característica de K, según vimos en la demostración del Corolario 4.3), tendremos $K = \mathbb{Z}_p[\alpha]$. Como la extensión $\mathbb{Z}_p \subset K$ es finita (por ser K un cuerpo finito), será algebraica por el Lema 4.8. Entonces α es algebraico sobre $\mathbb{Z}_p$, luego por el Lema 4.4 se tendrá $K \cong \mathbb{Z}_p[X]/(f)$, donde f es un polinomio irreducible de grado n. Veremos más adelante (Teorema 4.13) que para cada n existen cuerpos así y que son todos isomorfos.

Nuestra idea ahora será, a partir del Lema 4.7, ir añadiendo sucesivamente una a una todas las raíces que queramos de un polinomio dado. El resultado siguiente nos dice que la extensión total seguirá siendo finita (y por tanto algebraica).

Lema 4.11. *Sean $K \subset K' \subset L$ extensiones de cuerpos. Entonces la extensión $K \subset L$ es finita si y sólo si las extensiones $K \subset K'$ y $K' \subset L$ son finitas. Además, en tal caso se tiene $[L : K] = [L : K'][K' : K]$.*

Demostración: Si $K \subset L$ es una extensión finita, entonces L es un espacio vectorial de dimensión finita sobre K. Como K' es un subespacio vectorial de L, entonces necesariamente también tiene dimensión finita, por lo que $K \subset K'$ es una extensión finita. Por otra parte, si $\alpha_1, \ldots, \alpha_n$ es un sistema finito de generadores de L como espacio vectorial sobre K, es claro que también en un sistema de generadores como espacio vectorial sobre K'. Por tanto, L es un espacio vectorial de dimensión finita sobre K', es decir, la extensión $K' \subset L$ es finita.

Recíprocamente, supongamos que las extensiones $K \subset K'$ y $K' \subset L$ son finitas. En particular, L tendrá dimensión finita $n = [L : K']$ como espacio vectorial sobre K', y tendrá una base $\{\beta_1, \ldots, \beta_n\}$. Esto quiere decir que cualquier $\beta \in L$ se puede escribir de la forma

$$\beta = \mu_1\beta_1 + \ldots + \mu_n\beta_n$$

con $\mu_1, \ldots, \mu_n \in K'$. Si queremos coeficientes en K, podemos usar que K' es un espacio vectorial de dimensión finita $m = [K' : K]$, es decir, tiene una base $\{\alpha_1, \ldots, \alpha_m\}$. Por tanto, podremos escribir

$$\begin{aligned} \mu_1 &= \lambda_{11}\alpha_1 + \ldots + \lambda_{m1}\alpha_m \\ &\vdots \\ \mu_n &= \lambda_{1n}\alpha_1 + \ldots + \lambda_{mn}\alpha_m \end{aligned}$$

con los λ_{ij} en K. Sustituyendo en la expresión anterior, tenemos que cualquier $\beta \in L$ se puede escribir como

$$\beta = \lambda_{11}\alpha_1\beta_1 + \ldots + \lambda_{m1}\alpha_m\beta_1 + \ldots + \lambda_{1n}\alpha_1\beta_n + \ldots + \lambda_{mn}\alpha_m\beta_n$$

luego $\{\alpha_1\beta_1, \ldots, \alpha_m\beta_1, \ldots, \alpha_1\beta_n + \ldots, \alpha_m\beta_n\}$ es un sistema de generadores de L como espacio vectorial sobre K. En particular, es un espacio vectorial de dimensión finita. Como el sistema de generadores tiene $nm = [L : K'][K' : K]$ elementos, el lema quedará demostrado si vemos que forman una base, para lo que falta demostrar que son linealmente independientes. Para ello, suponemos que tenemos una combinación lineal

$$\lambda_{11}\alpha_1\beta_1 + \ldots + \lambda_{m1}\alpha_m\beta_1 + \ldots + \lambda_{1n}\alpha_1\beta_n + \ldots + \lambda_{mn}\alpha_m\beta_n = 0$$

con los λ_{ij} en K. Sacando factor común $\beta_1, \ldots, \beta_n$ tenemos

$$(\lambda_{11}\alpha_1 + \ldots + \lambda_{m1}\alpha_m)\beta_1 + \ldots + (\lambda_{1n}\alpha_1 + \ldots + \lambda_{mn}\alpha_m)\beta_n = 0,$$

que es una combinación lineal con coeficientes en K'. Al ser $\{\beta_1, \ldots, \beta_n\}$ un conjunto linealmente independiente sobre K' los coeficientes son necesariamente cero, es decir,

$$\begin{aligned} \lambda_{11}\alpha_1 + \ldots + \lambda_{m1}\alpha_m &= 0 \\ &\vdots \\ \lambda_{1n}\alpha_1 + \ldots + \lambda_{mn}\alpha_m &= 0 \end{aligned}$$

que ahora son combinaciones lineales con coeficientes en K. Pero ahora, usando que el conjunto $\{\alpha_1, \ldots, \alpha_m\}$ es un conjunto linealmente independiente se deduce que todos los coeficientes son cero, es decir, $\lambda_{11} = \ldots = \lambda_{m1} = \ldots = \lambda_{1n} = \ldots = \lambda_{mn} = 0$. Esto demuestra que $\{\alpha_1\beta_1, \ldots, \alpha_m\beta_1, \ldots, \alpha_1\beta_n + \ldots, \alpha_m\beta_n\}$ es un conjunto linealmente independiente, luego base. □

La construcción general de un cuerpo que contenga todas las raíces de un polinomio es más complicada que si pedimos que contenga sólo una raíz. Tal construcción requiere un argumento de inducción, y para que funcione la inducción necesitaremos un enunciado de apareciencia más complicada en que aparezca un isomorfismo σ. De todas formas, el lector puede pensar de momento el enunciado en el caso en que σ es la identidad (aunque el caso general con σ arbitrario será fundamental más adelante para demostrar la Proposición 5.7, que será crucial para la teoría de Galois).

Teorema 4.12. *Sea K un cuerpo y $f \in K[X]$ un polinomio de grado positivo. Entonces existe una extensión finita $K \subset L$ (única salvo isomorfismo) tal que:*

(i) f descompone en factores lineales en $L[X]$ (y por tanto tiene todas sus raíces en L).

(ii) Para todo isomorfismo de cuerpos $\sigma : K \to K'$ y todo cuerpo $L' \supset K'$ tal que $\sigma(f)$ (definido aplicando σ a los coeficientes de f) descompone en factores lineales, entonces existe un monomorfismo de cuerpos $\varphi : L \to L'$ tal que $\varphi_{|K} = \sigma$ y que manda las raíces de f en L a las raíces de $\sigma(f)$ en L'. Además, $\varphi(L) = K'[\alpha'_1, \ldots, \alpha'_n]$, donde $\alpha'_1, \ldots, \alpha'_n$ son las raíces de $\sigma(f)$.

Demostración: Demostraremos la existencia de L por inducción sobre el grado de f. Si f tiene grado uno, entonces es evidente que basta tomar $L = K$. Supongamos por tanto que f tiene grado mayor que uno y tomemos g una componente irreducible de f. Por el Lema 4.7, $K_1 = K[X]/(g)$, es un cuerpo que contiene a K y además $\alpha_1 = \bar{X}$ es una raíz de g, y por tanto una raíz de f. Como consecuencia, f se podrá factorizar en $K_1[X]$ como $f = (X - \alpha_1)h$, con $h \in K_1[X]$ de grado el grado de f menos uno. Aplicando entonces la hipótesis de inducción a h, tendremos que existe una extensión finita $K_1 \subset L$ en las condiciones del teorema y, en particular, h factoriza en factores lineales en $L[X]$. Evidentemente, f factoriza entonces en factores lineales en $L[X]$ y la extensión $K \subset L$ es finita por ser composición de extensiones finitas.

Supongamos ahora que tenemos un isomorfismo de cuerpos $\sigma : K \to K'$ y un cuerpo $L' \supset K'$ tal que $\sigma(f)$ descompone en factores lineales. Sea $\alpha'_1 \in L'$ una raíz de $\sigma(g)$ (que es un factor irreducible de $\sigma(f)$). Por el Lema 4.7(iii) se tiene un isomorfismo $\sigma_1 : K_1 \to K'_1 := K[\alpha'_1] \subset L$ tal que $\sigma_{1|K} = \sigma$ y $\sigma_1(\alpha_1) = \alpha'_1$. Además, $\sigma(f)$ factorizará en $K'_1[X]$ como $(X - \alpha'_1)\sigma_1(h)$ y $\sigma_1(h)$ factoriza en factores lineales en $L'[X]$. Aplicando hipótesis de inducción tomando como polinomio h y como isomorfismo de cuerpos σ_1, tendremos que existe un monomorfismo de cuerpos $\varphi : L \to L'$ tal que $\varphi_{|K_1} = \sigma_1$ que manda las raíces de h en L a las raíces de $\sigma(h)$ en L'. Por tanto, $\varphi_{|K} = \sigma$ y φ manda las raíces de f en L a las raíces de $\sigma(f)$ en L' (y concretamente $\varphi(\alpha_1) = \alpha'_1$). Además, si $\alpha'_2, \ldots, \alpha'_n$ son las raíces de $\sigma(h)$, entonces también por hipótesis de inducción se tiene que $\varphi(L) = K_1[\alpha'_2, \ldots, \alpha'_n] = K[\alpha'_1, \ldots, \alpha'_n]$.

La unicidad de L salvo isomorfismo se obtiene porque, por la propiedad (ii) aplicada a $\sigma = id$, si hubiera dos cuerpos L, L' que verificaran las mismas condiciones, habría monomorfismos $\varphi : L \to L'$ y $\varphi' : L' \to L$ que serían la identidad restringidos a K, en particular (por el Lema 4.2) monomorfismos de espacios vectoriales sobre K. Por tanto, $\dim_K L = \dim_K L'$, y necesariamente (por tratarse de espacios vectoriales de dimensión finita), φ sería suprayectiva, y por tanto un isomorfismo de cuerpos. □

Definición. Dado un cuerpo K y un polinomio $f \in K[X]$, se llama *cuerpo de descom-*

posición del polinomio f sobre el cuerpo K al cuerpo L cuya existencia garantiza el Teorema 4.12 (la propiedad (ii) se debe interpretar como que L es el cuerpo más pequeño que contiene todas las raíces de f).

La unicidad salvo isomorfismo del cuerpo de descomposición nos da la unicidad salvo isomorfismo, de cuerpos finitos de orden dado (de los que demostraremos también la existencia):

Teorema 4.13. *Para cada número primo p y cada natural $n \geq 1$ existe, y es único salvo isomorfismo, un cuerpo de orden p^n.*

Demostración: Veamos primero la parte de la unicidad, que nos dará la pista para demostrar la existencia. Ya sabemos que un cuerpo K de orden $q = p^n$ es una extensión de grado n de $\mathbb{Z}_p$. Además, como $K \setminus \{0\}$ es un grupo multiplicativo de orden $q-1$, se tiene $\alpha^{q-1} = 1$ para todo $\alpha \in K \setminus \{0\}$. Por tanto, todos los elementos de K son raíces del polinomio $f = X^q - X$, que podemos considerar como polinomio en $\mathbb{Z}_p[X]$. Por tanto, K puede verse como cuerpo de descomposición de f sobre $\mathbb{Z}_p$. La unicidad se sigue ahora de la unicidad del cuerpo de descomposición de un polinomio.

Para ver la existencia, hay que ver que, para cada $q = p^n$, el cuerpo de descomposición K de f tiene exactamente q elementos. Como $f' = p^n X^{q-1} - 1 = -1$, f y f' no tienen raíces comunes, luego f tiene exactamente q raíces. Veamos que K no puede contener más elementos. Para eso, por ser K el cuerpo de descomposición de f sobre $\mathbb{Z}_p$, bastará ver que el conjunto de raíces de f forman un subcuerpo de K. Esto es cierto porque, si α, β son raíces de f se tendrá, usando el Ejercicio 1.13,

$$f(a+b) = (a+b)^{p^n} - (a+b) = a^{p^n} + b^{p^n} - a - b = 0,$$

luego $a+b$ también es raíz y como las raíces de f menos el cero son las raíces de $x^{q-1}-1$, forman un grupo con el producto. Entonces K es exactamente el conjunto de raíces de f, luego tiene orden $q = p^n$. □

Ejemplo 4.14. Consideremos el polinomio $f = X^3 - 2 \in \mathbb{Q}[X]$ (que es irreducible por el criterio de Eisenstein). Las raíces de f (considerando $\mathbb{Q}$ dentro de $\mathbb{C}$) son

$$\alpha_1 = \sqrt[3]{2}$$

$$\alpha_2 = \sqrt[3]{2}(\frac{-1}{2} + \frac{\sqrt{3}}{2}i)$$

$$\alpha_3 = \sqrt[3]{2}(\frac{-1}{2} - \frac{\sqrt{3}}{2}i).$$

La parte (ii) del teorema anterior nos dice que podemos tomar el cuerpo de descomposición de f dentro de $\mathbb{C}$, concretamente sería $L = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]$. Como $\sqrt{3}i = \frac{\alpha_2 - \alpha_3}{\alpha_1}$, se tiene que L contiene a $\mathbb{Q}[\sqrt[3]{2}, \sqrt{3}i]$. Como el otro contenido es evidente, se deduce que el cuerpo de descomposición de f sobre $\mathbb{Q}$ es $L = \mathbb{Q}[\sqrt[3]{2}, \sqrt{3}i]$. Para calcular $[L : \mathbb{Q}]$ podemos tomar $K' = \mathbb{Q}[\sqrt[3]{2}]$ y considerar la cadena de extensiones $\mathbb{Q} \subset K' \subset L$, y por Lema 4.11 tendremos $[L : \mathbb{Q}] = [L : K'][K' : \mathbb{Q}]$. Por el Lema 4.7, $[K' : \mathbb{Q}] = 3$. Por otra parte, $L = K'[\sqrt{3}i]$, y $\sqrt{3}i$ es raíz de $X^2 + 3$. Por tanto, tenemos dos opciones: si $X^2 + 3$ es irreducible en $K'[X]$ tendremos que $[L : K'] = 2$ y $[L : \mathbb{Q}] = 6$, mientras que si $X^2 + 3$ fuese reducible, entonces es que $\sqrt{3}i$ es raíz de un polinomio de grado uno en $K'[X]$, es decir $\sqrt{3}i$ estaría en K' y entonces $L = K'$ y $[L : \mathbb{Q}] = 3$. Esta última posibilidad es claro que no se puede dar, ya que $\sqrt{3}i$ no es real, mientras que todos los elementos de K' son reales. De todas formas, veamos otro truco que se puede aplicar a casos más generales. Consideramos la cadena de extensiones $\mathbb{Q} \subset \mathbb{Q}[\sqrt{3}i] \subset L$, con lo que también tenemos $[L : \mathbb{Q}] = [L : \mathbb{Q}[\sqrt{3}i]][\mathbb{Q}[\sqrt{3}i] : \mathbb{Q}]$. Ahora es claro que $[\mathbb{Q}[\sqrt{3}i] : \mathbb{Q}] = 2$ (por el Lema 4.7, ya que $X^2 + 3$ es irreducible en $\mathbb{Q}[X]$), luego $[L : \mathbb{Q}]$ es divisible por 2, así que la única posibilidad es $[L : \mathbb{Q}] = 6$ (lo que demostraría de paso que $\sqrt{3}i$ no está en $\mathbb{Q}[\sqrt[3]{2}]$). Una última observación es que L no se puede simplificar más "separando" $\sqrt{3}$ e i, en el sentido de que $L \neq \mathbb{Q}[\sqrt[3]{2}, \sqrt{3}, i]$. En efecto, el truco de divisibilida anterior muestra que $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}] = 6$, y como $i \notin \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ entonces $[\mathbb{Q}[\sqrt[3]{2}, \sqrt{3}, i] : \mathbb{Q}[\sqrt{2}, \sqrt{3}]] = 2$, de donde $[\mathbb{Q}[\sqrt[3]{2}, \sqrt{3}, i] : \mathbb{Q}] = 12$.

Ejemplo 4.15. Consideremos ahora $f = X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$, que ya vimos en el Ejemplo 2.26 que es irreducible y que sus raíces son

$$\alpha_1 = \sqrt{2} + \sqrt{3}$$

$$\alpha_2 = \sqrt{2} - \sqrt{3}$$

$$\alpha_3 = -\sqrt{2} + \sqrt{3}$$

$$\alpha_4 = -\sqrt{2} - \sqrt{3}.$$

De nuevo por la parte (ii) del Teorema 4.12, el cuerpo de descomposición de f sobre $\mathbb{Q}$ será $L = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$, que se demuestra fácilmente que es $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Para calcular $[L : \mathbb{Q}]$, podemos hacer como en el ejemplo anterior, y considerar la cadena $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset L$. El problema sigue siendo decidir si $X^2 - 3$ es irreducible en $\mathbb{Q}[\sqrt{2}]$, es decir, si $\sqrt{3}$ está en $\mathbb{Q}[\sqrt{2}]$ (el lector puede pensar que es obvio que no, pero requiere una demostración rigurosa). Pero ahora no sirve el truco de considerar la nueva cadena $\mathbb{Q} \subset \mathbb{Q}[\sqrt{3}] \subset L$, ya que $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, y no se puede aplicar el truco de divisibilidad del Ejemplo 4.14. En realidad, aquí podemos usar un truco más sencillo, ya que L contiene por ejemplo a $\mathbb{Q}[\alpha_1]$, y sabemos que $[\mathbb{Q}[\alpha_1] : \mathbb{Q}] = 4$, por el Lema 4.7 (ya que f es irreducible

de grado 4). Por tanto, $\mathbb{Q}[\alpha_1]$ es un subespacio de dimensión cuatro de L, que por las observaciones anteriores tiene dimensión 2 o 4. Esto implica también que $L = \mathbb{Q}[\alpha_1]$ y $[L : \mathbb{Q}] = 4$. Este truco de poder poner una extensión de la forma $K[\alpha]$ va a resultar decisivo en la sección siguiente.

Definición. Dada una extensión $K \subset L$ y dados $\alpha_1, \ldots, \alpha_n \in L$, el mínimo subcuerpo de L que contiene a K y a $\alpha_1, \ldots, \alpha_n$, es el cuerpo de fracciones de $K[\alpha_1, \ldots, \alpha_n]$, que denotaremos por $K(\alpha_1, \ldots, \alpha_n)$. Una *extensión finitamente generada* es una extensión $K \subset L$ tal que $L = K(\alpha_1, \ldots, \alpha_n)$ para ciertos $\alpha_1, \ldots, \alpha_n \in L$. Si $L = K(\alpha)$, se dice que $K \subset L$ es una *extensión simple* y que α es un *elemento primitivo de la extensión*.

Ejemplo 4.16. Si K es un cuerpo finito, entonces cualquier extensión finita $K \subset L$ es simple. En efecto, L es también finito (si no, tendría dimensión infinita sobre K) y, por el Corolario 3.3, $L \setminus \{0\}$ es un grupo cíclico generado por un elemento, digamos α. Entonces $L = K(\alpha)$.

Lema 4.17. *Sea $K \subset L = K(\alpha_1, \ldots, \alpha_n)$ una extensión de cuerpos finitamente generada. Entonces son equivalentes:*

(i) La extensión $K \subset L$ es finita.

(ii) La extensión $K \subset L$ es algebraica.

(iii) $\alpha_1, \ldots, \alpha_n$ son algebraicos sobre K.

Además, en estas condiciones, $L = K[\alpha_1, \ldots, \alpha_n]$.

Demostración:

$(i) \Rightarrow (ii)$: Esta implicación es cierta siempre (Lema 4.8).

$(ii) \Rightarrow (iii)$: Por definición, al ser la extensión $K \subset L$ algebraica, los elementos $\alpha_1, \ldots, \alpha_n$ son algebraicos sobre K.

$(iii) \Rightarrow (i)$: Descomponemos la extensión $K \subset L$ en una cadena de extensiones simples:

$$K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \ldots \subset K(\alpha_1, \ldots, \alpha_{n-1}) \subset K(\alpha_1, \ldots, \alpha_n) = L.$$

Para el primer eslabón, observamos que, por hipótesis, α_1 es algebraico sobre K, luego por los Lemas 4.4 y 4.7 se tiene que $K[\alpha_1]$ es un cuerpo (luego coincide con su cuerpo de fracciones $K(\alpha_1)$) y la extensión $K \subset K[\alpha_1]$ es finita. Si escribimos ahora el segundo eslabón como $K(\alpha_1) \subset \big(K(\alpha_1)\big)(\alpha_2)$, de nuevo tenemos que α_2 es algebraico sobre K, y por tanto también es algebraico sobre $K(\alpha_1)$. Por el mismo argumento de antes, $\big(K(\alpha_1)\big)(\alpha_2) = \big(K(\alpha_1)\big)[\alpha_2]$ (y por tanto también es igual a $\big(K[\alpha_1]\big)[\alpha_2] = K[\alpha_1, \alpha_2]$) y la extensión $K[\alpha_1] \subset K[\alpha_1, \alpha_2]$ es finita. Reiterando el argumento, la cadena anterior es igual a

$$K \subset K[\alpha_1] \subset K[\alpha_1, \alpha_2] \subset \ldots \subset K[\alpha_1, \ldots, \alpha_{n-1}] \subset K[\alpha_1, \ldots, \alpha_n] = L$$

y además cada extensión en la cadena es finita. Por el Lema 4.11 se concluye que la extensión $K \subset L$ es finita.

Obsérvese que en esta última parte de la demostración ya hemos visto que $L = K[\alpha_1, \ldots, \alpha_n]$. □

Observación 4.18. En realidad, en el resultado anterior es también cierto que el hecho de que L coincida con $K[\alpha_1, \ldots, \alpha_n]$ caracteriza el que la extensión sea algebraica. Esto no es más que una de las infinitas versiones actuales del clásico Nullstellensatz (teorema de los ceros) de Hilbert. Veamos aquí al menos la demostración para $n = 1$. Si tenemos que el cuerpo L se puede expresar como $L = K[\alpha]$, entonces en particular el inverso de α se podrá escribir como una expresión polinomial en α, es decir, existen $a_0, \ldots, a_n \in K$ tales que

$$\alpha(a_0 + a_1\alpha + \ldots + a_n\alpha^n) = 1.$$

Por tanto, α verifica la igualdad polinomial $-1 + a_0\alpha + a_1\alpha^2 + \ldots + a_n\alpha^{n+1} = 0$, por lo que es algebraico sobre K. Por el Lema 4.7, tenemos entonces que la extensión $K \subset L$ es finita, es decir, algebraica.

Proposición 4.19. *Sean $K \subset K' \subset L$ extensiones de cuerpos. Entonces la extensión $K \subset L$ es algebraica si y sólo si las extensiones $K \subset K'$ y $K' \subset L$ son algebraicas.*

Demostración: Si $K \subset L$ es una extensión algebraica, es evidente que $K \subset K'$ también lo es. Además, cualquier elemento de L es raíz de un polinomio no nulo de $K[X]$, que es también un polinomio no nulo de $K'[X]$, luego la extensión $K' \subset L$ es algebraica.

Recíprocamente, supongamos ahora que las extensiones $K \subset K'$ y $K' \subset L$ son algebraicas. Sea $\alpha \in L$ y veamos que es algebraico sobre K. Como es algebraico sobre K', α es raíz de un polinomio $\alpha_0 + \alpha_1 X + \ldots + \alpha_n X^n$ con $\alpha_0, \alpha_1, \ldots, \alpha_n \in K'$. Por tanto, α es algebraico sobre $K(\alpha_0, \ldots, \alpha_n)$ y la extensión $K(\alpha_0, \ldots, \alpha_n) \subset K(\alpha_0, \ldots, \alpha_n)[\alpha]$ es finita. Como $\alpha_0, \ldots, \alpha_n \in K'$, son elementos algebraicos sobre K, por el Lema 4.17, la extensión $K \subset K(\alpha_0, \ldots, \alpha_n)$ es finita. Por tanto, por el Lema 4.11, la extensión $K \subset K(\alpha_0, \ldots, \alpha_n)[\alpha]$ es finita, luego algebraica (por el Lema 4.8). En particular, α es algebraico sobre K. □

Proposición 4.20. *Sea $K \subset L$ una extensión de cuerpos. Entonces el conjunto K' de los elementos de L que son algebraicos sobre K es un subcuerpo de L. Además, todo elemento de L algebraico sobre K' está en K'.*

Demostración: Sean $\alpha, \beta \in K'$. Por el Lema 4.17, $K[\alpha, \beta]$ es un cuerpo que es una extensión algebraica de K. Por tanto, $K[\alpha, \beta] \subset K'$, y en particular $\alpha + \beta, \alpha\beta \in K'$. Además, $\frac{1}{\alpha}, \frac{1}{\beta} \in K'$. Por tanto, K' es un cuerpo.

Por otra parte, sea $\alpha \in L$ un elemento algebraico sobre K'. Entonces la extensión $K' \subset K'(\alpha)$ es algebraica, y la Proposición 4.19 implica que la extensión $K \subset K'(\alpha)$ es algebraica, luego $\alpha \in K'$. □

Ejemplo 4.21. La Proposición 4.20 implica que el conjunto $\bar{\mathbb{Q}}$ de la Observación 4.1 es un cuerpo, llamada *cuerpo de los números algebraicos*. Nótese que, cuando demostremos en el Teorema 6.9 que $\mathbb{C}$ es algebraicamente cerrado (i.e., todo polinomio de grado positivo en $\mathbb{C}[X]$ tiene alguna raíz en $\mathbb{C}$), entonces $\bar{\mathbb{Q}}$ también lo será. En efecto, sea $f \in \bar{\mathbb{Q}}[X]$ un polinomio de grado positivo. Visto como polinomio en $\mathbb{C}[X]$, tendrá una raíz $\alpha \in \mathbb{C}$. Entonces α es algebraico sobre $\bar{\mathbb{Q}}$, y la Proposicion 4.20 implica $\alpha \in \bar{\mathbb{Q}}$. En realidad, $\bar{\mathbb{Q}}$ es el cuerpo algebraicamente cerrado más pequeño que contiene a $\mathbb{Q}$, es decir, es lo que se llama *clausura algebraica* de $\mathbb{Q}$. Todo cuerpo tiene clausura algebraica, aunque no vamos a demostrarlo aquí.

Ejemplo 4.22. Obsérvese que el Lema 4.17 nos vuelve a plantear el problema del Ejemplo 4.6 de racionalizar cocientes de elementos en $K[\alpha_1, \ldots, \alpha_n]$. Esto, al igual que el cálculo de polinomios mínimos, se puede seguir haciendo como en el Ejemplo 4.9. Por ejemplo, sea $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$ el cuerpo de descomposición sobre $\mathbb{Q}$ de $X^3 - 2$. Como ya vimos en el Ejemplo 4.14, la extensión $\mathbb{Q} \subset L$ se puede hacer a través de dos extensiones $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset L$. Según vimos en la demostración del Lema 4.7, una base de $\mathbb{Q}(\sqrt[3]{2})$ como espacio vectorial sobre $\mathbb{Q}$ es $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, mientras que una base de L como espacio vectorial sobre $\mathbb{Q}(\sqrt[3]{2})$ es $\{1, \sqrt{3}i\}$. La demostracion del Lema 4.11 nos dice entonces que una base de L como espacio vectorial sobre Q es

$$B = \{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt{3}i, \sqrt[3]{2}\sqrt{3}i, \sqrt[3]{4}\sqrt{3}i\}.$$

Si tomemos el elemento $\beta = \sqrt[3]{2} - \sqrt{3}i$, sí que es fácil en este caso encontrar a ojo un polinomio que se anule en β. En efecto, elevando al cubo la igualdad $\beta + \sqrt{3}i = \sqrt[3]{2}$, obtenemos

$$\beta^3 + 3\sqrt{3}i\beta^2 - 9\beta - 3\sqrt{3}i = 2$$

que reescribimos como

$$\beta^3 - 9\beta - 2 = (-3\beta^2 + 3)\sqrt{3}i.$$

Elevando ahora al cuadrado nos queda

$$\beta^6 - 18\beta^4 - 4\beta^3 + 81\beta^2 + 36\beta + 4 = -3(9\beta^4 - 18\beta^2 + 9)$$

con lo que obtenemos que β es raíz del polinomio $g = X^6 + 9X^4 - 4X^3 + 27X^2 + 36X + 31$ (obsérvese que el orden de las operaciones ha sido determinante, ya que si uno empieza

elevando al cuadrado la igualdad $\beta - \sqrt[3]{2} = \sqrt{3}i$ obtiene una expresión con demasiados radicales). El único problema aquí sería demostrar que el polinomio g el polinomio mínimo de β, es decir, que es irreducible en $\mathbb{Q}[X]$ (el lector paciente lo puede hacer como ejercicio calculando sus raíces, factorizándolo en factores lineales en $\mathbb{C}[X]$ y viendo que no se pueden agrupar factores en $\mathbb{Q}[X]$). Procedemos entonces como en el Ejemplo 4.9, escribiendo las coordenadas respecto de B de las primeras potencias de β:

$$\begin{aligned}
\beta^0 &= (1,0,0,0,0,0)_B \\
\beta^1 &= (0,1,0,-1,0,0)_B \\
\beta^2 &= (-3,0,1,0,-2,0)_B \\
\beta^3 &= (2,-9,0,3,0,-3)_B \\
\beta^4 &= (9,2,-18,-8,12,0)_B \\
\beta^5 &= (-60,45,2,-9,-10,30)_B \\
\beta^6 &= (-23,-90,135,120,-54,-12)_B
\end{aligned}$$

Mirando simplemente el determinante de las coordenadas, se observa que $1, \beta, \beta^2, \beta^3, \beta^4, \beta^5$ son linealmente independientes, luego no hay polinomios no nulos de grado menor o igual que cinco que tengan a β como raíz, luego g es efectivamente el polinomio mínimo de β. Si no lo hubiéramos calculado, bastaría encontrar la combinación lineal $\beta^6 = -31 - 36\beta - 27\beta^2 + 4\beta^3 - 9\beta^4$. Dejamos al lector el ejercicio de usar estas técnicas para escribir β^{-1} en función de la base B.

5. El grupo de Galois

Dado un polinomio f del que sabemos sus raíces, ¿son éstas arbitriamente intercambiables? Si el polinomio es irreducible, el Lema 4.4 parece indicar que sí. El grupo de Galois que vamos a definir consistirá precisamente en las permutaciones "razonables" de las raíces de un polinomio. El siguiente resultado va a ser la base de toda la teoría:

Teorema 5.1. *Sea K un cuerpo, $f \in K[X]$ un polinomio de grado n con raíces $\alpha_1, \ldots, \alpha_n$ (repetida cada una tantas veces como la multiplicidad) en un cuerpo de descomposición $L = K[\alpha_1, \ldots, \alpha_n]$. Entonces:*

(i) Para cada polinomio $H(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, el polinomio

$$h(X) := \Pi_{\sigma \in S_n}(X - h(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$$

tiene sus coeficientes en K.

(ii) Cualquier polinomio irreducible en $K[X]$ que tenga una raíz en L descompone totalmente como producto de factores lineales en $L[X]$.

Demostración: Consideramos el polinomio $\hat{H} := \Pi_{\sigma \in S_n}(X - h(\sigma(X_1), \ldots, \sigma(X_n))$. Visto como polinomio en la indeterminada X, es claro que sus coeficientes son polinomios simétricos en $K[X_1, \ldots, X_n]$. Por tanto, por el Teorema 3.18, los coeficientes de $\hat{H}$ son expresiones polinomiales, con coeficientes en K, en los polinomios simétricos elementales $e_1, \ldots, e_n$. Por tanto, sustituyendo las X_i por las α_i se tiene que los coeficientes de h son expresiones polinomiales, con coeficientes en K, de $e_1(\alpha_1, \ldots, \alpha_n), \ldots, e_n(\alpha_1, \ldots, \alpha_n)$, es decir, de los coeficientes de f (véase el Lema 3.9). Por tanto, los coeficientes de h están en K, lo que demuestra (i).

Para demostrar (ii), sea $g \in K[X]$ un polinomio irreducible y sea $\beta \in L$ una raíz de g. Como $L = K[\alpha_1, \ldots, \alpha_n]$, necesariamente $\beta = H(\alpha_1, \ldots, \alpha_n)$, para algún $H(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$. Además, si consideramos el polinomio $h \in K[X]$ del apartado (i) se tiene $h(\beta) = 0$, ya que, en la fórmula de h, para $\sigma = id$ se obtiene el factor $X - \beta$. Por tanto, h es divisible por el polinomio mínimo de β sobre K. Al ser g irreducible, tal polinomio mínimo será g dividido por el coeficiente de su término de mayor grado. Se sigue entonces que g divide a h (en $K[X]$ y por tanto también en $L[X]$), y al ser $L[X]$ un D.F.U. se concluye que g consiste en el producto de factores irreducibles de h, es decir, de factores lineales. □

Definición. Una *extensión normal* es una extensión algebraica de cuerpos $K \subset L$ tal que todo polinomio irreducible de $K[X]$ con una raíz en L factoriza completamente en $L[X]$.

Ejercicio 5.2. Demostrar que cualquier extensión de grado dos es normal.

Lema 5.3. *Una extensión de cuerpos $K \subset L$ es finita y normal si y sólo si L es el cuerpo de descomposición de un polinomio $f \in K[X]$.*

Demostración: Ya hemos visto que si L es cuerpo de descomposición de un polinomio $f \in K[X]$ entonces $K \subset L$ es finita (Teorema 4.12) y normal (Teorema 5.1), así que sólo hay que ver la otra implicación. Si $K \subset L$ es finita, entonces en particular es algebraica (Lema 4.8). Dados pues $\alpha_1, \ldots, \alpha_n \in L$ que generen la extensión, si $f_1, \ldots, f_n$ son respectivamente sus polinomios mínimos sobre K, se tendrá por la normalidad de la extensión que todas sus raíces están en L. Por tanto, $K(\alpha_1, \ldots, \alpha_n)$ es la mínima extensión de K que contiene todas las raíces de $f_1 \ldots f_n$, es decir, L es el cuerpo de descomposición de $f_1 \ldots f_n$ sobre K. □

Observación 5.4. El lema anterior prueba algo que a priori no es evidente (aunque no es difícil de demostrar): si tenemos una extensión finita y normal $K \subset L$, entonces, para cualquier cuerpo intermedio $K \subset K' \subset L$, la extensión $K' \subset L$ también es normal (ya que L es un cuerpo de descomposición sobre K de un polinomio $f \in K[X]$, luego también es cuerpo de descomposición sobre K' del mismo polinomio, visto como polinomio en $K'[X]$). Sin embargo, la extensión $K \subset K'$ no tiene por qué ser normal. Por ejemplo, la extensión $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt{2}i)$ sabemos que es normal, pero $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ no es normal, ya que el polinomio $X^3 - 2$ tiene una raíz en $\mathbb{Q}(\sqrt[3]{2})$, pero no las otras dos (puesto que son imaginarias y los elementos de $\mathbb{Q}(\sqrt[3]{2})$ son todos reales).

Tampoco es cierto que si $K \subset K'$ y $K' \subset L$ son normales entonces $K \subset L$ sea una extensión normal. Por ejemplo, las extensiones $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$ y $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt[4]{2}]$ son normales por tener grado dos (Ejercicio 5.2), mientras que $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$ no es normal, ya que las raíces imaginarias de $X^4 - 2$ (polinomio mínimo de $\sqrt[4]{2}$ sobre $\mathbb{Q}$) no están en $\mathbb{Q}[\sqrt{2}]$.

Ejemplo 5.5. Veamos cómo funciona el Teorema 5.1 en el cuerpo de descomposición de $f = X^3 - 2$ sobre $\mathbb{Q}$ del Ejemplo 4.14 (del que tomaremos las notaciones). El elemento $\beta = \sqrt[3]{2} - \sqrt{3}i$ se puede escribir como $\beta = \alpha_1 + \frac{(\alpha_2 - \alpha_3)^3}{6}$. Por tanto, el polinomio h que del teorema es

$$h = (X - \alpha_1 - \frac{(\alpha_2 - \alpha_3)^3}{6})(X - \alpha_1 - \frac{(\alpha_3 - \alpha_2)^3}{6})(X - \alpha_2 - \frac{(\alpha_1 - \alpha_3)^3}{6})$$

$$(X - \alpha_2 - \frac{(\alpha_3 - \alpha_1)^3}{6})(X - \alpha_3 - \frac{(\alpha_1 - \alpha_2)^3}{6})(X - \alpha_3 - \frac{(\alpha_2 - \alpha_1)^3}{6})$$

$$= X^6 + 9X^4 - 4X^3 + 27X^2 + 36X + 31$$

que es precisamente el polinomio mínimo de β sobre $\mathbb{Q}$. Si el lector tiene la paciencia de hacer las cuentas a mano y no con ordenador, podrá comprobar que, obrando con la

astucia de ir agrupando términos conjugados, las cuentas son en realidad las que hicimos en el Ejemplo 4.22.

Ejemplo 5.6. Si estudiamos ahora el comportamiento del cuerpo de descomposición de $f = X^4 - 10X^2 + 1$ (Ejemplo 4.15) el comportamiento es completamente distinto. De hecho, como el grado de la extensión es 4, el polinomio mínimo de cualquier elemento del cuerpo de descomposición es al máximo 4, mientras que el polinomio h que nos da el teorema es siempre de grado 24. Por ejemplo, si consideramos $\beta := \alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 = -4\sqrt{2} - 2\sqrt{3}$, su polinomio mínimo sobre $\mathbb{Q}$ es $g = X^4 - 88X^2 + 400$, mientras que el polinomio h que proporciona el teorema anterior es

$$h = (X^4 - 88X^2 + 400)(X^4 - 112X^2 + 1600)(X^2 - 12)^2(X^2 - 48)^2(X^2 - 8)^2(X^2 - 32)^2$$

y tiene, por tanto, más factores aparte de g (el segundo factor tiene como raíces $\pm 2\sqrt{2} \pm 4\sqrt{3}$). El motivo es que, desde el punto de vista algebraico, muchas permutaciones de las raíces no son "admisibles". Por ejemplo, no parece "razonable" aceptar la permutación que intercambia α_1 y α_2 dejando fijas α_3 y α_4. En efecto, si $\sqrt{2} + \sqrt{3} = \alpha_1$ se transforma en $\sqrt{2} - \sqrt{3} = \alpha_2$, lo "lógico" es que $-\sqrt{2} - \sqrt{3} = \alpha_4$ se transforme en $-\sqrt{2} + \sqrt{3} = \alpha_3$. De hecho, cualquier permutación admisible debería estar determinada por la imagen de α_1. En efecto, si por ejemplo α_1 se transforma en α_2, entonces parece razonable imponer que $\alpha_1^3 = 11\sqrt{2} + 9\sqrt{3}$ se transforme en $\alpha_2^3 = 11\sqrt{2} - 9\sqrt{3}$. De este modo, se deduce que $\alpha_2 = \alpha_1^3 - 10\alpha_1$ se debería transformar en $\alpha_2^3 - 10\alpha_2 = \alpha_1$. De este modo, encontramos sólo cuatro permutaciones admisibles de las raíces de f:

La permutación identidad σ_1

La permutación σ_2 que intercambia α_1 con α_2 y α_3 con α_4

La permutación σ_3 que intercambia α_1 con α_3 y α_2 con α_4

La permutación σ_4 que intercambia α_1 con α_4 y α_2 con α_3.

Si en el enunciado del Teorema 5.1 efectuamos el producto sólo para las permutaciones $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ obtendremos un nuevo polinomio a partir de β:

$$\bar{h} = (X - \alpha_1 - 2\alpha_2 - 3\alpha_3 - 4\alpha_4)(X - \alpha_2 - 2\alpha_1 - 3\alpha_4 - 4\alpha_3)$$

$$(X - \alpha_3 - 2\alpha_4 - 3\alpha_1 - 4\alpha_2)(X - \alpha_4 - 2\alpha_3 - 3\alpha_2 - 4\alpha_1)$$

$$= X^4 - 88X^2 + 400 = g$$

que ahora sí es el polinomio mínimo de β. Obsérvese que las permutaciones que hemos obtenido forman un subgrupo de S_4, que además es normal. No es tampoco casualidad que el orden de este subgrupo sea precisamente el grado de la extensión $\mathbb{Q} \subset L$. Observamos finalmente que los elementos de L que quedan fijos por $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ son precisamente los

elementos de $\mathbb{Q}$ (de hecho, por construcción, los coeficientes de $\bar{h}$ quedan fijos por dichas permutaciones, y por eso están en $\mathbb{Q}$).

El ejemplo anterior ilustra bastante bien lo que queremos hacer: quedarnos sólo con las permutaciones convenientes de las raíces de un polinomio. La idea que hay que tener en mente es que mientras más simetrías tengan las raíces, menos permutaciones tendremos que considerar (de hecho el número de permutaciones será el grado de la extensión dada por el cuerpo de descomposición del polinomio). Mientras que Galois en su trabajo trataba con permutaciones de las raíces, nosotros seguiremos el punto de vista moderno de Artin. El ejemplo que hay que tener en mente es el de la extensión $\mathbb{R} \subset \mathbb{C}$. Si vemos $\mathbb{C}$ como cuerpo de descomposición del polinomio $X^2 + 1$, la forma de conseguir todas las raíces de un polinomio $g \in \mathbb{R}[X]$ a partir de una se puede interpretar como permutando i con $-i$ o como conjugando las raíces (y además, $\mathbb{R}$ es el conjunto de elementos de $\mathbb{C}$ que quedan fijos por conjugación). En este sentido, obsérvese que las permutaciones que llamábamos admisibles respetaban la estructura de cuerpo, por lo que permitían definir un automofismo de L, que además dejaba invariantes los puntos de $\mathbb{Q}$. Así que el punto de partida de Artin no es un polinomio con sus raíces, sino directamente el cuerpo de descomposición, y en lugar de considerar permutaciones de raíces considerar "conjugaciones" del cuerpo. La definición precisa es:

Definición. Sea $K \subset L$. Se llama *grupo de Galois* de L sobre K al conjunto $\mathrm{Gal}(L/K)$ de automorfismos $\sigma : L \to L$ tales que $\sigma_{|K} = id_K$ (como cualquier homomorfismo de cuerpos $\sigma : L \to L$ es inyectivo y el Lema 4.2 implica que es además un homomorfismo de espacios vectoriales si $\sigma_{|K} = id_K$, no hay que pedir en la definición que σ sea isomorfismo, ya que es automático). Claramente, $\mathrm{Gal}(L/K)$ tiene estructura de grupo con la composición. Se llama *grupo de Galois de un polinomio* $f \in K[X]$ al grupo $\mathrm{Gal}(f/K) = \mathrm{Gal}(L/K)$, donde L es un cuerpo de descomposición de f sobre K.

La primera observación importante es que, como queríamos, los elementos del grupo de Galois permutan las raíces de los polinomios:

Proposición 5.7. *Sea $K \subset L$ una extensión de cuerpos y sea $\alpha \in L$ una raíz de un polinomio $f \in K[X]$. Entonces:*

(i) Para cualquier $\sigma \in \mathrm{Gal}(L/K)$ se tiene que $\sigma(\alpha)$ es una raíz de f.

(ii) Recíprocamente, si la extensión es finita y normal, y si f es irreducible, cualquier raíz de f es de la forma $\sigma(\alpha)$ para algún $\sigma \in \mathrm{Gal}(L/K)$.

Demostración: Para ver (i), escribimos $f = a_0 + a_1X + \ldots + a_nX^n$, con $a_0, a_1, \ldots, a_n \in K$. Que α sea raíz de f quiere decir $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. Aplicando σ y teniendo en

cuenta que es un isomorfismo de cuerpos que deja fijo K, tendremos

$$0 = \sigma(a_0 + a_1\alpha + \ldots + a_n\alpha^n) = a_0 + a_1\sigma(\alpha) + \ldots + a_n\sigma(\alpha)^n$$

lo que implica que $\sigma(\alpha)$ también es una raíz de f.

Sea ahora α' otra raíz de f y supongamos que f es irreducible. Por el Lema 4.7 tendremos un isomorfismo $\sigma' : K(\alpha) \cong K[X]/(f) \cong K(\alpha')$ tal que $\sigma'_{|K} = id_K$ y $\sigma'(\alpha) = \alpha'$. Por otra parte, la extensión $K \subset L$ es finita y normal, luego (por el Lema 5.3) L es el cuerpo de descomposición sobre K de un polinomio g. Es evidente entonces que L es también el cuerpo de descomposición de g sobre $K(\alpha)$. Por tanto, como claramente $\sigma'(g) = g$, podemos aplicar el Teorema 4.12(ii) (tomando $L' = L$) y obtenemos que existe un monomorfismo de cuerpos $\sigma : L \to L$ tal que $\sigma_{|K(\alpha)} = \sigma'$. En particular, $\sigma(\alpha) = \alpha'$ y $\sigma_{|K} = id_K$. Esto último muestra (Lema 4.2) que σ es también homomorfismo de espacios vectoriales, y al ser inyectivo es biyectivo también. Por tanto, σ es un isomorfismo de cuerpos, por lo que es el elemento de $\mathrm{Gal}(L/K)$ que buscábamos para demostrar (ii). □

La relación entre el punto de vista de Galois y el de Artin viene dada por el siguiente resultado.

Lema 5.8. *Sea $f \in K[X]$ un polinomio con raíces distintas $\alpha_1, \ldots, \alpha_n$. Entonces existe un monomorfismo natural de grupos $i : \mathrm{Gal}(f/K) \to S_n$, identificando S_n con el grupo de las permutaciones del conjunto $\{\alpha_1, \ldots, \alpha_n\}$.*

Demostración: Sea L un cuerpo de descomposición de f sobre K. Como por la Proposición 5.7(i) cualquier $\sigma \in \mathrm{Gal}(L/K)$ manda las raíces de f en raíces de f, tiene sentido definir $i : \mathrm{Gal}(L/K) \to S_n$ como $i(\sigma) = \sigma_{|\{\alpha_1,\ldots,\alpha_n\}}$. Además, como $L = K(\alpha_1, \ldots, \alpha_n)$, se tiene que cualquier σ está unívocamente determinado por sus valores en $\alpha_1, \ldots, \alpha_n$, con lo que i (que es claramente un homomorfismo de grupos) es inyectiva. □

Obsérvese que el lema anterior nos está diciendo cómo se puede interpretar el grupo de Galois de un polinomio $f \in K[X]$: es el subgrupo de aquellas permutaciones de sus raíces que se pueden extender a automorfismos de su cuerpo de descomposición. El siguiente ejemplo nos va a mostrar cuál tiene que ser nuestra estrategia en lo que sigue.

Ejemplo 5.9. Volvemos al Ejemplo 5.6, visto ahora como $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Obsérvese que, con este punto de vista, el Lema 5.8 se puede mejorar. En efecto, L se puede ver como el cuerpo de descomposición de $(X^2-2)(X^2-3)$ sobre $\mathbb{Q}$ (lo que de paso permite observar que un mismo cuerpo puede ser cuerpo de descomposición de distintos polinomios). Entonces, por la Proposición 5.7(i), cualquier elemento de $\mathrm{Gal}(L/\mathbb{Q})$ manda $\sqrt{2}$ a una raíz de X^2-2, es decir, $\pm\sqrt{2}$, y $\sqrt{3}$ a una raíz de X^2-3, es decir, $\pm\sqrt{3}$. Es decir, que podemos mejorar

el Lema 5.8 para concluir, con la misma demostración, que tenemos un monomorfismo de grupos:

$$i' : \mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow S_2 \times S_2$$
$$\sigma \mapsto (\sigma_{|\{\sqrt{2},-\sqrt{2}\}}, \sigma_{|\{\sqrt{3},-\sqrt{3}\}}).$$

Por tanto, $\mathrm{Gal}(L/\mathbb{Q})$ tendrá al máximo cuatro elementos. Por otra parte, recordando que L es el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $f(X) = X^4 - 10X^2 + 1$, que tiene cuatro raíces distintas $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, la Proposición 5.7(ii) implica (tomando $\alpha = \alpha_1$) que existen $\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in \mathrm{Gal}(L/\mathbb{Q})$ tales que

$$\sigma_1(\alpha_1) = \alpha_1$$
$$\sigma_2(\alpha_1) = \alpha_2$$
$$\sigma_3(\alpha_1) = \alpha_3$$
$$\sigma_3(\alpha_1) = \alpha_3$$

Como $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ son raíces distintas, entonces $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ son distintos, con lo que $\mathrm{Gal}(L/\mathbb{Q})$ tiene al menos cuatro elementos. Comparando con el resultado anterior, llegamos a que i' es un isomorfismo y que las cuatro "permutaciones admisibles" que habíamos encontrado en el Ejemplo 5.6 dan lugar a automorfismos de L sobre $\mathbb{Q}$. Usando la base $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ de L sobre $\mathbb{Q}$ (que se obtiene del Lema 4.11), tenemos entonces que el grupo de Galois está formado por los elementos

$$\sigma_1 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$
$$\sigma_2 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$
$$\sigma_3 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$
$$\sigma_4 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mapsto a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}.$$

El procedimiento visto en este ejemplo nos da la pista de los pasos que podemos seguir en una extensión normal finita general $K \subset L$:

–Acotar el orden del grupo de Galois $\mathrm{Gal}(L/K)$ por el grado de la extensión $[L : K]$.

–Tratar de escribir la extensión como extensión simple $K \subset L = K[\alpha]$ generada por un elemento primitivo $\alpha \in L$. Entonces, $[L : K]$ será el grado del polinomio mínimo de α sobre K.

–Ver en qué condiciones podemos asegurar que todas las raíces del polinomio mínimo de α sobre K son todas distintas. En tal caso, la Proposición 5.7(ii) nos garantizará que $\mathrm{Gal}(L/K)$ tiene al menos tantos elementos como el grado del polinomio mínimo, que es precisamente $[L : K]$.

La acotación del orden del grupo de Galois por el grado de la extensión se puede hacer de forma simple y en el caso más general:

Lema 5.10. *Sea $K \subset L$ una extensión normal finita. Entonces:*

(i) Para cada $\alpha \in L$ se tiene $|\operatorname{Gal}(L/K)| = n|\operatorname{Gal}(L/K(\alpha))|$, donde n es el número de raíces distintas del polinomio mínimo de α sobre K.

(ii) $|\operatorname{Gal}(L/K)| \leq [L : K]$.

Demostración: Sea f el polinomio mínimo de α sobre K y sean $\alpha_1, \ldots, \alpha_n$ las raíces distintas de f (que están en L por ser la extensión normal). Para cada $\sigma : L \to L$ en $\operatorname{Gal}(L/K)$, por la Proposición 5.7(i) se tiene que $\sigma(\alpha)$ es una raíz de de f, luego $\sigma(\alpha) = \alpha_i$ para algún $i \in \{1, \ldots, n\}$. Si para cada $i = 1, \ldots, n$ definimos

$$\Sigma_i = \{\sigma \in \operatorname{Gal}(L/K) \mid \sigma(\alpha) = \alpha_i\}$$

tendremos que $\operatorname{Gal}(L/K)$ es la unión disjunta de $\Sigma_1, \ldots, \Sigma_n$, con lo que bastará demostrar que cada Σ_i tiene el mismo cardinal que $\operatorname{Gal}(L/K(\alpha))$. En primer lugar, por la Proposición 5.7(ii), Σ_i es no vacío, luego podemos fijar $\sigma_i \in \Sigma_i$. Entonces, para cada $\sigma \in \Sigma_i$ se tiene que $\sigma_i^{-1} \circ \sigma$ es un automorfismo de L que deja fijo α y K, luego está en $\operatorname{Gal}(L/K(\alpha))$. Claramente, esto define una biyección $\Sigma_i \to \operatorname{Gal}(L/K(\alpha))$ (la inversa es $\tau \mapsto \sigma_i \circ \tau$), lo que concluye la demostración de (i).

La demostración de (ii) se hace por inducción sobre $[L : K]$. El caso $[L : K] = 1$ es trivial, ya que entonces $L = K$ y el único elemento de $\operatorname{Gal}(L/K)$ sería el automorfismo identidad. Si $[L : K] > 1$, tomamos $\alpha \in L \setminus K$. Entonces $[K(\alpha) : K] > 1$, con lo que $[L : K(\alpha)] = \frac{[L:K]}{[K(\alpha):K]} < [L : K]$ y, aplicando la hipótesis de inducción a la extensión $K(\alpha) \subset L$, tendremos $|\operatorname{Gal}(L/K(\alpha))| \leq [L : K(\alpha)]$. Si llamamos ahora n al número de raíces distintas del polinomio mínimo de α sobre K, es claro que $n \leq [K(\alpha) : K]$ (ya que $[K(\alpha) : K]$ es el grado de dicho polinomio mínimo). Entonces, usando la parte (i) tenemos $|\operatorname{Gal}(L/K)| = n|\operatorname{Gal}(L/K(\alpha))| \leq [K(\alpha) : K][L : K(\alpha)] = [L : K]$. □

El resultado anterior nos ratifica en la necesidad de obtener raíces distintas para polinomios. Veamos primero un caso patológico.

Ejemplo 5.11. Consideremos $K = \mathbb{Z}_p(t)$ (cuerpo de fracciones del anillo de polinomios con coeficientes en el cuerpo $\mathbb{Z}_p$) y sea $f = X^p - t \in K[X]$. Como $f' = 0$, se tiene que f tiene raíces repetidas. De hecho, si α es una raíz de f, entonces $\alpha^p = t$, luego $f = X^p - \alpha^p = (X - \alpha)^p$ (ver Ejercicio 1.13). Por tanto, f tiene en realidad una única raíz (con multiplicidad p), con lo que su cuerpo de descomposición es $K[\alpha] \cong K[X]/(f)$ y $\operatorname{Gal}(K[\alpha]/K)$ es un grupo trivial.

Definición. Un *polinomio separable sobre un cuerpo* K es un polinomio $f \in K[X]$ tal que ninguna componente irreducible de f tiene raíces múltiples (en un cuerpo de descomposición de f sobre K. Una *extensión separable* es una extensión $K \subset L$ en que el polinomio mínimo sobre K de cada elemento de L algebraico sobre K es un polinomio separable.

Observación 5.12. El Ejemplo 5.11 muestra que la noción de separabilidad depende del cuerpo K. En efecto, $f = X^p - t$ no es separable sobre $K = \mathbb{Z}_p(t)$, mientras que sí lo es sobre $K[\alpha]$, ya que, al ser $f = (X - \alpha)^p$, tiene un único factor irreducible: $X - \alpha$, que obviamente no tiene raíces múltiples (debe notarse que, para otros autores, la definición de separabilidad es que el polinomio no tenga raíces múltiples, con lo que el polinomio anterior no sería separable ni sobre $K[\alpha]$; de hecho, ccon tal definición, la separabilidad no depende del cuerpo base y es equivalente a que la resultante del polinomio y su derivada sea distinta de cero). En cualquier caso, la propiedad de separabilidad se conserva si ampliamos el cuerpo K, es decir, si $K \subset K'$ es una extensión y f es separable sobre K, entonces también lo es sobre K'. En efecto, cada factor irreducible g de f en $K'[X]$ es necesariamente un factor de un factor irreducible h de f en $K[X]$. Y como h no tiene raíces múltiples, tampoco las tiene g.

Observación 5.13. Cuando K tiene característica cero, entonces la derivada de cualquier polinomio f de grado d tiene grado $d - 1$, luego si f es irreducible, no puede compartir ningún factor con f', luego f es separable. Por tanto, en característica cero todas las extensiones son separables. Cuando la característica de K es un número primo p, el único modo de que un polinomio irreducible $f \in K[X]$ contenga raíces múltiples (es decir, raíces comunes con su derivada) es que f' sea el polinomio cero, por lo que f sólo puede tener monomios de grado un múltiplo de p.

El siguiente resultado nos muestra que ya con la condición de separabilidad obtenemos que el orden del grupo de Galois coincide con el grado de la extensión:

Teorema 5.14. *Sea $K \subset L$ una extensión finita y normal. Entonces son equivalentes:*

(i) *L es el cuerpo de descomposición de un polinomio separable $f \in K[X]$.*

(ii) $|\operatorname{Gal}(L/K)| = [L : K]$.

(iii) *Los únicos elementos de L que quedan fijos por todos los automorfismos de* $\operatorname{Gal}(L/K)$ *son los de K.*

(iv) *$K \subset L$ es una extensión separable.*

Demostración:

$(i) \Rightarrow (ii)$: Lo demostraremos por inducción sobre $[L : K]$, siendo trivial el caso $[L : K] = 1$. Supongamos entonces $[L : K] > 1$, con lo que f tendrá algún factor irreducible f_1 (que podemos suponer mónico) de grado $n > 1$. Si α es una raíz de f_1, entonces f_1 es su polinomio mínimo sobre K y se tendrá $[K(\alpha) : K] = n$. Además, como f es separable, f_1 tiene n raíces distintas. Podemos aplicar entonces el Lema 5.10(i) y concluir que, $|\operatorname{Gal}(L/K)| = n|\operatorname{Gal}(L/K(\alpha))|$. Por otra parte, como $[L : K] = [L : K(\alpha)][K(\alpha) : K] = n[L : K(\alpha)]$ y $n > 1$, entonces $[L : K(\alpha)] < [L : K]$ y, por hipótesis de inducción

$|\operatorname{Gal}(L/K(\alpha)| = [L : K(\alpha)]$ (obsérvese que L es el cuerpo de descomposición de f sobre $K(\alpha)$ y que f es también separable sobre $K(\alpha)$). Por tanto, $|\operatorname{Gal}(L/K)| = n[L : K(\alpha)] = [L : K]$.

$(ii) \Rightarrow (iii)$: Sea $\alpha \in L \setminus K$, y veamos que existe $\sigma \in \operatorname{Gal}(L/K)$ tal que $\sigma(\alpha) \neq \alpha$. En efecto, sea f el polinomio mínimo de α sobre K y sea n el número de raíces distintas de f. Por la Proposición 5.7(ii), bastará ver que $n \geq 2$, porque si f tiene al menos una raíz $\alpha' \neq \alpha$ entonces existe $\sigma \in \operatorname{Gal}(L/K)$ tal que $\sigma(\alpha) = \alpha' \neq \alpha$. Para ver que $n \geq 2$ aplicamos sucesivamente las partes (i) y (ii) del Lema 5.10 y tenemos que $|\operatorname{Gal}(L/K)| = n|\operatorname{Gal}(L/K(\alpha)| \leq n[L : K(\alpha)]$. Por otra parte, por hipótesis tenemos que $|\operatorname{Gal}(L/K)| = [L : K] = [K(\alpha) : K][L : K(\alpha)]$. Por tanto, $n \geq [K(\alpha) : K]$ (lo que en realidad implica la igualdad), y como $[K(\alpha) : K] > 1$ por ser $\alpha \notin K$ se sigue que $n \geq 2$.

$(iii) \Rightarrow (iv)$: Sea $\alpha \in L$, y veamos que su polinomio mínimo f sobre K no tiene raíces múltiples. Sean $\alpha_1, \ldots, \alpha_n$ las raíces distintas de f (que están todas en L, por ser la extensión $K \subset L$ normal). Como para cualquier $\sigma \in \operatorname{Gal}(L/K)$ se tiene (por la Proposición 5.7(i)) que cada $\sigma(\alpha_i)$ es otro α_j, entonces se tiene que el polinomio $g(X) = (X - \alpha_1) \ldots (X - \alpha_n) \in L[X]$ es invariante al aplicarle cualquier $\sigma \in \operatorname{Gal}(L/K)$, es decir, que sus coeficientes son fijos al aplicarle cualquier $\sigma \in \operatorname{Gal}(L/K)$. Por hipótesis, esto quiere decir que g está en $K[X]$, por lo que debe ser $f = g$, luego las raíces de f son todas distintas.

$(iv) \Rightarrow (i)$: Por el Lema 5.3, L es cuerpo de de descomposición sobre K de un polinomio $f \in K[X]$, que es separable por ser la extensión separable. □

Definición. Se llama *extensión de Galois* a una extensión de cuerpos $K \subset L$ que L está en las condiciones del Teorema 5.14. En particular, una condición necesaria y suficiente es que L sea cuerpo de descomposición de un polinomio separable sobre K.

Observación 5.15. En característica cero, todas las extensiones son separables (Observación 5.13), luego el Teorema 5.14 dice que, en este caso, cualquier extensión finita y normal es de Galois, es decir, verifica las propiedades (ii) y (iii). Tales propiedades son falsas si la extensión no es normal. Consideremos, por ejemplo, la extensión $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$, que no es normal (Observación 5.4). La propiedad (ii) no se satisface porque cualquier elemento $\sigma \in \operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ debe mandar $\sqrt[3]{2}$ a una raíz de $X^3 - 2$ que esté en $\mathbb{Q}(\sqrt[3]{2})$, luego necesariamente $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ y por tanto $\operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$. Así, el orden de $\operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ es uno, mientras que el grado de la extensión $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ es tres, en contraposición con (ii). Por otra parte, al ser $\operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{id\}$, es evidente que cualquier elemento de $\mathbb{Q}(\sqrt[3]{2})$, aunque no esté en $\mathbb{Q}$, es invariante por todos los elementos de $\operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, en contraste con (iii).

Del Teorema 5.14 podemos obtener un primer resultado característico de teoría de Galois, en el sentido de que podemos dar información sobre el grupo de Galois de un polinomio sin conocer las raíces del mismo:

Corolario 5.16. *Sea $f \in K[X]$ un polinomio separable con raíces $\alpha_1, \ldots, \alpha_n$ y sea i el monomorfismo del Lema 5.8. Entonces la imagen de i está contenida en A_n si y sólo si $\Delta \in K$.*

Demostración: Sea L un cuerpo de descomposición de f. Por el Teorema 5.14(iii) tendremos que $\Delta \in K$ si y sólo si $\sigma(\Delta) = \Delta$ para todo $\sigma \in \mathrm{Gal}(L/K)$. Como $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$, para cualquier $\sigma \in \mathrm{Gal}(L/K)$ se tiene $\sigma(\Delta) = \prod_{i<j}(\sigma(\alpha_i) - \sigma(\alpha_j))$, que por la Observación 3.15 es $\mathrm{sgn}(i(\sigma))\Delta$ (identificando mediante i el automorfismo σ con la permutación $i(\sigma)$). Es decir, que $\Delta \in K$ si y sólo si $\mathrm{sgn}(i(\sigma)) = 1$ para todo $\sigma \in \mathrm{Gal}(L/K)$, o sea si y sólo si $i(\sigma) \in A_n$ para todo $\sigma \in \mathrm{Gal}(L/K)$. □

El Teorema 5.14 muestra que las extensiones de Galois funcionan como queríamos al final del Ejemplo 5.6:

Corolario 5.17. *Sea $K \subset L$ una extensión de Galois y sea $\alpha \in L$, entonces el polinomio $g := \Pi_{\sigma \in \mathrm{Gal}(L/K)}(X - \sigma(\alpha))$ es un polinomio en $K[X]$. En particular, g es el polinomio mínimo de α sobre K si y sólo si $L = K(\alpha)$.*

Demostración: Es claro que los coeficientes de g son invariantes por los elementos de $\mathrm{Gal}(L/K)$. Por tanto, la parte (iii) del teorema implica que están en K, con lo que $g \in K[X]$. Además, g es el polinomio mínimo de α sobre K si y sólo si el grado de la extensión $K \subset K(\alpha)$ es el grado de g, que es $|\mathrm{Gal}(L/K)|$, que por el Teorema 5.14(iii) es también $[L : K]$. Ahora bien, $[K(\alpha) : K] = [L : K]$ es claramente equivalente a $L = K(\alpha)$. □

Cabe preguntarse si uno puede esperarse que existan elementos α como en el Corolario 5.17 (i.e. elementos primitivos de la extensión). El siguiente resultado (y su demostración) muestra que cualquier combinación lineal suficientemente general de los generadores de la extensión es un elemento primitivo.

Teorema 5.18 (del elemento primitivo)**.** *Sea $K \subset L$ una extensión de Galois. Entonces la extensión es simple, es decir, existe $\alpha \in L$ tal que $L = K(\alpha)$.*

Demostración: Si K es finito, la extensión es simple por el Ejemplo 4.16, por lo que supondremos que K es infinito. Como la extensión es finita, en particular es finitamente generada, as íque podemos escribir $L = K(\gamma_1, \ldots, \gamma_r)$. Demostremos el enunciado por inducción sobre r. Si $r = 1$, no hay nada que demostrar. Sea $r \geq 2$ y supongamos

demostrado el teorema para extensiones generadas por $r-1$ elementos. La extensión $K(\gamma_1,\ldots,\gamma_{r-2}) \subset K(\gamma_1,\ldots,\gamma_{r-2})(\gamma_{r-1},\gamma_r) = L$ es también de Galois, luego si supiéramos que el resultado es cierto para $r=2$ tendríamos que existiría $\gamma'_{r-1} \in L$ tal que $L = K(\gamma_1,\ldots,\gamma_{r-2},\gamma'_{r-1})$, y por hipótesis de inducción la extensión $K \subset L$ sería simple.

En definitiva, basta demostrar el resultado cuando L es de la forma $L = K(\alpha,\beta)$. La idea es demostrar que existe $\lambda \in K \setminus \{0\}$ tal que $L = K(\alpha+\lambda\beta)$. Como evidentemente $K(\alpha+\lambda\beta) \subset L$, hay que encontrar un λ tal que $L \subset K(\alpha+\lambda\beta)$, es decir, $\alpha,\beta \in K(\alpha+\lambda\beta)$. Como $\alpha = (\alpha+\lambda\beta)-\lambda\beta$, basta demostrar es que existe $\lambda \in K\setminus\{0\}$ tal que $\beta \in K(\alpha+\lambda\beta)$, porque entonces automáticamente α también estará en $K(\alpha+\lambda\beta)$.

La idea es entonces ver que $X-\beta$ está en $K(\alpha+\lambda\beta)[X]$ para una buena elección de λ, que es lo mismo que decir que $X-\beta$ es el polinomio mínimo de β sobre $K(\alpha+\lambda\beta)$. Para ello vamos a construir primero un par de polinomios que tengan a β como raíz. Uno de ellos es evidentemente el polinomio mínimo de β sobre K, que será un polinomio $g \in K[X]$ (y por tanto estará en cualquier $K(\alpha+\lambda\beta)[X]$). Como la extensión $K \subset L$ es separable, podremos escribir $g(X) = (X-\beta_1)\ldots(X-\beta_m)$, con $\beta_1,\ldots,\beta_m \in L$, todas ellas distintas, y por ejemplo $\beta_1 = \beta$. Si $h \in K(\alpha+\lambda\beta)[X]$ es el polinomio mínimo de β sobre $K(\alpha+\lambda\beta)$, entonces $h|g$, y por tanto h descompondrá en $L[X]$ como $h(X) = (X-\beta)(X-\beta_{j_1})\ldots(X-\beta_{j_r})$ (con $j_1,\ldots,j_r \in \{2,\ldots,m\}$), y lo que queremos ver es que sólo tenemos el primer factor.

Consideramos ahora $f \in K[X]$, el polinomio mínimo de α sobre K. Para obtener a partir de él un polinomio que se anule en β, definimos para cada $\lambda \in K\setminus\{0\}$ el polinomio $\tilde{f}_\lambda(X) := f(\alpha+\lambda\beta-\lambda X)$, que está en $K(\alpha+\lambda\beta)[X]$. Por tanto, $h|\tilde{f}_\lambda$, y se tendrá $\tilde{f}_\lambda(\beta_{j_1}) = \ldots = \tilde{f}_\lambda(\beta_{j_r}) = 0$. Esto implica que, si encontramos λ tal que $\tilde{f}_\lambda(\beta_j) \neq 0$ para cada $j = 2,\ldots,m$, entonces necesariamente $h(X) = X-\beta$, que es lo que queremos demostrar.

Si ocurriera $\tilde{f}_\lambda(\beta_j) = 0$, con $j \in \{2,\ldots,m\}$, entonces $f(\alpha+\lambda\beta-\lambda\beta_j) = 0$, lo que querría decir que $\alpha+\lambda\beta-\lambda\beta_j$ sería una raíz de f. Si $\alpha_1,\ldots,\alpha_n$ son las raíces de f, entonces sería $\alpha+\lambda\beta-\lambda\beta_j = \alpha_i$ para algún $i \in \{1,\ldots,n\}$, es decir, $\lambda = \frac{\alpha-\alpha_i}{\beta_j-\beta}$. Como K es infinito, podemos entonces escoger $\lambda \neq \frac{\alpha-\alpha_i}{\beta_j-\beta}$ para todo $i = 1,\ldots,n$ y $j = 2,\ldots,m$ (en particular $\lambda \neq 0$), y por tanto tendremos $\tilde{f}_\lambda(\beta_j) \neq 0$ para $j = 2,\ldots,m$, lo que demuestra, como hemos indicado, que $h = X-\beta$ y de aquí $\beta \in K(\alpha+\lambda\beta)$ y $K(\alpha+\lambda\beta)$. □

Observación 5.19. Un estudio atento de la demostración anterior muestra que el resultado sigue siendo cierto si sólo pedimos que la extensión $K \subset L$ sea finita y separable, aunque no sea necesariamente normal. La única diferencia es que entonces las raíces de f y g estarán en un cuerpo mayor que L.

Podemos demostrar ya los resultados centrales de la teoría de Galois:

Teorema 5.20. *Sea $K \subset L$ una extensión de Galois con $G = \mathrm{Gal}(L/K)$. Entonces:*

(i) Si $K \subset K' \subset L$ es un cuerpo intermedio, la extensión $K' \subset L$ es de Galois, y su grupo de Galois es un subgrupo $H < G$ con $|H| = [L : K']$ y $[G : H] = [K' : K]$. Además, $K' = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$

(ii) Recíprocamente, dado cualquier subgrupo $H < G$, sea $K' = L^H$, donde

$$L^H := \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}.$$

Entonces $K \subset K' \subset L$ y $\mathrm{Gal}(L/K') = H$.

Por tanto, las asignaciones $K' \mapsto \mathrm{Gal}(L/K')$ y $H \mapsto L^H$ definen aplicaciones inversas la una de la otra (en particular biyecciones) entre el conjunto de cuerpos intermedios de la extensión $K \subset L$ y subgrupos de $\mathrm{Gal}(L/K)$.

Demostración: (i) es inmediato del Teorema 5.14.

Para (ii), obtenemos de (i) que el orden de $\mathrm{Gal}(L/K')$ es $[L : K']$, mientras que por la definición de K' es evidente que $H \subset \mathrm{Gal}(L/K')$. Así que basta demostrar que $[L : K'] \leq |H|$. Por el teorema del elemento primitivo, podemos encontrar $\alpha \in L$ tal que $L = K'(\alpha)$. De la misma forma que en el Corolario 5.17, podemos considerar el polinomio $g = \Pi_{\sigma \in H}(X - \sigma(\alpha))$, que estará en $K'[X]$ (por definición de K', ya que sus coeficientes son invariantes por los elementos de H) y tiene grado $|H|$. Por tanto, g debe ser divisible por el polinomio mínimo de α sobre K', que tiene grado $[L : K']$, luego $[L : K'] \leq |H|$. □

La biyección entre del teorema anterior entre cuerpos intermedios de una extensión y el grupo de Galois de la extensión se llama *correspondencia de Galois*. El siguiente resultado nos dirá que en esta biyección las extensiones normales se corresponden con los subgrupos normales del grupo de Galois.

Teorema 5.21. *Sea $K \subset L$ una extensión de Galois y sea $K \subset K' \subset L$ un cuerpo intermedio. Entonces son equivalentes:*

(i) $\mathrm{Gal}(L/K')$ es un subgrupo normal de $\mathrm{Gal}(L/K)$.

(ii) $K \subset K'$ es una extensión normal.

(iii) Cualquier elemento $\sigma \in \mathrm{Gal}(L/K)$ verifica que $\sigma(K') \subset K'$.

(iv) Cualquier elemento $\sigma \in \mathrm{Gal}(L/K)$ verifica que $\sigma(K') = K'$.

Además, en estas condiciones, $\mathrm{Gal}(L/K)/\mathrm{Gal}(L, K') \cong \mathrm{Gal}(K'/K)$.

Demostración:

(i) $\Rightarrow$ (ii): Sea $f \in K[X]$ un polinomio irreducible con una raíz $\alpha \in K'$. Necesitamos ver que las demás raíces de f están en K'. Por la Proposición 5.7(ii) las raíces de f son de la

forma $\sigma(\alpha)$, con $\sigma \in \mathrm{Gal}(L/K)$. Para ver que están en K', hay que ver (por el Teorema 5.20(i)) que son invariantes por cada $\tau \in \mathrm{Gal}(L/K')$. En efecto, como $\mathrm{Gal}(L/K')$ es un subgrupo normal de $\mathrm{Gal}(L/K)$, se tiene que $\sigma^{-1}\tau\sigma$ está en $\mathrm{Gal}(L/K')$, por lo que deja fijo α, es decir,

$$\tau(\sigma(\alpha)) = \sigma(\sigma^{-1}\tau\sigma(\alpha)) = \sigma(\alpha)$$

lo que concluye que $\sigma(\alpha)$ está en K'.

$(ii) \Rightarrow (iii)$: Sean $\sigma \in \mathrm{Gal}(L/K)$ y $\alpha \in K'$, y queremos ver que $\sigma(\alpha)$ también está en K'. Sea $f \in K[X]$ el polinomio mínimo de α sobre K. Por la Proposición 5.7(i), $\sigma(\alpha)$ es una raíz de f. Y como la extensión $K \subset K'$ es normal, todas las raíces de f están en K', por lo que $\sigma(\alpha) \in K'$.

$(iii) \Rightarrow (iv)$: Por el Lema 4.2, cada elemento $\sigma \in \mathrm{Gal}(L/K)$ es un isomorfismo de espacios vectoriales. Por tanto, $\sigma(K')$ es un subespacio vectorial de la misma dimensión que K‘. Como por hipótesis $\sigma(K') \subset K'$, se sigue que ambos espacios son necesariamente iguales.

$(iv) \Rightarrow (i)$: Por hipótesis podemos definir un homomorfismo de grupos $\rho : \mathrm{Gal}(L/K) \to \mathrm{Gal}(K'/K)$ mediante $\sigma \mapsto \sigma_{|K'}$. Como $\mathrm{Gal}(L/K')$ es claramente el núcleo del homomorfismo, se tiene que es un subgrupo normal. Además, ρ es un epimorfismo por el Teorema 4.12 (véase la demostración de la Proposición 5.7(ii)), lo que demuestra la afirmación final del enunciado (por el primer teorema de isomorfía). □

Terminamos la sección con algunos ejemplos prácticos de aplicación de la teoría de Galois.

Ejemplo 5.22. Retomamos el Ejemplo 5.9 de la extensión $\mathbb{Q} \subset L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ahora que hemos completado todos los pasos que nos sugería. Ya vimos que $\mathrm{Gal}(L/\mathbb{Q})$ era isomorfo a $S_2 \times S_2$, es decir, a $\mathbb{Z}_2 \times \mathbb{Z}_2$ y que estaba formado por los automorfismos que denotábamos $\sigma_1, \sigma_2, \sigma_3, \sigma_4$, donde σ_1 era la identidad. Por tanto, los subgrupos no triviales de $\mathrm{Gal}(L/\mathbb{Q})$ son los subgrupos generados por $\sigma_2, \sigma_3, \sigma_4$. Claramente, sus respectivos cuerpos fijos son $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, y $\mathbb{Q}(\sqrt{6})$, que por tanto son los únicos cuerpos intermedios. Todas las extensiones de $\mathbb{Q}$ a los cuerpos intermedios son normales, ya que de hecho todos $\mathrm{Gal}(L/\mathbb{Q})$ es abeliano, luego todos sus subgrupos son normales.

Ejemplo 5.23. Si tomamos ahora el ejemplo de la extensión $\mathbb{Q} \subset L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$, como sabemos que tiene grado seis y que L es el cuerpo de descomposición de $f = X^3 - 2$, entonces necesariamente el grupo de Galois (que es un subgrupo de orden seis del grupo de permutaciones de las raíces de f) es el grupo simétrico S_3 de todas las permutaciones de las tres raíces de f. Por tanto, los únicos subgrupos no triviales son de orden dos (que necesariamente están generados por alguna de las tres transposiciones) o de orden tres (que es necesariamente el generado por uno de los dos 3-ciclos), a los que respectivamente

corresponden tres cuerpos intermedios de grado tres y un cuerpo intermedio de grado dos. Concretamente, los cuerpos intermedios son $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}(\frac{-1+\sqrt{3}i}{2}))$, $\mathbb{Q}(\sqrt[3]{2}(\frac{-1-\sqrt{3}i}{2}))$ y $\mathbb{Q}(\sqrt{3}i)$. De éstos, sólo la extensión $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}i)$ es normal, que corresponde al subgrupo generado por un 3-ciclo, el único normal.

Observación 5.24. Nótese también que la correspondencia de Galois sirve para demostrar que hay muchos elementos primitivos, y también permite calcularlos, sin necesidad de recurrir a la demostración del Teorema 5.18. En efecto, si $\alpha \in L$ no es un elemento primitivo de $K \subset L$, entonces $K(\alpha)$ es un cuerpo intermedio no trivial. Si $K \subset L$ es una extensión de Galois, entonces, como $\mathrm{Gal}(L/K)$ es un grupo finito, habrá una cantidad finita de cuerpos intermedios no triviales de $K \subset L$. Visto cada cuerpo intermedio como un subespacio vectorial de L, α está en una unión finita de subespacios vectoriales propios de L. Por ejemplo, en el Ejemplo 5.22, cualquier α fuera de $\mathbb{Q}(\sqrt{2}) \cup \mathbb{Q}(\sqrt{3}) \cup \mathbb{Q}(\sqrt{6})$ es primitivo. Más aún, si α no es primitivo, como $K(\alpha)$ no es el total corresponde a un subgrupo $\mathrm{Gal}(L/K(\alpha))$ que no consiste sólo en la identidad. Esto confirma, una vez más todavía, que $\sqrt{2}+\sqrt{3}$ es un elemento primitivo de la extensión del Ejemplo 5.22, ya que no queda fijo por ningún elemento del grupo de Galois.

Ejemplo 5.25. Estudiemos ahora el grupo de Galois para extensiones de cuerpos finitos. Ya vimos en la demostración de Teorema 4.13 que todo cuerpo finito L de orden p^n es cuerpo de descomposición sobre $\mathbb{Z}_p$ del polinomio $f(X) = X^{p^n} - X$, que tiene todas sus raíces distintas, luego es separable. Por tanto, la extensión $\mathbb{Z}_p \subset L$ es de Galois, y como $[L : \mathbb{Z}_p] = n$, entonces $\mathrm{Gal}(L/Z_p)$ tiene orden n. Veamos que $\mathrm{Gal}(L/Z_p)$ es cíclico generado por el llamado *automorfismo de Fröbenius* $\sigma : L \to L$ definido por $\sigma(\alpha) = \alpha^p$. En primer lugar, es un homomorfismo de anillos por el Ejercicio 1.13, y es la identidad sobre $\mathbb{Z}_p$ (por el Pequeño Teorema de Fermat), luego es un elemento de $\mathrm{Gal}(L/Z_p)$. Basta ver entonces que su orden es exactamente n. Esto es inmediato, porque si $k < n$ el polinomio $X^{p^k} - X$ tiene a lo más $p^k < p^n$ raíces, luego extiste algún $\alpha \in L$ tal que $\sigma^k(\alpha) = \alpha^{p^k} \neq \alpha$.

Si L contiene un cuerpo K, necesariamente también tiene característica p, luego tendremos $\mathbb{Z}_p \subset K \subset L$. Entonces $|K| = p^{n'}$, donde $n' = [K : \mathbb{Z}_p]$; y si $m = [L : K] = \frac{n}{n'}$, entonces por la correspondencia de Galois K corresponde a un subgrupo de $\mathrm{Gal}(L/Z_p)$ de orden m. Por el Ejercicio, 1.7, tal subgrupo es único, y está generado por $\sigma^{n'}$. Por tanto, L tiene un único subcuerpo K con $[L : K] = m$, y $K = \{\alpha \in L \mid \alpha^{p^{n'}} = \alpha\}$.

Definición. Una *extensión abeliana* es una extensión de Galois cuyo grupo de Galois es abeliano. Análogamente, una *extensión cíclica* es una extensión de Galois cuyo grupo de Galois es cíclico.

Ejemplo 5.26. (Extensiones ciclotómicas) Sea $f = X^n - 1 \in K[X]$ y sea L un cuerpo de descomposición de f. Por el Corolario 3.3, el conjunto de raíces de f es un grupo

cíclico. Sea ω un generador de este grupo (se dice que ω es una *raíz primitiva n-ésima de la unidad*). Por tanto, $L = K(\omega)$ y las raíces de $X^n - 1$ son de la forma ω^i, donde claramente se puede tomar $i \in \{0, 1, \ldots, n-1\}$. Distinguimos dos casos:

–Si K es de característica cero o de característica $p \not| n$, entonces $f'(\omega^i) = n\omega^{i(n-1)} \neq 0$, para cada $i = 0, 1, \ldots, n-1$, luego f tiene n raíces distintas, con lo que éstas son necesariamente $1, \omega, \ldots, \omega^{n-1}$. En particular, f es un polinomio separable y por el Teorema 5.14(i) la extensión $K \subset L = K(\omega)$ es de Galois.

–Si en cambio K es de característica p y $n = p^k q$ (con p, q primos entre sí), entonces $f = (X^q)^{p^k} - 1 = (X^q - 1)^{p^k}$. Por tanto, las raíces de f coinciden con las raíces de $X^q - 1$, que ahora son $1, \omega, \ldots, \omega^{q-1}$, ya todas distintas. Entonces L es cuerpo de descomposición de $X^q - 1$, que es separable, luego la extensión es también de Galois en este caso. Haciendo la reducción anterior, supondremos en el resto del ejemplo que la característica de K no divide a n.

Sea σ un elemento del grupo de Galois de L sobre K. Por la Proposición 5.7(i), $\sigma(\omega)$ es una raíz de f, luego será alguna potencia ω^i. Si i y n tuvieran un factor común $d > 1$, se tendría que $(\omega^i)^{\frac{n}{d}} = 1$, y aplicando σ^{-1} también se tendría $\omega^{\frac{n}{d}} = 1$, lo que es absurdo. Por tanto, i y d son primos entre sí. Como $L = K(\omega)$, el automorfismo σ está determinado por la imagen de ω, luego la aplicación $\mathrm{Gal}(K(\omega)/K) \to \mathbb{Z}_n^*$ dada por $\sigma \mapsto i$ (que se comprueba fácilmente que es un homomorfismo de grupos) es inyectiva. Esto implica que $\mathrm{Gal}(K(\omega)/K)$ es (isomorfo a) un subgrupo del grupo $\mathbb{Z}_n^*$, luego es abeliano. Si además n es un número primo p, entonces $\mathrm{Gal}(K(\omega)/K)$ es cíclico (por serlo $\mathbb{Z}_p^*$, de nuevo por el Corolario 3.3). En el caso concreto $K = \mathbb{Q}$, sabemos por el Ejemplo 2.22 que $X^{p-1} + X^{p-2} + \ldots + X + 1$ es irreducible en $\mathbb{Q}[X]$, luego es el polinomio mínimo de ω sobre $\mathbb{Q}$. Por tanto, en este caso, $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$ y $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})] \cong \mathbb{Z}_p^*$.

Claramente, una extensión de Galois de grado un número primo es necesariamente cíclica. El siguiente resultado caracteriza dichas extensiones cuando el cuerpo de partida es de característica cero y contiene todas las raíces p-ésimas de la unidad.

Proposición 5.27. *Sean p un número primo, K un cuerpo de característica cero o distinta de p, y que contiene las raíces p-ésimas de la unidad. Entonces una extensión $K \subset L$ es cíclica de grado p si y sólo si $L = K(\alpha)$, con $\alpha \in L \setminus K$ y $\alpha^p \in K$.*

Demostración: Veamos en primer lugar que toda extensión $K \subset L = K(\alpha)$, con $\alpha \notin K$ y $\alpha^p = a \in K$, es cíclica de grado p. Si ω es una raíz primitiva p-ésima de la unidad, se tiene que las raíces de $X^p - a$ son $\alpha, \alpha\omega, \ldots, \alpha\omega^{p-1}$ (todas distintas), que están en L. Por tanto, L es cuerpo de descomposición sobre K del polinomio separable $X^p - a$, con lo que la extensión $K \subset L$ es de Galois. Entonces el orden del grupo de Galois $\mathrm{Gal}(L/K)$ es el grado de la extensión $K \subset K(\alpha)$, luego a lo más es p (puesto que el polinomio mínimo

de α sobre K divide a $X^p - a$). Si vemos que $\mathrm{Gal}(L/K)$ tiene orden al menos p entonces tendrá orden necesariamente p, y por tanto será cíclico (y se demuestra de paso que $X^p - a$ es irreducible en $K[X]$).

Como $\alpha \notin K$, el grado de la extensión es al menos 1, luego existe $\sigma \neq id_L$ en $\mathrm{Gal}(L/K)$. Como σ debe mandar α a alguna raíz de α (distinta de α, porque si no σ sería la identidad), se tendrá $\sigma(\alpha) = \omega^i \alpha$ con i no divisible por p. Entonces, $\sigma^j(\alpha) = \omega^{ij}\alpha$. Se sigue entonces que $\sigma^j = id_L$ si y sólo si $\omega^{ij} = 1$, es decir, si y sólo si ij es divisible por p, que es equivalente a que j sea divisible por p (ya que p no divide a i). Esto implica que σ tiene orden p, luego $\mathrm{Gal}(L/K)$ tiene orden al menos p, como queríamos (de hecho hemos comprobado incluso que σ es un generador del grupo).

Recíprocamente, supongamos que $K \subset L$ es una extensión cíclica de grado p. Entonces $\mathrm{Gal}(L/K)$ tiene orden p y está generado por un elemento σ (de orden p). Si existe un α como el que buscamos, su imagen por σ debe ser otra raíz de $X^p - \alpha^p \in K[X]$, es decir de la forma $\omega^i\alpha$, donde ω es una raíz p-ésima primitiva de la unidad. En otras palabras, α debe ser un autovector de σ, visto como un endomorfismo del espacio vectorial L (que tiene dimensión p) sobre K. Veamos que tal autovector existe, para lo que tomamos A una matriz de σ respecto de cualquier base de L. De la igualdad $X^p - 1 = (X-1)(X-\omega)\dots(X-\omega^{p-1})$ se sigue que, como $\sigma^p = 1$, entonces

$$(A - I)(A - \omega I)\dots(A - \omega^{p-1}I) = 0$$

(siendo I la matriz identidad $p \times p$). Si las matrices $A - \omega I, \dots, A - \omega^{p-1}I$ tuvieran todas determinante no nulo, serían todas invertibles, y multiplicando por sus respectivas inversas en la igualdad anterior se obtendría $A - I = 0$, lo que es absurdo, porque $\sigma \neq id_L$. Por tanto, existe algún $i \in \{1, \dots, p-1\}$ tal que $\det(A - \omega^i I) = 0$, es decir, que ω^i es un autovalor de σ. Tomamos $\alpha \in L$ un autovector no nulo de autovalor ω^i. Entonces $\sigma(\alpha) = \omega^i\alpha$, que es distinto de α (ya que $\omega^i \neq 1$ y $\alpha \neq 0$), luego en particular $\alpha \notin K$. Por tanto, $[K(\alpha) : K] > 1$, y como $p = [L : K] = [L : K(\alpha)][K(\alpha) : K]$ y p es primo, se sigue que $[K(\alpha) : K] = p$ y $[L : K(\alpha)] = 1$, es decir, $L = K(\alpha)$. Además, $\sigma(\alpha^p) = \sigma(\alpha)^p = \omega^{ip}\alpha^p = \alpha^p$, luego α^p es invariante por todos los elementos de $\mathrm{Gal}(L/K)$ (ya que σ genera el grupo de Galois). Por el Teorema 5.14(iii) se concluye que α^p está en K. $\square$

6. Teoremas de Sylow

La teoría de Galois debería habernos acostumbrado a ver los grupos no como conjuntos "pasivos" a los que les pasan cosas, sino como conjuntos que se dedican a "mover" otros conjuntos (en el caso de la teoría de Galois, los grupos permutan las raíces de los polinomios). La definición precisa de lo que estamos diciendo es la siguiente:

Definición. Se llama *acción por la izquierda (resp. por la derecha) de un grupo G sobre un conjunto X* a una aplicación $\rho : G \times X \to X$, en que denotaremos $\rho(g, x)$ como $g * x$ o, cuando no haya confusión, gx (resp. $\rho(g, x)$ como $x * g$ o xg) tal que:

(i) $(gg')x = g * (g' * x)$ (resp. $x * (gg') = (x * g) * g'$) para cualesquiera $g, g' \in G$ y $x \in X$.

(ii) $1 * x = x$ (resp $x * 1 = x$) para todo $x \in X$.

La interpretación de la definición anterior es que podemos definir un homomorfismo $\hat{\rho} : G \to Biy(X)$ (donde $Biy(X)$ es el grupo de las biyecciones de X en sí mismo con la operación composición, en particular $Biy(X) = S_n$ si X es un conjunto de n elementos) dado por $\hat{\rho}(g) : x \mapsto g * x$ (resp. $\hat{\rho}(g) : x \mapsto x * g$). En efecto, la condición (ii) garantiza que $\hat{\rho}(g)$ es una biyección (ya que $\hat{\rho}(g^{-1})$ es su inversa), y la condición (i) equivale a decir que $\hat{\rho}$ es un homomorfismo. Recíprocamente un homomorfismo $\hat{\rho} : G \to Biy(X)$ define unívocamente una acción de G sobre X, por lo que es equivalente hablar de una acción o del homomorfismo $\hat{\rho}$ asociado. El homomorfismo $\hat{\rho}$ no es necesariamente inyectivo; cuando lo es, se dice que ρ es una *acción fiel*.

Observación 6.1. Dada una acción por la derecha $\rho : G \times X \to X$, se puede definir $\rho' : G \times X \to X$ como $\rho'(g, x) = \rho(g^{-1}, x)$, que resulta ser una acción por la izquierda (de la misma forma, cualquier acción por la izquierda da lugar a una acción por la derecha). Por ello, y porque las acciones por la izquierda tienen una notación casi siempre más natural, consideraremos (salvo que se diga explícitamente lo contrario) que las acciones son siempre por la izquierda.

Ejemplo 6.2. Veamos que cualquier grupo G define siempre alguna acción sobre algún conjunto (los detalles de algunos ejemplos quedan como simple ejercicio).

(i) En primer lugar, G actúa siempre sobre sí mismo, y de diversas formas. De hecho, la propia operación de grupo $G \times G \to G$ define dos acciones, una a la izquierda y otra a la derecha, ya que, dado $g \in G$ (considerando como elemento del grupo que actúa) y $x \in G$ (considerado como elemento del conjunto sobre el que actúa G) podemos definir $g * x$ como el producto gx en G (lo que define una acción por la izquierda) o $x * g$ como el producto xg en G(lo que define una acción por la derecha). Si consideramos por ejemplo la acción por la izquierda, tenemos entonces un homomorfismo $\hat{\rho} : G \to Biy(G)$, que se ve inmediatamente que es inyectivo (si $\hat{\rho}(g) = id_G$, entonces $gx = x$ para todo $x \in G$, lo que

evidentemente implica que $g = 1$). En particular, si G es finito de orden n, $\hat{\rho}$ define un isomorfismo entre G y un subgrupo de S_n.

(ii) Otro modo de hacer actuar G sobre sí mismo es lo que se llama *acción por conjugación*, que consiste en, dados $g, x \in G$, definir $g * x = gxg^{-1}$. En este caso, la aplicación $\hat{\rho} : G \to Biy(G)$ no es necesariamente inyectiva (por ejemplo, si G es abeliano, la aplicación $\hat{\rho}$ es constante y su imagen es id_G). Cabe notar también que cualquier $\hat{\rho}(g)$ es en realidad un automorfismo de G, ya que, además de ser biyectivo, es un homomorfismo de grupos $(g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}))$. Por ejemplo, si $G = S_n$, la acción de un elemento $\sigma \in G$ sobre un ciclo $(i_1\ i_2 \dots i_r)$ lo transforma en el ciclo $(\sigma(i_1)\ \sigma(i_2) \dots \sigma(i_r))$. Por tanto, la acción de σ sobre cualquier permutación τ es una nueva permutación $\sigma\tau\sigma^{-1}$ que tiene la misma descomposición que τ en ciclos disjuntos, pero en que se ha efectuado la sustitución de $1, 2, \dots, n$ por $\sigma(1), \sigma(2), \dots, \sigma(n)$.

(iii) Otra forma distinta de definir una acción es considerar X el conjunto de todos los subconjuntos de G con un cardinal fijado (que ya no tiene estructura de grupo). Entonces se puede definir la acción de G sobre X mediante $g * Y = gY = \{gh \mid h \in Y\}$ para cualquier $g \in G$ y cualquier subconjunto $Y \subset X$ del cardinal fijado. Esta acción define de nuevo un monomorfismo $\hat{\rho} : G \to Biy(X)$.

(iv) Si queremos que G actúe sobre subgrupos, el ejemplo anterior no vale (ya que el conjunto gH no es en general un subgrupo de G), sino que hay que actuar por conjugación. Si X es el conjunto de los subgrupos de G de cardinal fijado, podemos definir, dados $g \in G$ y $H < G$ del cardinal fijado, $g * H = gHg^{-1} = \{ghg^{-1} \mid h \in H\}$.

(v) Si $H < G$, entonces podemos definir una acción de G sobre $G/\sim_H$ mediante $g*(xH) = (gx)H$.

Ejemplo 6.3. Por otra parte, hay grupos que de forma más natural definen acciones sobre conjuntos (de nuevo dejamos los detalles al lector):

(i) El grupo S_n actúa de forma natural sobre el conjunto $\{1, 2, \dots, n\}$, mediante $\sigma * i = \sigma(i)$.

(ii) El *grupo diédrico* D_n (el grupo de isometrías del plano que dejan invariante un polígono regular de n lados) actúa sobre el conjunto de vértices del polígono.

(iii) El grupo $GL(n, K)$ actúa sobre el espacio vectorial K^n, el de las afinidades sobre $\mathbb{A}^n_K$, el de las proyectividades sobre $\mathbb{P}^n_K$, el de las isometrías sobre el espacio euclídeo,...

(iv) Complicando un poco más los ejemplos anteriores, por ejemplo $GL(n, K)$ actúa también sobre el espacio de formas cuadráticas sobre K^n. Representado en forma de matrices, si X es el espacio de matrices simétricas $n \times n$ con coeficientes en K, la representación en forma de matrices de la acción sería $A * B = ABA^t$, con $A \in GL(n, K)$, $B \in X$ (que es la fórmula que nos enseñan en Álgebra Lineal de cómo cambia la matriz B de una forma cuadrática al hacer un cambio de base de matriz A). Análogamente se puede definir una

acción de las afinidades sobre el espacio de cuádricas afines, o de las proyectividades sobre el espacio de cuádricas proyectivas,...

Definición. Se llama órbita de un elemento $x \in X$ bajo una acción de G sobre X al conjunto $O(x) = \{g * x \mid g \in G\}$. Una *acción transitiva* es una acción que tiene una sola órbita, es decir, que para cada $x, y \in X$ existe algún $g \in G$ tal que $g * x = y$.

Ejemplo 6.4. Veamos algunos ejemplos sencillos de cómo son las órbitas de algunas acciones.

(i) Las acciones (i) del Ejemplo 6.2 y (i) y (ii) del Ejemplo 6.3 son transitivas, luego sólo tienen una órbita. En cambio la acción (iii) del Ejemplo 6.3 no es transitiva, ya que tiene dos órbitas: la del vector cero y la de los vectores no nulos.

(ii) En la acción de S_n sobre sí mismo por conjugación (ver Ejemplo 6.2(ii)) las órbitas corresponden a los distintos tipos de descomposición de una permutación en producto de ciclos disjuntos. Por ejemplo, las órbitas de la acción para S_4 consisten en: la permutación identidad, la órbita de las transposiciones (6 elementos), la de los productos de 2 transposiciones disjuntas (3 elementos), la de los 3-ciclos (8 elementos), la de los 4-ciclos (6 elementos). Se deja como ejercicio para el lector el calcular las órbitas, con su correspondiente número de elementos, en el caso $n = 5$.

(iii) Consideremos la acción de $GL(n, \mathbb{C})$ sobre el conjunto $M_{n\times n}(\mathbb{C})$ de matrices dada por $A * B = ABA^{-1}$. Sabemos de Álgebra Lineal que, fijada $B \in M_{n\times n}(\mathbb{C})$, el conjunto de matrices ABA^{-1} es el conjunto de matrices semejantes a B, y están caracterizadas por el hecho de tener la misma forma canónica de Jordan. Por tanto, la acción tiene tantas órbitas como formas canónicas de Jordan.

(iv) Si ahora $GL(n, \mathbb{R})$ actúa sobre el conjunto X de matrices reales simétricas $n \times n$ mediante $A * B = ABA^t$, entonces ahora la órbita de una matriz B será el conjunto de matrices con el mismo rango y signatura. Como hay una cantidad finita de rangos y signaturas, hay una cantidad finita de órbitas.

(v) Si consideramos ahora el grupo de proyectividades de $\mathbb{P}^n_{\mathbb{C}}$ actuando sobre el conjunto de cuádricas, sabemos de Geometría Proyectiva que dos cuádricas complejas son proyectivamente equivalentes si y sólo si tienen el mismo rango. Por tanto, hay exactamente n órbitas, tantas como posibles rangos.

Observación 6.5. Si $O(x)$ es una órbita, entonces la acción de G sobre X se restringe a una acción de G sobre $O(x)$, ya que dado cualquier elemento $gx \in O(x)$ y cualquier $g' \in G$ se tiene que $g'(gx) = (g'g)x$ está en $O(x)$. Por tanto, tenemos un homomorfismo de G en las permutaciones de $O(x)$, que por definición de órbita es suprayectivo. Apliquemos esta observación al Ejemplo 6.4(iii). Hemos dicho que una órbita de la acción por conjugación

de S_4 sobre sí mismo es el conjunto O de los productos de dos transposiciones disjuntas. Es decir, $O = \{\sigma_1, \sigma_2, \sigma_3\}$, con $\sigma_1 = (1\ 2)(3\ 4), \sigma_2 = (1\ 3)(2\ 4), \sigma_3 = (1\ 4)(2\ 3)$. Tenemos por tanto un epimorfismo $\varphi : S_4 \to S_3$, en el que hemos identificado S_3 con el grupo de las permutaciones del conjunto O. Por ejemplo, si $\tau = (1\ 2\ 4)$, entonces $\varphi(\tau)$ consiste en la permutación de O que manda σ_1 a $\tau * \sigma_1 = \tau\sigma_1\tau^{-1} = \sigma_2$, manda σ_2 a $\tau\sigma_2\tau^{-1} = \sigma_3$ y manda σ_3 a $\tau\sigma_3\tau^{-1} = \sigma_1$; es decir, $\varphi(\tau)$ es el 3-ciclo $(1\ 2\ 3)$ de S_3. Es fácil ver que el núcleo de φ es el subgrupo $H = \{id, \sigma_1, \sigma_2, \sigma_3\}$ del Ejercicio 1.3. Por el primer teorema de isomorfía, el cociente S_4/H se identifica de forma natural con el grupo de las permutaciones de O.

Lema 6.6. *Sea $\rho : G \times X \to X$ una acción. Entonces:*

(i) Dados $x_1, x_2 \in X$, o bien $O(x_1) = O(x_2)$ o bien $O(x_1) \cap O(x_2) = \emptyset$. Por tanto X es unión disjunta de las órbitas de la acción.

(ii) Si el conjunto X es finito, para cada $x \in X$ el cardinal de $O(x)$ es $[G : Stab(x)]$, donde $Stab(x) = \{g \in G \mid gx = x\}$, que es un subgrupo de G.

(iii) Si X es un conjunto finito de cardinal n y $O(x_1), \ldots, O(x_r)$ son las órbitas de la acción, entonces $n = [G : Stab(x_1)] + \ldots + [G : Stab(x_r)]$.

Demostración: Para la parte (i), supongamos $O(x_1) \cap O(x_2) \neq \emptyset$, luego contiene un elemento $x \in X$. Por tanto, $x = g_1x_1$ e $x = g_2x_2$, para ciertos $g_1, g_2 \in G$. De aquí se tiene $g_1x_1 = g_2x_2$, luego $x_2 = (g_2^{-1}g_1)x_1$. Entonces, cada $gx_2 \in O(x_2)$ se puede poner como $(gg_2^{-1}g_1)x_1$, luego está también en $O(x_1)$. De modo simétrico, cualquier elemento de $O(x_1)$ está en $O(x_2)$, con lo que se tiene la igualdad buscada.

Para la parte (ii), es claro que $Stab(x)$ es un subgrupo de G, luego sólo hay que ver la igualdad para el cardinal. Para ello, observamos que $O(x)$ es la imagen de la aplicación $\phi : G \to X$ definida por $g \mapsto gx$. Además, $\phi(g) = \phi(g')$ si y sólo si $(g'^{-1}g)x = x$, es decir $g'^{-1}g \in Stab(x)$ o equivalentemente $g \sim_{Stab(x)} g'$. Por tanto, tenemos una biyección entre $G/\sim_{Stab(x)}$ y $O(x)$, lo que demuestra la igualdad.

Finalmente, (iii) es consecuencia inmediata de (i) y (ii). □

La idea ahora es usar la fórmula del apartado (iii) anterior para deducir numéricamente propiedades sobre grupos y conjuntos a partir de sus cardinales. El caso más sencillo es cuando G tiene como orden la potencia de un primo, porque entonces cada $[G : Stab(x)]$ es divisible por p, salvo que $Stab(x) = 1$. Eso es lo que haremos enseguida en el siguiente resultado. Primero, damos una definición de esta propiedad que queremos.

Definición. Dado un número primo p, se llama *p-grupo* a un grupo G cuyo cardinal sea de la forma p^k para algún $k \geq 1$.

Proposición 6.7. *Sea G un p-grupo de orden p^k. Entonces:*

(i) $Z(G) = \{g \in G \mid gx = xg \text{ para todo } x \in G\}$ *es un subgrupo normal de G distinto de $\{1\}$.*

(ii) G posee un subgrupo normal de índice p.

(iii) Para cada $i = 0, 1, \ldots, k$, G posee un subgrupo de orden p^i. Más aún, existe una cadena de subgrupos $\{1\} = H_0 \lhd H_1 \lhd \ldots \lhd H_{k-1} \lhd H_k = G$ tal que cada H_i tiene orden p^i.

(iv) Si $k = 2$, G es abeliano.

Demostración: Que $Z(G)$ es un subgrupo normal es un simple ejercicio que dejamos al lector. Para ver (i), basta demostrar entonces que $Z(G)$ tiene más de un elemento. Para ello, consideramos la acción de G sobre sí mismo por conjugación (ver Ejemplo 6.2(ii)). Por el Lema 6.6(iii) tenemos $p^k = [G : Stab(x_1)] + \ldots + [G : Stab(x_r)]$, donde $O(x_1), \ldots, O(x_r)$ son las órbitas de la acción. Obsérvese que $g * 1 = g1g^{-1} = 1$ para todo $g \in G$, luego $O(1) = \{1\}$, así que al menos uno de los $[G : Stab(x_i)]$ vale 1. Pero como la suma total de todos ellos es p^k, es decir, divisible por p, habrá algún $x_i \neq 1$ tal que $[G : Stab(x_i)]$ no es divisible por p. Por el teorema de Lagrange, $[G : Stab(x_i)]$ es un divisor de p^k, así que necesariamente debe ser $[G : Stab(x_i)] = 1$, es decir $Stab(x_i) = G$. Pero $Stab(x_i) = \{g \in G \mid gxg^{-1} = x\}$, luego $x_i \in Z(G)$, lo que completa la demostración de (i).

Demostraremos (ii) por inducción sobre k, donde p^k es el orden del p-grupo. Si $k = 1$, es evidente, ya que basta tomar el subgrupo $\{1\}$. Supongamos entonces $k > 1$. Si fuera $Z(G) = G$, entonces G sería abeliano, y el resultado se sigue a partir del teorema de estructura de los grupos finitos (ver el Ejercicio 1.8). Suponemos entonces que $Z(G)$ no es trivial (no es $\{1\}$ por (i)). Como $Z(G)$ es normal, $G/Z(G)$ es entonces un p-grupo de orden $p^{k'}$ con $0 < k' < k$. Por hipótesis de inducción, $G/Z(G)$ contiene un subgrupo normal de índice p, que se corresponde mediante la proyección canónica $G \to G/Z(G)$ con un subgrupo normal de índice p de G, que es lo que buscábamos.

La parte (iii) se demuestra por recurrencia. El apartado (ii) demuestra que G posee un subgrupo normal H de orden p^{k-1}. Como H es un p-grupo, de nuevo por (ii) poseerá un subgrupo normal H' de índice p, es decir, de orden p^{k-2}. Reiterando el proceso, ahora a partir de H', se obtiene que G posee subgrupos de órdenes todas las potencias de p de exponente a lo sumo k, y cada subgrupo normal en el siguiente.

Finalmente, para demostrar (iv) tenemos que ver que, si $k = 2$, entonces $Z(G) = G$. Si fuera $Z(G) \neq G$, como $Z(G) \neq \{1\}$ por (i), la única posibilidad es que $Z(G)$ tenga orden p. Por tanto, el cociente $G/Z(G)$ es un grupo de orden p, y por tanto cíclico. Si la clase de g es un generador de $G/Z(G)$, se tendrá entonces que todo elemento de G se puede

escribir como hg^i, con $h \in Z(G)$. Pero entonces dos elementos cualesquiera $hg^i, h'g^{i'} \in G$ conmutan, ya que (usando que h y h' conmutan con cualquier elemento de G por estar en $Z(G)$):

$$(hg^i)(h'g^{i'}) = hh'g^{i+i'} = (h'g^{i'})(hg^i)$$

lo que demuestra que G es abeliano. □

Definición. Se llama *centro de un grupo* G al conjunto $Z(G)$ de la proposición anterior.

En el siguiente resultado veremos que cualquier grupo finito tiene subgrupos que son p-grupos de todos los órdenes posibles.

Teorema 6.8. *Sea G un grupo de orden $p^k q$, con p primo y q no divisible por p. Entonces:*

(i) El número de subconjuntos de G de cardinal p^k no es divisible por p.

(ii) (Primer teorema de Sylow) *G posee algún subgrupo de orden p^k.*

(iii) Para cada $i = 1, \ldots, k$, G posee algún subgrupo de orden p^i.

(iv) (Teorema de Cauchy) *G posee algún elemento de orden p.*

Demostración: El número de subconjuntos de cardinal p^k de un conjunto de $p^k q$ elementos es

$$\binom{p^k q}{p^k} = \frac{p^k q(p^k q - 1)\ldots(p^k q - p^k + 1)}{p^k(p^k - 1)\ldots 1} = \prod_{i=0}^{p^k-1} \frac{p^k q - i}{p^k - i}.$$

Para demostrar (i), basta demostrar que en cada cociente $\frac{p^k q - i}{p^k - i}$ el numerador y el denominador son divisibles exactamente por la misma potencia de p. Para ver esto, observamos primero que tanto el numerador como el denominador son divisibles a lo sumo por la potencia k-ésima de p (ya que en p^k números consecutivos sólo hay uno divisible por p^k y ni $p^k q$ ni p^k son divisibles por potencias mayores de p). El resultado se obtiene entonces de observar que para cada $j \leq k$ se tiene que p^j divide a $p^k - i$ si y sólo si p^j divide a i si y sólo si p^j divide a $p^k q - i$.

Para demostrar (ii) consideramos la acción de G sobre el conjunto de los subconjuntos de G de cardinal p^k mediante $g * Y = gY = \{gh \mid h \in Y\}$. De nuevo por el Lema 6.6(iii) tenemos

$$\binom{p^k q}{p^k} = [G : Stab(Y_1)] + \ldots + [G : Stab(Y_r)]$$

donde $O(Y_1), \ldots, O(Y_r)$ son las órbitas de la acción. Por (i), $\binom{p^k q}{p^k}$ no es divisible por p, luego necesariamente existe algún $Y \subset G$ de cardinal p^k tal que $[G : Stab(Y)]$ no es divisible por p. Como, por el teorema de Lagrange, $[G : Stab(Y)]$ es un divisor de $p^k q$, se

tiene que es un divisor de q, luego en particular (de nuevo por el teorema de Lagrange) $|Stab(Y)| = \frac{p^k q}{[G:Stab(Y)]} \geq p^k$.

Por otra parte, fijado $y_0 \in Y$, es claro que la aplicación $Stab(Y) \to Y$ dada por $g \mapsto gy_0$ está bien definida y es inyectiva, luego $Stab(Y)$ tiene orden a lo más el cardinal de Y, que es p^k. Juntando esto a la desigualdad anterior se sigue que $Stab(Y)$, que es un subgrupo de G, tiene cardinal p^k, como queríamos.

Para el apartado (iii) basta aplicar la Proposición 6.7(iii) al p-grupo dado por un subgrupo de orden p^k de G, que existe por el apartado (ii). Finalmente, el apartado (iv) se sigue de que, como por (iii) G posee un subgrupo H de orden p y los subgrupos de orden primo son cíclicos, entonces H está generado por un elemento de orden p. □

Definición. Se llama *p-subgrupo de Sylow* a un subgrupo de orden p^k de un grupo de orden $p^k q$ con p primo y q coprimo con p. Un *p-subgrupo* es simplemente un subgrupo que es un p-grupo, es decir, que tiene orden p^l, pero no necesariamente con $l = k$.

Una aplicación importante del primer teorema de Sylow es el teorema fundamental del álgebra:

Teorema 6.9 (fundamental del álgebra)**.** *Todo polinomio de grado positivo en $\mathbb{C}[X]$ factoriza en factores lineales, es decir tiene tantas raíces (contadas con multiplicidad) como el grado.*

Demostración: Veamos que todo polinomio $g \in \mathbb{C}[X]$ de grado positivo tiene todas sus raíces en $\mathbb{C}$. Si $\bar{g}$ es el polinomio obtenido a partir de g conjugando los coeficientes, entonces $f = g\bar{g}$ es un polinomio en $\mathbb{R}[X]$ que tiene entre sus raíces las de g. Por tanto, bastará demostrar que cualquier polinomio en $f \in \mathbb{R}[X]$ de grado positivo tiene todas sus raíces en $\mathbb{C}$.

Sea pues $f \in \mathbb{R}[X]$ de grado positivo y sea L el cuerpo de descomposición de $(X^2+1)f$ sobre $\mathbb{R}$ (por tanto L contiene a $\mathbb{C}$ y a todas las raíces de f) y escribamos $[L : \mathbb{R}] = 2^k q$ con q impar. Sea $G = \mathrm{Gal}(L/\mathbb{R})$. Como la extensión $\mathbb{R} \subset L$ es de Galois, se tiene que $|G| = 2^k q$. Por el primer teorema de Sylow, G contiene un subgrupo H de orden 2^k. Y por el Teorema 5.20(ii) existe un cuerpo intermedio $\mathbb{R} \subset K \subset L$ tal que $[K : \mathbb{R}] = q$.

Supongamos $q > 1$. Entonces tomamos cualquier $\alpha \in K \setminus \mathbb{R}$ y consideramos su polinomio mínimo $g \in \mathbb{R}[X]$. Necesariamente g es un polinomio irreducible de grado impar mayor que uno. Pero esto es absurdo, ya que cualquier polinomio real de grado impar tiene alguna raíz real a (aquí hay que usar un poco de Análisis de Variable Real: el límite de $g(X)$ cuando $X \to \infty$ es $-\infty$, mientras que es $+\infty$ cuando $X \to +\infty$, por lo que, por el teorema del valor medio, existe algún $a \in \mathbb{R}$ tal que $g(a) = 0$); por tanto, $X - a$ sería un factor de g, lo que es imposible, ya que g es irreducible de grado mayor que uno.

Por tanto, $q = 1$ y entonces $|G| = [L : \mathbb{R}] = 2^k$. Como $\mathbb{R} \subset \mathbb{C} \subset L$, también $\mathbb{C} \subset L$ es una extensión de Galois de grado $|\operatorname{Gal}(L/\mathbb{C})| = 2^{k-1}$. Si $k > 1$, entonces por la Proposición 6.7(ii), $\operatorname{Gal}(L/\mathbb{C})$ tiene un subgrupo de índice dos, que por el Teorema 5.20 se corresponde con una extensión $\mathbb{C} \subset K$ de grado dos. Si tomamos $\alpha \in K \setminus \mathbb{C}$, entonces su polinomio mínimo es irreducible de grado dos, lo que es imposible, ya que cualquier polinomio en $\mathbb{C}[X]$ de grado dos tiene siempre dos raíces complejas. Por tanto, $k = 1$, lo que implica $L = \mathbb{C}$, es decir, que todas las raíces de f están en $\mathbb{C}$. □

Teorema 6.10 (Segundo teorema de Sylow)**.** *Sea G un grupo finito cuyo orden es divisible por un primo p y sea H un p-subgrupo de Sylow. Entonces, para cada p-subgrupo $H' < G$ existe $g \in G$ tal que $H' \subset gHg^{-1}$. Como consecuencia:*

(i) Cada p-subgrupo está contenido en un p-subgrupo de Sylow

(ii) Dos p-subgrupos de Sylow cualesquiera son siempre conjugados entre sí.

(iii) G posee un único p-subgrupo de Sylow si y sólo si existe un subgrupo de p-Sylow normal

Demostración: Consideramos la acción del Ejemplo 6.2(v), pero restringida a H', es decir, hacemos actuar H' sobre $G/\sim_H$ mediante $h' * (gH) = (h'g)H$. Usando, como siempre, la Proposición 6.6(iii) tenemos

$$[G : H] = [H' : Stab(g_1H)] + \ldots + [H' : Stab(g_rH)]$$

donde $O(g_1H), \ldots, O(g_rH)$ son las órbitas de la acción. Como H es un p-subgrupo de Sylow, $[G : H]$ no es divisible por p. Por tanto, debe existir algún $g \in \{g_1, \ldots, g_r\}$ tal que $[H' : Stab(gH)]$ no es divisible por p. Como H' es un p-subgrupo, $[H' : Stab(gH)]$ (que divide a $|H'|$ por el teorema de Lagrange), es una potencia de p, luego debe ser necesariamente $[H' : Stab(gH)] = 1$, es decir, $Stab(gH) = H'$. Por tanto, para cada $h' \in H'$ se tiene $(h'g)H = gH$, o equivalentemente $g^{-1}h'g = h \in H$, luego $h' = ghg^{-1} \subset gHg^{-1}$. Esto demuestra que efectivamente $H' \subset gHg^{-1}$.

El resto del enunciado es una consecuencia inmediata de este hecho: Claramente gHg^{-1} es un p-subgrupo de Sylow, lo que implica (i). Si H' es un p-subgrupo de Sylow, entonces coincide con gHg^{-1}, ya que tiene su mismo cardinal, lo que demuestra (ii). Finalmente, si H es normal, entonces $gHg^{-1} = H$ para todo $g \in G$, por lo que (ii) implica que cualquier p-subgrupo de Sylow de G coincide necesariamente con H; recíprocamente, si existe sólo un p-subgrupo de Sylow H, como gHg^{-1} es siempre un p-subgrupo de Sylow para todo $g \in G$, se tiene $gHg^{-1} = H$, por lo que H es normal. □

Teorema 6.11 (Tercer teorema de Sylow)**.** *Sea G un grupo finito cuyo orden es divisible por un primo p, y sea n_p el número de p-subgrupos de Sylow de G. Entonces:*

(i) $n_p = [G : N(H)]$, *donde* H *es un* p*-subgrupo de Sylow cualquiera y* $N(H)$ *es el mayor subgrupo de* G *que contiene a* H *y en el cual* H *es normal. En particular,* n_p *divide a* $[G : H]$.

(ii) $n_p \equiv 1 (\mathrm{mod} p)$.

Demostración: Sea X el conjunto de p-subgrupos de Sylow. Si hacemos actuar G sobre X por conjugación (es decir, $g * H = gHg^{-1}$), el segundo teorema de Sylow afirma que existe una sola órbita, con lo que en este caso la fórmula de la Proposición 6.6(iii) afirma $n_p = [G : Stab(H)]$, donde H es cualquier p-subgrupo de Sylow. Ahora bien, para esta acción, $Stab(H) = \{g \in G \mid gHg^{-1} = H\}$. Claramente, este subgrupo contiene a H, $H \lhd Stab(H)$ y cualquier otro subgrupo en el que H sea normal debe estar contenido en $Stab(H)$. Por tanto, $Stab(H) = N(H)$, lo que prueba la primera parte de (i). La segunda parte se deduce de $[G : H] = \frac{|G|}{|H|} = \frac{|G|}{|N(H)|}\frac{|N(H)|}{|H|} = [G : N(H)][N(H) : H]$.

Para demostrar (ii), restringimos ahora la acción anterior a $H \times X \to X$, donde de nuevo H es un p-subgrupo de Sylow. Usando una vez más la Proposición 6.6(iii) tenemos

$$n_p = [H : Stab(H_1)] + \ldots + [H : Stab(H_r)]$$

donde $O(H_1), \ldots, O(H_r)$ son las órbitas de la acción. Como H es un p-subgrupo, cada $[H : Stab(H_i)]$ es una potencia de p, luego será divisible por p excepto si $Stab(H_i) = H$. Pero $Stab(H_i) = \{h \in H \mid hH_ih^{-1} = H_i\} = N(H_i) \cap H$, luego $Stab(H_i) = H$ si y sólo si $H \subset N(H_i)$. Por tanto, en este caso tenemos que H y H_i son dos p-subgrupos de Sylow de $N(H_i)$. Como $H_i \lhd N(H_i)$, por el Teorema 6.10(iii) sabemos que $N(H_i)$ sólo contiene un p-subgrupo de Sylow, luego $H_i = H$ (en cuyo caso, evidentemente, $H \subset N(H_i)$, es decir, $Stab(H_i) = H$). Esto implica que sólo uno de los $[H : Stab(H_i)]$ es 1, mientras que el resto es divisible por p, lo que demuestra la congruencia. □

Definición. Se llama *normalizador de un subgrupo* $H < G$ al máximo subgrupo $N(H)$ de G tal que $H \lhd N(H)$.

Ejemplo 6.12. Los teoremas de Sylow permiten clasificar, salvo isomorfismo, grupos de orden pequeño. Por ejemplo, supongamos que queremos estudiar todos los grupos de orden $2p$, donde p es un número primo impar. Por el primer teorema de Sylow, un grupo G de orden $2p$ posee subgrupos de orden 2 y p. Por el tercer teorema de Sylow, el número de subgrupos de orden p es un divisor de 2 y es congruente con 1 módulo p, de donde se concluye que G posee un único subgrupo de orden p. De la misma forma, el número n_2 de subgrupos de orden 2 es un divisor de p y es congruente con 1 módulo 2. Esto da dos posibilidades para n_2, que analizamos separadamente:

Caso $n_2 = 1$: Analicemos en este caso el orden de los distintos elementos de G. Por el teorema de Lagrange, los posibles órdenes de los elementos de G son $1, 2, p, 2p$. Obviamente, el único elemento de orden uno es el neutro 1. Por otra parte, G posee un único elemento de orden dos (el generador del único subgrupo de orden dos), mientras que tiene $p-1$ elementos de orden p (los generadores del único subgrupo de orden p). Por tanto, el resto de los $p-1$ elementos de G deben tener orden $2p$. Como $p-1 > 0$, G posee algún elemento de orden $2p$, que necesariamente genera todo el grupo, luego en este caso G es cíclico y por tanto isomorfo a $\mathbb{Z}_{2p}$.

Caso $n_2 = p$: En este caso, una cuenta análoga a la anterior nos da un elemento de orden uno (el neutro), p elementos de orden dos (los generadores de los distintos subgrupos de orden dos) y $p-1$ de orden p (los generadores del único subgrupo de orden p). Sea ρ uno de los generadores del único subgrupo de orden p. Entonces el subgrupo de orden p consiste en los elementos (distintos) $1, \rho, \ldots, \rho^{p-1}$. Sea σ uno de los elementos de orden dos. Es claro que los elementos $\sigma, \sigma\rho, \ldots, \sigma\rho^{p-1}$ son todos distintos. Además, ningún $\sigma\rho^i$ puede coincidir con un ρ^j, ya que entonces $\sigma = \rho^{j-i}$, pero ρ^{j-i} tiene orden 1 ó p, mientras que σ tiene orden dos. Por tanto,

$$G = \{1, \rho, \ldots, \rho^{p-1}, \sigma, \sigma\rho, \ldots, \sigma\rho^{p-1}\}$$

y los elementos de orden dos son $\sigma, \sigma\rho, \ldots, \sigma\rho^{p-1}$. En particular, $\sigma\rho$ tiene orden dos, es decir, $\sigma\rho\sigma\rho = 1$, o equivalentemente $\rho\sigma = \sigma^{-1}\rho^{-1} = \sigma\rho^{p-1}$. En otras palabras, G está generado por ρ y σ, y a partir de las relaciones $\rho^p = 1$, $\sigma^2 = 1$ y $\rho\sigma = \sigma\rho^{p-1}$ podemos construir la tabla del producto para los $2p$ elementos de G que hemos hallado antes. Dicha tabla del producto coincide con la que se obtiene para el grupo diédrico D_p de las isometrías de un polígono regular de p lados (identificando ρ con una rotación de $\frac{2\pi}{p}$ grados) y σ con una simetría). Por tanto, en este caso G es isomorfo al grupo diédrico D_p.

El ejemplo anterior plantea una cuestión natural: ¿Es posible identificar salvo isomorfismo un grupo a partir de generadores y relaciones sin necesidad de construir su tabla de productos? La respuesta es afirmativa, y a ello dedicaremos el resto de la sección. Primero definimos la noción de grupo con generadores sin relaciones. La idea que hay que tener en mente es la de espacio vectorial, en que unos generadores sin relaciones forman una base. La idea que queremos generalizar aquí es que una base está caracterizada por el hecho de permitir definir (de forma única) homomorfismos enviando los elementos de la base a donde queramos.

Definición. Se llama *grupo libre de rango r* a un grupo G generado por elementos $g_1, \ldots, g_r$ y que verifica que para todo grupo G' y elementos $g'_1, \ldots, g'_r \in G'$ existe un único homomorfismo de grupos $\varphi : G \to G'$ tal que $\varphi(g_i) = g'_i$ para $i = 1, \ldots, r$. (Esta definición se puede extender sin dificultad a grupos libres de rango no necesariamente finito, pero preferimos restringirnos al caso finito, que es el que necesitamos).

El siguiente resultado muestra que todos los grupos libres del mismo rango son isomorfos (obsérvese que la demostración es idéntica a la de la Proposición 1.15, que caracterizaba salvo isomorfismos el anillo de polinomios por su propiedad universal).

Proposición 6.13. *Sean G y G' grupos libres de rango r con generadores respectivos $g_1, \ldots, g_r$ y $g'_1, \ldots, g'_r$. Entonces existe un (único) isomorfismo de grupos $\varphi : G \to G'$ tal que $\varphi(g_i) = g'_i$ para $i = 1, \ldots, r$.*

Demostración: Por ser G libre, existe un único homomorfismo de grupos $\varphi : G \to G'$ tal que $\varphi(g_i) = g'_i$ para $i = 1, \ldots, r$. Para ver que es isomorfismo, usamos ahora que G' es libre, y concluimos que existe un (único) homomorfismo de grupos $\psi : G' \to G$ tal que $\psi(g'_i) = g_i$ para $i = 1, \ldots, r$. Tenemos entonces que la composición $\psi \circ \varphi$ es un homomorfismo de G a G que deja fijos $g_1, \ldots, g_r$. Como la identidad verifica lo mismo y G es libre (tomando ahora en la definición $G' = G$) se tiene que $\psi \circ \varphi = id_G$. Análogamente, aplicando la definición de libre para G' se tiene $\varphi \circ \psi = id_{G'}$, de donde se deduce que φ y ψ son inversas la una de la otra y por tanto isomorfismos. □

Observación 6.14. La definición de grupo libre se puede hacer también para grupos abelianos. Concretamente, se llama *grupo abeliano libre de rango r* a un grupo abeliano G generado por elementos $g_1, \ldots, g_r$ y que verifica que para todo grupo abeliano G' y elementos $g'_1, \ldots, g'_r \in G'$ existe un único homomorfismo de grupos $\varphi : G \to G'$ tal que $\varphi(g_i) = g'_i$ para $i = 1, \ldots, r$. De la misma forma que en la Proposición 6.13 se demuestra que todos los grupos abelianos libres de rango r son isomorfos entre sí. Además, en este caso, no es difícil ver que $\mathbb{Z} \times \overset{r)}{\ldots} \times \mathbb{Z}$ es un grupo abeliano libre de rango r generado por $(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$. En efecto, dado cualquier otro grupo abeliano G' y elementos $g'_1, \ldots, g'_r \in G'$ es fácil comprobar que $\varphi(n_1, \ldots, n_r) = {g'}_1^{n_1} \ldots {g'}_r^{n_r}$ es el único homomorfismo de grupos $\mathbb{Z} \times \overset{r)}{\ldots} \times \mathbb{Z} \to G'$ tal que $\varphi(0, \ldots, 0, \overset{i)}{1}, 0, \ldots, 0) = g'_i$ para $i = 1, \ldots, r$. Nótese que, si $r > 1$, φ es un homomorfismo gracias a que G' es conmutativo ($\varphi((m_1, \ldots, m_r) + (n_1, \ldots, n_r)) = \varphi(m_1 + n_1, \ldots, m_r + n_r) = {g'}_1^{m_1+n_1} \ldots {g'}_r^{m_r+n_r} = {g'}_1^{m_1} {g'}_1^{n_1} \ldots {g'}_r^{m_r} {g'}_r^{n_r} = {g'}_1^{m_1} \ldots {g'}_r^{m_r} {g'}_1^{n_1} \ldots {g'}_r^{n_r} = \varphi(m_1, \ldots, m_r) + \varphi(n_1, \ldots, n_r)$). Por tanto, si $r > 1$, $\mathbb{Z} \times \overset{r)}{\ldots} \times \mathbb{Z}$ no es un grupo libre. En el siguiente ejemplo vemos la forma de construir un grupo libre para cada rango r.

Ejemplo 6.15. Fijamos *letras* $a_1, \ldots, a_r$ y consideramos el conjunto G que consiste en las expresiones formales del tipo $a_{i_1}^{n_1} \ldots a_{i_s}^{n_s}$ (llamadas *palabras*), con $n_1, \ldots, n_s \in \mathbb{Z}$ y cada $a_{i_j} \neq a_{i_{j+1}}$. Permitimos también $s = 0$, en cuyo caso hablaremos de la *palabra vacía*. Definiendo el producto de palabras mediante la concatenación de las mismas y agrupando potencias consecutivas (por ejemplo, el producto de $a_1 a_3^2 a_2^{-3}$ con $a_2^2 a_1 a_3 a_2^5$

sería $a_1a_3^2a_2^{-1}a_1a_3a_2^5$), se obtiene fácilmente que G tiene estructura de grupo; el elemento neutro es la palabra vacía y el elemento inverso de $a_{i_1}^{n_1}\dots a_{i_s}^{n_s}$ es $a_{i_s}^{-n_s}\dots a_{i_1}^{-n_1}$. Es también fácil comprobar que G es libre generado por $a_1,\dots,a_s$. Al grupo así construido se le suele denotar por $\mathbb{Z}*\overset{r)}{\dots}*\mathbb{Z}$.

Dado entonces cualquier grupo G con generadores $g_1,\dots,g_r$, se tiene que existe un único epimorfismo $\varphi:\mathbb{Z}*\overset{r)}{\dots}*\mathbb{Z}\to G$ tal que $\varphi(a_i)=g_i$ para $i=1,\dots,r$. Esto nos permite definir de forma precisa la noción de relación entre los generadores:

Definición. Se llama *relación entre los generadores* $g_1,\dots,g_r$ a cualquier elemento del núcleo del epimorfismo φ de arriba. Obsérvese que entonces el conjunto de relaciones es $\ker\varphi$, que es un subgrupo normal de $\mathbb{Z}*\overset{r)}{\dots}*\mathbb{Z}$. Si $\ker\varphi$ es el mínimo subgrupo normal que contiene a un número finito de elementos $R_1,\dots,R_s\subset\mathbb{Z}*\overset{r)}{\dots}*\mathbb{Z}$, diremos que G está *definido mediante los generadores* $g_1,\dots,g_r$ *y las relaciones* $R_1,\dots,R_s$.

Veamos cómo funciona esta construcción retomando nuestro ejemplo del grupo diédrico en el segundo caso del Ejemplo 6.12.

Ejemplo 6.16. Queremos caracterizar el grupo diédrico D_n a partir de saber que está generado una rotación ρ de ángulo $\frac{2\pi}{n}$ y una simetría σ y que se verifica $\rho^n=1$, $\sigma^2=1$ y $\rho\sigma=\sigma\rho^{n-1}$. La forma rigurosa de hacerlo entonces es considerar $\mathbb{Z}*\mathbb{Z}$ generado por las letras a,b, tomar el mínimo subgrupo normal N de $\mathbb{Z}*\mathbb{Z}$ que contiene a $a^n,b^2,abab$ y comprobar si $\mathbb{Z}*\mathbb{Z}/N$ es isomorfo a D_n. Antes de proseguir, hagamos alguna observación que es útil para aclarar cuál es el papel que juega el tomar "el mínimo subgrupo normal". Nótese, que la igualdad $\rho\sigma=\sigma\rho^{n-1}$ da lugar, de forma estricta, a la relación $\rho\sigma\rho^{1-n}\sigma^{-1}=1$, con lo que deberíamos haber tomado para generar N la palabra $aba^{1-n}b^{-1}$ en lugar $abab$. Lo que ocurre es que hemos usado las relaciones $\rho^n=1$ y $\sigma^2=1$ (que corresponden a las palabras a^n y b^2). Si al final ambas elecciones son equivalentes es porque existe una igualdad

$$aba^{1-n}b^{-1}=(abab)(b^{-1}a^{-n}b)(b^{-2})$$

que muestra que $aba^{1-n}b^{-1}$ está en el mínimo subgrupo normal que contiene a $a^n,b^2,abab$ (y análogamente $a^n,b^2,abab$ está en el mínimo subgrupo normal que contiene a $aba^{1-n}b^{-1}$). Veamos en primer lugar qué aspecto tiene el grupo $\mathbb{Z}*\mathbb{Z}/N$. La clave está en ir jugando con las relaciones del cociente para ir reduciendo cada palabra a una forma cada vez más sencilla. En concreto, daremos los siguientes pasos (usaremos una barra para denotar clases módulo N):

–Usando la relación $\bar a^{-1}=\bar a^{n-1}$ y $\bar b^{-1}=\bar b$, podemos escribir cualquier palabra de forma que los exponentes de $\bar a$ y $\bar b$ son siempre positivos.

–Usando la relación $\bar{b}\bar{a} = \bar{a}^{n-1}\bar{b}$ podemos ir pasando todas las $\bar{a}$ a la izquierda y todas las $\bar{b}$ a la derecha, con lo que la palabra quedará de la forma $\bar{a}^i\bar{b}^j$.

–Usando de nuevo $\bar{a}^n = 1$ y $\bar{b}^2 = 1$ podemos suponer que $i \in \{0 \dots, n-1\}$ y $j \in \{0, 1\}$.

En definitiva, hemos visto que los elementos de $\mathbb{Z} * \mathbb{Z}$ son $1, \bar{a}, \dots, \bar{a}^{n-1}, \bar{b}, \bar{a}\bar{b}, \dots, \bar{a}^{n-1}\bar{b}$, aunque el problema es que a priori no podemos decir si son distintos o no. De hecho, éste es en general un problema muy difícil, y en principio podría incluso ocurrir que el mínimo subgrupo normal que contiene a $a^n, b^2, abab$ fuese hasta todo el grupo libre y nuestro grupo sería el trivial. La ventaja que tenemos en este ejemplo es que disponemos de un "modelo", que es el grupo diédrico, lo que nos va a permitir concluir que $\mathbb{Z} * \mathbb{Z}/N$ es isomorfo a él. En efecto, tenemos un epimorfismo $\mathbb{Z} * \mathbb{Z} \to D_n$ que manda a a ρ y b a σ. Como $a^n, b^2, abab$ están en el núcleo, que es normal, se tendrá que el núcleo contiene a N, por lo que el epimorfismo anterior factoriza por otro epimorfismo $\mathbb{Z} * \mathbb{Z}/N \to D_n$. Como ya sabemos que $\mathbb{Z} * \mathbb{Z}/N$ tiene como mucho $2n$ elementos (que es el orden de D_n, se sigue que dicho epimorfismo es necesariamente biyectivo, y por tanto un isomorfismo.

Ejercicio 6.17. Si p es un número primo, demostrar que el grupo de Galois del cuerpo de descomposición de $X^4 - p$ sobre $\mathbb{Q}$ es el grupo diédrico D_4.

7. Resolubilidad de ecuaciones y de grupos

Como vimos en el Ejemplo 3.19, cualquier ecuación de grado tres se puede resolver mediante una fórmula que involucra sólo raíces (cuadradas y cúbicas) sucesivas de expresiones en los coeficientes de la ecuación. La ecuación cuártica se resuelve (ver el Ejemplo 3.26) resolviendo primero una ecuación cúbica y, a partir de sus soluciones, resolviendo ecuaciones cuadráticas. Por tanto, las soluciones de una cuártica tienen también el mismo aspecto a base de raíces sucesivas de expresiones en los coeficientes de la ecuación original. Para ser más precisos, si consideramos el polinomio $X^3+pX+q \in \mathbb{Q}[X]$, la fórmula (3.23) indica que las raíces del polinomio pueden escribir de la forma

$$\sqrt[3]{\frac{-q}{2}+\frac{\sqrt{\beta_1}}{2}}-\frac{p}{3\sqrt[3]{\frac{-q}{2}+\frac{\sqrt{\beta_1}}{2}}}$$

donde $\beta_1 = \frac{4p^3+27q^2}{27}$. Por tanto, una raíz se encuentra en el cuerpo L que se puede poner al final de una cadena de extensiones

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{\beta_1}) \subset \big(\mathbb{Q}(\sqrt{\beta_1})\big)(\sqrt[3]{\beta_2}) = L$$

con $\beta_2 = \frac{-q}{2} - \frac{\sqrt{\beta_1}}{2} \in \mathbb{Q}(\sqrt{\beta_1})$. En realidad, si queremos obtener todas las raíces, debemos permitir las tres raíces cúbicas de β_2, es decir, tenemos que adjuntar también una raíz cúbica primitiva de 1. De ese modo, obtendremos un cuerpo que contiene al cuerpo de descomposición del polinomio (recuérdese, como vimos en el Ejemplo 3.24, que el cuerpo obtenido puede ser mayor que el de descomposición, ya que las raíces pueden ser todas reales, y sin embargo estamos adjuntando números imaginarios).

Definición. Se llama *torre radical* a una cadena de cuerpos $K_0 \subset K_1 \subset \ldots \subset K_{r-1} \subset K_r$ tal que para cada $i = 1, \ldots, r$ se tiene $K_i = K_{i-1}(\alpha_i)$, con $\alpha_i^{n_i} \in K_{i-1}$ para algún $n_i \in \mathbb{N}$. Un polinomio $f \in K[X]$ se dice que es *resoluble por radicales* si existe una torre radical $K = K_0 \subset K_1 \ldots K_{r-1} \subset K_r$ tal que K_r contiene al cuerpo de descomposición de f sobre K.

Lema 7.1. *Sea K un cuerpo de característica cero y sea $f \in K[X]$ un polinomio. Entonces son equivalentes:*

(i) El polinomio f es resoluble por radicales

(ii) El cuerpo de descomposición de f sobre K está contenido en K_r, donde $K = K_0 \subset K_1 \subset \ldots \subset K_{r-1} \subset K_r$ es una torre radical tal que $K \subset K_r$ es una extensión de Galois.

(iii) El cuerpo de descomposición de f sobre K está contenido en K_r, donde $K = K_0 \subset K_1 \subset \ldots \subset K_{r-1} \subset K_r$ es una torre radical tal que $K \subset K_r$ es una extensión de Galois y para cada $i = 1, \ldots, r$ se tiene que $K_{i-1} \subset K_i$ una extensión cíclica de grado primo.

Demostración: Claramente, las condiciones (i), (ii), (iii) son cada una más fuerte que la anterior (ver Proposición 5.27), por lo que basta ver que de (i) podemos pasar a (ii) y de (ii) a (iii).

$(i) \Rightarrow (ii)$: Sea $K = K_0 \subset K_1 \subset \ldots \subset K_{r-1} \subset K_r$ con cada $K_i = K_{i-1}(\alpha_i)$ y $\alpha_i^{n_i} \in K_{i-1}$. Para cada α_i consideremos su polinomio mínimo $f_i \in K[X]$ sobre K. Sea entonces L el cuerpo de descomposición de $f_1 \ldots f_r$ sobre K (que contendrá $\alpha_1, \ldots, \alpha_r$, y por tanto al cuerpo de descomposición de f sobre K). La extensión $K \subset L$ es de Galois (al estar en característica cero) y estará generada por los α_i y sus conjugados respecto de K. Si $\sigma_1, \ldots, \sigma_m$ son los elementos de $\mathrm{Gal}(L/K)$, se tendrá que $\sigma_1(\alpha_i), \ldots, \sigma_m(\alpha_i)$ son las raíces de f_i (de este modo, cada raíz puede aparecer repetida muchas veces, pero obviamos ese detalle para obtener una escritura más simple). El resultado estará demostrado si vemos que la torre

$$K \subset L_{11} \subset \ldots \subset L_{1m} \subset L_{21} \subset \ldots \subset L_{r-1,m} \subset L_{r1} \subset \ldots \subset L_{rm}$$

es radical, donde cada L_{ij} está definido adjuntando al cuerpo anterior el elemento $\sigma_j(\alpha_i)$. Fijamos pues $i \in \{1, \ldots, r\}$ y $j \in \{1, \ldots, m\}$. Tenemos $\alpha_i^{n_i} \in K_{i-1} = K(\alpha_1, \ldots, \alpha_{i-1})$, luego $\sigma_j(\alpha_i)^{n_i}$ está en $K(\sigma_j(\alpha_1), \ldots, \sigma_j(\alpha_{i-1}))$, que a su vez está contenido en $L_{i-1,j}$, que es un subcuerpo de la cadena anterior a L_{ij}.

$(ii) \Rightarrow (iii)$: Supongamos ahora que tenemos una torre radical $K = K_0 \subset K_1 \ldots K_{r-1} \subset K_r$ tal que $K \subset K_r$ es una extensión de Galois que contiene al cuerpo de descomposición de f sobre K. Sea n el mínimo común múltiplo de $n_1, \ldots, n_r$ y sea ω una raíz primitiva n-ésima de la unidad. En primer lugar, cambiamos la torre de partida por la torre

$$K \subset K(\omega) \subset K_1(\omega) \subset \ldots \subset K_r(\omega)$$

que claramente sigue estando en las condiciones de (ii). Para obtener una torre que verifique (iii) sustituiremos cada eslabón de la cadena anterior por una subcadena.

En primer lugar, tenemos que $K \subset K(\omega)$ es una extensión abeliana (ver el Ejemplo 5.26). Si escribimos el orden de $\mathrm{Gal}(K(\omega)/K)$ como $p_1 \ldots p_s$ (con los primos $p_1, \ldots, p_s$ no necesariamente distintos), por el teorema de estructura de los grupos abelianos finitos (ver el Ejercicio 1.8) podemos encontrar un subgrupo G_1 de $\mathrm{Gal}(K(\omega)/K)$ de orden $p_2 \ldots p_r$, que necesariamente es normal. Reiterando este proceso, existe una cadena

$$\{1\} = G_s < G_{s-1} < \ldots < G_1 < G_0 = \mathrm{Gal}(K(\omega)/K)$$

de forma que cada G_{i-1}/G_i tiene orden p_i, por lo que necesariamente es cíclico. Por la correspondencia de Galois, esta cadena da lugar a una cadena

$$K = K'_s \subset K'_{s-1} \subset \ldots \subset K'_1 \subset K'_0 = K(\omega)$$

de extensiones cíclicas de grado primo.

Análogamente, para cada uno de los eslabones $K_{i-1}(\omega) \subset K_i(\omega)$ descomponemos $n_i = p_1 \ldots p_s$ en producto de números primos y sustituimos el eslabón por

$$K_{i-1}(\omega) \subset (K_{i-1}(\omega))(\alpha_i^{p_2 \cdots p_s}) \subset \ldots \subset (K_{i-1}(\omega))(\alpha_i^{p_s}) \subset (K_{i-1}(\omega))(\alpha_i) = K_i(\omega)$$

que es una cadena de extensiones cíclicas por la Proposición 5.27, ya que $K_{i-1}(\omega)$ contiene todas las raíces n_i-ésimas de la unidad. □

La versión algebraica del resultado anterior viene dada por la siguiente definición:

Definición. Un *grupo resoluble* es un grupo G que verifica una de las siguientes condiciones equivalentes:

(i) Existe una cadena de subgrupos $\{1\} = H_0 < H_1 < \ldots < H_{r-1} < H_r = G$ tal que cada H_{i-1} es normal en H_i y el cociente H_i/H_{i-1} es un grupo abeliano.

(ii) Existe una cadena de subgrupos $\{1\} = H_0 < H_1 < \ldots < H_{r-1} < H_r = G$ tal que cada H_{i-1} es normal en H_i y el cociente H_i/H_{i-1} es un grupo cíclico de orden primo.

Aunque en apariencia la condición (ii) es más fuerte, se obtiene fácilmente a partir de la condición (i). En efecto, si H_i/H_{i-1} es un grupo abeliano, entonces (recordando que los subgrupos de H_i/H_{i-1} son de la forma H'/H_{i-1} con $H_{i-1} < H' < H_i$) se puede encontrar (igual que hicimos en el paso $(ii) \Rightarrow (iii)$ de la demostración del Lema 7.1) una cadena $\{1\} = H'_0/H_{i-1} < H'_1/H_{i-1} < \ldots < H'_s/H_{i-1} = H_i/H_{i-1}$ tal que cada $(H'_j/H_{i-1})/(H'_{j-1}/H_{i-1})$ (que es isomorfo a H'_j/H'_{j-1} por el segundo teorema de isomorfía) tenga orden primo (y por tanto sea cíclico). De este modo, sustituyendo cada eslabón $H_{i-1} < H_i$ por $H_{i-1} = H'_0 < H'_1 < \ldots < H'_s = H_i$, se obtiene una cadena que verifica la condición (ii).

Lema 7.2. *Sea G un grupo y $K < G$. Entonces :*

(i) Si G es resoluble, entonces K es resoluble.

(ii) Si $K \lhd G$, entonces G es resoluble si y sólo si K y G/K son resolubles.

Demostración: Par ver (i), por ser G resoluble existe una cadena de subgrupos $\{1\} = H_0 < H_1 < \ldots < H_{r-1} < H_r = G$ tal que cada H_{i-1} es normal en H_i y el cociente H_i/H_{i-1} es un grupo abeliano. Si para cada $i = 0, \ldots, r$ escribimos $K_i = K \cap H_i$ tendremos entonces

una cadena $\{1\} = K_0 < K_1 < \ldots < K_{r-1} < K_r = G$ en que cada K_{i-1} es normal en K_i y el cociente K_i/K_{i-1} es un grupo abeliano, ya que está contenido en H_i/H_{i-1}. Por tanto, K es resoluble.

Para ver (ii), supongamos primero que G sea resoluble. Por (i) sabemos ya que K es resoluble, así que falta sólo demostrar le resolubilidad de G/K. Como en (i), consideramos una cadena de subgrupos $\{1\} = H_0 < H_1 < \ldots < H_{r-1} < H_r = G$ tal que cada H_{i-1} es normal en H_i y el cociente H_i/H_{i-1} es un grupo abeliano. De aquí, obtenemos en G/K la cadena de subgrupos $\{1\} = KH_0/K < KH_1/K < \ldots < KH_{r-1}/K < KH_r/K = G/K$ en que cada KH_{i-1}/K es normal en KH_i/K (por ser $KH_{i-1} \lhd KH_i$) y el cociente $(KH_i/K)/(KH_{i-1}/K)$ es isomorfo a KH_i/KH_{i-1}, que es un grupo abeliano por ser cociente del grupo abeliano K_i/K_{i-1}; por tanto, G/K es también resoluble.

Recíprocamente, supongamos que K y G/K son grupos resolubles. Por tanto existen cadenas

$$\{1\} = K_0 \lhd K_1 \lhd \ldots \lhd K_r = K$$

con cada K_i/K_{i-1} abeliano y (recordando la biyección entre subrupos de G/K y subgrupos de G que contienen a K)

$$\{1\} = H_0/K \lhd H_1/K \lhd \ldots \lhd H_s/K = G/K$$

con cada $(H_j/K)/(H_{j-1}/K)$ abeliano, o equivalentemente

$$K = H_0 \lhd H_1 \lhd \ldots \lhd H_s = G$$

con cada H_j/H_{j-1} abeliano. Juntando ambas cadenas, obtenemos una nueva

$$\{1\} = K_0 \lhd K_1 \lhd \ldots \lhd K_r = K = H_0 \lhd H_1 \lhd \ldots \lhd H_s = G$$

que demuestra que G es resoluble. □

Teorema 7.3. *Sea K un cuerpo de característica cero y sea L el cuerpo de descomposición de un polinomio $f \in K[X]$. Entonces f es resoluble por radicales si y sólo si* $\mathrm{Gal}(L/K)$ *es un grupo resoluble.*

Demostración: Si f es resoluble por radicales, entonces por el Lema 7.1 se tiene que existe una torre radical $K = K_0 \subset K_1 \subset \ldots \subset K_{r-1} \subset K_r$ tal que $K \subset K_r$ es una extensión de Galois, para cada $i = 1, \ldots, r$ se tiene que $K_{i-1} \subset K_i$ una extensión cíclica de grado primo y $K \subset L$. Entonces tendremos una cadena de subgrupos

$$\{1\} = \mathrm{Gal}(K_r/K_r) < \mathrm{Gal}(K_r/K_{r-1}) < \ldots < \mathrm{Gal}(K_r/K_0) = \mathrm{Gal}(K_r/K).$$

Como $K_{i-1} \subset K_i$ es una extensión normal (por ser cíclica, luego por definición de Galois) por el Teorema 5.21 (tomando como extensión $K_{i-1} \subset K_r$ y como cuerpo intermedio K_i) se tendrá que $\mathrm{Gal}(K_r/K_i)$ es normal en $\mathrm{Gal}(K_r/K_{i-1})$ y que el cociente $\mathrm{Gal}(K_r/K_{i-1})/\mathrm{Gal}(K_r/K_i)$ es isomorfo a $\mathrm{Gal}(K_i/K_{i-1})$, que es un grupo cíclico. Por tanto, la existencia de la cadena anterior demuestra que $\mathrm{Gal}(K_r/K)$ es un grupo resoluble. De nuevo por el Teorema 5.21 se sigue que $\mathrm{Gal}(K_r/L)$ es un subgrupo normal de $\mathrm{Gal}(K_r/K)$ y que el cociente $\mathrm{Gal}(K_r/K)/\mathrm{Gal}(K_r/L)$ es isomorfo a $\mathrm{Gal}(L/K)$. Por el Lema 7.2 se concluye que $\mathrm{Gal}(L/K)$ es resoluble.

Recíprocamente, supongamos que $\mathrm{Gal}(L/K)$ es resoluble. Como querremos usar la Proposición 5.27 vamos a adjuntar primero suficientes raíces de la unidad. Concretamente, consideramos n el producto de todos los números primos distintos que dividen a $m!$ (donde m es el número de raíces distintas de f) y tomamos ω una raíz primitiva n-ésima de la unidad. Obsérvese que la nueva extensión $K \subset L(\omega)$ es también de Galois, ya que $L(\omega)$ será el cuerpo de descomposición sobre K de $(X^n-1)f$. Como $K \subset L$ es una extensión normal, se tiene (por el Teorema 5.21) que $\mathrm{Gal}(L(\omega)/L)$ es un subgrupo normal de $\mathrm{Gal}(L(\omega)/K)$ y que el cociente $\mathrm{Gal}(L(\omega)/K)/\mathrm{Gal}(L(\omega)/L)$ es isomorfo a $\mathrm{Gal}(L/K)$, que es un grupo resoluble. Como $\mathrm{Gal}(L(\omega)/L)$ es abeliano (ver el Ejemplo 5.26) y por tanto resoluble, se sigue del Lema 7.2 que $\mathrm{Gal}(L(\omega)/K)$ es resoluble. Del mismo lema se sigue entonces que $\mathrm{Gal}(L(\omega)/K(\omega))$ es un grupo resoluble. Existirá entonces una cadena de subgrupos

$$\{1\} = H_0 < H_1 < \ldots < H_{r-1} < H_r = \mathrm{Gal}(L(\omega)/K(\omega))$$

tal que cada H_{i-1} es normal en H_i y el cociente H_i/H_{i-1} es un grupo cíclico de orden primo. Por el Teorema 5.20, llamando $K_i = L(\omega)^{H_{r-i}}$ tendremos entonces una cadena de subcuerpos

$$K(\omega) = K_0 \subset K_1 \subset \ldots \subset K_r = L(\omega)$$

donde cada $\mathrm{Gal}(L(\omega)/K_i) \lhd \mathrm{Gal}(L(\omega)/K_{i-1})$ con $\mathrm{Gal}(L(\omega)/K_{i-1})/\mathrm{Gal}(L(\omega)/K_i)$ cíclico de orden primo. Usando ahora el Teorema 5.21 para la extensión $K_{i-1} \subset L(\omega)$ con cuerpo intermedio K_i, cada extensión $K_{i-1} \subset K_i$ es cíclica de orden primo, digamos p_i. Obsérvese que p_i es un divisor del orden de $\mathrm{Gal}(L(\omega)/K(\omega))$, y como $L(\omega)$ es el cuerpo de descomposición de f sobre $K(\omega)$, entonces $\mathrm{Gal}(L(\omega)/K(\omega))$ tiene orden un divisor de $m!$ (por el Lema 5.8), luego $p_i | n$. Por tanto, como K_{i-1} contiene a la raíz n-ésima primitiva de la unidad ω, contiene en particular a las raíces p_i-ésimas de la unidad, luego por la Proposición 5.27 se tendrá que existe $\alpha_i \in K_i$ tal que $\alpha_i^{p_i} \in K_{i-1}$. Como consecuencia, tenemos una torre radical $K \subset K_0 \subset K_1 \subset \ldots \subset K_r = L(\omega)$, que demuestra que f es resoluble por radicales. □

El teorema anterior muestra por qué se pueden resolver las ecuaciones cúbica y cuártica: El grupo de Galois de un polinomio de grado tres (resp. cuatro) es, por el Lema

5.8, un subgrupo de S_3 (resp. S_4) y S_3 y S_4 son grupos resolubles, ya que tenemos que A_3 es cíclico de orden tres y el subgrupo normal $H = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \lhd S_4$ con $S_4/H \cong S_3$ (Observación 6.5). Veamos ahora explícitamente cómo esto nos proporciona la resolubilidad de las ecuaciones cúbica y cuártica.

Ejemplo 7.4. Supongamos que tenemos una cúbica irreducible $f = X^3 + aX^2 + bX + c \in K[X]$ con tres raíces distintas $\alpha_1, \alpha_2, \alpha_3$. Veamos en primer lugar que el cuerpo de descomposición de f sobre K es $L = K(\Delta, \alpha_1)$, con $\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$. Evidentemente L está contenido en el cuerpo de descomposición, así que basta ver que $\alpha_2, \alpha_3 \in L$. Observamos primero que $\alpha_1 + \alpha_2 + \alpha_3 = -a \in K \subset L$, luego $\alpha_2 + \alpha_3 \in L$. De la misma forma, $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = b \in K \subset L$, y como $\alpha_1\alpha_2 + \alpha_1\alpha_3 = \alpha_1(\alpha_2 + \alpha_3) \in L$ (según acabamos de ver), se sigue que $\alpha_2\alpha_3$ también está en L. Por tanto, $(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) = \alpha_1^2 - \alpha_1(\alpha_2 + \alpha_3) + \alpha_2\alpha_3 \in L$, de donde se sigue que $\alpha_2 - \alpha_3 = \frac{\Delta}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)}$ está en L. Finalmente, escribiendo

$$\alpha_2 = \frac{\alpha_2 + \alpha_3}{2} + \frac{\alpha_2 - \alpha_3}{2}$$

$$\alpha_3 = \frac{\alpha_2 + \alpha_3}{2} - \frac{\alpha_2 - \alpha_3}{2}$$

(suponemos que K no es de característica dos) se concluye que $\alpha_2, \alpha_3 \in L$, lo que demuestra $L = K(\Delta, \alpha_1)$. Tenemos por tanto una cadena

$$K \subset K(\Delta) \subset L = K(\Delta, \alpha_1)$$

que, de acuerdo con la Observación 3.15, corresponde con la restricción a $\mathrm{Gal}(L/K)$ de la cadena

$$\{id\} \subset A_3 \subset S_3.$$

Como $\Delta^2 \in K$ (Corolario 3.14), la extensión $K \subset K(\Delta)$ tiene grado uno o dos, y como la extensión $K \subset K(\alpha_1)$ tiene grado tres (por ser f irreducible y, por tanto, el polinomio mínimo de α_1 sobre K), entonces $3|[L : K]$, de donde se deduce que el grado de la extensión $K(\Delta) \subset L = K(\Delta, \alpha_1)$ es exactamente tres (es a lo sumo tres porque el polinomio mínimo de α_1 sobre $K(\Delta)$ debe ser un divisor de f). Obtenemos así que $\mathrm{Gal}(L/K) = A_3$ si $\Delta \in K$ y $\mathrm{Gal}(L/K) = S_3$ si $\Delta \notin K$. La extensión $K(\Delta) \subset L = K(\Delta, \alpha_1)$ es cíclica de grado tres, luego si K contiene las raíces cúbicas de la unidad, por el Teorema 5.27 L se obtiene adjuntando a $K(\Delta)$ una raíz cúbica, que es exactamente lo que dice la fórmula (3.23).

Ejemplo 7.5. Supongamos que tenemos ahora $f = X^4 + aX^3 + bX^2 + cX + d \in K[X]$ con raíces distintas $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Veamos cómo se obtiene la resolubilidad de f a partir de la cadena

$$H_1 = \{id, (1\ 2)(3\ 4)\} \lhd H = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \lhd S_4.$$

Si $L = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, consideramos en virtud del Lema 5.8 $\mathrm{Gal}(L/K)$ como un subgrupo de S_4, y llamamos H' y H_1' a las respectivas intersecciones de H y H_1 con $\mathrm{Gal}(L/K)$. Identifiquemos primero el cuerpo $L^{H'}$. Claramente, los elementos

$$\beta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$$

$$\beta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$$

$$\beta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$$

son invariantes por las permutaciones de H, luego están en $L^{H'}$ y por tanto se tiene $K(\beta_1, \beta_2, \beta_3) \subset L^{H'}$. Por otra parte, los elementos $\beta_1, \beta_2, \beta_3$ son distintos entre sí, ya que por ejemplo $\beta_3 - \beta_2 = (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4) \neq 0$. De aquí se concluye fácilmente que cualquier permutación $\sigma \notin H$ no deja fijos simultáneamente $\beta_1, \beta_2, \beta_3$ sino que los permuta entre ellos. Esto quiere decir que $\mathrm{Gal}(L/K(\beta_1, \beta_2, \beta_3)) \subset H'$, y por la correspondencia de Galois $L^{H'}$ está contenido en $K(\beta_1, \beta_2, \beta_3)$, luego ambos coinciden (ya que hemos demostrado el otro contenido). De forma análoga se obtiene que $L^{H_1'} = K(\alpha_1 + \alpha_2, \alpha_3 + \alpha_4, \beta_2, \beta_3)$.

La primera observación importante es que $\beta_1, \beta_2, \beta_3$ son raíces de un mismo polinomio cúbico en $K[X]$. Los coeficientes de tal polinomio cúbico deben ser, salvo el signo, los polinomios simétricos elementales en $\beta_1, \beta_2, \beta_3$ (Lema 3.9), que a su vez son polinomios simétricos en $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, por lo que el resultado seguirá del Teorema 3.18. Pongamos las cuentas explícitamente (que se obtienen como en el Ejemplo 3.17):

$$\beta_1 + \beta_2 + \beta_3 = 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4) = 2b$$

y, poniendo directamente el resultado en los otros casos:

$$\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 = ac + b^2 - 4d$$

$$\beta_1\beta_2\beta_3 = abc - c^2 - a^2d$$

con lo que $\beta_1, \beta_2, \beta_3$ son las raíces del polinomio

$$g = X^3 - 2bX^2 + (ac + b^2 - 4d)X - abc + c^2 + a^2d$$

que es precisamente el polinomio que aparecía en el Ejemplo 3.26, y que se llama *resolvente cúbica de* f. En este contexto, el isomorfismo $S_4/H \cong S_3$ de la Observacion 6.5 debe interpretarse como el paso de las permutaciones de $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ a las permutaciones de $\beta_1, \beta_2, \beta_3$. En concreto, restringiendo todo a $\mathrm{Gal}(L/K)$ obtenemos el isomorfismo del Teorema 5.21: $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/K(\beta_1, \beta_2, \beta_3)) \cong \mathrm{Gal}(K(\beta_1, \beta_2, \beta_3)/K)$, y este último grupo es el el grupo de Galois del polinomio $g \in K[X]$.

Obsérvese ahora que, una vez calculadas las raíces de g, la extensión $K(\beta_1, \beta_2, \beta_3) \subset K(\alpha_1 + \alpha_2, \alpha_3 + \alpha_4, \beta_2, \beta_3)$ viene determinada porque de las relaciones

$$(\alpha_1 + \alpha_2) + (\alpha_3 + \alpha_4) = -a$$

$$(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = \beta_1$$

se obtiene que $\alpha_1+\alpha_2, \alpha_3+\alpha_4$ son las raíces del polinomio $X^2+aX-\beta_1$. Nótese que $\alpha_1\alpha_2$ y $\alpha_3\alpha_4$ también están en $L^{H_1'}$, luego deberían poder ponerse en función de los generadores. Esto se hace a partir de las relaciones:

$$b = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 = \alpha_1\alpha_2 + \alpha_3\alpha_4 + \beta_1$$

$$-c = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4 = \alpha_1\alpha_2(\alpha_3 + \alpha_4) + \alpha_3\alpha_4(\alpha_1 + \alpha_2)$$

que permiten despejar $\alpha_1\alpha_2$ y $\alpha_3\alpha_4$ en función de $b, c, \beta_1, \alpha_1+\alpha_2, \alpha_3+\alpha_4$ (el lector avispado habrá notado que existe un problema si $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4$; una forma de evitarlo es reordenando los subíndices, ya que no puede ocurrir que cada suma $\alpha_i + \alpha_j$ coincida con la suma de las otras dos raíces de f, pues en tal caso todas las raíces de f tendrían que ser iguales). También $\alpha_1\alpha_4 + \alpha_2\alpha_3$ y $\alpha_1\alpha_3 + \alpha_2\alpha_4$ están en $L^{H_1'}$, y se puede ver la expresión explícita escribiendo $\alpha_1\alpha_4+\alpha_2\alpha_3 = \beta_2 - \alpha_1\alpha_2 - \alpha_3\alpha_4$ y $\alpha_1\alpha_3+\alpha_2\alpha_4 = \beta_3 - \alpha_1\alpha_2 - \alpha_3\alpha_4$.

Finalmente, la extensión $K(\alpha_1+\alpha_2, \alpha_3+\alpha_4, \beta_2, \beta_3) \subset K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ viene determinada porque α_1 y α_2 son raíces de un polinomio cuadrático mónico con coeficientes $-\alpha_1 - \alpha_2$ y $\alpha_1\alpha_2$, y una vez determinadas α_1, α_2 se pueden determinar también α_3, α_4 mediante

$$\alpha_3 = \frac{\alpha_1(\alpha_3 + \alpha_4) - (\alpha_1\alpha_4 + \alpha_2\alpha_3)}{\alpha_1 - \alpha_2}$$

$$\alpha_4 = \frac{\alpha_2(\alpha_3 + \alpha_4) - (\alpha_1\alpha_4 + \alpha_2\alpha_3)}{\alpha_2 - \alpha_1}.$$

Para ecuaciones de grado al menos cinco, la situación es completamente diversa, ya que vamos a ver que S_n no es resoluble, puesto que A_n no lo es. De hecho, demostraremos algo más fuerte, que A_n no tiene siquiera subgrupos normales no triviales.

Definición. Un *grupo simple* es un grupo cuyos únicos subgrupos normales son él mismo y el $\{1\}$.

Observación 7.6. Nótese que un grupo simple G es resoluble si y sólo si es cíclico de orden primo. En efecto, si G es simple, la única cadena de subgrupos normales cada uno en el siguiente es $\{1\} \lhd G$. Entonces, por la definición (ii) de grupo resoluble, G será resoluble si y sólo si $G/\{1\}$ (es decir, G) es cíclico de orden primo.

Teorema 7.7 (Abel)**.** *Si $n \geq 5$, el grupo alternado A_n es simple.*

Demostración: Supongamos que tenemos $H \lhd A_n$ que no es ni el trivial ni el total. Veamos que H no puede contener ningún 3-ciclo. Para eso, usamos la igualdad, dados $i, j, k, l \in \{1, 2, \ldots, n\}$ distintos,

$$(j\ i\ l) = \big((i\ j)(k\ l)\big)\ (i\ j\ k)\ \big((i\ j)(k\ l)\big)^{-1}.$$

Como $(i\ j)(k\ l) \in A_n$ y H es normal, dicha igualdad demuestra que, cada vez que tenemos un 3-ciclo $(i\ j\ k)$ en H, tenemos también el 3-ciclo $(j\ i\ l)$ (y su cuadrado $(i\ j\ l)$). Por tanto, si tenemos un 3-ciclo en H, usando reiteradamente la observación anterior, se llega a que cualquier 3-ciclo está en H. Como A_n está generado por los 3-ciclos, se concluiría que $H = A_n$, contra nuestra hipótesis.

Tomemos ahora un elemento $\sigma \in H$ que no sea la identidad, y distingamos tres casos según se descomponga en producto de ciclos disjuntos:

Caso 1: Si algún ciclo de la factorización de σ tiene longitud al menos cuatro, podemos escribir $\sigma = (i\ j\ k\ l \ldots)\sigma_1 \ldots \sigma_r$. Como $(i\ j\ k) \in A_n$ y H es normal, tendremos que también $(i\ j\ k)\sigma(i\ j\ k)^{-1} = (j\ k\ i\ l \ldots)\sigma_1 \ldots \sigma_r$ está en H. Por tanto, también estará en H la permutación $(j\ k\ i\ l \ldots)\sigma_1 \ldots \sigma_r\sigma^{-1} = (i\ j\ l)$, lo que contradice el hecho de que H no contiene 3-ciclos.

Caso 2: Si σ factoriza en 3-ciclos y transposiciones, con al menos una transposición, como σ es par, los 3-ciclos son pares y las transposiciones son impares, habrá al menos dos transposiciones en la descomposición. Por tanto, podremos escribir $\sigma = (i\ j)(k\ l)\sigma_1 \ldots \sigma_r$. De la normalidad de H obtenemos ahora que $(i\ j\ k)\sigma(i\ j\ k)^{-1} = (j\ k)(i\ l)\sigma_1 \ldots \sigma_r$ está en H, luego también estará en H la permutación $(j\ k)(i\ l)\sigma_1 \ldots \sigma_r\sigma^{-1} = (i\ k)(j\ l)$. Como $n \geq 5$, podemos tomar $m \in \{1, 2, \ldots, n\}$ distinto de i, j, k, l. Tendremos entonces que $(i\ k\ m)(i\ k)(j\ l)(i\ k\ m)^{-1} = (k\ m)(j\ l)$ también está en H, con lo que también estará $(i\ k)(j\ l)(k\ m)(j\ l) = (i\ k\ m)$, lo que contradice de nuevo el hecho de que H no contiene 3-ciclos.

Caso 3: Si σ factoriza en 3-ciclos, como H no contiene 3-ciclos, habrá al menos dos factores, luego podemos escribir $\sigma = (i\ j\ k)(i'\ j'\ k')\sigma_1 \ldots \sigma_r$. La normalidad de H implica ahora que $(i\ i')(j\ j')\sigma((i\ i')(j\ j'))^{-1} = (i'\ j'\ k)(i\ j\ k')\sigma_1 \ldots \sigma_r$ está también en H. Por tanto, también estará en H la permutación $(i'\ j'\ k)(i\ j\ k')\sigma_1 \ldots \sigma_r\sigma^{-1} = (i\ i')(k\ k')$, posibilidad que hemos eliminado en el caso anterior.

Por tanto, llegamos siempre a una contradicción por lo que no existe tal H, lo que implica que A_n es un grupo simple. □

Corolario 7.8. *Sea $f \in K[X]$ un polinomio de grado $n \geq 5$ cuyo grupo de Galois sea S_n o A_n. Entonces f no es resoluble por radicales.*

Demostración: Por el Teorema 7.3, hay que ver que ni S_n ni A_n son resolubles. Por el Lema 7.2 basta ver que A_n no es resoluble. Pero esto es evidente por la Observación 7.6, ya que A_n no tiene orden primo, mientras que, por el Teorema 7.7, es simple. □

Veamos algún ejemplo concreto de polinomio no resoluble.

Corolario 7.9. *Sea $f \in \mathbb{Q}[X]$ un polinomio irreducible de grado primo $p \geq 5$, con $p-2$ raíces reales y un par de raíces imaginarias conjugadas. Entonces f no es resoluble por radicales.*

Demostración: Sea L el cuerpo de descomposición de f sobre $\mathbb{Q}$. Como L contiene a $Q[X]/(f)$, que tiene grado p sobre $\mathbb{Q}$, se sigue que $[L : \mathbb{Q}]$ es divisible por p. Como $[L : \mathbb{Q}] = |\operatorname{Gal}(L/\mathbb{Q})|$, por el Teorema de Cauchy (Teorema 6.8(iv)) se tiene que $\operatorname{Gal}(L/K)$ posee un elemento de orden p. Viendo $\operatorname{Gal}(L/K)$ como un subgrupo de S_p (por el Lema 5.8), y teniendo en cuenta que los únicos elementos de S_p de orden p son los p-ciclos, se concluye que $\operatorname{Gal}(L/K)$ contiene un p-ciclo. Por otra parte, la restricción a L de la conjugación en $\mathbb{C}$ define un elemento de $\operatorname{Gal}(L/\mathbb{Q})$, que visto como elemento en S_p consiste en la transposición de las dos raíces imaginarias de f. Por tanto, $\operatorname{Gal}(L/\mathbb{Q})$ contiene un p-ciclo y una transposición, que generan todo S_p (véase el Ejercicio 1.2(iii)), luego $\operatorname{Gal}(L/\mathbb{Q})$ es S_p, de donde se concluye por el Corolario 7.8 que f no es resoluble por radicales. □

Ejemplo 7.10. El primer caso en que se puede aplicar el corolario anterior es para polinomios de grado cinco. En este caso, según la Observación 3.16, el hecho de que un polinomio irreducible de grado cinco tenga exactamente dos raíces imaginarias conjugadas viene caracterizado por $D < 0$. Por el Corolario 3.14 sabemos que $D = \Delta^2 = R(f, f')$. Por calcularlo en un caso sencillo, si $f = X^5 + aX + b$, entonces $D = 256a^5 + 3125b^4$ (en realidad, con un poco de análisis real sobre el crecimiento y decrecimiento del polinomio es muy fácil ver que f tiene exactamente tres raíces reales si y sólo si $= 256a^5 + 3125b^4 < 0$). Si, fijado p un número primo, tomamos entonces $f = X^5 - cpX + dp$, con $p \not| d$ (luego f será irreducible por el criterio de Eisenstein) y $256c^5p > 3125d^4$ tendremos que f no es resoluble por radicales. Por poner un ejemplo concreto, $X^5 - 4X + 2$ no es resoluble por radicales.

Ejercicio 7.11. Demostrar que el polinomio $15X^7 - 84X^5 - 35X^3 + 420X + 7 \in \mathbb{Q}[X]$ no es resoluble por radicales.

Cabe preguntarse si, para cada grado n, existe un polinomio de grado n con grupo de Galois S_n. La respuesta es afirmativa, y el siguiente ejemplo da un modo de hacerlo (aunque posiblemente no sea el modo que desearía el lector, ya que no se trata de dar números concretos a los coeficientes sino de construir un polinomio "universal").

Ejemplo 7.12. Sea K un cuerpo y sea $L = K(X_1, \ldots, X_n)$ el cuerpo de fracciones del anillo de polinomios con coeficientes en K en las indeterminandas $X_1, \ldots, X_n$. Si $e_1, \ldots, e_n$ son los polinomios simétricos elementales en $X_1, \ldots, X_n$, tomamos $K' = K(e_1, \ldots, e_n) \subset L$. Sea el polinomio $f = X^n - e_1 X^{n-1} + \ldots + (-1)^{n-1} e_{n-1} X + (-1)^n e_n \in K'[X]$. Por el Lema 3.9, $f = (X - X_1) \ldots (X - X_n)$, es decir, $X_1, \ldots, X_n$ son las raíces de f, lo que demuestra que L es el cuerpo de descomposición de f sobre K'. Además, la extensión $K' \subset L$ es de Galois, por ser f separable al tener las raíces distintas. Claramente, para cualquier $\sigma \in S_n$ se tiene que la asignación $\frac{P(X_1,\ldots,X_n)}{Q(X_1,\ldots,X_n)} \mapsto \frac{P(X_{\sigma(1)},\ldots,X_{\sigma(n)})}{Q(X_{\sigma(1)},\ldots,X_{\sigma(n)}}$ es un automorfismo de L que deja fijos los elementos de K', por lo que $\mathrm{Gal}(L/K') = S_n$. Por tanto, si $n \geq 5$, f no es resoluble por radicales. Esto está diciendo que no existe una fórmula usando sólo radicales que dé las raíces de f en función de sus coeficientes $e_1, \ldots, e_n$.

Otra consecuencia interesante de esta construcción es que implica que cualquier grupo finito es grupo de Galois de alguna extensión de cuerpos. En efecto, como observamos en el Ejemplo 6.2(i), cualquier grupo finito G es isomorfo a un subgrupo de S_n. Aplicando la correspondencia de Galois a nuestro ejemplo, G será entonces el grupo de Galois de L sobre L^G.

Finalizamos la sección observando que en general no es fácil encontrar grupos simples. De hecho, que un grupo sea simple es una condición muy fuerte, ya que en particular todo homomorfismo de un grupo simple a otro grupo es necesariamente constante o inyectivo (ya que el núcleo es un grupo normal) . Además, los teoremas de Sylow obligan muchas veces a que exista un único p-subgrupo de Sylow para algún p, y por tanto el grupo no es simple. Veamos un par de ejemplos concretos de cómo se puede aplicar toda la teoría de grupos que hemos visto. Primero recordamos la acción del Ejemplo Ejemplo 6.2(v), de la que sacamos ya una primera conclusión (que generaliza el hecho de que los subgrupos de índice dos son normales):

Proposición 7.13. *Sea H un subgrupo de un grupo G. Entonces:*

(i) Si $\rho : G \times G/\sim H \to G/\sim H$ es la acción definida por $g * (xH) = (gx)H$, se tiene $\ker \hat{\rho} \subset H$.

(ii) $\ker \hat{\rho} = H$ *si y sólo si* $H \lhd G$.

(iii) Si $[G : H]$ es el menor número primo que divide a $|G|$, entonces H es normal en G.

Demostración: Para demostrar (i), sea $g \in \ker \hat{\rho}$, por lo que se tendrá $g * (xH) = xH$ (es decir, $(gx)H = xH$) para todo $x \in G$. En particular, si tomamos $x = 1$, se obtiene $gH = H$ y, por tanto, $g \in H$.

Para ver (ii), tendremos que $\ker \hat{\rho} = H$ si y sólo si para cada $h \in H$ y cada $x \in G$ se tiene $(hx)H = xH$. Esto es equivalente a decir $x^{-1}hx \in H$, es decir, $H \lhd G$.

Para demostrar (iii), escribimos $p = [G : H]$ y $n = |H|$. Podemos ver entonces la acción ρ como un homomorfismo de grupos $\hat{\rho} : G \to S_p$. Por el primer teorema de isomorfía, tendremos un monomorfismo $G/\ker\hat{\rho} \hookrightarrow S_p$ y, por tanto $[G : \ker\hat{\rho}]$ divide a $p!$. Como $\ker\hat{\rho} \subset H$, se tendrá que el orden de $\ker\hat{\rho}$ es un divisor n' de n, es decir, $[G : \ker\hat{\rho}] = p\frac{n}{n'}$. Tenemos pues que $\frac{n}{n'}$ divide a $(p-1)!$. Como por hipótesis ningún factor primo de np es menor que p, se tiene que necesariamente $\frac{n}{n'} = 1$, es decir, $\ker\hat{\rho} = H$. Por (iii), H es normal en G. □

Ejemplo 7.14. Sea G un grupo de orden 120 y veamos que no puede ser simple. Por el tercer tercer teorema de Sylow, el número de 5-subgrupos de Sylow de G es uno o seis. Si fuera $n_5 = 1$, entonces ya tendríamos que G tiene un grupo normal, así que supondremos $n_5 = 6$ y buscaremos una contradicción. Por el tercer teorema de Sylow (Teorema 6.11), G tiene un subgrupo H de índice seis (el normalizador de cualquier 5-subgrupo de Sylow). Considerando la acción ρ de G sobre G/H (véase el Ejemplo 6.2(v)) tendremos un homomorfismo $\hat{\rho} : G \to S_6$. Como $\ker\hat{\rho} \subset H$, no puede ser $\ker\hat{\rho} = G$, y como G es simple y $\ker\hat{\rho} \lhd G$, se sigue que $\ker\hat{\rho} = \{1\}$. Por tanto, $\hat{\rho}$ permite identificar G con un subgrupo de S_6. Como A_6 es normal en S_6, entonces $G \cap A_6$ es normal en G, lo que implica que $G \cap A_6$ es G, es decir, $G \subset A_6$. Se tiene entonces que A_6 contiene un subgrupo de G de índice tres. Esto implica que, haciendo actuar ahora A_6 sobre A_6/G, se obtiene un homomorfismo $A_6 \to S_3$ que no puede ser constante (ya que el núcleo está contenido en G). Esto es absurdo, ya que por ser A_6 normal, entonces la aplicación debería ser inyectiva.

Proposición 7.15. *Sea G un grupo de orden p^2q^2 con $p < q$ primos distintos. Entonces G no es simple.*

Demostración: Por los teoremas de Sylow, el número de q-subgrupos de Sylow de G es 1 o p^2 (no puede ser p, porque al ser $p < q$ no puede ocurrir $p \equiv 1 \ (mod\ q)$). Si G es simple, necesariamente el número de q-subgrupos de Sylow de G es p^2. Si demostramos que dos q-subgrupos de Sylow cualesquiera tienen sólo en común el elemento neutro habremos terminado. En efecto, en tal caso, la unión de los q-subgrupos de Sylow quitando tendrá $p^2(q^2-1)$ elementos si excluimos el neutro, y todos ellos tendrán orden q o q^2. Quedan por tanto otros p^2 elementos del grupo con los que poder formar p-subgrupos de Sylow, por lo que sólo hay un p-subgrupo de Sylow y por tanto G no es simple.

Veamos por tanto que, dados H, H' dos q-subgrupos de Sylow distintos, se tiene $H \cap H' = \{1\}$. Si no fuera así, entonces $H \cap H'$ tendría orden q. Como H y H' son abelianos (véase la Proposición 6.7(iv)), necesariamente $H \cap H'$ es normal en H y H'. Entonces el normalizador $N(H \cap H')$ contiene a H y H' y por tanto su orden es mayor que q^2. Como $H \cap H'$ no puede ser normal en G, la única posibilidad es que $N(H \cap H')$ tenga

orden pq^2. Pero por el tercer teorema de Sylow, $N(H \cap H')$ tendría un único q-subgrupo de Sylow, lo que es absurdo, ya que contiene a H y H'. Esta contradicción concluye la demostración. □

Un buen ejercicio para usar todas estas técnicas es estudiar los grupos hasta orden 200:

Ejercicio 7.16. Demostrar que si p, q y r son primos distintos, cualquier grupo de orden p^k, pq, p^2q ó pqr no es simple. Concluir que no hay grupos simples de orden menor o igual que 200, excepto para orden primo, orden 60 (en que el grupo es necesariamente A_5) y orden 168 (en que se puede demostrar que el grupo es isomorfo a $GL_3(\mathbb{Z}_2)$; se sugiere al lector probar a demostrar la parte menos difícil, que $GL_3(\mathbb{Z}_2)$ es, en efecto, simple).

En realidad, se sabe mucho más de lo que hemos indicado aquí. Por ejemplo, un teorema de Burnside afirma que todos los grupos de orden p^kq^l, donde p, q son números primos, son resolubles (y por tanto no son simples, salvo que tengan orden primo). Además, los grupos finitos simples estásn clasificados, y son o bien de varios familias concretas (los grupos cíclicos de orden primo, los grupos alternados A_n con $n \geq 5$, los grupos especiales lineales o proyectivos sobre cuerpos finitos,...) o bien 26 ejemplos particulares, llamados *grupos esporádicos*. El mayor de estos grupos esporádicos tiene orden 808.017.424.794.512.875.886.459.904.961.710.757.005.754.368.000.000.000, o factorizado en primos 2^{46} 3^{20} 5^9 7^6 11^2 13^3 17 19 23 31 41 47 59 71, (por lo que se le llama *grupo monstruo*). La demostración de esta clasificación es tan larga que no todos la dan por buena, y de hecho actualmente se continúa trabajando en una demostración simplificada.

8. Constructibilidad con regla y compás

Dados dos puntos O y A en el plano euclídeo, nos preguntamos cuántos puntos podemos ir construyendo con una regla (que permite trazar la recta $L(P,Q)$ entre dos puntos P y Q ya construidos) y un compás (que permite trazar la circunferencia $C(P,Q)$ con centro un punto P ya construido y que pasa por otro punto Q ya construido) a partir de de cortar rectas y circunferencias entre sí. La relación con lo que hemos visto hasta ahora es que para hacer esas intersecciones hay que resolver ecuaciones algebraicas, y lo que queremos ver es cómo de complicadas son esas ecuaciones al ir reiterando construcciones de este tipo.

Definición. Dados puntos P, Q, R, S (no necesariamente distintos), diremos que el punto T es constructible a partir de ellos si T pertenece a una de las siguientes intersecciones:

(i) $L(P,Q) \cap L(R,S)$ (si las dos rectas son distintas).

(ii) $L(P,Q) \cap C(R,S)$.

(iii) $C(P,Q) \cap C(R,S)$ (si las dos circunferencias son distintas).

Un *punto constructible* es un punto P que o bien es O, A o bien existen $P_1, \ldots, P_n = P$ tales que cada P_i es constructible a partir de un subconjunto de $\{O, A, P_1, P_2, \ldots, P_{i-1}\}$. Por extensión llamaremos *recta constructible* a una recta determinanda por dos puntos constructibles y *circunferencia constructible* a una circunferencia de centro un punto constructible que pasa por otro punto constructible. Del mismo modo, un *ángulo constructible* es un ángulo formado por dos rectas constructibles.

Veamos los ejemplos más sencillos de constructibilidad:

Lema 8.1. *Si P, Q son dos puntos constructibles distintos, entonces también es constructible el punto simétrico de P respecto de Q.*

Demostración: Basta intersecar la recta $L(P,Q)$ con la circunferencia $C(P,Q)$; un punto de intersección es Q y el otro es el simétrico de P respecto de Q. □

Lema 8.2. *Si P, Q son dos puntos constructibles distintos, entonces también son constructibles el punto medio R de ambos y la recta perpendicular a $L(P,Q)$ que pasa por R.*

Demostración: La intersección de las circunferencias $C(P,Q)$ y $C(Q,P)$ dan dos puntos (que por definición son constructibles) de la perpendicular a $L(P,Q)$ por el punto R, luego tal perpendicular es constructible. El punto R es entonces la intersección de dicha perpendicular con la recta $L(P,Q)$, y por tanto también es constructible. □

Lema 8.3. *Si P, Q son dos puntos constructibles distintos y R es otro punto constructible (no necesariamente fuera de la recta $L(P,Q)$), entonces es constructible la recta perpendicular a $L(P,Q)$ que pasa por R. En particular, si R no está en la recta $L(P,Q)$, entonces es constructible el punto simétrico de R respecto de la recta $L(P,Q)$.*

Demostración: Como P y Q son distintos, R es distinto de al menos uno de ellos, supongamos que P. Entonces podemos construir el otro punto P' (distinto de P) en la intersección de la recta $L(P,Q)$ y la circunferencia $C(R,P)$. Por el Lema 8.2, como podemos construir entonces la recta perpendicular a $L(P,P') = L(P,Q)$ que pasa por el punto medio de P y P', que necesariamente pasa por R. Si $R \notin L(P,Q)$, entonces su simétrico se contruye a partir de la intersección de esta recta perpendicular con la circunferencia de centro el punto medio de P y P' que pasa por R. □

Lema 8.4. *Si P, Q son dos puntos constructibles distintos y R es otro punto constructible, entonces es constructible la recta paralela a $L(P,Q)$ que pasa por R.*

Demostración: Por el Lema 8.3, podemos construir la recta r perpendicular a $L(P,Q)$ que pasa por R. De nuevo por el Lema 8.3, construimos ahora la recta r' perpendicular a r que pasa por R. Como r' y $L(P,Q)$ son ambas perpendiculares a r', se sigue que son paralelas, luego r' es la recta buscada. □

Lema 8.5. *Sean P, Q dos puntos construibles distintos y sea R un punto construible en una recta construible r. Entonces se pueden construir los puntos de r que distan de R lo mismo que la distancia de P a Q.*

Demostración: Veamos en primer lugar que podemos suponer que el punto P no está en la recta r. Si lo estuviera, consideramos la intersección de la circunferencia $C(Q,P)$ con la perpendicular a r que pasa por Q. Esta intersección consiste necesariamente en ds puntos constructibles, y al menos uno de ellos, llamémoslo P', no está en r. Como Q equidista de P y P', basta encontrar una solución al problema tomando P' en vez de P.

Supuesto entonces que P no está en r, construimos, usando el Lema 8.4, la recta paralela a r que pasa por P (que no coincidirá con r porque $P \notin r$). Tomamos un punto Q' en la intersección de esta recta con $C(P,Q)$, con lo que se tendrá que $L(P,Q')$ es la paralela a r por P y que la distancia de P a Q' es la misma que la distancia de P a Q. Usando de nuevo el Lema 8.4, podemos construir la intersección R' de r con la paralela a $L(P,R)$ que pasa por Q'. Este punto verifica que dista a R la distancia de P a Q (el otro se obtiene cortando r con $C(R,R')$). □

Obsérvese que en realidad la construcción del lema anterior se puede hacer con cualquier compás normal: se "pincha" el compás en el punto P, se abre hasta que llegue al punto

Q y se levanta el compás hasta pincharlo en el punto R; sin embargo, este movimiento de levantar el compás no está contemplado en nuestra definición de constructibilidad. Del mismo modo, hay que demostrar rigurosamente que con nuestros axiomas se pueden trasladar ángulos.

Lema 8.6. *Si α es un ángulo constructible, entonces dada una recta r constructible y un punto $P \in r$ constructible se puede construir una recta que pase por P y forme con r un ángulo α.*

Demostración: Como se puede construir α, esto quiere decir que se pueden construir tres puntos P', Q', R' tales que el ángulo que forman en P' las rectas $L(P', Q')$ y $L(P, R')$ es α. Construimos en primer lugar un punto $Q \in r$ que diste de P exactamente la longitud de P' a Q' (lo que se puede hacer por el Lema 8.5). En segundo lugar (y aplicando el mismo resultado) podemos construir las circunferencias de centro P y radio la distancia de P' a R' y de centro Q y radio la distancia de Q' a R'. Si R es un punto en la intersección de ambas circunferencias (y por tanto constructible) se sigue que las rectas $r = L(P, Q)$ y $L(P, R)$ forman en P un ángulo α. □

Trasladamos todo lo visto hasta ahora al lenguaje de las coordenadas cartesianas en el plano euclídeo. Para ello, escogemos un sistema de coordenadas en que el punto O es el origen $(0, 0)$, la distancia de O a A es la unidad y tomamos A como el punto $(1, 0)$. En particular, la recta $\{Y = 0\}$ es constructible. Por el Lema 8.3, también es constructible la perpendicular a $\{Y = 0\}$ desde el punto $(0, 0)$, es decir, la recta $\{X = 0\}$. La primera observación importante es la siguiente:

Proposición 8.7. *El punto (x, y) es constructible si y sólo si los puntos $(x, 0)$ y $(0, y)$ son constructibles.*

Demostración: Si (x, y) es constructible, por el Lema 8.3, son constructibles las perpendiculares a $\{Y = 0\}$ y $\{X = 0\}$ que pasan por (x, y), es decir, las rectas $\{X = x\}$ e $\{Y = y\}$. Cortando respectivamente dichas rectas con $\{Y = 0\}$ y $\{X = 0\}$ tenemos que son constructibles los puntos $(x, 0)$ y $(0, y)$.

Recíprocamente, si son constructibles los puntos $(x, 0)$ y $(0, y)$, por el Lema 8.3 es constructible la recta que pasa por $(x, 0)$ perpendicular a $\{Y = 0\}$ y la recta que pasa por $(0, y)$ perpendicular a $\{X = 0\}$. Es decir, son constructibles las rectas $\{X = x\}$ e $\{Y = y\}$. Intersecando ambas rectas, se obtiene que es constructible el punto (x, y). □

Observación 8.8. Obsérvese que, por el Lema 8.5, el punto $(x, 0)$ es constructible si y sólo si se pueden construir dos puntos que estén a distancia $|x|$, ya que en tal caso basta

construir los puntos de la recta $\{Y = 0\}$ que están a distancia $|x|$ del punto $(0, 0)$, que son precisamente los puntos $(\pm x, 0)$. De la misma forma, el punto $(0, y)$ es constructible si y sólo si se pueden construir dos puntos que estén a distancia $|y|$. En particular, el punto $(x, 0)$ es constructible si y sólo si es constructible el punto $(0, x)$. Basta por tanto estudiar los números $x \in \mathbb{R}$ tales que $(x, 0)$ es constructible. El resultado siguiente muestra que el conjunto de tales números tiene estructura de cuerpo.

Teorema 8.9. *El conjunto* $K = \{x \in \mathbb{R} \mid (x, 0) \text{ es constructible}\}$ *es un subcuerpo de* $\mathbb{R}$.

Demostración: Basta sólo demostrar que, dados $x, x' \in K$ entonces $x - x' \in K$ y, suponiendo $x' \neq 0$, también $\frac{x}{x'} \in K$.

En primer lugar, como podemos construir la distancia $|x'|$, podemos construir los puntos de la recta $\{Y = 0\}$ que distan $|x'|$ de $(x, 0)$; estos puntos son precisamente $(x \pm x', 0)$, lo que demuestra la primera parte.

En segundo lugar, construimos la recta que pasa por $(0, x')$ y $(x, 0)$ (de ecuación $x'X + xY - xx' = 0$). El Lema 8.4 permite construir la recta paralela a la recta anterior que pasa por $(0, 1)$ (que tiene ecuación $x'X + xY - x = 0$). Entonces $(\frac{x}{x'}, 0)$ es el punto de intersección de esta última recta con $\{Y = 0\}$, luego $\frac{x}{x'} \in K$. □

Lema 8.10. *Si* $x > 0$ *está en el cuerpo* K*, entonces* $\pm\sqrt{x} \in K$.

Demostración: Usamos en primer lugar que K es un cuerpo que contiene a $\mathbb{Q}$, luego $\frac{x\pm1}{2} \in K$. Construimos pues la circunferencia de centro $(\frac{x-1}{2}, 0)$ de radio $\frac{x+1}{2}$ (de ecuación $X^2 + Y^2 - (x - 1)X = x$) y la cortamos con el eje vertical $\{X = 0\}$. Obtenemos entonces los puntos $(0, \pm\sqrt{x})$, luego $\pm\sqrt{x} \in K$. □

Observación 8.11. El lema anterior implica que la extensión $\mathbb{Q} \subset K$ no es finita. En efecto, si $[K : \mathbb{Q}]$ fuera un número finito, siempre podríamos encontrar $n \in \mathbb{N}$ tal que $2^n > [K : \mathbb{Q}]$, y por el lema anterior $\sqrt[2^n]{2} \in K$. Como $[\mathbb{Q}(\sqrt[2^n]{2}) : \mathbb{Q}] = 2^n$ debe dividir a $[K : \mathbb{Q}]$, se llegaría a un absurdo. El Teorema 8.12 siguiente probará que, sin embargo, la extensión $[K : \mathbb{Q}]$ es algebraica.

La idea ahora es que para ir construyendo puntos hay que cortar dos rectas (que son ecuaciones lineales), una recta y una circunferencia (que da lugar a una ecuación de grado dos) o dos circunferencias (que geométricamente es la intersección de una recta y una circunferencia). Parece por tanto que las coordenadas de cada punto constructible (es decir, los elementos de K) se obtienen después de resolver una cantidad finita de ecuaciones cuadráticas. Esto es lo que afirma el siguiente resultado:

Teorema 8.12. *Sea α un número real. Entonces $\alpha \in K$ si y sólo si existe una cadena de cuerpos $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_r$ tal que $\alpha \in K_r$ y cada extensión $K_{i-1} \subset K_i$ tiene grado dos. En particular, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ es una potencia de dos.*

Demostración: Supongamos en primer lugar que $\alpha \in K$, es decir, que $(\alpha, 0)$ es un punto constructible. Bastará ver que cada vez que un punto (α, β) es constructible a partir de $(\alpha_1, \beta_1), (\alpha_2, \beta_2), (\alpha_3, \beta_3), (\alpha_4, \beta_4)$, entonces α, β están en una extensión de grado a lo sumo dos de $\mathbb{Q}(\alpha_1, \beta_1, \alpha_2, \beta_2, \alpha_3, \beta_3, \alpha_4, \beta_4)$. Lo demostraremos según los tres posibles casos de constructibilidad:

–Si $(\alpha, \beta) \in L((\alpha_1, \beta_1), (\alpha_2, \beta_2)) \cap L((\alpha_3, \beta_3), (\alpha_4, \beta_4))$, entonces se tiene

$$(\beta_1 - \beta_2)\alpha - (\alpha_1 - \alpha_2)\beta = \alpha_2\beta_1 - \alpha_1\beta_2$$

$$(\beta_3 - \beta_4)\alpha - (\alpha_3 - \alpha_4)\beta = \alpha_4\beta_3 - \alpha_3\beta_4.$$

Como las rectas $L((\alpha_1, \beta_1), (\alpha_2, \beta_2))$ y $L((\alpha_3, \beta_3), (\alpha_4, \beta_4))$ son distintas, el sistema tiene una única solución α, β, que evidentemente está en $\mathbb{Q}(\alpha_1, \beta_1, \alpha_2, \beta_2, \alpha_3, \beta_3, \alpha_4, \beta_4)$.

–Si $(\alpha, \beta) \in L((\alpha_1, \beta_1), (\alpha_2, \beta_2)) \cap C((\alpha_3, \beta_3), (\alpha_4, \beta_4))$, entonces se tiene ahora

$$(\beta_1 - \beta_2)\alpha - (\alpha_1 - \alpha_2)\beta = \alpha_2\beta_1 - \alpha_1\beta_2$$

$$(\alpha - \alpha_3)^2 + (\beta - \beta_3)^2 = (\alpha_4 - \alpha_3)^2 + (\beta_4 - \beta_3)^2.$$

Como $(\alpha_1, \beta_2) \neq (\alpha_2, \beta_2)$, de la primera ecuación se puede despejar α ó β en función (lineal) de la otra coordenada, y sustituyendo en la otra ecuación tenemos que β ó α es raíz de un polinomio cuadrático con coeficientes en $\mathbb{Q}(\alpha_1, \beta_1, \alpha_2, \beta_2, \alpha_3, \beta_3, \alpha_4, \beta_4)$. Por tanto, α y β están en una extensión de grado al menos dos de dicho cuerpo.

–Si finalmente $(\alpha, \beta) \in C((\alpha_1, \beta_1), (\alpha_2, \beta_2)) \cap C((\alpha_3, \beta_3), (\alpha_4, \beta_4))$, se tiene

$$(\alpha - \alpha_1)^2 + (\beta - \beta_1)^2 = (\alpha_2 - \alpha_1)^2 + (\beta_2 - \beta_1)^2$$

$$(\alpha - \alpha_3)^2 + (\beta - \beta_3)^2 = (\alpha_4 - \alpha_3)^2 + (\beta_4 - \beta_3)^2.$$

Restando ambas ecuaciones, dichas ecuaciones son equivalentes a

$$(2\alpha_3 - 2\alpha_1)\alpha + (2\beta_3 - 2\beta_1)\beta = \alpha_2^2 - 2\alpha_1\alpha_2 + \beta_2^2 - 2\beta_1\beta_2 - \alpha_4^2 + 2\alpha_3\alpha_4 - \beta_4^2 + 2\beta_3\beta_4$$

$$(\alpha - \alpha_3)^2 + (\beta - \beta_3)^2 = (\alpha_4 - \alpha_3)^2 + (\beta_4 - \beta_3)^2,$$

que como en el caso de recta y circunferencia dan lugar a una extensión de grado a lo más dos de $\mathbb{Q}(\alpha_1, \beta_1, \alpha_2, \beta_2, \alpha_3, \beta_3, \alpha_4, \beta_4)$.

Recíprocamente, supongamos ahora que tenemos una cadena de cuerpos $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_r$ tal que $\alpha \in K_r$ y cada extensión $K_{i-1} \subset K_i$ tiene grado dos. Veamos por inducción sobre r que $(\alpha, 0)$ es constructible. Si $r = 0$, entonces $(\alpha, 0)$ tiene coordenadas racionales, luego es constructible. Supongamos entonces $r > 0$, y que $\alpha \in K_r$, donde $K_{r-1} \subset K_r$ es una extensión de grado dos. Por tanto, existe una relación de grado dos $\alpha^2 + a\alpha + b = 0$, con $a, b \in K_{r-1}$. Es decir, $\alpha = \frac{a}{2} \pm \frac{\sqrt{a^2-4b}}{2}$ (obsérvese que el radicando es positivo, ya que α es real). Por hipótesis de inducción $a, b \in K$, luego por el Lema 8.10 también $\pm\sqrt{a^2 - 4b} \in K$, luego $\alpha \in K$. □

Un modo alternativo de hacer la construcción anterior es identificando un punto (x, y) del plano con el número complejo $x + yi$. En este caso, el resultado es el siguiente

Teorema 8.13. *El conjunto* $L = \{x + yi \in \mathbb{C} \mid (x, y) \text{ es constructible}\}$ *es el subcuerpo de* $K[i]$ *de* $\mathbb{C}$. *Por tanto, un número complejo* z *está en* L *si y sólo si existe una cadena de cuerpos* $\mathbb{Q} = L_0 \subset L_1 \subset \ldots \subset L_r$ *tal que* $z \in L_r$ *y cada extensión* $L_{i-1} \subset L_i$ *tiene grado dos. En particular,* $[\mathbb{Q}(z) : \mathbb{Q}]$ *es una potencia de dos.*

Demostración: Por definición $z = x + yi \in K$ si y sólo si el punto (x, y) es constructible, lo que es equivalente, por la Proposición 8.7, a que los puntos $(x, 0)$ y $(0, y)$ sean constructibles. Por la Observación 8.8, esto equivale a que $x, y \in K$, que es lo mismo que decir $z = x + yi \in K[i]$. □

Ejercicio 8.14. Demostrar que las rectas del plano complejo son los subconjuntos de ecuación $\alpha z + \bar{\alpha}\bar{z} + r = 0$, con $\alpha \in \mathbb{C} \setminus \{0\}$ y $r \in \mathbb{R}$, y que las circunferencias son los subconjuntos de ecuación $z\bar{z} + \alpha z + \bar{\alpha}\bar{z} + r = 0$, con $\alpha \in \mathbb{C}$, $r \in \mathbb{R}$ y $||\alpha||^2 - r > 0$. Completando $\mathbb{C}$ con un punto en el infinito (por ejemplo, considerando $\mathbb{P}^1_{\mathbb{C}}$), demostrar que las *transformaciones de Möbius* $z \mapsto \frac{az+b}{cz+d}$ (con $a, b, c, d \in \mathbb{R}$ y $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$) son biyecciones que mandan rectas y/o circunferencias a rectas y/o circunferencias. Estudiar cuándo la imagen de una recta es una circunferencia y viceversa. Lo mismo para transformaciones del tipo $z \mapsto \frac{a\bar{z}+b}{c\bar{z}+d}$.

Veamos finalmente algunas aplicaciones usuales (alguna de ellas problemas clásicos) del Teorema 8.12.

Ejemplo 8.15. (Trisección del ángulo) Veamos en primer lugar que no se puede construir con regla y compás un ángulo que mida la tercera parte de un ángulo dado. Si fuera posible, en particular se podría construir un ángulo de 10^o, ya que un ángulo de 30^o se puede construir, así que veamos que es imposible construir un ángulo de 10^o. Si pudiera

construirse, por el Lema 8.5 se podría construir una circunferencia de radio uno centrada en el vértice del ángulo, es decir, se podría construir un triángulo isósceles con dos lados de longitud uno y ángulo opuesto de 10^o. Trazando la altura desde uno de los vértices con ángulo 85^o (que se puede construir por el Lema 8.2), obtendríamos un segmento de longitud $\operatorname{sen} 10^o$, luego $\operatorname{sen} 10^o \in K$. Sin embargo, de la fórmula $\cos 3\alpha + i \operatorname{sen} 3\alpha = e^{3i\alpha} = (\cos\alpha + i \operatorname{sen}\alpha)^3$ se deduce que $\operatorname{sen} 3\alpha = 3\cos^2\alpha \operatorname{sen}\alpha - \operatorname{sen}^3\alpha = 3\operatorname{sen}\alpha - 4\operatorname{sen}^3\alpha$. Aplicado al caso en que $\alpha = 10^o$, tendremos que $\operatorname{sen} 10^o$ es raíz del polinomio $8X^3 - 6X + 1$. Este polinomio es irreducible en $\mathbb{Q}[X]$ (ya que, aplicando la Proposición 2.28, es inmediato ver que no tiene raíces en $\mathbb{Q}$). Por tanto, la extensión $\mathbb{Q} \subset \mathbb{Q}(\operatorname{sen} 20^o)$ tiene grado tres, luego, por el Teorema 8.12, $\operatorname{sen} 10^o \notin K$.

Ejemplo 8.16. (Duplicidad del cubo) Dado la longitud de la arista de un cubo, no se puede construir con regla y compás la longitud de la arista de un segundo cubo que tenga como volumen el doble del volumen del primer cubo. En efecto, si se pudiera, en particular se podría duplicar el cubo de arista uno, es decir, se podría construir la arista de un cubo de volumen dos. Sin embargo, la longitud de tal cubo es $\sqrt[3]{2}$, y como $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, se sigue del Teorema 8.12 que $\sqrt[3]{2} \notin K$.

Ejemplo 8.17. (Cuadratura del círculo) Dada una circunferencia, no se puede construir con regla y compás un cuadrado que tenga de área la misma que el círculo abarcado por la circunferencia. Si se pudiera, para "cuadrar" una circunferencia de radio uno se debería poder construir la longitud $\sqrt{\pi}$, y por tanto también π. Sin embargo, puede demostrarse que π no es algebraico sobre $\mathbb{Q}$ (este resultado, que intuitivamente puede parecer evidente, no es tan sencillo de demostrar).

Ejemplo 8.18. (Polígonos constructibles) Estudiamos finalmente qué polígonos regulares pueden construirse con regla y compás. Nos centraremos sólo en el caso en que el número de lados es un primo p. Si se puede construir un polígono regular de p lados, entonces se puede construir el ángulo $\frac{2\pi}{p}$ radianes, y por el Lema 8.6 podremos construir una recta que pase por el origen y forme un ángulo de $\frac{2\pi}{p}$ con el eje horizontal. Cortando esta recta con la circunferencia unidad e identificando el plano euclídeo con $\mathbb{C}$, tendremos entonces que L contiene una raíz primitiva p-ésima de la unidad ω. Como $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$ (como vimos en el Ejemplo 5.26), se tiene, por el Teorema 8.13, que si ω es constructible entonces $p - 1$ debe ser una potencia de dos (así que, por ejemplo, no se puede construir un heptágono regular). En este caso, el recíproco también es cierto, ya que si $p - 1 = 2^k$, entonces $\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ es un 2-grupo, y por la Proposición 6.7 existe una cadena de subgrupos

$$\{1\} = H_0 < H_1 < \ldots < H_{k-1} < H_k = \operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$$

tal que cada H_i tiene orden 2^i. Por la correspondencia de Galois (la extensión $\mathbb{Q} \subset \mathbb{Q}(\omega)$ es

de Galois, como vimos en el Ejemplo 5.26), tendremos entonces una cadena de subcuerpos

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_{k-1} \subset K_k = \mathbb{Q}(\omega)$$

en la que cada extensión $K_{i-1} \subset K_i$ tiene grado dos. El Teorema 8.13 implica entonces que ω es constructible. Por tanto, el polígono regular de p lados se puede construir si y sólo si $p - 1 = 2^k$ para algún $k \in \mathbb{N}$. Si fuera $k = (2r+1)s$, entonces

$$2^k + 1 = (2^s)^{2r+1} + 1 = (2^s + 1)\big((2^s)^{2r} - (2^s)^{2r-1} + \ldots - 2^s + 1\big)$$

luego $2^k + 1$ no podría ser primo. Se sigue entonces que k no puede tener factores impares, luego debe ser una potencia de dos. En otras palabras, $p = 1 + 2^{2^t}$ para algún $t \in \mathbb{N}$. Un primo de esta forma se llama *primo de Gauss*. Para $t = 0, 1, 2, 3, 4$ obtenemos respectivamente $p = 3, 5, 17, 257, 65537$ y no se conoce ningún otro primo de Gauss (aunque se sabe que primeros valores de $t \geq 5$ dan números que no son primos).

9. Extensiones transcendentes

En esta sección discutiremos brevemente las extensiones transcendentes, en contraposición a las extensiones algebraicas a las que hemos dedicado tanto espacio. El modelo que hay que tener siempre en la cabeza es el de los espacios vectoriales. Lo que queremos es construir un análogo de las bases de un espacio vectorial. La noción buena de base que queremos generalizar es la de "mayor conjunto de vectores linealmente independientes de un espacio vectorial". Para ello, debemos generalizar la noción de dependencia lineal. En el caso de espacios vectoriales la dependencia lineal se hace con combinaciones lineales, ya que la estructura de espacio vectorial viene dada precisamente por ellas (es decir, suma de vectores y productos por escalares). Para el caso de extensiones de cuerpos, la noción análoga será la que involucre expresiones polinomiales (ya que sas son las operaciones, sumas y productos). Por tanto, debemos usar la definición de dependencia algebraica que ya vimos en la sección 1 en el caso de anillos, y que recordamos a continuación:

Definición. Sea $K \subset L$ una extensión de cuerpos. Se dice que los elementos $\alpha_1, \ldots, \alpha_r \in L$ son *algebraicamente dependientes sobre* K si existe un polinomio no nulo $f \in K[X_1, \ldots, X_r]$ tal que $f(\alpha_1, \ldots, \alpha_r) = 0$. En caso contrario, se dice que $\alpha_1, \ldots, \alpha_r$ son *algebraicamente independientes sobre* K.

En el caso de espacios vectoriales, para ampliar un conjunto de vectores linealmente independientes hay que añadir vectores que no dependan linealmente de los anteriores. El resultado análogo para extensiones de cuerpos es el siguiente:

Lema 9.1. *Si $K \subset L$ es una extensión de cuerpos y $\alpha_1, \ldots, \alpha_r \in L$ son algebraicamente independientes sobre K, entonces un elemento $\alpha \in L$ es transcendente sobre $K(\alpha_1, \ldots, \alpha_r)$ si y sólo si $\alpha_1, \ldots, \alpha_r, \alpha$ son algebraicamente independientes sobre K.*

Demostración: Decir que $\alpha \in L$ no es transcendente sobre $K(\alpha_1, \ldots, \alpha_r)$ es equivalente a decir que existe una relación

$$\beta_0 + \beta_1\alpha + \ldots + \beta_r\alpha^d = 0$$

con $\beta_0, \ldots, \beta_d \in K(\alpha_1, \ldots, \alpha_d)$ y no todos nulos. Para cada $i = 0, \ldots, d$ se podrá escribir

$$\beta_i = \frac{g_i(\alpha_1, \ldots, \alpha_r)}{h_i(\alpha_1, \ldots, \alpha_r)}$$

donde $g_i, h_i \in K[X_1, \ldots, X_n]$. Si multiplicamos la relación anterior por el producto $h_0(\alpha_1, \ldots, \alpha_r) \ldots h_d(\alpha_1, \ldots, \alpha_r)$, podemos eliminar todos los denominadores. En otras palabras, decir que $\alpha \in L$ no es transcendente sobre $K(\alpha_1, \ldots, \alpha_r)$ es equivalente a decir que existe una relación

$$g_0(\alpha_1, \ldots, \alpha_r) + g_1(\alpha_1, \ldots, \alpha_r)\alpha + \ldots + g_d(\alpha_1, \ldots, \alpha_r)\alpha^d = 0$$

con $g_i \in K[X_1, \ldots, X_n]$ y al menos algún $g_i(\alpha_1, \ldots, \alpha_r) \neq 0$ (necesariamente $i \neq 0$). Obsérvese que, al ser $\alpha_1, \ldots, \alpha_r \in L$ algebraicamente independientes sobre K, la condición $g_i(\alpha_1, \ldots, \alpha_r) \neq 0$ es equivalente a $g_i(X_1, \ldots, X_r) \neq 0$. Por tanto, la relación anterior es equivalente a que exista un polinomio no nulo en $f \in K[X_1, \ldots, X_r, X]$ (que se podrá siempre escribir como $f = g_0(X_1, \ldots, X_r) + g_1(X_1, \ldots, X_r)X + \ldots + g_d(X_1, \ldots, X_r)X^d$) tal que $f(\alpha_1, \ldots, \alpha_r, \alpha) = 0$. Como esto es equivalente a que $\alpha_1, \ldots, \alpha_r, \alpha$ no son algebraicamente independientes, se concluye la demostración. □

Podemos dar ya la definición análoga a base de un espacio vectorial como conjunto más grande posible de elementos independientes (no valdría en nuestro caso definir base como generadores que son independientes, ya que por ejemplo en la extensión $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ cualquier elemento de $\mathbb{Q}(\sqrt{2})$ no forma un conjunto algebraicamente independiente).

Definición. Se llama *base de transcendencia de una extensión de cuerpos* $K \subset L$ a un conjunto $\alpha_1, \ldots, \alpha_r \in L$ tal que L es algebraico sobre $K(\alpha_1, \ldots, \alpha_r)$.

Aunque pueda darse la definición de base de transcendencia infinita, nos vamos a limitar sólo al caso finito (al igual que suele hacerse en un primero curso de Álgebra Lineal). Para asegurar la existencia de bases de transcendencia en este caso necesitamos poner una hipótesis adicional a la extensión (de la misma forma que para tener bases finitas en espacios vectoriales se pide que stos sean finitamente generados):

Teorema 9.2. *Sea $K \subset L$ una extensión de cuerpos finitamente generada. Entonces L tiene una base de transcendencia sobre K.*

Demostración: Al ser $K \subset L$ una extensión finitamente generada podemos escribir $L = K(\alpha_1, \ldots, \alpha_r)$. Sea s el mayor número de elementos entre $\alpha_1, \ldots, \alpha_r$ que son algebraicamente independientes sobre K. Reordenando los generadores si hiciera falta, podemos suponer que $\alpha_1, \ldots, \alpha_s$ son algebraicamente independientes sobre K. Entonces, para cada $i = s+1, \ldots, r$, se tendrá que $\alpha_1, \ldots, \alpha_s, \alpha_i$ no son algebraicamente independientes, luego, por el Lema 9.1, α_i no será transcendente sobre $K(\alpha_1, \ldots, \alpha_s)$. Por tanto, $\alpha_{s+1}, \ldots, \alpha_r$ son algebraicos sobre $K(\alpha_1, \ldots, \alpha_s)$. El Lema 4.17 implica entonces que la extensión $K(\alpha_1, \ldots, \alpha_s) \subset K(\alpha_1, \ldots, \alpha_s, \alpha_{s+1}, \ldots, \alpha_r) = L$ es algebraica, lo que demuestra que $\alpha_1, \ldots, \alpha_s$ es una base de transcendencia de L sobre K. □

De la misma forma que para espacios vectoriales todas las bases tienen el mismo número de elementos, para bases de trascendencia ocurre lo mismo (y de hecho la demostración es calcada del caso de espacios vectoriales):

Teorema 9.3. *Si $K \subset L$ es una extensión de cuerpos y $\alpha_1, \ldots, \alpha_r \in L$ es una base de transcendencia de L sobre K, entonces todas las bases de transcendencia sobre K tienen n elementos.*

Demostración: Sean $\alpha_1, \ldots, \alpha_r$ y $\alpha'_1, \ldots, \alpha'_s$ dos bases de transcendencia. La idea es ir sustituyendo uno a uno los elementos de la primera base por elementos de la segunda. Empezamos por el primero. Como α_1 es transcendente sobre $K(\alpha_2, \ldots, \alpha_r)$ (por el Lema 9.1) entonces la extensión $K(\alpha_2, \ldots, \alpha_r) \subset L$ es transcendente. No puede ser que $\alpha'_1, \ldots, \alpha'_s$ sean algebraicos sobre $K(\alpha_2, \ldots, \alpha_r)$, porque entonces tendríamos que cada eslabón de

$$K(\alpha_2, \ldots, \alpha_r) \subset K(\alpha_2, \ldots, \alpha_r, \alpha'_1, \ldots, \alpha'_s) \subset L$$

sería una extensión algebraica, luego la extensión $K(\alpha_2, \ldots, \alpha_r) \subset L$ también sería algebraica (por la Proposición 4.19), lo que es absurdo. Por tanto, algún α'_i (supondremos $i = 1$, reordenando) es transcendente sobre $K(\alpha_2, \ldots, \alpha_r)$. Por el Lema 9.1, $\alpha'_1, \alpha_2 \ldots, \alpha_r$ son algebraicamente independientes. Además α_1 no puede ser transcendente sobre $K(\alpha'_1, \alpha_2 \ldots, \alpha_r)$, ya que en tal caso, una vez más por el Lema 9.1, $\alpha'_1, \alpha_1, \alpha_2 \ldots, \alpha_r$ serían algebraicamente independientes, en contra del hecho de que $\alpha_1, \alpha_2 \ldots, \alpha_r$ es una base de transcendencia de L sobre K (y por tanto $\alpha'_1 \in L$ tiene que ser algebraico sobre $K(\alpha_1, \alpha_2 \ldots, \alpha_r)$, contradiciendo el Lema 9.1). Por tanto, los eslabones de

$$K(\alpha'_1, \alpha_2 \ldots, \alpha_r) \subset K(\alpha'_1, \alpha_1, \alpha_2 \ldots, \alpha_r) \subset L$$

son extensiones algebraicas, lo que implica que (por la Proposición 4.19) que la extensión compuesta es algebraica. Esto demuestra que $\alpha'_1, \alpha_2 \ldots, \alpha_r$ es una nueva base de transcendencia de L sobre K.

Veamos que podemos ir repitiendo el proceso. Es decir, supongamos que ya sabemos que $\alpha'_1, \ldots, \alpha'_i, \alpha_{i+1} \ldots, \alpha_r$ es una base de transcendencia de L sobre K. y que $i+1 \leq r, s$. Veamos que podemos sustituir ahora α_{i+1} repitiendo todo el procedimento anterior. De nuevo, la extensión $K(\alpha'_1, \ldots, \alpha'_i, \alpha_{i+2} \ldots, \alpha_r) \subset L$ es transcendente ya que α_{i+1} es trascendente sobre $K(\alpha'_1, \ldots, \alpha'_i, \alpha_{i+2} \ldots, \alpha_r)$. Por tanto, no todos los $\alpha'_1, \ldots, \alpha'_s$ pueden ser algebraicos sobre $K(\alpha'_1, \ldots, \alpha'_i, \alpha_{i+2} \ldots, \alpha_r)$, porque sería algebraica la extensión composición

$$K(\alpha'_1, \ldots, \alpha'_i, \alpha_{i+2} \ldots, \alpha_r) \subset K(\alpha_{i+2}, \ldots, \alpha_r, \alpha'_1, \ldots, \alpha'_s) \subset L.$$

La única diferencia ahora con el caso $i = 0$ es que, como obviamente $\alpha'_1, \ldots, \alpha'_i$ son algebraicos sobre $K(\alpha'_1, \ldots, \alpha'_i, \alpha_{i+2} \ldots, \alpha_r)$, concluimos que alguno entre $\alpha'_{i+1}, \ldots, \alpha'_s$ es transcendente sobre $K(\alpha'_1, \ldots, \alpha'_i, \alpha_{i+2} \ldots, \alpha_r)$. Reordenando si hiciera falta, podemos suponer que α'_{i+1} es transcendente sobre $K(\alpha'_1, \ldots, \alpha'_i, \alpha_{i+2} \ldots, \alpha_r)$, luego por el Lema 9.1 se tendrá que $\alpha'_1, \ldots, \alpha'_i, \alpha'_{i+1}, \alpha_{i+2} \ldots, \alpha_r$ son algebraicamente independientes sobre K. Además, α_{i+1} es algebraico sobre $K(\alpha'_1, \ldots, \alpha'_i, \alpha'_{i+1}, \alpha_{i+2} \ldots, \alpha_r)$, pues en caso contrario $\alpha'_1, \ldots, \alpha'_i, \alpha'_{i+1}, \alpha_{i+1}, \alpha_{i+2} \ldots, \alpha_r$ serían algebraicamente independientes sobre K, en contra de que $\alpha'_1, \ldots, \alpha'_i, \alpha_{i+1}, \alpha_{i+2} \ldots, \alpha_r$ es una base de transcendencia de L sobre K. Por tanto, la extensión compuesta

$$K(\alpha'_1, \ldots, \alpha'_i, \alpha'_{i+1}, \alpha_{i+2} \ldots, \alpha_r) \subset K(\alpha'_1, \ldots, \alpha'_i, \alpha'_{i+1}, \alpha_{i+1}, \alpha_{i+2} \ldots, \alpha_r) \subset L$$

es algebraica, lo que termina de demostrar que $\alpha'_1, \ldots, \alpha'_i, \alpha'_{i+1}, \alpha_{i+2} \ldots, \alpha_r$ es una base de transcendencia de L sobre K.

Evidentemente, este proceso lo pdemos llevar adelante siempre que i no supere ni a r ni a s. Queremos ver que $r = s$, así que veamos que se llega a un absurdo si $r < s$ y si $s < r$.

Si fuera $r < s$ llegaríamos a que $\alpha'_1, \ldots, \alpha'_r$ formaría una base de transcendencia. Por tanto, α'_{r+1} debería ser algebraico sobre $K(\alpha'_1, \ldots, \alpha'_r)$, lo que implicaría, por el Lema 9.1, que $\alpha'_1, \ldots, \alpha'_r, \alpha'_{r+1}$ son algebraicamente dependientes sobre K, lo que contradice que $\alpha'_1, \ldots, \alpha'_s$ sea una base de transcendencia (y por tanto un conjunto algebraicamente independiente) sobre K

Si en cambio fuera $s < r$, llegaríamos a que $\alpha'_1, \ldots, \alpha'_s, \alpha_{s+1}, \ldots, \alpha_r$ es una base de transcendencia de L sobre K. Pero esto es también absurdo, ya que por ser $\alpha'_1, \ldots, \alpha'_s$ una base de transcendencia de L sobre K, la extensión $K(\alpha'_1, \ldots, \alpha'_s) \subset L$ es algebraica. Y esto implicaría que α_{s+1} sería algebraico sobre $K(\alpha'_1, \ldots, \alpha'_s)$, luego por el Lema 9.1 los elementos $\alpha'_1, \ldots, \alpha'_s, \alpha_{s+1}$ serían algebraicamente dependientes sobre $K(\alpha'_1, \ldots, \alpha'_s)$, contradiciendo el hecho de que $\alpha'_1, \ldots, \alpha'_s, \alpha_{s+1}, \ldots, \alpha_r$ es una base de transcendencia de L sobre K. □

Definición. Se llama *grado de transcendencia de una extensión de cuerpos* $K \subset L$ al cardinal de cualquier base de transcendencia de L sobre K, y lo denotaremos por gr.tr.(L/K)

Ejemplo 9.4. Aunque se salga del alcance de estas notas, mencionemos brevemente una de las principales utilidades del concepto de grado de transcendencia: la noción de dimensión. Consideremos por ejemplo la cuádrica en $\mathbb{C}^n$ de ecuación $X_1^2 + \ldots + X_n^2 + 1 = 0$. Aunque no tenga puntos reales, intuitivamente debe tratarse de un objeto de dimensión $n-1$. Una primera observación es que, si $n \geq 2$, el polinomio $f = X_1^2 + \ldots + X_n^2 + 1$ es irreducible (puede hacerse por inducción mediante el criterio de Eisenstein y demotrando el caso $n = 2$ a mano), luego el anillo $\mathbb{C}[X_1, \ldots, X_n]/(f)$ es un dominio de integridad, y por tanto tiene un cuerpo de fracciones L, que será una extensión de $\mathbb{C}$. Aunque no hagamos los detalles, no es difícil ver que, llamando α_i a la clase de X_i en L, los elementos $\alpha_1, \ldots, \alpha_{n-1}$ son algebraicamente independientes sobre $\mathbb{C}$. El motivo es que, si existiera $g \in \mathbb{C}[X_1, \ldots, X_{n-1}]$ tal que $g(\alpha_1, \ldots, \alpha_{n-1}) = 0$, entonces el polinomio g debería ser un múltiplo de f, lo que es absurdo, ya que los múltiplos no nulos de f tienen grado positivo en la variable X_n. Por otra parte, como en L se tiene la igualdad $\alpha_1^2 + \ldots + \alpha_n^2 + 1 = 0$, se sigue que $\alpha_1, \ldots, \alpha_n$ son algebraicamente dependientes sobre $\mathbb{C}$, o equivalentemente que α_n es algebraico sobre $\mathbb{C}(\alpha_1, \ldots, \alpha_{n-1})$. Por tanto, $\alpha_1, \ldots, \alpha_{n-1}$ forma una base de transcendencia de L sobre $\mathbb{C}$, es decir, el grado de transcendencia es $n-1$, que es exactamente la dimensión de la cuádrica.

El motivo intuitivo por el que sale la dimensión es que el grado de transcendencia mide "el número de variable libres", que sería como decir el número de parámetros independientes. De hecho, la definición de dimensión de esta forma se puede hacer general. Consideremos en $\mathbb{C}^n$ el conjunto X definido como puntos que se anulan para un número finito de polinomios $f_1, \ldots, f_m$ y supongamos que el ideal I generado por ellos sea primo (esto tiene una interpretación precisa que no vamos a detallar: que I sea primo significa que el conjunto X no se pueda escribir como unión finita de otros conjuntos también definidos por polinomios). Entonces, como antes, el cociente $\mathbb{C}[X_1, \ldots, X_n]/I$ es un dominio de integridad, y su cuerpo de fracciones L es una extensión de $\mathbb{C}$. Entonces la dimensión de X es, por definición, el grado de transcendencia de L sobre $\mathbb{C}$. Nótese que es fundamental usar $\mathbb{C}$ (o bien otro cuerpo algebraicamente cerrado) ya que, si por ejemplo en el ejemplo de la cuádrica ponemos $\mathbb{R}$, nos encontraríamos con el conjunto vacío, mientras que el grado de transcendencia sigue siendo $n-1$.

Terminamos con el resultado fundamental sobre grados de transcendencia. Con la interpretación de dimensión anterior, el resultado puede llegar a traducirse en que la dimensión de un producto de dos conjuntos de dimensiones r y s tiene dimensión $r+s$ (más en general, se puede interpretar como que si tenemos una aplicación polinomial suprayectiva $X \to Y$ entre dos conjuntos polinomiales de dimensiones respectivas r y s, entonces la preimagen de un punto "suficientemente general" de Y tiene dimensión $r-s$).

Teorema 9.5. *Si $K \subset K' \subset L$ es una cadena de cuerpos, entonces*

$$\text{gr.tr.}(L/K) = \text{gr.tr.}(L/K') + \text{gr.tr.}(K'/K).$$

Demostración: Sea $\alpha_1, \ldots, \alpha_r$ una base de transcendencia de K' sobre K y $\beta_1, \ldots, \beta_s$ una base de transcendencia de L sobre K'. Como ningún β_i puede estar en K' (puesto que en tal caso β_i sería obviamente algebraico sobre K'), entonces el conjunto $\{\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s\}$ tiene $r+s$ elementos. Por tanto, el teorema estará demostrado si vemos que tal conjunto es una base de transcendencia de L sobre K.

En primer lugar, la extensión $K(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s) \subset L$ es algebraica porque se puede descomponer como $K(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s) \subset K'(\beta_1, \ldots, \beta_s)$ y $K'(\beta_1, \ldots, \beta_s) \subset L$, y ambos eslabones son extensiones algebraicas (la primera extensión lo es por serlo $K(\alpha_1, \ldots, \alpha_r) \subset K'$).

Veamos entonces que $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ son algebraicamente independientes sobre K. Para ello vamos a ir añadiendo uno a uno los elementos de $\beta_1, \ldots, \beta_s$ a $\alpha_1, \ldots, \alpha_r$. Como β_1 es transcendente sobre K', lo es también sobre $K(\alpha_1, \ldots, \alpha_r)$, luego el Lema 9.1 implica que $\alpha_1, \ldots, \alpha_r, \beta_1$ son algebraicamente independientes sobre K.

En general, si ya sabemos que $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_i$ son algebraicamente independientes sobre K, consideremos β_{i+1}. Como $\beta_1, \ldots, \beta_{i+1}$ son algebraicamente independientes

sobre K', el Lema 9.1 implica que β_{i+1} es transcendente sobre $K'(\beta_1, \ldots, \beta_i)$, luego también es transcendente sobre $K(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_i)$. Aplicando de nuevo el Lema 9.1 llegamos a que $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_i, \beta_{i+1}$ son algebraicamente independientes sobre K.

Por tanto, repitiendo este proceso s veces llegamos a que $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ son algebraicamente independientes sobre K. □