ECUACIONES ALGEBRAICAS:

EXTENSIONES DE CUERPOS Y TEORÍA DE GALOIS

José F. Fernando

J. Manuel Gamboa

Prefacio

Este libro, que es fruto de la experiencia de los autores en la impartición de cursos similares, es una iniciación al estudio de la Teoría de Galois para extensiones finitas de cuerpos de característica cero, y que incluye un capítulo sobre cuerpos finitos. Hemos decidido excluir de nuestro estudio la Teoría de Galois de extensiones no finitas y las extensiones de cuerpos de característica positiva, por lo que en ningún momento aparece la noción de separabilidad. Con este texto se pretende cubrir la materia de la asignatura Ecuaciones Algebraicas que se imparte en los grados en Matemáticas, en Ingeniería Matemática y en Matemáticas y Estadística, así como los dobles Grados en Matemáticas y Física y Matemáticas e Informática.

Los dos primeros Capítulos tienen carácter muy elemental; sirven de apoyo a todo el texto y la noción clave que en ellos se aborda es la de cuerpo de descomposición. El Capítulo III y el Apéndice B en el que, entre otras cosas, se prueba la transcendencia de e y π, son suprimibles si el limitado número de horas lectivas obliga a ello. Los Capítulos IV, V y VI constituyen el núcleo del curso, pero también aquí se puede hacer una lectura completa y otra más relajada. En particular, todo lo relativo al grupo de Galois de los polinomios de grado 5, que aparece en las páginas de la sección primera del Capítulo VI que siguen a VI.4.1 puede ser omitido sin que la exposición se resienta. Otro tanto cabe decir de la demostración de la Forma débil del Teorema del número primo de Dirichlet VI.1.14, que se apoya en el Lema VI.1.13. Más aún, el no disponer de suficientes horas lectivas puede obligar a suprimir la demostración de la Ley de reciprocidad cuadrática V.2.8 y sus preparativos.

El libro contiene numerosos ejemplos y 138 ejercicios, todos ellos resueltos, de dificultad variable. Algunos son auténticos ejercicios, propuestos para que su resolución permita consolidar los conocimientos adquiridos, pero otros son problemas que ponen a prueba el ingenio y la madurez matemática de quienes los aborden. Hemos decidido incluir las soluciones, a pesar del trabajo que esto conlleva y de que no son pocos los docentes que lo consideran un desacierto.

Para no darles la razón instamos a los lectores a intentar resolverlos por su cuenta y acudir a la solución que presentamos sólo tras esforzarse seriamente.

Pocos de estos ejercicios son originales, aunque sí lo son las soluciones propuestas, y los hemos escogido de fuentes diversas. Entre ellas cabe citar las listas de problemas elaboradas a lo largo de muchos años por nuestra compañera y amiga, la profesora Concha Fuertes, a la que desde aquí mostramos nuestro agradecimiento, que hacemos extensivo a los profesores Félix Delgado y Sebastián Xambó cuyo texto de Álgebra, escrito junto con Concha, ha inspirado en parte el nuestro. También hemos empleado el precioso libro *Introducció a l'àlgebra abstracta* escrito por Ramon Antoine, Rosa Camps y Jaume Moncasi, que Rosa nos regaló hace algún tiempo.

Ya hemos señalado que presentamos un algoritmo para calcular el grupo de Galois de los polinomios de grado 5. Esto no habría sido posible sin la ayuda de nuestro amigo y compañero, el profesor Juan Ramón Delgado, que nos explicó la solución del problema y nos facilitó la bibliografía adecuada. También nos ayudó en esto Alfonso Zamora, que nos proporcionó ejemplos de polinomios irreducibles de grado 5 con coeficientes racionales con grupo de Galois prefijado. Alfonso, que ya es doctor, es uno de los magníficos estudiantes de la Facultad de Matemáticas de la Universidad Complutense que han sido alumnos nuestros en los últimos años, y que han aportado soluciones muy originales a algunos de los ejercicios propuestos. Sobresalen las contribuciones de Javier Alcaide, Berardo Castiñeira, Gema Cuesta, Sergio Díaz Aranda, Hugo Fernández Hervás, Javier Fresán, Gabriel Fürstenheim, Lucía Galguera, Victor Gallego, Miguel Hernaiz, Luis Hernández Corbato, Sara Herrero, Vicente Lorenzo, Ignacio Luján, Ana María Martínez, Javier Martínez, Blanca Pablos, Arturo Rodríguez Rodríguez, María Belén Rodríguez Rodríguez y Robert Tomasz Wielgos.

El prerrequisito esencial para estudiar este texto es la madurez matemática. A ello se deben añadir un curso elemental de álgebra lineal, otro de iniciación a la teoría de grupos finitos que incluya las nociones de grupo resoluble y subgrupo transitivo de un grupo de permutaciones, y un tercero en el que se estudien con cierta profundidad los anillos de polinomios en una y varias variables con coeficientes en un cuerpo. En particular son imprescindibles el teorema fundamental de los polinomios simétricos, la resultante y el discriminante.

José F. Fernando Galván & J. Manuel Gamboa Mutuberría.

Madrid, 20 de junio, 2015

Contenido

CAPÍTULO I

Generalidades sobre cuerpos

En este capítulo se introduce la noción de extensión de cuerpos, que surge de modo natural al estudiar raíces de polinomios. En la primera sección se señala que si $L|K$ es una extensión de cuerpos entonces L tiene una estructura natural de K-espacio vectorial. En la segunda se distinguen los elementos algebraicos de los transcendentes y se estudian las extensiones algebraicas, y entre ellas las finitas.

1. Definiciones y conceptos básicos de la teoría de cuerpos

El objetivo de esta sección es introducir parte de la terminología y notación que nos permitirá estudiar *extensiones de cuerpos*.

Definición I.1.1 Una *extensión de cuerpos* $L|K$ es una terna $(K, \mathtt{j}, L)$, donde K y L son cuerpos y $\mathtt{j} : K \to L$ es un homomorfismo. Vimos en II.1.5, vol. II, que todo homomorfismo de cuerpos es inyectivo, por lo que podemos identificar K con su imagen $\mathtt{j}(K)$ y considerar las extensiones de cuerpos como inclusiones de cuerpos $K \subset L$. Diremos entonces que K es un *subcuerpo* de L. Si $K \subset E \subset L$ son cuerpos se dice que $E|K$ es una *subextensión* de $L|K$.

Ejemplos I.1.2 (1) Denotemos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$, respectivamente, los cuerpos de los números racionales, reales y complejos. Como $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ y las operaciones en cada uno de estos cuerpos son las inducidas por la suma y producto de números complejos, $\mathbb{C}|\mathbb{R}$ es una extensión de cuerpos y $\mathbb{R}|\mathbb{Q}$ es una subextensión de $\mathbb{C}|\mathbb{Q}$.

(2) Sean K un cuerpo y $f \in K[\mathtt{t}]$ irreducible. Como $K[\mathtt{t}]$ es un DIP, por V.1.5 vol. II, el polinomio f genera un ideal maximal en $K[\mathtt{t}]$ y por tanto el cociente $L := K[\mathtt{t}]/(f)$ es un cuerpo donde, por simplicidad, hemos denotado (f) el ideal principal $f \cdot K[\mathtt{t}]$. Se comprueba inmediatamente que la aplicación

$$\mathtt{j} : K \to L,\ a \mapsto a + (f)$$

es un homomorfismo, y por tanto $(K, \mathtt{j}, L)$ es una extensión de cuerpos.

(3) El siguiente ejemplo explica porqué conviene utilizar la notación $L|K$ en lugar de $K \subset L$. Sean $\sqrt{2}$ el único número real positivo cuyo cuadrado vale 2 y el homomorfismo *evaluación en* $\sqrt{2}$ definido por

$$\varphi : \mathbb{Q}[\mathtt{t}] \to \mathbb{R},\ f \mapsto f(\sqrt{2}).$$

Su imagen es $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} :\ a, b \in \mathbb{Q}\}$. En efecto, $g(\mathtt{t}) := \mathtt{t}^2 - 2 \in \mathbb{Q}[\mathtt{t}]$, que es un polinomio irreducible en $\mathbb{Z}[\mathtt{t}]$, y por tanto en $\mathbb{Q}[\mathtt{t}]$, por el Criterio de Eisenstein, VI.2.6 vol. II, cumple $\varphi(g) = 0$. Al dividir cada $f \in \mathbb{Q}[\mathtt{t}]$ entre $g(\mathtt{t})$ existen $q \in \mathbb{Q}[\mathtt{t}]$ y $a, b \in \mathbb{Q}$ tales que $f(\mathtt{t}) = g(\mathtt{t})q(\mathtt{t}) + b\mathtt{t} + a$. En consecuencia, $\varphi(f) = a + b\sqrt{2}$.

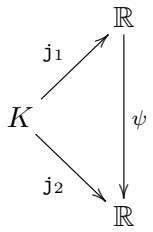
Además $(g) = \ker \varphi$ pues es obvio que $(g) \subset \ker \varphi$ y la igualdad se deduce por ser el ideal (g) maximal. Así, por el Primer Teorema de isomorfía,

$$\mathbb{Q}[\mathtt{t}]/(g) = \mathbb{Q}[\mathtt{t}]/\ker \varphi \cong \operatorname{im} \varphi = \mathbb{Q}[\sqrt{2}],$$

de donde en particular se deduce que $K := \mathbb{Q}[\sqrt{2}]$ es un cuerpo. Consideramos los homomorfismos de cuerpos

$$\mathtt{j}_1 : K \to \mathbb{R},\ a + b\sqrt{2} \mapsto a + b\sqrt{2} \quad \& \quad \mathtt{j}_2 : K \to \mathbb{R},\ a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

Las extensiones $(K, \mathtt{j}_1, \mathbb{R})$ y $(K, \mathtt{j}_2, \mathbb{R})$ son esencialmente distintas, pues no existe ningún homomorfismo de cuerpos $\psi : \mathbb{R} \to \mathbb{R}$ que haga conmutativo el diagrama:



En efecto, si existiese tal homomorfismo se tendría

$$-\sqrt{2} = \mathtt{j}_2(\sqrt{2}) = \psi(\mathtt{j}_1(\sqrt{2})) = \psi(\sqrt{2}) = \psi\big((\sqrt[4]{2})^2\big) = (\psi(\sqrt[4]{2}))^2 > 0,$$

que es una contradicción.

(4) La situación del ejemplo anterior no es tampoco la regla general, en el sentido de que, en ocasiones, fijados un cuerpo L y un subcuerpo suyo K existe un único homomorfismo $\mathtt{j} : K \to L$, lo que hace superflua la mención al

homomorfismo $\mathtt{j}$. Consideramos por ejemplo el cuerpo $\mathbb{C}$, su subcuerpo $\mathbb{Q}$, y sea $\mathtt{j} : \mathbb{Q} \to \mathbb{C}$ un homomorfismo de cuerpos. Vamos a comprobar que $\mathtt{j}(q) = q$ para cada $q \in \mathbb{Q}$. Como $\mathtt{j}(1) = 1$, se tiene $\mathtt{j}(n) = n$ para cada entero positivo n pues si suponemos por inducción que $\mathtt{j}(n-1) = n-1$, entonces

$$\mathtt{j}(n) = \mathtt{j}((n-1)+1) = \mathtt{j}(n-1) + \mathtt{j}(1) = (n-1) + 1 = n.$$

Además $\mathtt{j}(0) = 0$ y si $m \in \mathbb{Z}$ es negativo su opuesto $n := -m$ es positivo, y

$$0 = \mathtt{j}(0) = \mathtt{j}(m+n) = \mathtt{j}(m) + \mathtt{j}(n) = \mathtt{j}(m) + n,$$

así que $\mathtt{j}(m) = -n = m$. Finalmente, para todo número racional $q = m/n$, donde $m, n \in \mathbb{Z}$ y $n \neq 0$ se tiene

$$m = \mathtt{j}(m) = \mathtt{j}(qn) = \mathtt{j}(q)\mathtt{j}(n) = \mathtt{j}(q)n \quad \Longrightarrow \quad \mathtt{j}(q) = m/n = q.$$

(5) Sea K un cuerpo y consideremos el homomorfismo $\varphi : \mathbb{Z} \to K$, $k \mapsto k \cdot 1_K$. Su núcleo es un ideal primo de $\mathbb{Z}$ luego, o bien $\ker\varphi = (0)$ o bien existe un número primo $p \in \mathbb{Z}$ tal que $\ker\varphi = p\mathbb{Z}$. En el primer caso $\mathrm{char}(K) = 0$ y el homomorfismo φ se extiende al cuerpo de fracciones $\mathbb{Q}$ de $\mathbb{Z}$ mediante $\overline{\varphi} : \mathbb{Q} \to K$, $m/n \mapsto \varphi(m)/\varphi(n)$, donde $m, n \in \mathbb{Z}$ y $n \neq 0$.

Si $\ker\varphi = p\mathbb{Z}$ entonces $\mathrm{char}(K) = p$ y, por el Primer Teorema de isomorfía, existe un homomorfismo inyectivo $\overline{\varphi} : \mathbb{Z}_p = \mathbb{Z}/\ker\varphi \to K$, $k + p\mathbb{Z} \mapsto \varphi(k)$.

En el primer caso se dice que $\mathbb{Q}$ es *el cuerpo primo de* K, y en el segundo dicho cuerpo primo es $\mathbb{Z}_p$. Nótese que si un cuerpo K es finito su característica es un primo p, pues en otro caso contendría un cuerpo isomorfo a $\mathbb{Q}$, contra la finitud de K. El recíproco es falso; el cuerpo de fracciones del anillo de polinomios $\mathbb{Z}_p[\mathtt{t}]$ es infinito y de característica p.

(6) Se dice que las extensiones $(K, \mathtt{j}_1, E)$ y $(K, \mathtt{j}_2, L)$ son *isomorfas* si existe un isomorfismo $\varphi : E \to L$ tal que $\varphi \circ \mathtt{j}_1 = \mathtt{j}_2$. Si suponemos que $\mathtt{j}_1$ y $\mathtt{j}_2$ son inclusiones conjuntistas la condición anterior equivale a que la restricción de φ al cuerpo K es la identidad.

Observación I.1.3 Si $L|K$ es una extensión de cuerpos identificamos K como subcuerpo de L, por lo que L admite una estructura canónica de K-espacio vectorial. Para ello se consideran como operaciones la suma de L y el producto por escalares de K definido por

$$\cdot : K \times L \to L, (\lambda, x) \mapsto \lambda \cdot x = \lambda x,$$

donde el producto $\lambda \cdot x$ es su producto como elementos de L. Este hecho justifica las siguientes definiciones.

Definiciones I.1.4 Sea $L|K$ una extensión de cuerpos.

(1) Se llama *grado* $[L : K]$ de la extensión a la dimensión $\dim_K L$ de L como K-espacio vectorial.

(2) Se dice que la extensión $L|K$ es *finita* si lo es su grado. En caso contrario se dice que $L|K$ es *infinita.*

Ejemplo I.1.5 Sean K un cuerpo, $f \in K[\mathtt{t}]$ un polinomio irreducible en $K[\mathtt{t}]$ y $L := K[\mathtt{t}]/(f)$. La extensión $L|K$ es finita y su grado coincide con el del polinomio f. De hecho, si denotamos $n := \deg(f)$ entonces

$$\mathcal{B} := \{1 + (f),\ \mathtt{t} + (f), \ldots,\ \mathtt{t}^{n-1} + (f)\}$$

es una base de L como K-espacio vectorial. En efecto, para cada $\alpha \in L$ existe un polinomio $g \in K[\mathtt{t}]$ tal que $\alpha := g + (f)$. Dividiendo g entre f, existen $q, r \in K[\mathtt{t}]$ tales que $\deg(r) < n$ y $g = qf + r$, luego $\alpha = r + (f)$. Escribimos $r := \sum_{j=0}^{n-1} a_j \mathtt{t}^j$ donde cada $a_j \in K$, y así

$$\alpha = r + (f) = \sum_{j=0}^{n-1} a_j \mathtt{t}^j + (f) = \sum_{j=0}^{n-1} a_j (\mathtt{t}^j + (f)),$$

lo que demuestra que $\mathcal{B}$ es sistema generador de L como K-espacio vectorial. En cuanto a la independencia lineal, sean $b_0, b_1, \ldots, b_{n-1} \in K$ tales que

$$0 = \sum_{k=0}^{n-1} b_k (\mathtt{t}^k + (f)) = \sum_{k=0}^{n-1} b_k \mathtt{t}^k + (f),$$

o equivalentemente, $g := b_0 + b_1\mathtt{t} + \cdots + b_{n-1}\mathtt{t}^{n-1} \in (f)$. Esto significa que f, que tiene grado n, divide al polinomio g, cuyo grado es menor o igual que $n - 1$. Por tanto $g = 0$, es decir, $b_j = 0$ para $0 \leq j \leq n - 1$.

Proposición I.1.6 (Transitividad del grado) *Sean $L|K$ y $E|L$ extensiones de cuerpos. Las siguientes afirmaciones son equivalentes:*

(1) *$L|K$ y $E|L$ son finitas.*

(2) *$E|K$ es finita.*

Si se cumplen las condiciones anteriores $[E : K] = [E : L] \cdot [L : K]$, y dadas sendas bases $\mathcal{B}_1 := \{u_1, \ldots, u_n\}$ y $\mathcal{B}_2 := \{v_1, \ldots, v_m\}$ de E como L-espacio vectorial y de L como K-espacio vectorial, respectivamente, entonces

$$\mathcal{B}_3 := \{u_i v_j :\ 1 \leq i \leq n,\ 1 \leq j \leq m\} \subset E$$

es una base de E como K-espacio vectorial.

Demostración. Podemos suponer que $K \subset L \subset E$, y así L es un subespacio vectorial de E como K-espacio vectorial.

(1) $\Longrightarrow$ (2) Veamos que $\mathcal{B}_3$ es base de E como K-espacio vectorial, lo que prueba la finitud de la extensión $E|K$ y la igualdad $[E:K] = [E:L] \cdot [L:K]$ del enunciado, pues $\mathcal{B}_3$ tiene mn elementos. En primer lugar, comprobaremos que $\mathcal{B}_3$ es sistema generador. Para cada $x \in E$ existen $\lambda_1, \ldots, \lambda_n \in L$ tales que

$$x = \sum_{i=1}^{n} \lambda_i u_i.$$

Como cada $\lambda_i \in L$ existen $\mu_{i1}, \ldots, \mu_{im} \in K$ tales que $\lambda_i = \sum_{j=1}^{m} \mu_{ij} v_j$. Por tanto,

$$x = \sum_{i=1}^{n} \lambda_i u_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \mu_{ij} v_j u_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \mu_{ij} u_i v_j,$$

lo que demuestra que $\mathcal{B}_3$ es un sistema generador de E como K-espacio vectorial. Veamos a continuación que también es un conjunto de vectores K-linealmente independientes. En efecto, consideramos la ecuación

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{ij} u_i v_j = 0,$$

donde cada $\lambda_{ij} \in K$. Denotamos $\alpha_i := \sum_{j=1}^{m} \lambda_{ij} v_j \in L$ para $1 \leq i \leq n$, por lo que la igualdad anterior se reescribe como

$$\sum_{i=1}^{n} \alpha_i u_i = 0,$$

y, por tanto, cada $\alpha_i = 0$, pues $\mathcal{B}_1$ es una base de E como L-espacio vectorial. De este modo, para $1 \leq i \leq n$ tenemos la igualdad

$$\sum_{j=1}^{m} \lambda_{ij} v_j = 0,$$

donde cada $\lambda_{ij} \in K$. Como $\mathcal{B}_2$ es una base de L como K-espacio vectorial, concluimos que cada $\lambda_{ij} = 0$ y, por tanto, $\mathcal{B}_3$ es un conjunto de vectores K-linealmente independientes.

(2) $\Longrightarrow$ (1) Observamos que $\dim_K L \leq \dim_K E < +\infty$ puesto que L es un K-subespacio vectorial de E. Por otro lado, como $K \subset L$, cualquier base de E como K-espacio vectorial genera E como L-espacio vectorial. Esto implica que $\dim_L E \leq \dim_K E$ o lo que es igual, $[E:L] \leq [E:K] < +\infty$. $\square$

Observaciones I.1.7 (1) Sean $L|K$ y $E|L$ dos extensiones finitas de cuerpos tales que $[E:L]=[E:K]$. Entonces $L=K$.

En efecto, por la transitividad del grado, I.1.6, L es un K-espacio vectorial de dimensión 1, luego cualquier elemento no nulo de L, por ejemplo 1, constutuye una base de L como K-espacio vectorial. Por tanto, para cada $v\in L$ existe $\lambda\in K$ tal que $v=\lambda\cdot 1=\lambda\in K$, lo que prueba que $L=K$.

(2) Si $E|K$ es una extensión finita y el grado $[E:K]$ es un número primo, entonces no existe ningún cuerpo L tal que $K\subsetneq L\subsetneq E$, es decir, $E|K$ no admite ninguna *subextensión propia.* En efecto, si existiese un cuerpo L estrictamente contenido en E y que contiene estrictamente a K, los números enteros $m:=[E:L]$ y $n:=[L:K]$ serían mayores que 1 y $[E:K]=[E:L]\cdot[L:K]=mn$ no sería primo.

1.a. Subextensión generada por un conjunto. Sean $L|K$ una extensión de cuerpos y $A\subset L$ un subconjunto. Como siempre, podemos suponer que $K\subset L$. La familia Σ_A formada por todos los subcuerpos de L que contienen a $K\cup A$ es no vacía, pues $L\in\Sigma_A$, y se define $K(A):=\bigcap_{F\in\Sigma_A}F$. Desde luego $K\cup A\subset K(A)\subset L$, y de hecho $K(A)$ es el menor subcuerpo de L que contiene a $K\cup A$. Para comprobarlo es suficiente, por estar contenido en el cuerpo L, demostrar que $K(A)$ es un cuerpo. Pero, dados $x,y\in K(A)\setminus\{0\}$, tanto la resta $x-y$ como el producto xy^{-1} pertenecen a cada cuerpo $F\in\Sigma_A$, luego pertenecen a $K(A)$. Se dice que $K(A)$ es el *cuerpo generado por A sobre K,* y también que $K(A)|K$ es la subextensión de $L|K$ *generada por A.*

Si $A:=\{a_1,\dots,a_r\}$ es un conjunto finito, entonces el subcuerpo $K(A)$ se denota por $L:=K(a_1,\dots,a_r)$ y se dice que es una extensión *finitamente generada* sobre K. Diremos en este caso que $a_1,\dots,a_r$ son *unos generadores* de la extensión $L|K$. Si $r=1$, es decir, $A:=\{a\}$, entonces se dice que $K(a)|K$ es una *extensión simple* y que a es un *elemento primitivo* de la extensión $L|K$.

Proposición I.1.8 *Sean $L|K$ una extensión de cuerpos y $a,a_1,\dots,a_r\in L$. Entonces,*

(1) $K(a_1,\dots,a_r)=\left\{\frac{f(a_1,\dots,a_r)}{g(a_1,\dots,a_r)}:\ f,g\in K[\mathtt{x}_1,\dots,\mathtt{x}_r]\quad\&\quad g(a_1,\dots,a_r)\neq 0\right\}$.

(2) $K(a)=\left\{\frac{f(a)}{g(a)}:\ f,g\in K[\mathtt{t}]\quad\&\quad g(a)\neq 0\right\}$.

Demostración. (1) En VII.1.3, vol. II vimos que el menor subanillo de L que contiene a K y a $a_1,\dots,a_r$ es

$$K[a_1,\dots,a_r]:=\{f(a_1,\dots,a_r):\ f\in K[\mathtt{x}_1,\dots,\mathtt{x}_r]\},$$

por lo que su cuerpo de fracciones es el menor subcuerpo de L que contiene a K y a $a_1, \ldots, a_r$, y eso es lo que afirma el enunciado.

(2) Este apartado es un caso particular del anterior con $r = 1$. □

Proposición I.1.9 *Sean $L|K$ una extensión de cuerpos, $A \subset L$ y $\{E_i\}_{i\in I}$ una familia de subcuerpos de L que contienen a K.*

(1) *Supongamos que para cada par de índices $i, j \in I$ existe $k \in I$ tal que $E_i \cup E_j \subset E_k$. Entonces $F := \bigcup_{i\in I} E_i$ es un subcuerpo de L que contiene a K.*

(2) *Un elemento $x \in L$ pertenece a $K(A)$ si y sólo si existen $a_1, \ldots, a_r \in A$ y $f, g \in K[\mathtt{x}_1, \ldots, \mathtt{x}_r]$ tales que $g(a_1, \ldots, a_r) \neq 0$ y*

$$x := \frac{f(a_1, \ldots, a_r)}{g(a_1, \ldots, a_r)}.$$

Demostración. (1) Sólo tenemos que probar que si $x, y \in F \setminus \{0\}$, entonces $xy^{-1},\ x - y \in F$. Como $x, y \in F \setminus \{0\}$, existen $i, j \in I$ tales que $x \in E_i$ e $y \in E_j$. Por hipótesis existe $k \in I$ tal que $E_i \cup E_j \subset E_k$ y, por tanto, $x, y \in E_k$, que es un cuerpo. En consecuencia, $x - y,\ xy^{-1} \in E_k \subset F$.

(2) Sea $\mathcal{F} := \{K(M) : M \in \mathcal{P}_F(A)\}$, donde $\mathcal{P}_F(A)$ es el conjunto formado por todos los subconjuntos finitos de A. La familia $\mathcal{F}$ está en las condiciones del apartado anterior, pues dados subconjuntos finitos M y N de A también $M \cup N \in \mathcal{P}_F(A)$, por lo que $K(M \cup N) \in \mathcal{F}$ es un cuerpo que contiene a $K(M) \cup K(N)$. Se deduce del apartado (1) que $F := \bigcup_{M\in\mathcal{P}_F(A)} K(M)$ es un subcuerpo de L que contiene a K.

De hecho $F = K(A)$. En efecto, si $M \in \mathcal{P}_F(A)$ se tiene $M \subset A$, luego $K \cup M \subset K \cup A$, por lo que $K(M) \subset K(A)$ y esto implica que $F \subset K(A)$. Además, $a \in K(a) \subset F$ para cada $a \in A$, luego F contiene a $K \cup A$, así que también contiene a $K(A)$. □

Observaciones I.1.10 (1) Toda extensión finita es finitamente generada. En efecto, si $L|K$ es una extensión finita y $\mathcal{B} := \{u_1, \ldots, u_n\} \subset L$ es una base de L como K-espacio vectorial, entonces $L = K(u_1, \ldots, u_n)$, por lo que $L|K$ es una extensión finitamente generada. En efecto, L contiene a $K \cup \mathcal{B}$, luego $K(u_1, \ldots, u_n) \subset L$. El contenido recíproco es evidente pues para cada $x \in L$ existen $\lambda_1, \ldots, \lambda_n \in K$ tales que $x = \sum_{j=1}^n \lambda_j u_j \in K(u_1, \ldots, u_n)$.

(2) Si K es un cuerpo numerable, el anillo de polinomios $K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es numerable. En efecto, denotemos $K_d[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ el conjunto de los polinomios

de $K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ de grado $\leq d$, para cada entero no negativo d. Como la unión numerable de conjuntos numerables es numerable y

$$K[\mathtt{x}_1, \ldots, \mathtt{x}_n] = \bigcup_{d \geq 0} K_d[\mathtt{x}_1, \ldots, \mathtt{x}_n],$$

es suficiente probar que cada $K_d[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es un conjunto numerable. Ahora bien,

$$\mathcal{B}_d := \{\mathtt{x}_1^{\nu_1} \cdots \mathtt{x}_n^{\nu_n} : \ \nu_1, \ldots, \nu_n \geq 0 \quad \& \quad \nu_1 + \cdots + \nu_n \leq d\}$$

es base de $K_d[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ como K-espacio vectorial, luego éste es un K-espacio vectorial de dimensión finita $\mu(d)$, así que $K_d[\mathtt{x}_1, \ldots, \mathtt{x}_n] \cong K^{\mu(d)}$, por lo que es numerable.

(3) Sean K un cuerpo numerable y $L|K$ una extensión finitamente generada. Entonces también L es numerable. En efecto, sean $a_1, \ldots, a_n \in L$ tales que $L = K(a_1, \ldots, a_n)$ y

$$D := \{g \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n] : \ g(a_1, \ldots, a_n) \neq 0\}.$$

Por la Proposición I.1.8 la aplicación

$$K[\mathtt{x}_1, \ldots, \mathtt{x}_n] \times D \to L, \ (f, g) \mapsto f(a_1, \ldots, a_n)/g(a_1, \ldots, a_n)$$

es sobreyectiva, y el producto $K[\mathtt{x}_1, \ldots, \mathtt{x}_n] \times D$ es, por el apartado (2), un conjunto numerable, luego también L es numerable.

(4) Se deduce de (3) que las extensiones $\mathbb{C}|\mathbb{Q}$ y $\mathbb{R}|\mathbb{Q}$ no son finitamente generadas, porque $\mathbb{Q}$ es un conjunto numerable pero ni $\mathbb{R}$ ni $\mathbb{C}$ lo son.

(5) Sean $L|K$ una extensión y $A, B \subset L$. Entonces,

$$K(A)(B) = K(A \cup B) = K(B)(A).$$

En efecto, $K(A \cup B)$ es un cuerpo que contiene a $K \cup A$, luego contiene a $K(A)$. Como también contiene a B se deduce que $K(A)(B) \subset K(A \cup B)$. El otro contenido es evidente pues, por la definición, $K(A)(B)$ contiene a $K \cup (A \cup B)$. Hemos probado la igualdad $K(A)(B) = K(A \cup B)$ y la otra se deduce de ésta y de que $A \cup B = B \cup A$.

(6) El cuerpo $K(A)$ no determina el conjunto A. Lo único que se puede afirmar al respecto es que $K(A) = K(B)$ si y sólo si $A \subset K(B)$ y $B \subset K(A)$. En efecto, si $K(A) = K(B)$ entonces $A \subset K(A) = K(B)$ y $B \subset K(B) = K(A)$. Recíprocamente, si $A \subset K(B)$ el cuerpo $K(B)$ contiene a $K \cup A$, luego contiene al menor cuerpo $K(A)$ que contiene a $K \cup A$. Esto demuestra que $K(A) \subset K(B)$ y para probar la otra inclusión es suficiente intercambiar los roles de A y B.

2. Extensiones algebraicas

En esta sección se introducen las nociones de elementos algebraicamente dependientes e independientes sobre un cuerpo y se obtienen algunos resultados básicos acerca de las llamadas *extensiones algebraicas.*

Definición I.2.1 Sea $L|K$ una extensión de cuerpos, $a = (a_1, \ldots, a_n) \in L^n$ y

$$\mathrm{ev}_a : K[\mathtt{x}_1, \ldots, \mathtt{x}_n] \to L,\ f \mapsto f(a_1, \ldots, a_n)$$

el homomorfismo evaluación.

(1) Se dice que $a_1, \ldots, a_n$ son *algebraicamente independientes sobre* K si ev_a es inyectivo, esto es, $f(a_1, \ldots, a_n) \neq 0$ para cada $f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ no nulo. En caso contrario $a_1, \ldots, a_n$ son *algebraicamente dependientes* sobre K.

(2) Se dice que $a = a_1$ es *transcendente* sobre K si es algebraicamente independiente sobre K, es decir, si $f(a) \neq 0$ para cada polinomio no nulo $f \in K[\mathtt{t}]$. En caso contrario se dice que a es *algebraico* sobre K.

(3) Se dice que una extensión $E|K$ es *algebraica* si cada $a \in E$ es algebraico sobre K. Si E contiene algún elemento transcendente sobre K, se dice que la extensión $E|K$ es *transcendente.* Nótese que si $L|K$ es una subextensión de una extensión algebraica $E|K$, entonces también $L|K$ es algebraica.

Observaciones y Ejemplos I.2.2 (1) Cada $a \in K$ es raíz de $\mathtt{t} - a \in K[\mathtt{t}]$, luego es algebraico sobre K.

(2) Si a es algebraico sobre K, el núcleo del homomorfismo evaluación

$$\mathrm{ev}_a : K[\mathtt{t}] \to L,\ g \to g(a)$$

es un ideal primo no nulo de $K[\mathtt{t}]$, pues L es un dominio. Como $K[\mathtt{t}]$ es un DIP, el núcleo $\ker \mathrm{ev}_a$ está generado por un polinomio irreducible $f \in K[\mathtt{t}]$. Así, por V.1.9, vol. II, $K[\mathtt{t}]/(f) \cong \mathrm{im}\, \mathrm{ev}_a = K[a]$. Como $K[\mathtt{t}]$ es un DIP y f es irreducible, (f) es ideal maximal, luego $K[a]$ es un cuerpo que contiene a $K \cup \{a\}$. Como $K[a] \subset K(a)$ concluimos que $K[a] = K(a)$. El polinomio f que genera $\ker \mathrm{ev}_a$ es único salvo multiplicación por unidades de $K[\mathtt{t}]$, es decir, por elementos no nulos de K. Para elegir sin ambigüedad un generador f de $\ker \mathrm{ev}_a$ exigimos que, además, sea mónico, propiedad que lo hace único. El polinomio mónico f que genera $\ker \mathrm{ev}_a$ recibe el nombre de *polinomio mínimo* o *irreducible* de a sobre K y lo denotaremos $P_{K,a}$. El nombre de polinomio

mínimo proviene de que es el polinomio mónico de grado mínimo entre los polinomios de $K[\mathtt{t}]$ que tienen a a por raíz.

(3) Por el Ejemplo I.1.5 y la Proposición I.1.8, si a es algebraico sobre K la extensión $K(a)|K$ es finita, y de hecho $[K(a) : K] = \deg(P_{K,a})$. Más aún, si denotamos $\mathfrak{m} := P_{K,a}K[\mathtt{t}]$ el ideal maximal generado por $P_{K,a}$, la aplicación

$$L := K[\mathtt{t}]/\mathfrak{m} \to K[a],\ f + \mathfrak{m} \mapsto f(a)$$

es, por el apartado (2), un isomorfismo de cuerpos que deja fijos los elementos de K, luego es un isomorfismo de K-espacios vectoriales. Vimos en el Ejemplo I.1.5 que si $P_{K,a}$ tiene grado n,

$$\mathcal{B} := \{1 + \mathfrak{m},\ \mathtt{t} + \mathfrak{m}, \ldots,\ \mathtt{t}^{n-1} + \mathfrak{m}\}$$

es base de L, luego $\{1, a, \ldots, a^{n-1}\}$ es base de $K[a]$ como K-espacio vectorial.

(4) Sean $L|K$ una extensión, $a \in L$ algebraico sobre K y $f \in K[\mathtt{t}]$ un polinomio mónico e irreducible en $K[\mathtt{t}]$ tal que $f(a) = 0$. Entonces $f = P_{K,a}$. En efecto, $f \in P_{K,a} \cdot K[\mathtt{t}]$ por la propia definición de $P_{K,a}$ y, como f es irreducible, existe $\lambda \in K \setminus \{0\}$ tal que $f = \lambda P_{K,a}$. Pero tanto f como $P_{K,a}$ son mónicos por lo que $\lambda = 1$, esto es, $f = P_{K,a}$.

(5) Si $L|E$ y $E|K$ son extensiones de cuerpos y $a \in L$ es algebraico sobre K, entonces también es algebraico sobre E, pues el polinomio mínimo de a sobre K tiene coeficientes en E. De hecho $P_{K,a} \in E[\mathtt{t}]$ y se anula en a, luego es múltiplo en $E[\mathtt{t}]$ de $P_{E,a}$.

(6) Sean $L|K$ una extensión y $a \in L$ transcendente sobre K. Entonces el homomorfismo $\mathrm{ev}_a : K[\mathtt{t}] \to L,\ g \to g(a)$ es inyectivo, por lo que es un isomorfismo entre $K[\mathtt{t}]$ y $K[a]$, que en consecuencia se extiende a un isomorfismo entre los cuerpos de fracciones:

$$K(\mathtt{t}) \to K(a),\ f/g \mapsto f(a)/g(a).$$

(7) El isomorfismo anterior es también un isomorfismo de K-espacios vectoriales, lo que implica que la extensión $K(a)|K$ es infinita. En efecto, basta probar que lo es $K(\mathtt{t})|K$, y esto es consecuencia de que las potencias $\{\mathtt{t}^j : j \in \mathbb{N}\}$ son K-linealmente independientes.

(8) En particular, toda extensión transcendente $L|K$ es infinita, pues existe un elemento $a \in L$ transcendente sobre K, luego el K-espacio vectorial L contiene al subespacio $K(a)$, que tiene dimensión infinita, por lo que también $\dim_K L$ es infinita.

(9) Sean $L|K$ una extensión y $a_1, \ldots, a_n \in L$ algebraicamente independientes sobre K. Entonces, el homomorfismo evaluación

$$\mathrm{ev} : K[\mathtt{x}_1, \ldots, \mathtt{x}_n] \to L,\ g \to g(a_1, \ldots, a_n)$$

es inyectivo, luego se extiende a un isomorfismo entre sus cuerpos de fracciones

$$K(\mathtt{x}_1, \ldots, \mathtt{x}_n) \to K(a_1, \ldots, a_n),\ f/g \mapsto f(a_1, \ldots, a_n)/g(a_1, \ldots, a_n).$$

(10) En las condiciones del apartado anterior y fijados $1 \leq i_1 < \cdots < i_r \leq n$, es claro que los elementos $a_{i_1}, \ldots, a_{i_r}$ son también algebraicamente independientes sobre K.

(11) Sean K un cuerpo, $\mathtt{t}$ una indeterminada sobre K y $L := K(\mathtt{t})$. Entonces, los elementos $a_1 := \mathtt{t},\ a_2 := \mathtt{t}^2 \in L$ son algebraicamente dependientes sobre K porque el polinomio $f := \mathtt{x}_1^2 - \mathtt{x}_2 \in K[\mathtt{x}_1, \mathtt{x}_2]$ es no nulo y $f(a_1, a_2) = 0$.

Corolario I.2.3 *Sea $L|K$ una extensión de cuerpos. Se cumplen las siguientes propiedades.*

(1) *Si $L|K$ es finita, entonces es algebraica.*

(2) *Si $a \in L$ es algebraico sobre K, entonces la extensión $K(a)|K$ es finita, luego algebraica. Además $K(a) = K[a]$.*

(3) *Si $a_1, \ldots, a_n \in L$ son algebraicos sobre K, entonces $K(a_1, \ldots, a_n)|K$ es una extensión finita y, por tanto, algebraica. Además,*

$$K(a_1, \ldots, a_n) = K[a_1, \ldots, a_n].$$

(4) *Dos elementos $a, b \in L$ son algebraicos sobre K si y sólo si $a + b$ y ab son algebraicos sobre K.*

Demostración. (1) Para cada $a \in L$ se tiene $K \subset K(a) \subset L$ y la finitud de $L|K$ implica, por la Proposición I.1.6, la de $K(a)|K$. Por ello, si $n := [K(a) : K]$, las potencias $1, a, \ldots, a^n$ son K-linealmente dependientes, o sea, existe una $(n+1)$-upla $(\lambda_0, \ldots, \lambda_n) \in K^{n+1}$ no nula tal que $\lambda_0 + \lambda_1 a + \cdots + \lambda_n a^n = 0$. Esto significa que el polinomio $f(\mathtt{t}) := \sum_{j=0}^{n} \lambda_j \mathtt{t}^j \in K[\mathtt{t}]$ es no nulo y $f(a) = 0$, luego a es algebraico sobre K.

(2) Hemos visto en I.2.2 (2) que la extensión $K(a)|K$ es finita, luego por (1) es también algebraica. También hemos demostrado en I.2.2 (2) la igualdad $K(a) = K[a]$.

(3) El caso $n = 1$ es el que acabamos de probar, y procedemos por inducción sobre n. Supongamos el resultado cierto para $n-1$ y veamos que también es cierto para n. Nótese que como a_n es algebraico sobre K también lo es sobre el cuerpo $E := K(a_1, \ldots, a_{n-1})$. Por la hipótesis de inducción se cumple que $E = K[a_1, \ldots, a_{n-1}]$, y por la Observación I.1.10 (4),

$$\begin{aligned} K(a_1, \ldots, a_n) &= K(a_1, \ldots, a_{n-1})(a_n) = E(a_n) = E[a_n] \\ &= K[a_1, \ldots, a_{n-1}][a_n] = K[a_1, \ldots, a_n]. \end{aligned}$$

Además, por hipótesis de inducción, las extensiones $E|K$ y $E(a_n)|E$ son finitas, luego también lo es $E(a_n)|K$, esto es, $K(a_1, \ldots, a_n)|K$ es una extensión finita.

(4) Si a, b son algebraicos sobre K, se sigue del apartado (3) que la extensión $K(a,b)|K$ es algebraica. Como $u := a + b,\ v := ab \in K(a,b)$, tanto u como v son algebraicos sobre K.

Supongamos ahora que u y v son algebraicos sobre K. Por el apartado (3) la extensión $K(u,v)|K$ es finita. Además, a y b son algebraicos sobre $L := K(u,v)$ por ser raíces del polinomio $f(\mathtt{t}) := \mathtt{t}^2 - u\mathtt{t} + v \in L[\mathtt{t}]$, luego se deduce del apartado (3) que la extensión $L(a,b)|L$ es finita. Como también $L|K$ lo es, se sigue de la Proposición I.1.6 que la extensión $L(a,b)|K$ es finita. Esto implica la finitud de $K(a,b)|K$, puesto que $K \subset K(a,b) \subset L(a,b)$. En particular a y b son, por el apartado (1), algebraicos sobre K. □

Ejemplos I.2.4 (1) Dada una extensión de cuerpos $E|K$ y dados $a, b \in E$ elementos algebraicos sobre K, escribimos $L := K(a,b)$ y denotamos

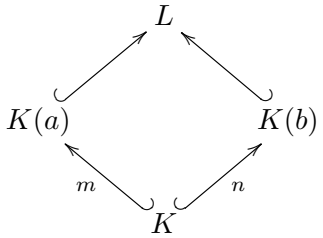
$$m := [K(a) : K] \quad \& \quad n := [K(b) : K].$$

Entonces,

(1.1) Se cumple $L : K(b)] = m$ si y sólo si $[L : K(a)] = n$.

(1.2) Si m y n son primos entre sí, entonces $[L : K] = mn$.

En efecto, empleando la transitividad del grado en el diagrama



tenemos $m\cdot[L:K(a)] = n\cdot[L:K(b)]$, lo que prueba (1.1). Para (1.2), y puesto que m y n son primos entre sí, se deduce de la igualdad anterior y el Teorema Fundamental de la Aritmética que $[L:K(a)]$ es múltiplo de n y $[L:K(b)]$ es múltiplo de m.

Como $L = K(a)(b)$ lo anterior nos dice que el grado del polinomio mínimo $P_{K(a),b}$ de b sobre $K(a)$ es múltiplo del grado de $P_{K,b}$. En particular $\deg(P_{K,b}) \leq \deg(P_{K(a),b})$. Recíprocamente, como $K \subset K(a)$, el polinomio mínimo $P_{K,b}$ de b sobre K es múltiplo en $K(a)[\mathtt{t}]$ de $P_{K(a),b}$, y en consecuencia $\deg(P_{K(a),b}) \leq \deg(P_{K,b})$. En conclusión,

$$[L:K(a)] = \deg(P_{K(a),b}) = \deg(P_{K,b}) = [K(b):K] = n,$$

y por tanto $[L:K] = [L:K(a)]\cdot[K(a):K] = mn$.

(2) Como caso particular de lo anterior, sean p un número primo y m y n dos enteros positivos primos entre sí. Los polinomios $\mathtt{t}^m - p$ y $\mathtt{t}^n - p$ son irreducibles en $\mathbb{Z}[\mathtt{t}]$ por el Criterio de Eisenstein, luego también lo son en $\mathbb{Q}[\mathtt{t}]$, y tienen a los números $a := \sqrt[m]{p}$ y $b := \sqrt[n]{p}$, respectivamente, por raíces. En consecuencia $P_{\mathbb{Q},a}(\mathtt{t}) = \mathtt{t}^m - p$ y $P_{\mathbb{Q},b}(\mathtt{t}) = \mathtt{t}^n - p$, por lo que $[\mathbb{Q}(a):\mathbb{Q}] = m$ y $[\mathbb{Q}(a):\mathbb{Q}] = n$. Como $\mathrm{mcd}(m,n) = 1$ deducimos que $[\mathbb{Q}(a,b):\mathbb{Q}] = mn$.

(3) Sean p_1, p_2 y p_3 tres números primos distintos. Vamos a calcular los grados de las extensiones

$$\mathbb{Q}(\sqrt{p_1},\sqrt{p_2})|\mathbb{Q} \quad \& \quad \mathbb{Q}(\sqrt{p_1},\sqrt{p_2},\sqrt{p_3})|\mathbb{Q}.$$

Sea $E := \mathbb{Q}(\sqrt{p_1},\sqrt{p_2})$. Para $i = 1, 2$ el polinomio $\mathtt{t}^2 - p_i \in \mathbb{Q}[\mathtt{t}]$ es irreducible, por el Criterio de Eisenstein, y tiene a $\sqrt{p_i}$ por raíz, luego $[\mathbb{Q}(\sqrt{p_i}):\mathbb{Q}] = 2$, y por tanto,

$$\begin{aligned}[E:\mathbb{Q}] = [\mathbb{Q}(\sqrt{p_1})(\sqrt{p_2}):\mathbb{Q}] &= [\mathbb{Q}(\sqrt{p_1})(\sqrt{p_2}):\mathbb{Q}(\sqrt{p_1})]\cdot[\mathbb{Q}(\sqrt{p_1}):\mathbb{Q}] \\ &\leq [\mathbb{Q}(\sqrt{p_2}):\mathbb{Q}]\cdot[\mathbb{Q}(\sqrt{p_1}):\mathbb{Q}] = 4,\end{aligned}$$

y se da la igualdad si y sólo si $[\mathbb{Q}(\sqrt{p_1})(\sqrt{p_2}):\mathbb{Q}(\sqrt{p_1})] = 2$ o, equivalentemente, si $\sqrt{p_2} \notin \mathbb{Q}(\sqrt{p_1})$. Comprobemos que efectivamente es así. En caso contrario existirían $a, b \in \mathbb{Q}$ tales que $\sqrt{p_2} = a + b\sqrt{p_1}$, luego

$$0 = (a + b\sqrt{p_1})^2 - p_2 = a^2 + p_1b^2 - p_2 + 2ab\sqrt{p_1} = 0.$$

Como $\{1, \sqrt{p_1}\}$ son $\mathbb{Q}$-linealmente independientes deducimos que $a^2 + p_1b^2 = p_2$ y $ab = 0$. Si $a = 0$ entonces $p_2 = p_1b^2$, lo que es imposible, ya que p_1 es primo y distinto de p_2. Por tanto $b = 0$ así que $p_2 = a^2$, o lo que es lo mismo, $\sqrt{p_2} \in \mathbb{Q}$, lo que es falso también. Esto demuestra que $[\mathbb{Q}(\sqrt{p_1},\sqrt{p_2}):\mathbb{Q}] = 4$.

Para la segunda parte escribimos $L := \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}) = E(\sqrt{p_3})$ y observamos que

$$\begin{aligned}[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}) : \mathbb{Q}] &= [L : E] \cdot [E : \mathbb{Q}] \\ &= 4 \cdot [E(\sqrt{p_3}) : E] \leq 4 \cdot [\mathbb{Q}(\sqrt{p_3}) : \mathbb{Q}] = 8,\end{aligned}$$

y se da la igualdad si y sólo si $\sqrt{p_3} \notin E$. Comprobemos que así es. En caso contrario, y puesto que

$$\mathcal{B} := \{1, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_1 p_2}\}$$

es una base de E como $\mathbb{Q}$-espacio vectorial, existen números racionales a, b, c y d tales que

$$\sqrt{p_3} = a + b\sqrt{p_1} + c\sqrt{p_2} + d\sqrt{p_1 p_2}.$$

Entonces, $(\sqrt{p_3} - a - b\sqrt{p_1})^2 = p_2(c + d\sqrt{p_1})^2$, y desarrollando estos cuadrados,

$$p_3 + a^2 + p_1 b^2 - 2a\sqrt{p_3} - 2b\sqrt{p_1 p_3} + 2ab\sqrt{p_1} = p_2(c^2 + p_1 d^2 + 2cd\sqrt{p_1}).$$

Consideremos los números racionales

$$e := p_3 + a^2 + p_1 b^2 - p_2(c^2 + p_1 d^2) \quad \& \quad f := 2(ab - p_2 cd).$$

La igualdad anterior se reescribe

$$e \cdot 1 + f \cdot \sqrt{p_1} - 2a \cdot \sqrt{p_3} - 2b \cdot \sqrt{p_1 p_3} = 0,$$

y como $\{1, \sqrt{p_1}, \sqrt{p_3}, \sqrt{p_1 p_3}\}$ son independientes sobre $\mathbb{Q}$, $a = b = e = f = 0$.

De aquí se desprende que $cd = 0$ y $p_3 = p_2(c^2 + p_1 d^2)$. Por tanto $c = 0$ o $d = 0$. En el primer caso $p_3 = p_1 p_2 d^2$, lo que es falso porque p_3 es primo. En consecuencia $d = 0$, así que $p_3 = p_2 c^2$, lo que también es imposible, ya que p_3 es primo y distinto de p_2. En conclusión,

$$[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}) : \mathbb{Q}] = 8.$$

(4) Vimos en el Ejemplo VI.2.7, vol. II, que para cada primo p el polinomio ciclotómico $\Phi_p(\mathtt{t}) := \sum_{j=0}^{p-1} \mathtt{t}^j$ es irreducible en $\mathbb{Z}[\mathtt{t}]$, luego en $\mathbb{Q}[\mathtt{t}]$. Si $i := \sqrt{-1}$ y $\zeta := e^{2\pi i/p}$, se tiene $\zeta^p = 1$, luego $0 = \zeta^p - 1 = (\zeta - 1)\Phi_p(\zeta)$, así que $\Phi_p(\zeta) = 0$, esto es, $\Phi_p = P_{\mathbb{Q},\zeta}$ es el polinomio mínimo de ζ sobre $\mathbb{Q}$.

Corolario I.2.5 *Sea $L|K$ una extensión de cuerpos. Entonces,*

$$\overline{K}_L := \{a \in L : \ a \text{ es algebraico sobre } K\}$$

es un cuerpo, denominado cierre algebraico de K en L. *La extensión $\overline{K}_L|K$ es algebraica.*

Demostración. La segunda parte es inmediata una vez probado que $\overline{K}_L$ es un cuerpo. Para esto basta probar que si $a, b \in \overline{K}_L$ y $b \neq 0$, entonces $a - b$ y ab^{-1} pertenecen a $\overline{K}_L$. Ahora bien, la extensión $K(a,b)|K$ es finita, por I.2.3 (3), luego algebraica, y $a - b, ab^{-1} \in K(a,b)$, así que $a - b$ y ab^{-1} son algebraicos sobre K. □

Observaciones I.2.6 (1) Existen extensiones algebraicas que no son finitas. Por ejemplo, sea $E := \overline{\mathbb{Q}}_{\mathbb{C}}$ el cierre algebraico de $\mathbb{Q}$ en $\mathbb{C}$. Acabamos de ver que la extensión $E|\mathbb{Q}$ es algebraica. Supongamos, por reducción al absurdo, que es finita, y denotemos $n := [E : \mathbb{Q}]$. Sean $m := n + 1$ y $a := \sqrt[m]{2}$ el único número real positivo cuya potencia m-ésima es 2. Nótese que $a \in E$ por ser raíz del polinomio $f(\mathtt{t}) := \mathtt{t}^m - 2$. Además este polinomio es irreducible en $\mathbb{Z}[\mathtt{t}]$, por el Criterio de Eisenstein, VI.2.6, vol. II, luego también lo es en $\mathbb{Q}[\mathtt{t}]$, en virtud del Lema VI.1.5, vol. II. Por tanto $f = P_{\mathbb{Q},a}$ es el polinomio mínimo de a sobre $\mathbb{Q}$. Como $\mathbb{Q} \subset \mathbb{Q}(a) \subset E$, se obtiene una contradicción, ya que

$$m = \deg(f) = [\mathbb{Q}(a) : \mathbb{Q}] \leq [E : \mathbb{Q}] = n = m - 1.$$

(2) La extensión $\overline{\mathbb{Q}}_{\mathbb{C}}|\mathbb{Q}$ no es finitamente generada pues si lo fuese, como también es algebraica, sería finita, por el Corolario I.2.3 (3), y acabaamos de ver que no es así.

(3) Para cada entero positivo m sea $a_m := \sqrt[m]{2}$ el único número real positivo cuya potencia m-ésima es 2, y denotemos $A := \{a_m : m \in \mathbb{Z}^+\}$. Hemos señalado en el apartado (1) que cada a_m es algebraico sobre $\mathbb{Q}$, luego $\mathbb{Q} \cup A \subset \overline{\mathbb{Q}}_{\mathbb{C}}$. Por ello $\mathbb{Q}(A) \subset \overline{\mathbb{Q}}_{\mathbb{C}}$, luego la extensión $\mathbb{Q}(A)|\mathbb{Q}$ es algebraica. Sin embargo no es finitamente generada, pues si lo fuese sería finita, de grado digamos m, y puesto que $\mathbb{Q} \subset \mathbb{Q}(a_{m+1}) \subset \mathbb{Q}(A)$, se tiene la siguiente contradicción:

$$m + 1 = \deg(\mathtt{t}^{m+1} - 2) = \deg(P_{\mathbb{Q},a_{m+1}}) = [\mathbb{Q}(a_{m+1}) : \mathbb{Q}] \leq [\mathbb{Q}(A) : \mathbb{Q}] = m.$$

(4) Por el Corolario I.2.3 (4), dados a y b algebraicos sobre K, también $a + b$ y ab son algebraicos sobre K. Veamos ahora cómo encontrar, a partir de los polinomios mínimos $f := P_{K,a}$ y $g := P_{K,b}$ de a y b sobre K, polinomios no nulos con coeficientes en K que tienen a la suma $a + b$ y al producto ab por raíces. Sean $\mathtt{t}$ y $\mathtt{x}$ dos indeterminadas, denotamos $A := K[\mathtt{x}]$ y consideremos

$$f(\mathtt{t}) \in K[\mathtt{t}] \subset A[\mathtt{t}] \quad \& \quad \ell(\mathtt{t}) := h(\mathtt{x}, \mathtt{t}) = g(\mathtt{x} - \mathtt{t}) \in A[\mathtt{t}],$$

Sean $L := K(a,b)$ y $h_{a+b}(\mathtt{t}) := h(a + b, \mathtt{t}) \in L[\mathtt{t}]$. Los polinomios $f(\mathtt{t})$ y $h_{a+b}(\mathtt{t})$ tienen al elemento a por raíz común, pues

$$f(a) = 0 \quad \& \quad h_{a+b}(a) = h(a + b, a) = g(a + b - a) = g(b) = 0.$$

Por tanto, la resultante $\mathrm{Res}(f(\mathtt{t}), h_{a+b}(\mathtt{t}))$ se anula, en virtud del Corolario VII.2.5, vol. II. Por otro lado, podemos calcular la resultante

$$p_1(\mathtt{x}) = \mathrm{Res}_{\mathtt{t}}(f(\mathtt{t}), \ell(\mathtt{t})) = \mathrm{Res}_{\mathtt{t}}(f(\mathtt{t}), g(\mathtt{x}-\mathtt{t})) \in K[\mathtt{x}]$$

de $f(\mathtt{t})$ y $\ell(\mathtt{t})$ vistos como polinomios en la indeterminada $\mathtt{t}$. Este es un polinomio no nulo y, como la resultante es especializable para polinomios mónicos, (pues en tal caso la especialización preserva el grado) se deduce que

$$p_1(a+b) = \mathrm{Res}(f(\mathtt{t}), g(a+b-\mathtt{t})) = \mathrm{Res}(f(\mathtt{t}), h_{a+b}(\mathtt{t})) = 0.$$

Para el producto, sea $q(\mathtt{t}, \mathtt{x}) = g(\mathtt{x}/\mathtt{t})\mathtt{t}^{\deg(g)} \in A[\mathtt{t}]$. Los polinomios $f(\mathtt{t})$ y $q(ab, \mathtt{t})$ tienen al elemento a por raíz común, porque

$$f(a) = 0 \quad \& \quad q(ab, a) = g(ab/a)a^{\deg(g)} = g(b)a^{\deg(g)} = 0.$$

Se deduce de nuevo del Corolario VII.2.5, vol. II., y por la especializabilidad de la resultante, que el polinomio

$$p_2(\mathtt{x}) = \mathrm{Res}_{\mathtt{t}}(f(\mathtt{t}), g(\mathtt{x}/\mathtt{t})\mathtt{t}^{\deg(g)}) \in K[\mathtt{x}]$$

es no nulo y $p_2(ab) = 0$.

Proposición I.2.7 *Sean $E|L$ y $L|K$ extensiones de cuerpos. Las siguientes afirmaciones son equivalentes:*

(1) *La extensión $E|K$ es algebraica.*

(2) *Las extensiones $E|L$ y $L|K$ son algebraicas.*

Demostración. (1) $\Longrightarrow$ (2) Cada elemento de E es algebraico sobre K, luego lo es sobre L ya que este cuerpo contiene a K. Además cada elemento de L pertenece a E luego, por hipótesis, es algebraico sobre K.

(2) $\Longrightarrow$ (1) Veamos que cada $u \in E$ es algebraico sobre K. Como la extensión $E|L$ es algebraica, existen un entero $n \geq 1$ y $f(\mathtt{t}) := \mathtt{t}^n + \sum_{k=0}^{n-1} a_k \mathtt{t}^k \in L[\mathtt{t}]$ tales que $f(u) = 0$. Así, u es algebraico sobre el cuerpo $F := K(a_0, a_1, \ldots, a_{n-1})$ y, por tanto, la extensión $F(u)|F$ es finita.

Como cada a_i es algebraico sobre K por ser algebraica la extensión $L|K$, se deduce de la Proposición I.2.3 (3) que la extensión $F|K$ es finita. Así, por la transitividad del grado, también es finita la extensión $F(u)|K$, luego es algebraica. En particular, u es algebraico sobre K. □

Proposición I.2.8 *Sea $L|K$ una extensión de cuerpos generada por un subconjunto $A = \{u_i : i \in I\}$ de L cuyos elementos son algebraicos sobre K. Entonces, la extensión $L|K$ es algebraica y*

$$L = K(A) = \{f(u_{i_1}, \ldots, u_{i_r}) : \ f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_r], \ r \geq 1, \ i_1, \ldots, i_r \in I\}.$$

Demostración. Sea $b \in L$. Por la Proposición I.1.9 (2), existen $u_{i_1}, \ldots, u_{i_r}$ tales que $b \in K(u_{i_1}, \ldots, u_{i_r})$. Como $u_{i_1}, \ldots, u_{i_r}$ son algebraicos sobre K entonces, por el Corolario I.2.3, $K(u_{i_1}, \ldots, u_{i_r}) = K[u_{i_1}, \ldots, u_{i_r}]$ y, por tanto, existe $h \in K[\mathtt{x}_1, \ldots, \mathtt{x}_r]$ tal que

$$b = h(u_{i_1}, \ldots, u_{i_r}) \in K[u_{i_1}, \ldots, u_{i_r}].$$

Empleando de nuevo el Corolario I.2.3, se sigue que b es algebraico sobre K. Así, $L = K(A)$ es una extensión algebraica de K y se cumple la igualdad del enunciado. □

Ejercicios y problemas propuestos

Número I.1 Caracterizar los números complejos α tales que $E := \{a + b\alpha : a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{C}$. Dar un ejemplo de un α que satisface esta condición y otro que no la cumple.

Número I.2 Encontrar una extensión de cuerpos $L|K$ tal que existan $\alpha, \beta \in L \setminus K$, de modo que $\alpha \neq \pm\beta$ y $K(\alpha) = K(\beta)$. ¿Qué relación hay entre los polinomios mínimos de α y de β sobre K?

Número I.3 ¿Cuáles son las raíces en un cuerpo K de característica p del polinomio $\mathtt{t}^p - 1$?

Número I.4 Para los siguientes valores de $\alpha \in \mathbb{C}$ encontrar el polinomio mínimo de α sobre $\mathbb{Q}$ y el grado de la extensión $\mathbb{Q}(\alpha)|\mathbb{Q}$:

$$\alpha := (\sqrt{3} - 1)/2, \quad \alpha := (i + 1)\sqrt{5}/3 \quad \& \quad \alpha := \sqrt{1 - \sqrt{11}}.$$

Número I.5 (1) Sean $L|K$ una extensión finita y $f \in K[\mathtt{t}]$ un polinomio irreducible. Probar que si f tiene alguna raíz en L entonces el grado de f divide al grado $[L : K]$ de la extensión.

(2) Supongamos que $[L : K]$ es un número primo. Demostrar que cada elemento $\alpha \in L \setminus K$ cumple que $L = K(\alpha)$.

Número I.6 Sean $a := \sqrt{5} + \sqrt{-5}$ y $b := \sqrt[4]{5}$. Calcular el grado de la extensión $\mathbb{Q}(a, b)|\mathbb{Q}(b)$.

Número I.7 Sean $E|K$ una extensión y $\alpha \in E$ un elemento algebraico sobre K. Demostrar que si el grado de la extensión $K(\alpha)|K$ es impar entonces $K(\alpha^2) = K(\alpha)$.

Número I.8 Sean $L|K$ una extensión de cuerpos, $f \in K[\mathtt{t}] \setminus K$ y $\alpha \in L$ transcendente sobre K.

(1) Demostrar que $f(\alpha)$ es transcendente sobre K.

(2) Demostrar que si $\beta \in L$ satisface $f(\beta) = \alpha$ entonces β es transcendente sobre K.

Número I.9 Sea $K(\alpha, \beta)|K$ una extensión de cuerpos de modo que $\alpha \notin K$ es algebraico sobre K y β es transcendente sobre K. Demostrar que la extensión $K(\alpha, \beta)|K$ no es simple.

Número I.10 Sean K un cuerpo y $f(\mathtt{t}) := \mathtt{t}^n - a \in K[\mathtt{t}]$. Supongamos que f es irreducible en $K[\mathtt{t}]$. Dados un divisor m de n y una raíz α de f, calcular el polinomio mínimo de α^m sobre K.

Número I.11 Hallar los polinomios mínimos de $\alpha := \sqrt[3]{5}$ sobre $\mathbb{Q}$ y $K := \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Número I.12 Dados $k \in \mathbb{Z}\backslash 7\mathbb{Z}$ y $\alpha_k := 2k\pi/7$ calcular el polinomio mínimo de $u := 2\cos\alpha_k$ sobre $\mathbb{Q}$.

Número I.13 Sea $\mathfrak{a}$ el ideal de $\mathbb{Q}[\mathtt{t}]$ generado por los polinomios

$$f(\mathtt{t}) := \mathtt{t}^4 + \mathtt{t}^3 + 2\mathtt{t}^2 + \mathtt{t} + 1 \quad \& \quad g(\mathtt{t}) := \mathtt{t}^3 + 4\mathtt{t}^2 + 4\mathtt{t} + 3.$$

Probar que el cociente $K := \mathbb{Q}[\mathtt{t}]/\mathfrak{a}$ es un cuerpo extensión de $\mathbb{Q}$. Hallar el grado y un elemento primitivo de la extensión $K|\mathbb{Q}$.

Número I.14 (1) Probar que el polinomio $f(\mathtt{t}) := \mathtt{t}^5 - \mathtt{t} - 1$ es irreducible en $\mathbb{Q}[\mathtt{t}]$.

(2) Sean $a, b \in \mathbb{Q}$. ¿Tienen los polinomios $\mathtt{t}^5 - \mathtt{t} - 1$ y $\mathtt{t}^3 + a\mathtt{t} + b$ alguna raíz compleja común?

(3) Sea $\alpha := [\mathtt{t}]$ la clase de $\mathtt{t}$ en $\mathbb{Q}[\mathtt{t}]/(\mathtt{t}^5 - \mathtt{t} - 1)$. Escribir el elemento $1/(1 + \alpha + \alpha^3)$ como expresión polinómica en α con coeficientes en $\mathbb{Q}$.

Número I.15 Sean K un cuerpo, $E := K(\mathtt{t})$ y $L := K\big(\mathtt{t}^3(1 + \mathtt{t})^{-1}\big)$, donde $\mathtt{t}$ es una indeterminada. Probar que $E|L$ es una extensión algebraica simple y calcular $[E : L]$.

CAPÍTULO II

Cuerpo de descomposición de un polinomio

En este capítulo abordamos el problema de encontrar, fijado un cuerpo K y polinomios en $K[\mathtt{t}]$, una extensión $L|K$ de modo que los polinomios dados factoricen en $L[\mathtt{t}]$ como producto de factores de grado 1. Comenzamos resolviendo este problema para un único polinomio f, y se dice que L es un *cuerpo de descomposición* de f sobre K. Esto proporciona también la solución cuando el conjunto de polinomios dados $f_1, \ldots, f_r$ es finito; basta considerar un cuerpo de descomposición del producto $f := f_1 \cdots f_r$. El problema es más difícil para familias infinitas; por ejemplo la formada por todos los polinomios de $K[\mathtt{t}]$, pues los productos infinitos carecen de sentido. Esto lleva a construir el llamado *cierre algebraico* del cuerpo K. Una propiedad fundamental del cuerpo de descomposición y del cierre algebraico es que son esencialmente únicos.

1. Cuerpo de descomposición

Antes de abordar la prueba de la existencia y unicidad del cuerpo de descomposición de un polinomio necesitamos un lema auxiliar.

Lema II.1.1 *Sea $\phi : K_1 \to K_2$ un isomorfismo entre los cuerpos K_1 y K_2.*

(1) *La aplicación*

$$\Phi : K_1[\mathtt{t}] \to K_2[\mathtt{t}],\ f(\mathtt{t}) := \sum_{j=0}^{m} b_j \mathtt{t}^j \mapsto \Phi(f)(\mathtt{t}) := \sum_{j=0}^{m} \phi(b_j)\mathtt{t}^j$$

es un isomorfismo de anillos.

(2) *Sean $L_1|K_1$ y $L_2|K_2$ extensiones de cuerpos y $\alpha_1 \in L_1$ y $\alpha_2 \in L_2$ elementos algebraicos sobre K_1 y K_2 respectivamente. Denotemos $f_i := P_{K_i,\alpha_i}$ el polinomio mínimo de α_i sobre K_i, para $i = 1, 2$. Las siguientes afirmaciones son equivalentes:*

(2.1) *Existe un isomorfismo* $\psi : K_1(\alpha_1) \to K_2(\alpha_2)$ *con* $\psi|_{K_1} = \phi$ *y* $\psi(\alpha_1) = \alpha_2$.

(2.2) *El homomorfismo* Φ *del apartado* (1) *cumple la igualdad* $f_2 = \Phi(f_1)$.

Demostración. (1) La comprobación de que Φ es homomorfismo es inmediata, mientras que su sobreyectividad se deduce directamente de la de ϕ. Por último, Φ es inyectivo porque si $f(\mathtt{t}) := \sum_{j=0}^{m} b_j \mathtt{t}^j \in \ker \Phi$, entonces $\phi(b_j) = 0$ para $0 \leq j \leq m$. Como ϕ es inyectivo cada $b_j = 0$, luego $f = 0$.

(2) Veamos que (2.1) implica (2.2). Sea $f_1(\mathtt{t}) := \mathtt{t}^n + \sum_{k=0}^{n-1} a_k \mathtt{t}^k$, que cumple $f_1(\alpha_1) = 0$. Se tiene entonces

$$0 = \psi(f_1(\alpha_1)) = \psi\Big(\alpha_1^n + \sum_{k=0}^{n-1} a_k \alpha_1^k\Big) = \alpha_2^n + \sum_{k=0}^{n-1} \phi(a_k)\alpha_2^k = \Phi(f_1)(\alpha_2).$$

Como f_1 es irreducible en $K_1[\mathtt{t}]$ y Φ es isomorfismo, $\Phi(f_1) \in K_2[\mathtt{t}]$ es un polinomio irreducible y mónico que se anula en α_2, luego $\Phi(f_1) = f_2$.

Probamos ahora que (2.2) implica (2.1) Según hemos visto en I.2.2, para $i = 1, 2$ existe un isomorfismo $\varphi_i : K_i(\alpha_i) \to K_i[\mathtt{t}]/(f_i)$ tal que $\varphi_i(\alpha_i) = \mathtt{t} + (f_i)$ y $\varphi_i(a) = a + (f_i)$ para cada $a \in K_i$. Además, el isomorfismo Φ del apartado (1) induce, puesto que $\Phi(f_1) = f_2$, un isomorfismo

$$\Psi : K_1[\mathtt{t}]/(f_1) \to K_2[\mathtt{t}]/(f_2),$$

que cumple $\Psi(\mathtt{t} + (f_1)) = \mathtt{t} + (f_2)$. Nótese que para cada $a \in K_1$

$$\Psi(a + (f_1)) = \Phi(a) + (f_2) = \phi(a) + (f_2).$$

Obtenemos así un isomorfismo $\psi = \varphi_2^{-1} \circ \Psi \circ \varphi_1 : K_1(\alpha_1) \to K_2(\alpha_2)$ y

$$\psi(\alpha_1) = (\varphi_2^{-1} \circ \Psi)\big(\mathtt{t} + (f_1)\big) = \varphi_2^{-1}\big(\mathtt{t} + (f_2)\big) = \alpha_2,$$

y para cada $a \in K_1$ se tiene

$$\psi(a) = (\varphi_2^{-1} \circ \Psi)(a + (f_1)) = \varphi_2^{-1}(\phi(a) + (f_2)) = \phi(a),$$

es decir, $\psi|_{K_1} = \phi$. □

Teorema II.1.2 (Cuerpo de descomposición de un polinomio) *Sea* K *un cuerpo y sea* $f \in K[\mathtt{t}]$ *un polinomio de grado* ≥ 1. *Entonces, existe una única extensión de cuerpos* $L|K$, *salvo isomorfismo que restringido a* K *es*

la identidad, tal que la factorización de f en $L[\mathtt{t}]$ como producto de factores irreducibles es

$$f(\mathtt{t}) := a_n(\mathtt{t}-\alpha_1)\cdots(\mathtt{t}-\alpha_n),$$

donde $\alpha_1,\ldots,\alpha_n \in L$ y $a_n \in K$, y además $L = K(\alpha_1,\ldots,\alpha_n)$. La extensión $L|K$ es finita y el cuerpo $L := L_f$ se denomina cuerpo de descomposición de f sobre K.

Demostración. Veamos en primer lugar la existencia de una extensión $L|K$ en las condiciones del enunciado. Para ello procedemos por inducción sobre el grado de f. Si $\deg(f) = 1$, existen $a_1, \alpha_1 \in K$ tales que $f(\mathtt{t}) := a_1(\mathtt{t}-\alpha_1)$, luego $L = K$ cumple lo requerido.

Suponemos probado el resultado para polinomios de grado menor que n y veamos que también es cierto para los de grado n. Si f es reducible en $K[\mathtt{t}]$ de grado n, existen $g, h \in K[\mathtt{t}]$ de grado ≥ 1 tales que $f := gh$. Esto implica que $\deg(g),\ \deg(h) < n$. Por la hipótesis de inducción, existe una extensión $L_1|K$ tal que g es producto de factores de grado 1 en $L_1[\mathtt{t}]$. En particular, existe $\alpha_1 \in L_1$ tal que $g(\alpha_1) = 0$. Esto implica que $f(\alpha_1) = 0$ y, por la Regla de Ruffini, existe $f_1 \in L_1[\mathtt{t}]$ de grado $n-1 < n$ tal que $f(\mathtt{t}) := (\mathtt{t}-\alpha_1)f_1(\mathtt{t})$. Por la hipótesis de inducción, existen una extensión $L_2|L_1$, $a_n \in K$ y $\alpha_2,\ldots,\alpha_n \in L_2$ tales que

$$f_1(\mathtt{t}) := a_n(\mathtt{t}-\alpha_2)\cdots(\mathtt{t}-\alpha_n),$$

y en consecuencia

$$f(\mathtt{t}) = (\mathtt{t}-\alpha_1)f_1(\mathtt{t}) = a_n(\mathtt{t}-\alpha_1)\cdots(\mathtt{t}-\alpha_n).$$

Podemos pues suponer que f es irreducible en $K[\mathtt{t}]$. Vimos en el Ejemplo I.1.2 que $F_1 := K[\mathtt{t}]/(f)$ es un cuerpo que contiene a K. Además, si denotamos $\alpha_1 := \mathtt{t} + (f) \in F_1$ y $f(\mathtt{t}) = \sum_{i=0}^{d} a_j\mathtt{t}^j$, se cumple que

$$f(\alpha_1) = \sum_{i=0}^{d} a_j\alpha^j = \sum_{i=0}^{d} a_j(\mathtt{t}+(f))^j = \Big(\sum_{i=0}^{d} a_j\mathtt{t}^j\Big) + (f) = f(\mathtt{t}) + (f) = 0.$$

Por la Regla de Ruffini, existe $p \in F_1[\mathtt{t}]$ tal que $f(\mathtt{t}) = (\mathtt{t}-\alpha_1)p(\mathtt{t})$. Como $\deg(p) = n-1$ existen, por hipótesis de inducción, una extensión $F_2|F_1$, $a_n \in K$ y $\alpha_2,\ldots,\alpha_n \in F_2$ con $p(\mathtt{t}) = a_n(\mathtt{t}-\alpha_2)\cdots(\mathtt{t}-\alpha_n)$. En consecuencia, el cuerpo $L := K(\alpha_1,\ldots,\alpha_n) \subset F_2$ cumple lo requerido. Nótese que cada α_i es algebraico sobre K pues $f(\alpha_i) = 0$, luego $L|K$ es extensión finita, por I.2.3 (3).

Veamos a continuación la unicidad. Supongamos que existen otra extensión $E|K$ y $\beta_1, \ldots, \beta_n \in E$ tales que

$$f(\mathtt{t}) := a_n(\mathtt{t} - \beta_1) \cdots (\mathtt{t} - \beta_n) \quad \& \quad E := K(\beta_1, \ldots, \beta_n).$$

Hemos de construir un isomorfismo $\phi : L \to E$ tal que $\phi|_K$ sea la identidad. Consideramos los cuerpos $K_0 := K$ y $K_i := K(\alpha_1, \ldots, \alpha_i)$ para $1 \leq i \leq n$, que cumplen

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = L.$$

Construiremos inductivamente una sucesión de homomorfismos $\phi_i : K_i \to E$ de modo que

$$\phi_0 := \mathtt{j} : K \hookrightarrow E \text{ es la inclusión} \quad \& \quad \phi_i|_{K_{i-1}} = \phi_{i-1} \quad \text{para } 1 \leq i \leq n.$$

Supongamos ya construido el homomorfismo $\phi_{i-1} : K_{i-1} \to E$. Si $\alpha_i \in K_{i-1}$ entonces $K_i := K_{i-1}(\alpha_i) = K_{i-1}$ y tomando $\phi_i := \phi_{i-1}$ hemos acabado. Por tanto, supondremos que $\alpha_i \notin K_{i-1}$. Como $f(\alpha_i) = 0$ y $f \in K[\mathtt{t}] \subset K_{i-1}[\mathtt{t}]$, el elemento α_i es algebraico sobre K_{i-1}. Sean $g := P_{K_{i-1},\alpha_i} \in K_{i-1}[\mathtt{t}]$ el polinomio mínimo de α_i sobre K_{i-1} y $K'_{i-1} := \phi_{i-1}(K_{i-1})$. Por el Lema II.1.1 los anillos $K_{i-1}[\mathtt{t}]$ y $K'_{i-1}[\mathtt{t}]$ son isomorfos vía el isomorfismo

$$\Phi_{i-1} : K_{i-1}[\mathtt{t}] \to K'_{i-1}[\mathtt{t}], \ \sum_{j=0}^{m} a_j \mathtt{t}^j \to \sum_{j=0}^{m} \phi_{i-1}(a_j)\mathtt{t}^j.$$

Sea $h := \Phi_{i-1}(g) \in K'_{i-1}[\mathtt{t}]$. Como $g(\alpha_i) = f(\alpha_i) = 0$, el polinomio g divide a f en $K_{i-1}[\mathtt{t}]$, por lo que h divide a $f := \Phi_{i-1}(f)$ en $K'_{i-1}[\mathtt{t}]$, luego también en $E[\mathtt{t}]$. Puesto que el grado de h es mayor o igual que 1 y $E[\mathtt{t}]$ es un DFU en el que f factoriza como

$$f(\mathtt{t}) := a_n(\mathtt{t} - \beta_1) \cdots (\mathtt{t} - \beta_n),$$

existe un índice $1 \leq j \leq n$ tal que $\mathtt{t} - \beta_j$ divide a h y, por tanto, $h(\beta_j) = 0$. De este modo, por el Lema II.1.1, existe un isomorfismo

$$\phi_i : K_i = K_{i-1}(\alpha_i) \to K'_{i-1}(\beta_j)$$

tal que $\phi_i|_{K_{i-1}} = \phi_{i-1}$ y $\phi_i(\alpha_i) = \beta_j$.

Para terminar, sólo queda probar que $\phi_n : L = K(\alpha_1, \ldots, \alpha_n) \to E$ es un epimorfismo. Denotemos $\gamma_i := \phi_n(\alpha_i) \in E$ para $1 \leq i \leq n$. En $E[\mathtt{t}]$ se tiene

$$a_n(\mathtt{t} - \beta_1) \cdots (\mathtt{t} - \beta_n) = f(\mathtt{t}) = \Phi_n(f)(\mathtt{t}) = a_n(\mathtt{t} - \gamma_1) \cdots (\mathtt{t} - \gamma_n),$$

donde $\Phi_n : K_n[\mathtt{t}] \to K'_n[\mathtt{t}]$ es el isomorfismo inducido por ϕ_n. Como $E[\mathtt{t}]$ es un DFU, podemos suponer, tras reordenar los índices, que $\beta_j = \gamma_j$ y, por tanto,

$$\phi_n(K_n) = K'_n = K(\gamma_1, \ldots, \gamma_n) = K(\beta_1, \ldots, \beta_n) = E.$$

De este modo, ϕ_n es un epimorfismo y, por tanto, un isomorfismo. □

Observaciones II.1.3 Mantenemos las hipótesis y notaciones del Teorema anterior II.1.2.

(1) La extensión $L_f|K$ es "minimal", esto es, L_f es, salvo isomorfía, "el menor cuerpo" que contiene a K de modo que f factoriza en $L_f[\mathtt{t}]$ en producto de factores de grado 1.

(2) En general, las raíces $\alpha_1, \ldots, \alpha_n$ de f no son necesariamente distintas, pero sí lo son si $\mathrm{char}(K) = 0$ y f es irreducible en $K[\mathtt{t}]$. En efecto, se trata de probar que entonces todas las raíces de f son simples. En caso contrario existiría una raíz α de f que es también raíz de la derivada f'. Pero el ideal (f) de $K[\mathtt{t}]$ generado por f es el núcleo de la evaluación en α, luego $f|f'$. Esto es imposible porque $\deg(f') < \deg(f)$ y $f' \not\equiv 0$, al ser $\mathrm{char}(K) = 0$.

(3) El grado de la extensión $L_f|K$ es finito y de hecho $[L_f : K] \leq n!$. En efecto, denotemos, como en la prueba del Teorema II.1.2, $K_i := K(\alpha_1, \ldots, \alpha_i)$ para $1 \leq i \leq n$, de modo que $L_f = K_n$, y veamos, por inducción sobre n, que $[L_f : K] \leq n!$. Si $n = 1$, entonces $L_f = K$, luego $[L_f : K] = 1$. Supongamos el resultado cierto para polinomios de grado $n-1$ y probemos que también lo es para polinomios de grado n.

Como $f(\alpha_1) = 0$ existe, por la Regla de Ruffini, un polinomio $g \in K_1[\mathtt{t}]$ de grado $n-1$ tal que $f(\mathtt{t}) := (\mathtt{t} - \alpha_1)g(\mathtt{t})$. Por tanto g factoriza en $L_f[\mathtt{t}]$ como producto

$$g(\mathtt{t}) := a_n(\mathtt{t} - \alpha_2) \cdots (\mathtt{t} - \alpha_n),$$

luego $L_g := K_1(\alpha_2, \ldots, \alpha_n)$ es un cuerpo de descomposición de g sobre K_1. Además,

$$[L_f : K] = [L_g : K_1] \cdot [K_1 : K].$$

Como $[K_1 : K] = \deg(P_{K,\alpha_1}) \leq \deg(f) = n$ y, por la hipótesis de inducción, el grado $[L_g : K_1]$ de la extensión $L_g|K_1$ es menor o igual que $(n-1)!$,

$$[L_f : K] = [L_g : K_1] \cdot [K_1 : K] \leq (n-1)! \cdot n = n!$$

(4) Si f es reducible en $K[\mathtt{t}]$, entonces $[L_f : K] < n!$. En efecto, escribimos $f := f_1 f_2$ donde $f_1, f_2 \in K[\mathtt{t}]$ son polinomios de grados $r, s \geq 1$. Sean $L_1|K$

y $L_2|K$ cuerpos de descomposición de f_1 y f_2 sobre K. Si $\alpha_1, \ldots, \alpha_r \in L_1$ y $\beta_1, \ldots, \beta_s \in L_2$ son, respectivamente, las raíces de f_1 y f_2 en L_1 y L_2, tenemos

$$L_1 := K(\alpha_1, \ldots, \alpha_r), \quad L_2 := K(\beta_1, \ldots, \beta_s) \quad \& \\ L_f := K(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s).$$

Nótese que $L_1(\beta_1, \ldots, \beta_s)$ es un cuerpo de descomposición de f_2 sobre L_1. Entonces, por el apartado (3),

$$[L_f : K] = [L_f : L_1] \cdot [L_1 : K] = [L_1(\beta_1, \ldots, \beta_s) : L_1] \cdot [L_1 : K] \\ \leq s! \cdot r! < (r+s)! = n!.$$

Debemos justificar la desigualdad $s! \cdot r! < (r+s)!$ que acabamos de emplear. Ahora bien,

$$r! \cdot s! = r! \cdot 1 \cdot 2 \cdots s < r! \cdot (r+1) \cdot (r+2) \cdots (r+s) = (r+s)!$$

(5) Dada una familia finita de polinomios $f_1, \ldots, f_r \in K[\mathtt{t}]$ existe una extensión esencialmente única $L|K$ de modo que cada f_i factoriza en $L[\mathtt{t}]$ en producto de factores de grado 1 y es "minimal" entre dichas extensiones; basta tomar como L un cuerpo de descomposición sobre K del producto $f := f_1 \cdots f_r$.

(6) La observación (2) deja de ser cierta si $\mathrm{char}(K) \neq 0$, lo que tiene importantes consecuencias. Por ejemplo, la prueba del Teorema del elemento primitivo II.2.2 en el caso en que $\mathrm{char}(K) = 0$ no se extiende a característica p, y de hecho se muestra en el Ejercicio III.7 una extensión finita y no simple de cuerpos de característica p.

Esto da lugar a la introducción del concepto de *separabilidad*. Se dice que un polinomio irreducible $f \in K[\mathtt{t}]$ es *separable* si tiene tantas raíces distintas en un cuerpo de descomposición sobre K como grado. Dada una extensión $L|K$ se dice que un elemento $a \in L$ es *separable sobre* K si es algebraico sobre K y su polinomio mínimo sobre K es *separable*. Una extensión $L|K$ es *separable* si los elementos de L algebraicos sobre K son separables sobre K.

Con esta terminología, se deduce de (2) que las extensiones de un cuerpo de característica 0 son separables. Se puede desarrollar toda una teoría acerca de las extensiones que son separables y las que no lo son, pero hemos decidido no hacerlo en este texto buscando una mayor simplicidad en la exposición.

Ejemplos II.1.4 (1) Si $L|K$ es una extensión de grado 2, entonces existe un polinomio $f \in K[\mathtt{t}]$ tal que L es un cuerpo de descomposición de f sobre K.

En efecto, como $[L : K] \neq 1$ existe $a \in L \setminus K$, y vamos a probar que L es un cuerpo de descomposición sobre K del polinomio mínimo $f := P_{K,a}$ de a sobre K. Comprobemos primero que $L = K(a)$. Nótese que $K \subsetneq K(a) \subset L$ y, por la transitividad del grado,

$$2 = [L : K] = [L : K(a)] \cdot [K(a) : K],$$

y como $[K(a) : K] > 1$ se deduce que $[K(a) : K] = 2$ y $[L : K(a)] = 1$, es decir, $L = K(a)$. En consecuencia, es suficiente demostrar que f factoriza en $K(a)[\mathtt{t}]$ como producto de factores de grado 1. Esto es inmediato, ya que si b es otra raíz de f en un cuerpo de descomposición de f sobre K, se tiene

$$f(\mathtt{t}) = (\mathtt{t} - a)(\mathtt{t} - b) = \mathtt{t}^2 - (a + b)\mathtt{t} + ab \in K[\mathtt{t}],$$

luego $a+b \in K \subset K(a)$, así que $b \in K(a)$, por lo que f es producto de factores de grado 1 en $K(a)[\mathtt{t}]$.

(2) Sea p un número primo. Vamos a calcular generadores de un cuerpo de descomposición L_f sobre $\mathbb{Q}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^4 - p$. Como $\mathbb{C}$ es algebraicamente cerrado, f factoriza en $\mathbb{C}[\mathtt{t}]$ como producto de factores de grado 1, y para hallarlos buscamos las raíces de f en $\mathbb{C}$. Una de ellas es $\rho := \sqrt[4]{p}$, el único número real positivo cuya potencia cuarta es p. Si η es otra raíz de f en $\mathbb{C}$ se tiene $\rho^4 = p = \eta^4$, luego $(\eta/\rho)^4 = 1$, así que existe $k \in \mathbb{Z}$ tal que $\eta/\rho = i^k$, donde $i := \sqrt{-1}$. Como $i^4 = 1$ las raíces de f en $\mathbb{C}$ son $\{\rho, \rho i, -\rho, -\rho i\}$. Así,

$$f(\mathtt{t}) = (\mathtt{t} - \rho) \cdot (\mathtt{t} + \rho) \cdot (\mathtt{t} - \rho i) \cdot (\mathtt{t} + \rho i),$$

y en consecuencia $L_f = \mathbb{Q}(\rho, \rho i, -\rho, -\rho i) = \mathbb{Q}(\rho, i)$.

1.a. Cierre algebraico de un cuerpo En VII.2.6 vol. II se introdujo la noción de cuerpo algebraicamente cerrado. El objetivo en lo que queda de sección es estudiar detalladamente este concepto y probar que cada cuerpo K admite un *cierre algebraico* esencialmente único, o sea, un cuerpo algebraicamente cerrado L de modo que la extensión $L|K$ es algebraica.

Definición y Proposición II.1.5 Se dice que un cuerpo E es *algebraicamente cerrado* si cumple alguna de las siguientes condiciones equivalentes, y por tanto todas.

(1) *Todo polinomio $f \in E[\mathtt{t}]$ de grado ≥ 1 factoriza en $E[\mathtt{t}]$ como producto de factores de grado* 1.

(2) *Todo polinomio $f \in E[\mathtt{t}]$ de grado ≥ 1 tiene alguna raíz en E.*

(3) *Existe un subcuerpo $K \subset E$ tal que la extensión $E|K$ es algebraica y cada $f \in K[\mathtt{t}]$ de grado ≥ 1 factoriza en $E[\mathtt{t}]$ como producto de factores de grado* 1.

(4) *El cuerpo E no admite extensiones algebraicas no triviales.*

Demostración. La implicación (1) $\Longrightarrow$ (2) es trivial y para (2) $\Longrightarrow$ (3) basta elegir $K := E$.

(3) $\Longrightarrow$ (4) Sea $L|E$ una extensión algebraica. Como $E|K$ también lo es se sigue de la Proposición I.2.7 que la extensión $L|K$ es algebraica. Para cada $\alpha \in L$ su polinomio mínimo $P_{K,\alpha} \in K[\mathtt{t}]$ sobre K factoriza en $E[\mathtt{t}]$ como producto de factores de grado 1, uno de los cuales es, por la Regla de Ruffini, $\mathtt{t} - \alpha$. En particular $\alpha \in E$ y por ello $E = L$.

(4) $\Longrightarrow$ (1) Dado $f \in E[\mathtt{t}]$ con $\deg(f) \geq 1$ existe, por II.1.2, una extensión algebraica $L|E$ tal que f factoriza en $L[\mathtt{t}]$ como producto de factores de grado 1. Por hipótesis, $L = E$, luego f factoriza como producto de factores de grado 1 en $E[\mathtt{t}]$. □

Ejemplos II.1.6 (1) El cuerpo $\mathbb{C}$ de los números complejos es, por el Teorema Fundamental del Álgebra, V.2.13, Vol. II, un cuerpo algebraicamente cerrado, pues cumple la condición (2) en la Proposición anterior.

(2) Vimos en el Corolario I.2.5 que

$$\overline{\mathbb{Q}}_{\mathbb{C}} := \{a \in \mathbb{C} : \ a \text{ es algebraico sobre } \mathbb{Q}\}$$

es un cuerpo y que la extensión $\overline{\mathbb{Q}}_{\mathbb{C}}|\mathbb{Q}$ es algebraica. De hecho $\overline{\mathbb{Q}}_{\mathbb{C}}$ es un cuerpo algebraicamente cerrado porque cumple la condición (3) en la Proposición II.1.5. En efecto, para cada $f \in \mathbb{Q}[\mathtt{t}]$ de grado ≥ 1 existen, por el Teorema Fundamental del Álgebra, $a \in \mathbb{Q}$ y $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ tales que

$$f(\mathtt{t}) = a \prod_{i=1}^{n} (\mathtt{t} - \alpha_i).$$

Como $f \in \mathbb{Q}[\mathtt{t}]$ cada α_i es algbraico sobre $\mathbb{Q}$, luego pertenece a $\overline{\mathbb{Q}}_{\mathbb{C}}$, es decir, cada factor $\mathtt{t} - \alpha_i \in \overline{\mathbb{Q}}_{\mathbb{C}}[\mathtt{t}]$.

Definiciones y Observaciones II.1.7 (1) Ya se puede formular con precisión el problema central en lo que queda de sección. Dado un cuerpo K queremos construir una extensión algebraica $L|K$ tal que L sea algebraicamente

cerrado. Se dice entonces que L es un *cierre algebraico* de K. La solución consiste en adjuntar a K las raíces de todos los polinomios de $K[\mathtt{t}]$. Vimos en II.1.3 (5) cómo hacerlo para un conjunto finito de polinomios.

(2) Necesitamos varias nociones acerca de conjuntos ordenados. Algunas, incluido el Lema de Zorn, se introdujeron en I.2.2, vol. II. Este resultado es equivalente al Principio de buena ordenación de Zermelo, que afirma que todo conjunto no vacío admite un buen orden, esto es, un orden respecto del cual todos sus subconjuntos no vacíos poseen elemento mínimo.

(3) Sean $(I, \leq)$ un conjunto ordenado y $a \in I$. Se definen los conjuntos de *predecesores* y *sucesores* de a en I, respectivamente, como

$$\mathcal{P}(a) := \{x \in I : \ x < a\} \quad \& \quad \mathcal{S}(a) := \{x \in I : \ x > a\}.$$

(4) Dado un conjunto bien ordenado $(I, \leq)$, denotaremos $0 := \min I$. Si $a \in I$ y $\mathcal{S}(a)$ es no vacío, entonces tiene mínimo, que se denota $a + 1 := \min \mathcal{S}(a)$. Diremos que un elemento $b \in I$ es de tipo *sucesor* si existe $a \in I$ tal que $b := a + 1$. Este a es único, pues es el máximo de $\mathcal{P}(b)$. Diremos que a es de tipo *límite* si no es de tipo sucesor. Por ejemplo, $0 \in I$ es de tipo límite y, si I tiene más de un elemento, $1 = 0 + 1 \in I$ es de tipo sucesor.

Teorema II.1.8 (Inducción transfinita) (1) *Sean $(I, \leq)$ un conjunto bien ordenado y $J \subset I$ un subconjunto no vacío tal que para cada $a \in I$ con $\mathcal{P}(a) \subset J$ se cumple que $a \in J$. Entonces, $I = J$.*

(2) *Sean $(I, \leq)$ un conjunto bien ordenado y $J \subset I$ un subconjunto no vacío que cumple las siguientes dos propiedades.*

(2.1) *Si $a \in I$ es de tipo límite y $\mathcal{P}(a) \subset J$, entonces $a \in J$.*

(2.2) *Si $a := b + 1 \in I$ es de tipo sucesor y $b \in J$, entonces $a \in J$.*

Entonces $I = J$.

Demostración. (1) Si $I \neq J$ el conjunto $X := I \setminus J$ no es vacío, luego existe $a := \min(X)$, pues $(I, \leq)$ está bien ordenado. En consecuencia $\mathcal{P}(a) \subset J$, pues si $x < a$ necesariamente $x \notin X$, así que $x \in J$. La hipótesis implica que $a \in J$, y esto es una contradicción, luego $I = J$.

(2) Supongamos de nuevo que $I \neq J$, o sea, $X := I \setminus J \neq \varnothing$. Como $(I, \leq)$ está bien ordenado existe $a := \min(X)$. Si a es de tipo límite, $\mathcal{P}(a) \subset J$ por ser $a = \min(X)$, lo que implica, por (2.1), que $a \in J$, que es una contradicción, luego $I = J$. Si a es de tipo sucesor, existe $b \in I$ tal que $a = b + 1$. Como $b < a$

resulta que $b \notin X$, o sea, $b \in J$ y, por la condición (2.2), también $a \in J$, que es una contradicción. □

Teorema II.1.9 (Existencia de cierre algebraico) *Todo cuerpo K admite un cierre algebraico.*

Demostración. Sea $\mathcal{S} := \{f \in K[\mathtt{t}] : \deg(f) \geq 1\} = \{f_i\}_{i\in I}$. Por el Principio de buena ordenación de Zermelo existe un orden $\leq$ en I de modo que $(I, \leq)$ es un conjunto bien ordenado. Sea ∞ un elemento no perteneciente a I y consideramos $I^* := I \cup \{\infty\}$ y extendemos el orden $\leq$ a I^*, definiendo $i < \infty$ para cada $i \in I$. Es decir, hemos añadido un último elemento a I. Probaremos, mediante el Principio de inducción transfinita II.1.8, que para cada $j \in I^*$ existe un cuerpo K_j que satisface las siguientes propiedades.

(1) Si $i < j$ entonces $K_i \subset K_j$.

(2) Para cada $i < j$ el polinomio f_i factoriza en $K_j[\mathtt{t}]$ en producto de factores de grado 1.

(3) La extensión $K_j|K$ es algebraica.

Todo consiste en demostrar la igualdad $J = I^*$, donde

$$J := \{\ell \in I^* : \ \exists\ K_\ell \text{ cumpliendo (1), (2) \& (3)}\}.$$

Para ello basta probar, por el Principio de inducción transfinita, que se cumplen las condiciones (2.1) y (2.2) de II.1.8. En primer lugar, $J \neq \varnothing$, ya que $0 \in J$ sin más que tomar $K_0 := K$. Sea $j \in I^*$ y distinguimos los dos casos que corresponden a las condiciones (2.1) y (2.2) de II.1.8. En el primero de ellos j es de tipo límite y $\mathcal{P}(j) := \{i \in I : \ i < j\} \subset J$. Hemos de probar que $j \in J$, para lo que definimos $K_j := \bigcup_{i\in\mathcal{P}(j)} K_i$, que es un cuerpo como consecuencia de la Proposición I.1.9 (1) y el hecho de que el conjunto I^* está totalmente ordenado. Además, K_j cumple las condiciones (1), (2) y (3), con lo que $i \in J$.

En efecto, la condición (1) se cumple por la definición de K_j. Para (2), dado $i < j$, y puesto que j es de tipo límite, el sucesor $i+1$ de i es menor que j, esto es, $i + 1 \in \mathcal{P}(j) \subset J$, por lo que $K_{i+1} \subset K_j$. Como $i < i + 1 \in J$, el polinomio f_i factoriza en $K_{i+1}[\mathtt{t}]$ en producto de factores de grado 1, lo que implica que también lo hace en $K_j[\mathtt{t}]$. Por último, la extensión $K_j|K$ es algebraica, por serlo $K_i|K$ para cada $i \in \mathcal{P}(i) \subset J$.

Supongamos ahora que $j := \ell + 1$ es de tipo sucesor para cierto $\ell \in J$, y comprobemos que también en este caso $j \in J$. Por el Teorema II.1.2, existe una

extensión algebraica $K_{\ell+1}|K_\ell$ de modo que f_ℓ factoriza en $K_{\ell+1}[\mathtt{t}]$ en producto de factores de grado 1. Veamos que $K_j = K_{\ell+1}$ cumple las condiciones (1), (2) y (3), con lo que $j \in J$. En efecto, si $i < j = \ell + 1$, entonces $i \leq \ell$ y, como $\ell \in J$, se tiene $K_i \subset K_\ell \subset K_j$.

Para comprobar (2), sea $i < j$, así que $i \leq \ell$. Si $i = \ell$, el polinomio $f_i = f_\ell$ factoriza en producto de factores de grado 1 en $K_j[\mathtt{t}]$, por la definición de K_j. Por otro lado, si $i < \ell \in J$, entonces f_i factoriza en producto de factores de grado 1 en $K_\ell[\mathtt{t}] \subset K_j[\mathtt{t}]$. Por último la algebricidad de la extensión $K_j|K$ se deduce de la Proposición I.2.7, ya que $K_j|K_\ell$ y $K_\ell|K$ son extensiones algebraicas.

Una vez probada la igualdad $J = I^*$, veamos que $K_\infty = \bigcup_{j\in I^*} K_j$ es un cierre algebraico de K. Hay que probar que K_∞ es un cuerpo, que la extensión $K_\infty|K$ es algebraica y que K_∞ es algebraicamente cerrado. Por la Proposición I.1.8 (1), K_∞ es un cuerpo, y la extensión $K_\infty|K$ es algebraica por serlo cada $K_j|K$ con $j \in I^*$. Por último, que K_∞ es algebraicamente cerrado se sigue de la Proposición II.1.5, pues cada $f_j \in K[\mathtt{t}]$ de grado ≥ 1 factoriza en $K_{j+1}[\mathtt{t}]$, luego en $K_\infty[\mathtt{t}]$, en producto de factores de grado 1. □

Antes de demostrar que el cierre algebraico de un cuerpo es esencialmente único necesitamos el siguiente lema.

Lema II.1.10 *Sea $\mathtt{j} : K_1 \to K_2$ un homomorfismo de cuerpos de modo que K_2 es algebraicamente cerrado, y sea $L|K_1$ una extensión algebraica. Entonces, existe un homomorfismo $\psi : L \to K_2$ tal que $\psi|_{K_1} = \mathtt{j}$.*

Demostración. Sea Σ el conjunto de todos los pares (F, φ), donde $F|K_1$ es una subextensión de $L|K_1$ y $\varphi : F \to K_2$ es un homomorfismo tal que $\varphi|_{K_1} = \mathtt{j}$. El conjunto Σ es no vacío ya que el par $(K_1, \mathtt{j}) \in \Sigma$, y definimos en Σ el orden:

$$(F_1, \varphi_1) \preceq (F_2, \varphi_2) \text{ si } F_1 \subset F_2 \quad \& \quad \varphi_2|_{F_1} = \varphi_1.$$

Vamos a probar que Σ admite algún elemento maximal respecto de este orden, para lo que basta comprobar que satisface la hipótesis del Lema de Zorn, es decir, que toda cadena $\mathcal{C} := \{(F_i, \varphi_i)\}_{i\in I}$ en Σ está acotada superiormente. Para encontrar dicha cota observamos que, como consecuencia de la Proposición I.1.9 (1), la unión $F := \bigcup_{i\in I} F_i$ es un cuerpo y $F|K$ es subextensión de $L|K$ por serlo cada $K_i|K$. Además la aplicación

$$\varphi : F \to K_2, \ x \mapsto \varphi_i(x) \quad \text{si } x \in F_i$$

está bien definida, porque si $x \in F_i \cap F_j$ podemos suponer, por ser $\mathcal{C}$ una cadena, que $(F_i, \varphi_i) \preceq (F_j, \varphi_j)$, y así $\varphi_i(x) = \varphi_j(x)$. De hecho φ es homomorfismo, pues dados $x, y \in F$ existen $i, j \in I$ tales que $x \in F_i$ e $y \in F_j$ y, puesto que $\mathcal{C}$ es una cadena, podemos suponer que $(F_i, \varphi_i) \preceq (F_j, \varphi_j)$. Por tanto,

$$\varphi(x+y) = \varphi_j(x+y) = \varphi_j(x) + \varphi_j(y) = \varphi(x) + \varphi(y) \quad \&$$
$$\varphi(xy) = \varphi_j(xy) = \varphi_j(x)\varphi_j(y) = \varphi(x)\varphi(y).$$

Nótese que $\varphi|_{K_1} = \mathtt{j}$, luego el par $(F, \varphi) \in \Sigma$ y, $(F_i, \varphi_i) \preceq (F, \varphi)$ para cada $i \in I$, luego $(F, \varphi) \in \Sigma$ es cota superior de $\mathcal{C}$. Por el lema de Zorn, Σ tiene un elemento maximal (E, ψ), y basta probar que $E = L$. Desde luego $E|K_1$ es subextensión de $L|K_1$, y si $E \subsetneq L$ existe $\alpha \in L \setminus E$. Este elemento es algebraico sobre K_1, y si denotamos

$$f_1(\mathtt{t}) := P_{K_1,\alpha} = \mathtt{t}^m + \sum_{k=1}^{m-1} a_k \mathtt{t}^k$$

definimos $f_2(\mathtt{t}) := \mathtt{t}^m + \sum_{k=0}^{m-1} \mathtt{j}(a_k)\mathtt{t}^k \in K_2[\mathtt{t}]$, que tiene alguna raíz $\beta \in K_2$ por ser este cuerpo algebraicamente cerrado. Entonces, por el Lema II.1.1, existe un homomorfismo $\widehat{\psi} : E(\alpha) \to K_2$ tal que $\widehat{\psi}(\alpha) = \beta$ y $\widehat{\psi}|_E = \psi$, luego $(E(\alpha), \widehat{\psi}) \in \Sigma$ y $(E, \psi) \prec (E(\alpha), \widehat{\psi})$, contra la maximalidad de (E, ψ) en Σ. Por tanto, $L = E$, como queríamos. □

Teorema II.1.11 (Unicidad del cierre algebraico) *Sean K un cuerpo y $(K, \mathtt{j}_1, L_1)$ y $(K, \mathtt{j}_2, L_2)$ dos cierres algebraicos de K. Entonces, existe un isomorfismo $\varphi : L_1 \to L_2$ tal que $\mathtt{j}_2 = \varphi \circ \mathtt{j}_1$.*

Demostración. Como la extensión $L_1|K$ es algebraica y $\mathtt{j}_2 : K \to L_2$ es un homomorfismo existe, por el Lema anterior II.1.10, y por ser L_2 algebraicamente cerrado, un homomorfismo $\varphi : L_1 \to L_2$ tal que $\varphi \circ \mathtt{j}_1 = \mathtt{j}_2$. En particular, $L_1 \cong \varphi(L_1) \subset L_2$. Como L_1 es algebraicamente cerrado, también lo es $\varphi(L_1)$, que contiene a K. Como la extensión $L_2|K$ es algebraica, también lo es $L_2|\varphi(L_1)$ luego, por la Proposición II.1.5, $\varphi(L_1) = L_2$. Así, $\varphi : L_1 \to L_2$ es un isomorfismo que cumple $\mathtt{j}_2 = \varphi \circ \mathtt{j}_1$. □

Observaciones II.1.12 Sea L un cierre algebraico de un cuerpo K.

(1) Toda extensión algebraica $E|K$ es una subextensión de $L|K$. En efecto, podemos suponer que $K \subset E$ y $K \subset L$ y así, por el Lema II.1.10, el homomorfismo inclusión $\mathtt{j}_1 : K \hookrightarrow L$ se extiende a un homomorfismo $\varphi : E \to L$ tal que $\varphi|_K = \mathtt{j}_1$, es decir, $\varphi \circ \mathtt{j}_2 = \mathtt{j}_1$, donde $\mathtt{j}_2 : K \hookrightarrow E$ es la inclusión.

(2) Sea $F|K$ una extensión, de modo que F es algebraicamente cerrado. Entonces $L|K$ es una subextensión de $F|K$. En efecto, podemos suponer que $K \subset L$ y $K \subset F$. Como la extensión $L|K$ es algebraica, la inclusión $\mathtt{j}_1 : K \hookrightarrow F$ se extiende a un homomorfismo $\varphi : L \to F$ tal que $\varphi|_K = \mathtt{j}_1$, es decir, $\varphi \circ \mathtt{j}_2 = \mathtt{j}_1$, donde $\mathtt{j}_2 : K \hookrightarrow L$ es la inclusión.

(3) Si L_1 es un cuerpo algebraicamente cerrado que contiene a L, entonces L es el cierre algebraico $\overline{K}_{L_1}$ de K en L_1, (véase el Corolario I.2.5). En efecto, vimos en el Corolario I.2.5 que $\overline{K}_{L_1}$ es un cuerpo y, como la extensión $\overline{K}_{L_1}|K$ es algebraica, se deduce de (1) que $\overline{K}_{L_1} \subset L$. Recíprocamente, todos los elementos de L son algebraicos sobre K, por lo que $L \subset \overline{K}_{L_1}$, así que $L = \overline{K}_{L_1}$.

(4) Se desprende de los Ejemplos II.1.6 que $\mathbb{C}$ es un cierre algebraico de $\mathbb{R}$ y que $\overline{\mathbb{Q}}_{\mathbb{C}}$ es un cierre algebraico de $\mathbb{Q}$, llamado *cuerpo de los números algebraicos.*

(5) No demostraremos que un cierre algebraico del cuerpo de fracciones del anillo de series formales en una variable con coeficientes en $\mathbb{C}$ es el cuerpo $\mathbb{C}((\mathtt{t}^*)) := \bigcup_{n\geq 2} \mathbb{C}((\mathtt{t}^{1/n}))$ de series de Puiseux, donde para cada $n \geq 2$

$$\mathbb{C}((\mathtt{t}^{1/n})) := \{g(\mathtt{t}^{1/n}) : g \in \mathbb{C}((\mathtt{t}))\}.$$

2. Extensiones finitas simples

Nuestro objetivo fundamental en esta sección es demostrar el Teorema del elemento primitivo II.2.2, que afirma que toda extensión finita de cuerpos de característica 0 es simple. Antes de ello necesitamos un resultado auxiliar.

Lema II.2.1 *Sean K un cuerpo y $f, g \in K[\mathtt{t}]$. Entonces, f y g comparten un factor irreducible en $K[\mathtt{t}]$ si y sólo si existe una extensión de K en la que f y g comparten alguna raíz. En tal caso, las raíces comunes de f y g en un cuerpo de descomposición L de fg sobre K son las raíces en L de $h := \mathrm{mcd}(f, g)$.*

Demostración. Supongamos que f y g comparten un factor irreducible h en $K[\mathtt{t}]$. Como $\deg(h) \geq 1$ existe, por el Teorema II.1.2, una extensión $L_h|K$ de modo que h factoriza en $L_h[\mathtt{t}]$ como producto de factores de grado 1. En particular, existe $\beta \in L_h$ tal que $h(\beta) = 0$, y como h divide a f y a g resulta que $f(\beta) = 0$ y $g(\beta) = 0$.

Supongamos, recíprocamente, que existen una extensión $L|K$ y $\beta \in L$ con $f(\beta) = g(\beta) = 0$. Entonces, el polinomio mínimo $P_{K,\beta}$ de β sobre K divide a f y a g, por lo que f y g comparten un factor irreducible en $K[\mathtt{t}]$.

Por último, sea L un cuerpo de descomposición de fg sobre K. Tanto f como g factorizan en $L[\mathtt{t}]$ como producto de factores de grado 1, y para acabar basta ver que las raíces de $h := \mathrm{mcd}(f, g)$ en L son las raíces comunes en L de f y g. Desde luego las raíces de h lo son de f y de g, mientras que, por la Identidad de Bezout, existen $f_1, g_1 \in K[\mathtt{t}]$ tales que $h = ff_1 + gg_1$, y si $f(a) = g(a) = 0$ para un $a \in L$, entonces $h(a) = 0$. □

Nuestro siguiente objetivo es enunciar y demostrar el Teorema del elemento primitivo, uno de los más importantes en la teoría elemental de cuerpos.

Teorema II.2.2 (Elemento primitivo) *Sean K un cuerpo de característica 0 y $L|K$ una extensión finita. Entonces existe $\theta \in L$ tal que $L = K(\theta)$.*

Demostración. Como la extensión $L|K$ es finita es, por I.1.10 (1) finitamente generada, luego existen $a_1, \ldots, a_n \in L$ tales $L := K(a_1, \ldots, a_n)$. Además, por I.2.2 (8), cada a_i es algebraico sobre K. Todo se reduce a demostrar que existe $\lambda \in K$ tal que

$$K(a_1, a_2) = K(a_1 + \lambda a_2). \tag{2.1}$$

Supongamos (2.1) ya probado. Argumentando por inducción sobre n, se deduce que existen $\lambda_2, \ldots, \lambda_{n-1} \in K$ tales que

$$K_1 := K(a_1, \ldots, a_{n-1}) = K(a_1 + \lambda_2 a_2 + \cdots + \lambda_{n-1} a_{n-1})$$

y, utilizando (2.1) de nuevo, existe $\lambda_n \in K$ tal que

$$\begin{aligned} L = K(a_1, \ldots, a_n) = K_1(a_n) &= K(a_1 + \lambda_2 a_2 + \cdots + \lambda_{n-1} a_{n-1}, a_n) \\ &= K(a_1 + \lambda_2 a_2 + \cdots + \lambda_{n-1} a_{n-1} + \lambda_n a_n), \end{aligned}$$

y tomando $\theta := a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n$ resulta finalmente $L = K(\theta)$.

Demostramos (2.1). Basta probar que existe $\lambda \in K$ tal que $a_2 \in K(a_1 + \lambda a_2)$, ya que entonces también $a_1 = (a_1 + \lambda a_2) - \lambda a_2 \in K(a_1 + \lambda a_2)$, y por tanto,

$$K(a_1 + \lambda a_2) \subset K(a_1, a_2) \subset K(a_1 + \lambda a_2),$$

de donde se desprende la igualdad (2.1). Sea $f_i := P_{K,a_i} \in K[\mathtt{t}]$ el polinomio mínimo de a_i sobre K para $i = 1, 2$. Por la Observación II.1.3 (2) f_2 no tiene raíces múltiples, luego por el Teorema II.1.2, existen una extensión $L_2|K$ y $a_2 := \beta_1, \beta_2, \ldots, \beta_r \in L_2$ tales que

$$f_2(\mathtt{t}) = (\mathtt{t} - \beta_1) \cdots (\mathtt{t} - \beta_r) \quad \& \quad \beta_i \neq \beta_j \ \text{ si } \ i \neq j.$$

Basta ver que existe $\lambda \in K$ tal que $\mathtt{t} - a_2 \in K(a_1 + \lambda a_2)[\mathtt{t}]$, pues esto implica que $a_2 \in K(a_1 + \lambda a_2)$. Para ello demostraremos que existe $\lambda \in K$ tal que, si denotamos $K_\lambda := K(a_1 + \lambda a_2)$ y $h_\lambda(\mathtt{t}) := f_1(a_1 + \lambda(a_2 - \mathtt{t})) \in K_\lambda[\mathtt{t}]$, se tiene

$$\mathrm{mcd}_{K_\lambda[\mathtt{t}]}(f_2, h_\lambda) = \mathtt{t} - a_2. \tag{2.2}$$

Para probar (2.2) basta, por el Lema II.2.1, ver que existe $\lambda \in K$ tal que la única raíz común de los polinomios f_2 y h_λ en un cuerpo de descomposición L_3 de $f_2 h_\lambda$ sobre L_2 es a_2. Nótese que a_2 es raíz de h_λ para cada $\lambda \in K$, pues

$$h_\lambda(a_2) = f_1(a_1 + \lambda(a_2 - a_2)) = f_1(a_1) = 0.$$

Todas las raíces de f_2 en L_3 pertenecen a L_2, y son $a_2 = \beta_1, \beta_2, \ldots, \beta_r$. Además se cumple que $\beta_i \neq \beta_1 = a_2$ para $i = 2, \ldots, r$. Ahora bien, β_i es raíz de h_λ si y sólo si $a_1 + \lambda(a_2 - \beta_i)$ es raíz de f_1 en L_2. Como f_1 es un polinomio no nulo y L_2 es un cuerpo, f_1 tiene una cantidad finita de raíces en L_2 digamos $\zeta_1, \ldots, \zeta_s$. Consideramos el conjunto finito

$$\mathcal{S} := \big\{(\zeta_j - a_1)/(a_2 - \beta_i) : \ 2 \leq i \leq r, \ 1 \leq j \leq s\big\},$$

que a lo sumo tiene $(r-1)s$ elementos. Como $\mathrm{char}(K) = 0$ contiene a $\mathbb{Q}$ y, por tanto, es un conjunto infinito. De este modo, existe $\lambda \in K \setminus \mathcal{S}$ y para este λ se cumple que la única raíz común de f_2 y h_λ en L_3 es a_2. □

Ejemplo II.2.3 Hemos probado en el Ejemplo II.1.4 que $L_f := \mathbb{Q}(\rho, i)$ es un cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^4 - p$, donde p es un número primo y $\rho := \sqrt[4]{p}$ es el único número real positivo cuya potencia cuarta es p. Vamos a demostrar que $\rho + i$ es un elemento primitivo de la extensión $L_f|\mathbb{Q}$, es decir, $L_f = \mathbb{Q}(\rho + i)$.

Según la demostración del Teorema del elemento primitivo, II.2.2, existe $\lambda \in \mathbb{Q}$ tal que $\theta := \rho + \lambda i$ es elemento primitivo de la extensión $L_f|\mathbb{Q}$, y se trata de comprobar que $\lambda := 1$ cumple lo requerido en dicha prueba. Con aquellas notaciones, los polinomios mínimos sobre $\mathbb{Q}$ de $a_1 := \rho$ y $a_2 := i$ son, respectivamente, $f_1 := f$ y $f_2(\mathtt{t}) := \mathtt{t}^2 + 1$. Las raíces de f_1 en $\mathbb{C}$ son $\zeta_1 := a_1$, $\zeta_2 := -a_1$, $\zeta_3 := a_1 i$ y $\zeta_4 := -a_1 i$, y las de f_2 son $\beta_1 := a_2$ y $\beta_2 := -a_2$. Con las notaciones de la prueba del Teorema del elemento primitivo,

$$\mathcal{S} = \big\{(\zeta_j - a_1)/(a_2 - \beta_2) : \ 1 \leq j \leq 4\big\} = \{0, \ \rho i, \ \rho(1+i)/2, \ \rho(-1+i)/2\}.$$

Por tanto, $\lambda := 1 \in \mathbb{Q} \setminus \mathcal{S}$, y se deduce de la prueba del Teorema del elemento primitivo que $\theta := a_1 + \lambda a_2 = \rho + i$ es elemento primitivo de la extensión $L_f|\mathbb{Q}$.

Por supuesto, existen muchos más elementos primitivos; de hecho hay una infinidad de ellos, todos los de la forma $\rho + \lambda i$ con $\lambda \in \mathbb{Q} \setminus \mathcal{S}$.

2.a. Caracterización de las subextensiones simples. Terminamos este capítulo caracterizando las extensiones algebraicas simples $L|K$ de cuerpos de característica 0, de la que se desprende que las subextensiones de una extensión algebraica simple $L|K$ son también simples. Antes presentamos un resultado auxiliar sin restricciones sobre la característica.

Lema II.2.4 *Sea $L|K$ una extensión de cuerpos que admite tan sólo una cantidad finita de subextensiones. Entonces $L|K$ es finitamente generada.*

Demostración. Existe algún subconjunto A de L tal que $L = K(A)$; por ejemplo $A = L$ y, por el Lema de Zorn, podemos escoger A minimal con esta propiedad. Entonces, dados $a, b \in A$ distintos, los cuerpos $K(a)$ y $K(b)$ son distintos, pues en caso contrario $B := A \setminus \{b\} \subsetneq A$ y $K(A) = K(B)$, contra la minimalidad de A. En consecuencia la aplicación

$$A \to \mathcal{F} = \{\text{subextensiones de } L|K\},\ a \mapsto K(a)|K$$

es inyectiva, y la finitud de $\mathcal{F}$ implica la de A. □

Teorema II.2.5 *Sea $L|K$ una extensión algebraica de cuerpos de característica 0. Entonces, $L|K$ es una extensión simple si y sólo si admite una cantidad finita de subextensiones.*

Demostración. Supongamos que la extensión $L|K$ es simple y algebraica. Así, existe $\theta \in L$ tal que $L := K[\theta]$, y denotamos $f := P_{K,\theta}$ el polinomio mínimo de θ sobre K. Este polinomio es irreducible en $K[\mathtt{t}]$ y, como $\mathrm{char}(K) = 0$, se deduce de la Observación II.1.3 (2) que las raíces de f en un cuerpo de descomposición E de f sobre L son simples. Por tanto f factoriza en $E[\mathtt{t}]$ como producto de r factores mónicos de grado 1 distintos. Esto implica que f tiene $2^r - 1$ divisores mónicos en $E[\mathtt{t}]$, tantos como subconjuntos no vacíos tiene un conjunto con r elementos. En particular, f tiene un número finito de divisores mónicos en $L[\mathtt{t}]$.

Sea $F|K$ una subextensión de $L|K$. Entonces $L = F[\theta]$ y consideramos el polinomio mínimo $g := P_{F,\theta}$ de θ sobre F. Es claro que

$$g(\mathtt{t}) := a_0 + a_1\mathtt{t} + \cdots + a_{s-1}\mathtt{t}^{s-1} + \mathtt{t}^s \in F[\mathtt{t}]$$

es un divisor mónico de f en $L[\mathtt{t}]$. Se cumple que $F_0 := K(a_0, a_1, \ldots, a_{s-1})$ es un subcuerpo de F y $g \in F_0[\mathtt{t}]$ es un polinomio irreducible que tiene a θ por

raíz. Así, $g = P_{F_0,\theta}$ y, como $L = F_0[\theta]$, resulta que $[L : F_0] = \deg(g) = [L : F]$, luego $F_0 = F$. Esto implica que $F = K(a_0, a_1, \ldots, a_{s-1})$ está completamente determinado por g, por lo que el número de subextensiones de $L|K$ es menor o igual que el de divisores mónicos de f en $L[\mathtt{t}]$, así que es finito.

Supongamos, recíprocamente, que la extensión $L|K$ admite una cantidad finita de subextensiones. Por el Lema II.2.4 la extensión $L|K$ es finitamente generada. Como $L|K$ es algebraica y finitamente generada es también finita, por I.2.3 (3), y se deduce del Teorema del elemento primitivo II.2.2 que $L|K$ es simple. □

Corolario II.2.6 *Las subextensiones de una extensión algebraica simple $L|K$ de cuerpos de característica 0 son simples.*

Demostración. Sea $E|K$ una subextensión de $L|K$, que es algebraica por serlo $L|K$. Como ésta es simple se deduce del Teorema II.2.5 que el conjunto de subextensiones de $L|K$ es finito, por lo que también lo es el de subextensiones de $E|K$. Empleando el Teorema II.2.5 de nuevo concluimos que la extensión $E|K$ es simple. □

Ejercicios y problemas propuestos

Número II.1 Sean $f(\mathtt{t}) := \mathtt{t}^6 - 1$, $i := \sqrt{-1}$ y $\omega \neq 1$ tal que $\omega^3 = 1$. Hallar el grado de la extensión $L_f|L$, donde L_f denota un cuerpo de descomposición de f sobre cada uno de los siguientes cuerpos L: $\mathbb{Q}$, $\mathbb{Q}(i)$ y $\mathbb{Q}(\omega)$.

Número II.2 Probar que si L_f es un cuerpo de descomposición sobre K de un polinomio irreducible $f(\mathtt{t}) := \mathtt{t}^4 + a\mathtt{t}^2 + b \in K[\mathtt{t}]$, entonces existe una subextensión $E|K$ de $L_f|K$ tal que $[E : K] = 2$.

Número II.3 Sean K un cuerpo, $a \in K$ y m y n enteros positivos primos entre sí. Demostrar que el polinomio $f(\mathtt{t}) := \mathtt{t}^{mn} - a$ es irreducible en $K[\mathtt{t}]$ si y sólo si los polinomios $g(\mathtt{t}) := \mathtt{t}^m - a$ y $h(\mathtt{t}) := \mathtt{t}^n - a$ son irreducibles en $K[\mathtt{t}]$.

Número II.4 Sean K un cuerpo con $\mathrm{char}(K) \neq 2$ y $u, v \in K$ que no son un cuadrado en K. Sean $\sqrt{u}$ y $\sqrt{v}$ raíces del polinomio $f(\mathtt{t}) := (\mathtt{t}^2 - u)(\mathtt{t}^2 - v)$ en un cuerpo de descomposición L_f de f sobre K tales que $K(\sqrt{u}) \neq K(\sqrt{v})$. Probar que

$$K(\sqrt{u}, \sqrt{v}) = K(\sqrt{u} + \sqrt{v}) \quad \& \quad [K(\sqrt{u}, \sqrt{v}) : K] = 4.$$

Número II.5 Sean $p \in \mathbb{Z}$ un número primo y L_f un cuerpo de descomposición del polinomio $f(\mathtt{t}) := \mathtt{t}^p - 3$ sobre $\mathbb{Q}$. Calcular el grado $[L_f : \mathbb{Q}]$.

Número II.6 Probar que $u := \mathrm{tg}(2\pi/5)$ es un número algebraico sobre $\mathbb{Q}$ y encontrar su polinomio mínimo. ¿Es $\mathbb{Q}(u)$ un cuerpo de descomposición sobre $\mathbb{Q}$ de algún polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$?

Número II.7 (1) Sean $E|K$ una extensión de cuerpos de grado m y $f \in K[\mathtt{t}]$ un polinomio irreducible de grado n. Sean $d := \mathrm{mcd}(m, n)$ y $D := n/d$. Probar que el grado de cada factor irreducible de f en $E[\mathtt{t}]$ es múltiplo de D.

(2) Demostrar que para cada $k \in \mathbb{Z}$ el polinomio

$$f_k(\mathtt{t}) := \mathtt{t}^4 - 2\mathtt{t}^3 + 4\mathtt{t}^2 - 2\mathtt{t} + (4k + 2)$$

es irreducible en el anillo de polinomios $\mathbb{Q}(\sqrt{2})[\mathtt{t}]$.

Número II.8 Sean K un cuerpo en el que el polinomio $f(\mathtt{t}) := \mathtt{t}^2 + 1$ no tiene ninguna raíz, y denotemos i una raíz de f en un cierre algebraico de K. Supongamos que todo elemento de $K(i)$ es el cuadrado de un elemento de $K(i)$. Probar que toda suma de cuadrados en K es un cuadrado en K y calcular la característica de K.

Número II.9 Encontrar elementos primitivos de las subextensiones $L_f|\mathbb{Q}$ de $\mathbb{C}|\mathbb{Q}$, donde L_f es un cuerpo de descomposición de f sobre $\mathbb{Q}$, en los siguientes casos:

$$f(\mathtt{t}) := \mathtt{t}^9 - 1, \quad f(\mathtt{t}) := \mathtt{t}^4 + 5\mathtt{t}^2 + 6 \quad \& \quad f(\mathtt{t}) := \mathtt{t}^6 - 8.$$

Encontrar los grados de las extensiones $L_f|\mathbb{Q}$.

Número II.10 Hallar un elemento primitivo u de la extensión $L_f|\mathbb{Q}$, donde L_f es un cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^3 - 7$. Hallar el polinomio mínimo de u sobre $\mathbb{Q}$.

Número II.11 Sea $\alpha := 1/(\sqrt{2} + \sqrt[3]{3})$. Encontrar el polinomio mínimo de α sobre $\mathbb{Q}$. Escribir α como expresión polinómica en $\sqrt{2}$ y $\sqrt[3]{3}$ con coeficientes racionales.

Número II.12 Sea $L|K$ una extensión algebraica de cuerpos de característica 0. Supongamos que existe un entero positivo n tal que $[K(u) : K] \leq n$ para cada $u \in L$. Demostrar que la extensión $L|K$ es finita, de grado menor o igual que n.

Número II.13 Sean K un cuerpo y $f(\mathtt{t}) := \mathtt{t}^5 - a \in K[\mathtt{t}]$, donde $a \in K$ es un elemento no nulo.

(1) Demostrar que f posee cinco raíces distintas en un cierre algebraico $\overline{K}$ de K si y sólo si la característica de K es distinta de 5.

(2) Suponemos que $\mathrm{char}(K) \neq 5$. Demostrar que f es irreducible en $K[\mathtt{t}]$ si y sólo si a no es potencia quinta de un elemento de K.

Número II.14 Un cuerpo K es *real* si -1 no es suma de cuadrados de elementos de K.

(1) Demostrar que todo cuerpo real tiene característica cero.

(2) Sean K un cuerpo real y $L|K$ una extensión finita de grado impar. Probar que L es real.

Número II.15 Sean K un cuerpo, $a \in K \setminus \{0\}$, p un número primo y $f(\mathtt{t}) := \mathtt{t}^p - a$.

(1) Demostrar que si u es una raíz de f en un cierre algebraico $\overline{K}$ de K, toda raíz de f en $\overline{K}$ es de la forma ζu para cierto $\zeta \in \overline{K}$ tal que $\zeta^p = 1$.

(2) Demostrar que si f es reducible en $K[\mathtt{t}]$, entonces f tiene alguna raíz en K.

Número II.16 Calcular el polinomio mínimo de $a + b$ sobre $\mathbb{Q}$, donde

$$a := \sqrt[5]{2} \quad \& \quad b := \sqrt[3]{-7/2 - \sqrt{3981}/18} + \sqrt[3]{-7/2 + \sqrt{3981}/18}.$$

Número II.17 (1) Dado un primo $p \in \mathbb{Z}$, ¿cuál es el polinomio mínimo de $\sqrt[3]{p}$ sobre $\mathbb{Q}$?

(2) Demostrar que $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$.

(3) Calcular el grado de la extensión $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})|\mathbb{Q}$.

(4) Calcular el polinomio mínimo de $\sqrt[3]{2} + \sqrt[3]{3}$ sobre $\mathbb{Q}$.

Extensiones transcendentes

En la primera sección de este capítulo se prueba el Teorema de Lüroth, que afirma que toda subextensión de una extensión transcendente simple es también transcendente simple. En la segunda introducimos la noción de grado de transcendencia de una extensión y probamos el Teorema de Steinitz y la transitividad del grado de transcendencia. En el Apéndice B se prueba la existencia de infinitos números reales *transcendentes,* esto es, transcendentes sobre $\mathbb{Q}$, y algunos ejemplos: e, π y el número de ℓ de Liouville son transcendentes. El lector necesitará algunos resultados de dicho Apéndice para resolver los tres últimos ejercicios de este capítulo.

1. Teorema de Lüroth

Teorema III.1.1 (Lüroth) *Cada subextensión de una extensión transcendente simple es también transcendente simple.*

Demostración. Sean K un cuerpo y $L := K(\mathtt{t})$, donde $\mathtt{t}$ es una indeterminada sobre K. Veamos primero que para cada cuerpo intermedio $K \subsetneq F \subsetneq L$ la extensión $F|K$ es transcendente. De hecho vamos a comprobar que cada elemento $\alpha \in F \setminus K$ es transcendente sobre K. Sean $h_1, h_2 \in K[\mathtt{t}]$ polinomios no nulos tales que $\alpha = h_1/h_2$ donde $h_1, h_2 \in K[\mathtt{t}]$. Nótese que $h_2\alpha - h_1 = 0$, luego $\mathtt{t}$ es algebraico sobre $K(\alpha)$, y por tanto sobre F. Para verlo, si $h_1(\mathtt{t}) = \sum_{j=0}^{d} b_j \mathtt{t}^j$ y $h_2(\mathtt{t}) = \sum_{k=0}^{e} c_k \mathtt{t}^k$, donde $b_j, c_k \in K$, la igualdad $h_2\alpha - h_1 = 0$ significa que $\sum_{k=0}^{e} \alpha c_k \mathtt{t}^k - \sum_{j=0}^{d} b_j \mathtt{t}^j = 0$, o lo que es lo mismo, $\mathtt{t}$ es raíz del polinomio

$$h(\mathtt{x}) = \sum_{k=0}^{e} \alpha c_k \mathtt{x}^k - \sum_{j=0}^{d} b_j \mathtt{x}^j \in K(\alpha)[\mathtt{x}],$$

y basta probar que $h \neq 0$. En caso contrario $e = d$ y $\alpha c_d = b_d$, por lo que $\alpha = b_d/c_d \in K$, y esto es falso. Hemos visto que la extensión $K(\mathtt{t})|F$ es algebraica, y como $K(\mathtt{t})|K$ no lo es deducimos que $F|K$ es transcendente.

Demostremos ahora que $F|K$ es una extensión simple. Consideremos el polinomio mínimo $q := P_{F,\mathtt{t}} \in F[\mathtt{x}] \subset K(\mathtt{t})[\mathtt{x}]$ de $\mathtt{t}$ sobre F y sea $n := \deg(q)$. Puesto que $K[\mathtt{t}]$ es un DFU, existen $a_0, \ldots, a_n \in K[\mathtt{t}]$ tales que

$$a_n q(\mathtt{x}) = a_0 + a_1\mathtt{x} + \cdots + a_n\mathtt{x}^n \in K[\mathtt{t}][\mathtt{x}]$$

es un polinomio primitivo, VI.1.3, vol. II. Como $\mathtt{t}$ no es algebraico sobre K alguno de los coeficientes a_i/a_n de q no pertenece a K. Escogemos un índice $0 \le i \le n-1$ tal que $u := a_i/a_n \in F \setminus K$ y sean $f, g \in K[\mathtt{t}]$ polinomios primos entre sí tales que $u = f/g$. Ahora, si $r := \text{máx}\{\deg(f), \deg(g)\}$ tenemos que $g(\mathtt{x})u - f(\mathtt{x}) \in K(u)[\mathtt{x}]$ es un polinomio de grado $\le r$ del que $\mathtt{t}$ es raíz. Por tanto, la extensión $K(\mathtt{t})|K(u)$ es algebraica de grado $[K(\mathtt{t}) : K(u)] \le r$. Como $K(u) \subset F$ todo se reduce a demostrar que $[K(\mathtt{t}) : F] = n \ge r$, pues en tal caso, por la transitividad del grado,

$$r \ge [K(\mathtt{t}) : K(u)] = [K(\mathtt{t}) : F] \cdot [F : K(u)] = n \cdot [F : K(u)] \ge r \cdot [F : K(u)]$$

y, por tanto, $1 \le [F : K(u)] \le 1$. De este modo, $[F : K(u)] = 1$ con lo que $F = K(u)$, así que $F|K$ es una extensión simple.

Comprobemos pues que $r \le n$. En efecto, recordamos que $u = f(\mathtt{t})/g(\mathtt{t})$ y observemos que $\mathtt{t}$ es una raíz del polinomio

$$g(\mathtt{x})u - f(\mathtt{x}) \in K(u)[\mathtt{x}] \subset K(\mathtt{t})[\mathtt{x}].$$

Consideramos el polinomio en dos variables

$$\psi(\mathtt{t}, \mathtt{x}) := g(\mathtt{x})f(\mathtt{t}) - g(\mathtt{t})f(\mathtt{x}) \in K[\mathtt{t}][\mathtt{x}] = K[\mathtt{t}, \mathtt{x}] = K[\mathtt{x}][\mathtt{t}].$$

Obsérvese que $\deg_{\mathtt{t}}(\psi) \le \text{máx}\{\deg(f), \deg(g)\} = r$. Vamos a demostrar que de hecho $r = \deg_{\mathtt{x}}(\psi) = \deg_{\mathtt{t}}(\psi) = n$, con lo que concluirá la demostración.

En efecto, $q \in K(\mathtt{t})[\mathtt{x}]$ divide a ψ en $K(\mathtt{t})[\mathtt{x}]$ porque $\psi(\mathtt{t}, \mathtt{t}) = 0$. Como $a_n q \in K[\mathtt{t}][\mathtt{x}]$ es un polinomio primitivo y q divide a ψ en $K(\mathtt{t})[\mathtt{x}]$, se deduce que $a_n q$ divide a ψ en $K[\mathtt{t}, \mathtt{x}]$. Existe por tanto $p \in K[\mathtt{t}, \mathtt{x}]$ tal que $a_n q p = \psi$.

Como $a_i/a_n = u = f/g$, tenemos $f a_n = a_i g$, y al ser f y g primos entre sí, f divide a a_i y g divide a a_n. En particular,

$$\deg_{\mathtt{t}}(f) \le \deg_{\mathtt{t}}(a_i) \quad \& \quad \deg_{\mathtt{t}}(g) \le \deg_{\mathtt{t}}(a_n),$$

y esto implica que

$$\begin{aligned} \deg_{\mathtt{t}}(a_n q) &= \deg_{\mathtt{t}}(a_0 + a_1\mathtt{x} + \cdots + a_n\mathtt{x}^n) = \text{máx}\{\deg_{\mathtt{t}}(a_j) : \ 0 \le j \le n\} \\ &\ge \text{máx}\{\deg_{\mathtt{t}}(a_i), \ \deg_{\mathtt{t}}(a_n)\} \ge \text{máx}\{\deg_{\mathtt{t}}(f), \ \deg_{\mathtt{t}}(g)\} = r. \end{aligned}$$

Así, $\deg_{\mathtt{t}}(\psi) \leq r \leq \deg_{\mathtt{t}}(a_n q)$, pero $\deg_{\mathtt{t}}(\psi) = \deg_{\mathtt{t}}(a_n q) + \deg_{\mathtt{t}}(p)$, luego $\deg_{\mathtt{t}}(p) = 0$ y $\deg_{\mathtt{t}}(\psi) = r = \deg_{\mathtt{t}}(a_n q)$.

En particular $p \in K[\mathtt{x}]$, luego como polinomio en $K[\mathtt{t}][\mathtt{x}]$ es primitivo. Por el Lema de Gauss VI.1.4, vol. II, el producto $\psi = (a_n q)p \in K[\mathtt{t}][\mathtt{x}]$ es un polinomio primitivo. Por otro lado, se cumple que

$$\psi(\mathtt{x},\mathtt{t}) = g(\mathtt{t})f(\mathtt{x}) - g(\mathtt{x})f(\mathtt{t}) = -\big(g(\mathtt{x})f(\mathtt{t}) - g(\mathtt{t})f(\mathtt{x})\big) = -\psi(\mathtt{t},\mathtt{x})$$

y, por tanto, $\psi \in K[\mathtt{x}][\mathtt{t}]$ es también un polinomio primitivo. Pero $p \in K[\mathtt{x}]$ divide a $\psi \in K[\mathtt{x}][\mathtt{t}]$, que es primitivo, por lo que concluimos que p es una unidad de $K[\mathtt{x}]$. Esto implica, por V.1.2 vol. II, que $p \in K \setminus \{0\}$. De este modo

$$n = \deg_{\mathtt{x}}(q) = \deg_{\mathtt{x}}(a_n q) = \deg_{\mathtt{x}}(\psi) = \deg_{\mathtt{t}}(\psi) = r,$$

con lo que concluye la demostración. □

Observaciones III.1.2 (1) En la demostración del Teorema de Lüroth hemos probado que dado $u := f/g$, donde $f, g \in K[\mathtt{t}] \setminus \{0\}$ son primos entre sí y

$$n := \text{máx}\{\deg(f), \deg(g)\} \geq 1,$$

entonces $K(\mathtt{t})|K(u)$ es una extensión finita de grado n.

(2) El cuerpo K es algebraicamente cerrado en $K(\mathtt{t})$, es decir,

$$K = \{u \in K(\mathtt{t}) : u \text{ es algebraico sobre } K\}.$$

En efecto, supongamos que existe $u \in K(\mathtt{t})\setminus K$ algebraico sobre K. Entonces, la extensión $K(u)|K$ es finita y, por la observación anterior, también $K(\mathtt{t})|K(u)$ lo es. Se deduce de la Proposición I.1.6 que $K(\mathtt{t})|K$ es una extensión finita, lo que contradice I.2.2 (7).

2. Teorema de Steinitz

El objetivo de esta sección es introducir el concepto de grado de *transcendencia de una extensión* y demostrar el Teorema de Steinitz y la transitividad del grado de transcendencia.

Definición y Observación III.2.1 Se llama *grado de transcendencia* de la extensión $L|K$, y se denota $= \operatorname{tr}\deg\ L|K$, al mayor número de elementos de L algebraicamente independientes sobre K. Si tal número no existe decimos que $\operatorname{tr}\deg L|K = +\infty$. Obsérvese que $\operatorname{tr}\deg\ L|K = 0$ si y sólo si $L|K$ es una extensión algebraica.

El Teorema de Steinitz al que hemos hecho referencia es el siguiente:

Teorema III.2.2 (Steinitz) *El grado de transcendencia de una extensión no finita pero finitamente generada $L|K$, es un entero $s \geq 1$ caracterizado por la siguiente propiedad: existen $\alpha_1, \ldots, \alpha_s \in L$ algebraicamente independientes sobre K, tales que la extensión $L|K(\alpha_1, \ldots, \alpha_s)$ es finita. Se dice que $\{\alpha_1, \ldots, \alpha_s\}$ es una* base de transcendencia *de la extensión $L|K$.*

Antes de abordar su prueba necesitamos algunos resultados preliminares.

Lema III.2.3 *Dados una extensión $L|K$ y $a_1, \ldots, a_n \in L$, sean $K_0 := K$ y $K_i := K(a_1, \ldots, a_i)$ para $1 \leq i \leq n$. Las siguientes afirmaciones son equivalentes:*

(1) *Los elementos $a_1, \ldots, a_n$ son algebraicamente independientes sobre K.*

(2) *Para $1 \leq i \leq n$ el elemento a_i es transcendente sobre K_{i-1}.*

Demostración. (1) $\Longrightarrow$ (2) Supongamos, por reducción al absurdo, que existe un índice $1 \leq i \leq n$ tal que a_i es algebraico sobre K_{i-1}. Así, existe un polinomio no nulo $f \in K_{i-1}[\mathtt{t}]$ tal que $f(a_i) = 0$. Como $a_1, \ldots, a_{i-1}$ son algebraicamente independientes sobre K, los cuerpos $K(a_1, \ldots, a_{i-1})$ y $K(\mathtt{x}_1, \ldots, \mathtt{x}_{i-1})$ son isomorfos. Por tanto, existe un polinomio no nulo $g_0 \in K(\mathtt{x}_1, \ldots, \mathtt{x}_{i-1})[\mathtt{x}_i]$ tal que $g_0(a_1, \ldots, a_{i-1})(\mathtt{t}) = f(\mathtt{t})$. Multiplicando por un múltiplo no nulo $g \in K[\mathtt{x}_1, \ldots, \mathtt{x}_{i-1}]$ de los denominadores de los coeficientes de g_0 se obtiene $h := gg_0 \in K[\mathtt{x}_1, \ldots, \mathtt{x}_i]$, que es no nulo, pues tanto g como g_0 no lo son. Se tiene entonces

$$\begin{aligned} h(a_1, \ldots, a_{i-1}, a_i) &= g(a_1, \ldots, a_{i-1}) g_0(a_1, \ldots, a_{i-1})(a_i) \\ &= g(a_1, \ldots, a_{i-1}) f(a_i) = 0, \end{aligned}$$

y como $a_1, \ldots, a_i$ son algebraicamente independientes, $h = 0$ lo que es falso.

(2) $\Longrightarrow$ (1) Veamos por inducción sobre n que los elementos $a_1, \ldots, a_n$ son algebraicamente independientes sobre K. Si $n = 1$, entonces a_1 es transcendente sobre $K_0 = K$, lo que significa que es algebraicamente independiente sobre K. Supongamos que $a_1, \ldots, a_i$ son algebraicamente independientes sobre K para $i \leq n - 1$ y veamos que también es cierto para $i = n$.

Hemos de probar que si $f(a_1, \ldots, a_n) = 0$ para cierto $f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$, entonces $f = 0$. En caso contrario $\deg(f) > 0$, luego existe $1 \leq i \leq n$ tal que

$\deg_{\mathtt{x}_i}(f) > 0$ y $\deg_{\mathtt{x}_j}(f) = 0$ para los índices $j > i$. De hecho $i = n$, es decir, $\deg_{\mathtt{x}_n}(f) > 0$, ya que $a_1, \ldots, a_{n-1}$ son algebraicamente independientes sobre K. Escribimos

$$f := \sum_{k=0}^{m} f_k \mathtt{x}_n^k$$

donde cada $f_k \in K(\mathtt{x}_1, \ldots, \mathtt{x}_{n-1})$ y $f_m \neq 0$. Por la hipótesis de inducción $a_1, \ldots, a_{n-1}$ son algebraicamente independientes, luego $f_m(a_1, \ldots, a_{n-1}) \neq 0$. Esto implica que el polinomio $g(\mathtt{x}_n) := f(a_1, \ldots, a_{n-1}, \mathtt{x}_n) \in K_{n-1}[\mathtt{x}_n]$ es no nulo y $g(a_n) = 0$, lo que significa que a_n es algebraico sobre K_{n-1} contra la hipótesis. □

Lema III.2.4 *Sea $L|K$ es una extensión no finita pero finitamente generada, digamos por n elementos. Entonces, existen $\beta_1, \ldots, \beta_s \in L$ algebraicamente independientes sobre K, con $1 \leq s \leq n$, tales que la extensión $L|K(\beta_1, \ldots, \beta_s)$ es finita.*

Demostración. Por ser $L|K$ finitamente generada existen $\beta_1, \ldots, \beta_n \in L$ tales que $L := K(\beta_1, \ldots, \beta_n)$. Si $\beta_1, \ldots, \beta_n$ fuesen algebraicos sobre K entonces, por el Corolario I.2.3 (3), la extensión $L|K$ sería finita, contra la hipótesis.

Podemos suponer, por tanto, que β_1 es transcendente sobre K. Si la extensión $L|K(\beta_1)$ es finita hemos terminado. Si no, podemos suponer, por el Corolario I.2.3 (3), que β_2 es transcendente sobre $K(\beta_1)$, es decir, β_1, β_2 son algebraicamente independientes sobre K. Repitiendo el proceso $s \leq n$ veces, deducimos que existen $\beta_1, \ldots, \beta_s \in L$ algebraicamente independientes sobre K tales que la extensión $L|K(\beta_1, \ldots, \beta_s)$ es finita. □

Lema III.2.5 *Sean $L|K$ una extensión finitamente generada y $\beta_1, \ldots, \beta_r \in L$ algebraicamente independientes sobre K tales que la extensión $L|K(\beta_1, \ldots, \beta_r)$ es finita. Entonces, para cada $\alpha \in L$ transcendente sobre K, existe un índice i, con $1 \leq i \leq r$, tal que $\beta_1, \ldots, \beta_{i-1}, \alpha, \beta_{i+1}, \ldots, \beta_r$ son algebraicamente independientes sobre K y la extensión*

$$L|K(\beta_1, \ldots, \beta_{i-1}, \alpha, \beta_{i+1}, \ldots, \beta_r)$$

es finita.

Demostración. Como la extensión $L|K(\beta_1, \ldots, \beta_r)$ es finita, el elemento α es algebraico sobre $K(\beta_1, \ldots, \beta_r)$ y, por el Lema III.2.3, $\alpha, \beta_1, \ldots, \beta_r$ son algebraicamente dependientes. Pero α es transcendente sobre K luego, de nuevo por el

Lema III.2.3, existe $1 \leq i \leq r$ tal que β_i es algebraico sobre $K(\alpha, \beta_1, \ldots, \beta_{i-1})$. Reordenando los índices si fuese necesario podemos suponer que β_r es algebraico sobre el cuerpo $F_1 := K(\alpha, \beta_1, \ldots, \beta_{r-1})$.

Se trata por tanto de probar que $\alpha, \beta_1, \ldots, \beta_{r-1}$ son algebraicamente independientes sobre K y que la extensión $L|F_1$ es finita. En efecto, como $L|K(\beta_1, \ldots, \beta_r)$ es una extensión finita y finitamente generada, existen elementos $\zeta_1, \ldots, \zeta_\ell \in L$ algebraicos sobre $K(\beta_1, \ldots, \beta_r)$ tales que

$$L = K(\beta_1, \ldots, \beta_r)[\zeta_1, \ldots, \zeta_\ell].$$

Por tanto, como β_r es algebraico sobre F_1,

$$\begin{aligned} L &= K(\alpha, \beta_1, \ldots, \beta_{r-1}, \beta_r)[\zeta_1, \ldots, \zeta_\ell] = K(\alpha, \beta_1, \ldots, \beta_{r-1})(\beta_r)[\zeta_1, \ldots, \zeta_\ell] \\ &= K(\alpha, \beta_1, \ldots, \beta_{r-1})[\beta_r, \zeta_1, \ldots, \zeta_\ell]. \end{aligned}$$

Si denotamos $F_2 := K(\alpha, \beta_1, \ldots, \beta_{r-1})[\beta_r]$, la extensión $F_2|F_1$ es finita, pues β_r es algebraico sobre F_1. Por otro lado, como $\zeta_1, \ldots, \zeta_\ell \in L$ son algebraicos sobre F_2, también es finita la extensión $L|F_2$. Por la transitividad del grado, $L|F_1$ es una extensión finita.

Veamos para terminar que $\alpha, \beta_1, \ldots, \beta_{r-1}$ son algebraicamente independientes sobre K. Para ello, a la vista del Lema III.2.3 y ya que $\beta_1, \ldots, \beta_{r-1}$ son algebraicamente independientes sobre K, basta probar que α es transcendente sobre $K(\beta_1, \ldots, \beta_{r-1}) := F_0$. Procedemos por reducción al absurdo. Si α fuese algebraico sobre F_0,

$$F_1 = K(\alpha, \beta_1, \ldots, \beta_{r-1}) = K(\beta_1, \ldots, \beta_{r-1})(\alpha) = K(\beta_1, \ldots, \beta_{r-1})[\alpha] = F_0[\alpha],$$

luego $F_1|F_0$ sería una extensión finita de F_0. Como $F_2|F_1$ es también finita, de nuevo la transitividad del grado implica que $F_2|F_0$ es una extensión finita y en particular algebraica. Por tanto β_r es algebraico sobre $K(\beta_1, \ldots, \beta_{r-1})$, lo que implica, por el Lema III.2.3, que $\beta_1, \ldots, \beta_r$ son algebraicamente dependientes sobre K, que es falso. □

Demostración de III.2.2 Se deduce del Lema III.2.4 que existen $s \geq 1$ y $\beta_1, \ldots, \beta_s \in L$ algebraicamente independientes sobre K tales que la extensión $L|K(\beta_1, \ldots, \beta_s)$ es finita. Supongamos que existen $\alpha_1, \ldots, \alpha_s, \alpha_{s+1} \in L$ algebraicamente independientes sobre K. Por el Lema III.2.5 podemos suponer que los elementos $\beta_1, \ldots, \beta_{s-1}, \alpha_s$ son algebraicamente independientes sobre K y que la extensión $L|K(\beta_1, \ldots, \beta_{s-1}, \alpha_s)$ es finita.

Por el Lema III.2.3, $\beta_1, \ldots, \beta_{s-1}$ son algebraicamente independientes sobre $K(\alpha_s)$ y α_{s-1} es transcendente sobre $K(\alpha_s)$.

Además, la extensión $L|K(\alpha_s)(\beta_1,\ldots,\beta_{s-1})$ es finita. Por el Lema III.2.5 podemos suponer que $\beta_1,\ldots,\beta_{s-2},\alpha_{s-1}$ son algebraicamente independientes sobre $K(\alpha_s)$ y que la extensión $L|K(\alpha_s)(\beta_1,\ldots,\beta_{s-2},\alpha_{s-1})$ es finita. Reiterando el proceso podemos suponer que la extensión $L|K(\alpha_1,\ldots,\alpha_s)$ es finita, lo que por el Lema III.2.3 contradice que $\alpha_1,\ldots,\alpha_s,\alpha_{s+1}\in L$ son algebraicamente independientes sobre K.

Por tanto, s es el máximo número de elementos algebraicamente independientes sobre K. Esto significa que $\operatorname{tr\,deg} L|K = s$, con lo que concluye la demostración. □

Corolario III.2.6 *Si la extensión $L|K$ está generada por n elementos, entonces* $\operatorname{tr\,deg} L|K \leq n$.

Demostración. Se sigue directamente del Lema III.2.4 y el Teorema de Steinitz III.2.2. □

Ejemplos III.2.7 (1) Si $L := K(\mathtt{x}_1,\ldots,\mathtt{x}_n)$, donde $\mathtt{x}_1,\ldots,\mathtt{x}_n$ son indeterminadas sobre el cuerpo K, entonces $\mathtt{x}_1,\ldots,\mathtt{x}_n$ son también elementos de L algebraicamente independientes sobre K. Como la extensión $L|K(\mathtt{x}_1,\ldots,\mathtt{x}_n)$ es finita, el grado de transcendencia de $K(\mathtt{x}_1,\ldots,\mathtt{x}_n)|K$ es n.

(2) Si $K(\alpha)|K$ es una extensión transcendente simple, se deduce de (1) que el grado de transcendencia de $K(\alpha)|K$ es 1, pues las extensiones $K(\alpha)|K$ y $K(\mathtt{t})|K$ son isomorfas.

Acabamos la sección probando la fórmula de transitividad aditiva del grado de transcendencia.

Corolario III.2.8 *Sean $E|L$ y $L|K$ extensiones finitamente generadas. Entonces $E|K$ es también finitamente generada y*

$$\operatorname{tr\,deg} E|K = \operatorname{tr\,deg} E|L + \operatorname{tr\,deg} L|K.$$

La fórmula anterior se denomina *transitividad del grado de transcendencia.*

Demostración. Sean $r := \operatorname{tr\,deg} E|L$ y $s := \operatorname{tr\,deg} L|K$. Por el Teorema de Steinitz, III.2.2, existen $\alpha_1,\ldots,\alpha_r\in E$ y $\beta_1,\ldots,\beta_s\in L\subset E$ algebraicamente independientes sobre L y K respectivamente, tales que las extensiones

$$E|L(\alpha_1,\ldots,\alpha_r) \quad \& \quad L|K(\beta_1,\ldots,\beta_s)$$

son finitas. Existen por tanto $\eta_1, \ldots, \eta_k \in E$ y $\xi_1, \ldots, \xi_\ell \in L$ que son algebraicos sobre L y K respectivamente, tales que

$$E = L(\alpha_1, \ldots, \alpha_r)[\eta_1, \ldots, \eta_k] \quad \& \quad L = K(\beta_1, \ldots, \beta_s)[\xi_1, \ldots, \xi_\ell].$$

Nótese que

$$E = K(\beta_1, \ldots, \beta_s, \alpha_1, \ldots, \alpha_r, \xi_1, \ldots, \xi_\ell, \eta_1, \ldots, \eta_k),$$

así que la extensión $E|K$ es finitamente generada. Además, los elementos $\eta_1, \ldots, \eta_k$ son algebraicos sobre el cuerpo

$$F_1 := K(\beta_1, \ldots, \beta_s, \alpha_1, \ldots, \alpha_r)[\xi_1, \ldots, \xi_\ell]$$

y observamos que $E = F_1[\eta_1, \ldots, \eta_k]$. En particular se deduce de I.2.3 (3) que la extensión $E|F_1$ es finita.

Denotemos $F_2 := K(\beta_1, \ldots, \beta_s, \alpha_1, \ldots, \alpha_r)$. La extensión $F_1|F_2$ es finita, pues $\xi_1, \ldots, \xi_\ell$ son algebraicos sobre F_2. Si comprobamos que los elementos $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \in E$ son algebraicamente independientes sobre K tendremos, por el Teorema de Steinitz,

$$\operatorname{tr\,deg} E|K = r + s = \operatorname{tr\,deg} E|L + \operatorname{tr\,deg} L|K,$$

y habrá concluido la demostración.

En efecto, como $\alpha_1, \ldots, \alpha_r$ son algebraicamente independientes sobre L también lo son sobre $K_s := K(\beta_1, \ldots, \beta_s)$. Por el Lema III.2.3, el elemento α_i es transcendente sobre $K_{s+i-1} := K_s(\alpha_1, \ldots, \alpha_{i-1})$ para $i = 1, \ldots, r$ y, aplicando de nuevo el Lema III.2.3, y denotando $K_0 := K$, cada β_j es transcendente sobre $K_{j-1} := K(\beta_1, \ldots, \beta_{j-1})$ para $1 \leq j \leq s$. Así, por el Lema III.2.3, $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \in E$ son algebraicamente independientes sobre K. □

Ejercicios y problemas propuestos

Número III.1 Sean $F := K(\mathtt{t})$ y $L := K\big(\mathtt{t}^2/(1+\mathtt{t}^3)\big)$, donde K es un cuerpo y $\mathtt{t}$ es una indeterminada. Demostrar que $F|L$ es una extensión algebraica y simple y calcular su grado.

Número III.2 Sean $E|K$ una extensión de cuerpos y $u \in E \setminus K$.

(1) Demostrar que existe una subextensión $L|K$ de $E|K$ que es maximal entre las que no contienen a u.

(2) Demostrar que u es algebraico sobre L y que la extensión $E|L$ es algebraica.

Número III.3 Sea $K(u)|K$ una extensión transcendente de cuerpos. Demostrar que también $K(u^4, u^6)|K$ es una extensión transcendente y calcular su grado de transcendencia.

Número III.4 Sea $\{u, v\}$ una base de transcendencia de la extensión de cuerpos $L|K$. Calcular el grado de transcendencia de la extensión $K(u^2, uv)|K$.

Número III.5 Sean $E|K$ una extensión de cuerpos y $x, y \in E$. Determinar razonadamente la veracidad o falsedad de las siguientes afirmaciones.

(1) Si x o y es transcendente sobre K entonces $x + y$ o xy es transcendente sobre K.

(2) Si x es transcendente sobre K pero y es algebraico sobre K, entonces $x+y$ es transcendente sobre K.

(3) Si x es transcendente sobre K mientras que y es algebraico sobre K, entonces xy es transcendente sobre el cuerpo K.

(4) Si tanto x como y son elementos transcendentes sobre K entonces, x, y son algebraicamente independientes sobre K.

(5) Si x es transcendente sobre K e y es transcendente sobre $K(x)$, entonces x, y son algebraicamente independientes sobre K.

Número III.6 Dada una extensión de cuerpos $L|K$, y elementos $t_1, \ldots, t_n \in L$ algebraicamente independientes sobre K se denota $E := K(t_1, \ldots, t_n)$. Sea $F := K(t_1^{m_1}, \ldots, t_n^{m_n})$, donde $m_1, \ldots, m_n$ son enteros positivos. Demostrar que la extensión $E|F$ es finita y calcular su grado.

Número III.7 Sean p un número primo, $\mathtt{x}$ e $\mathtt{y}$ indeterminadas sobre $\mathbb{Z}_p$ y consideremos los cuerpos $E := \mathbb{Z}_p(\mathtt{x}, \mathtt{y})$ y $K := \mathbb{Z}_p(\mathtt{x}^p, \mathtt{y}^p)$. Demostrar que la extensión $E|K$ es finita y calcular su grado. ¿Cuál es el grado de transcendencia de la extensión $K|\mathbb{Z}_p$? Demostrar que $E|K$ no es una extensión simple.

Número III.8 (1) Sean $L|E$ y $E|F$ extensiones de cuerpos y $A \subset L$. Probar que si $E|F$ es algebraica también lo es $E(A)|F(A)$. Probar que si $t_1, \ldots, t_n \in L$ son algebraicamente independientes sobre F también son algebraicamente independientes sobre E.

(2) Dadas extensiones de cuerpos $L|E$ y $E|K$ demostrar que $L|K$ es finitamente generada si y sólo si tanto $L|E$ como $E|K$ lo son.

Número III.9 Utilizar el Teorema de Lindemann-Weierstrass para demostrar que dados números algebraicos $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ linealmente independientes sobre $\mathbb{Q}$, entonces los números $e^{\alpha_1}, \ldots, e^{\alpha_n}$ son algebraicamente independientes sobre $\mathbb{Q}$.

Número III.10 Utilizar el Teorema de Lindemann-Weierstrass para demostrar que para cada número algebraico $\alpha \in \mathbb{R} \setminus \{0\}$ los números $\operatorname{senh}\alpha$, $\cosh\alpha$ y $\operatorname{tgh}\alpha$ son transcendentes.

Número III.11 Emplear el Teorema de Gelfond-Schneider para probar que $e^{-\pi/2}$ es un número transcendente. ¿Es transcendente e^{π}?

CAPÍTULO IV

Grupo de automorfismos de una extensión

En la primera sección de este capítulo, se introduce el grupo de automorfismos de una extensión de cuerpos, a partir del que se define la noción de extensión de Galois. El resultado más relevante de la sección es la caracterización IV.1.6 de las extensiones de Galois de cuerpos de característica 0 como cuerpos de descomposición. En la segunda sección enunciamos y demostramos el Teorema fundamental de la teoría de Galois.

En cada extensión de cuerpos $L|K$ supondremos que $K \subset L$. Por ello los isomorfismos entre dos extensiones de cuerpos $L_1|K$ y $L_2|K$ son los isomorfismos $\phi : L_1 \to L_2$ cuya restricción a K es la identidad.

1. Grupo de automorfismos de una extensión de cuerpos. Extensiones de Galois.

Definición IV.1.1 Denotamos $G(L : K)$ el conjunto de *automorfismos* de la extensión de cuerpos $L|K$, es decir, los isomorfismos de la extensión $L|K$ en sí misma, también llamados K-automorfismos de L. Es inmediato que $G(L : K)$ es un grupo con respecto a la operación

$$G(L : K) \times G(L : K) \to G(L : K),\ (\sigma, \tau) \mapsto \sigma \cdot \tau = \tau \circ \sigma,$$

que se denomina *grupo de Galois* de $L|K$, y cuyo elemento neutro es el automorfismo identidad de L, que denotamos id_L.

Observaciones IV.1.2 (1) $G(L : K)$ es un subgrupo del grupo $\mathrm{Aut}(L)$ de automorfismos de L, pues si $\phi, \varphi \in G(L : K)$ y $x \in K$, la igualdad $\varphi(x) = x$ implica que $x = \varphi^{-1}(x)$, por lo que

$$(\varphi^{-1} \cdot \phi)(x) = (\phi \circ \varphi^{-1})(x) = \phi(\varphi^{-1}(x)) = \phi(x) = x,$$

así que $\varphi^{-1} \cdot \phi \in G(L:K)$.

(2) Frecuentemente $G(L:K)$ es un subgrupo propio de $\mathrm{Aut}(L)$. Por ejemplo, sean $\mathtt{x}$ e $\mathtt{y}$ indeterminadas sobre $\mathbb{Q}$ y sean $L := \mathbb{Q}(\mathtt{x},\mathtt{y})$ y $K := \mathbb{Q}(\mathtt{x})$. El automorfismo

$$\phi : L \to L,\ f(\mathtt{x},\mathtt{y})/g(\mathtt{x},\mathtt{y}) \mapsto f(\mathtt{y},\mathtt{x})/g(\mathtt{y},\mathtt{x})$$

que intercambia las variables $\mathtt{x}$ e $\mathtt{y}$ no pertenece a $G(L:K)$.

(3) Si L es un cuerpo de característica 0, contiene a $\mathbb{Q}$ y cada homomorfismo $\phi : \mathbb{Q} \to L$ cumple que $\phi(x) = x$ para cada $x \in \mathbb{Q}$. En efecto, para cada entero positivo n se cumple que $\phi(n) = n$, pues $\phi(1) = 1$ y, si suponemos probado por inducción que $\phi(n-1) = n-1$, entonces

$$\phi(n) = \phi((n-1)+1) = \phi(n-1) + \phi(1) = (n-1) + 1 = n.$$

Además, $\phi(0) = 0$ y si $n < 0$ es un entero y denotamos $m := -n > 0$ se tiene

$$\phi(n) + \phi(m) = \phi(n+m) = \phi(0) = 0 \quad \Longrightarrow \quad \phi(n) = -\phi(m) = -m = n.$$

Ahora, para cada $q \in \mathbb{Q}$ existen $m, n \in \mathbb{Z}$ tales que $n \neq 0$ y $q = m/n$, es decir, $m = qn$, por lo que

$$m = \phi(m) = \phi(qn) = \phi(q) \cdot \phi(n) = n \cdot \phi(q) \quad \Longrightarrow \quad \phi(q) = m/n = q.$$

En particular, el único automorfismo de $\mathbb{Q}$ es la identidad, y para cada extensión de cuerpos $L|\mathbb{Q}$ se cumple que $\mathrm{Aut}(L) = G(L:\mathbb{Q})$. En efecto, para cada $\phi \in \mathrm{Aut}(L)$ su restricción $\phi|_{\mathbb{Q}} : \mathbb{Q} \to L$ cumple que $\phi(x) = x$ para cada $x \in \mathbb{Q}$, esto es, $\phi \in G(L:\mathbb{Q})$.

(4) El único automorfismo $\phi : \mathbb{R} \to \mathbb{R}$ es la identidad. En efecto, si existiese $x \in \mathbb{R}$ tal que $x \neq \phi(x)$ podemos suponer, cambiando x por $-x$ si es preciso, que $x < \phi(x)$. Por ser $\mathbb{Q}$ denso en $\mathbb{R}$ existe $q \in \mathbb{Q}$ tal que $x < q < \phi(x)$ y, como $q - x > 0$, existe $a \in \mathbb{R}$ tal que $a^2 = q - x$. Pero entonces,

$$0 \leq \phi(a)^2 = \phi(a^2) = \phi(q-x) = \phi(q) - \phi(x) = q - \phi(x),$$

esto es, $\phi(x) \leq q$, que es una contradicción.

(5) Denotemos $i := \sqrt{-1} \in \mathbb{C}$ y sea $\tau : \mathbb{C} \to \mathbb{C}$, $z := a + bi \mapsto a - bi$ la conjugación. Veamos que $G(\mathbb{C}:\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \tau\}$. En efecto, es obvio que tanto la identidad como la conjugación son automorfismos de $\mathbb{C}$ cuya restricción a $\mathbb{R}$ es

la identidad. Para probar que son los únicos, sea $\phi : \mathbb{C} \to \mathbb{C}$ un automorfismo. Como $1 + i^2 = 0$ deducimos que

$$0 = \phi(0) = \phi(1 + i^2) = \phi(1) + \phi(i^2) = 1 + \big(\phi(i)\big)^2,$$

luego $\phi(i) = \varepsilon i$ donde $\varepsilon = \pm 1$. Así, para cada $z := a + bi \in \mathbb{C}$ con $a, b \in \mathbb{R}$, se tiene

$$\phi(z) = \phi(a + bi) = \phi(a) + \phi(b)\phi(i) = a + \varepsilon bi,$$

luego $\phi = \mathrm{id}_{\mathbb{C}}$ si $\varepsilon = 1$ y $\phi = \tau$ si $\varepsilon = -1$.

(6) Dadas extensiones de cuerpos $L_1|K_1$ y $L_2|K_2$ tales que existe un isomorfismo de cuerpos $\psi : L_1 \to L_2$ que cumple $\psi(K_1) = K_2$, entonces los grupos $G(L_1 : K_1)$ y $G(L_2 : K_2)$ son isomorfos, vía el isomorfismo

$$\Psi : G(L_1 : K_1) \to G(L_2 : K_2),\ \phi \mapsto \psi \circ \phi \circ \psi^{-1}.$$

En efecto, es suficiente comprobar que si $\phi \in G(L_1 : K_1)$ y $x \in K_2$, entonces $\Psi(\phi)(x) = x$. Ahora bien, $y := \psi^{-1}(x) \in K_1$, por lo que $\phi(y) = y$ y por tanto

$$\Psi(\phi)(x) = (\psi \circ \phi \circ \psi^{-1})(x) = (\psi \circ \phi)(y) = \psi(\phi(y)) = \psi(y) = x.$$

Aunque estamos interesados fundamentalmente en el estudio del grupo de Galois de las extensiones finitas, antes de hacerlo vamos a estudiar el caso infinito más sencillo, que es el de las extensiones transcendentes simples.

1.a. Grupo de Galois de una extensión transcendente simple.

Teorema IV.1.3 *Sean K un cuerpo, $\mathrm{GL}_2(K)$ el grupo multiplicativo de las matrices cuadradas de orden 2 con coeficientes en K y determinante no nulo y $\mathcal{H}$ su subgrupo formado por las matrices de la forma*

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \quad \textit{con } \lambda \in K \setminus \{0\}.$$

Si $\mathtt{t}$ es una indeterminada sobre K, entonces $G(K(\mathtt{t}) : K) \cong \mathrm{GL}_2(K)/\mathcal{H}$.

Demostración. Los automorfismos de $K(\mathtt{t})|K$ quedan determinados por la imagen de $\mathtt{t}$, y si $\phi \in G(K(\mathtt{t}) : K)$ y $\alpha := \phi(\mathtt{t})$, existen $f, g \in K[\mathtt{t}]$ no nulos y primos entre sí tales que $\alpha = f(\mathtt{t})/g(\mathtt{t})$. Nótese que $K(\mathtt{t}) = \mathrm{im}\,\phi = K(\alpha)$, y por III.1.2 (1), se tiene

$$\text{máx}\{\deg(f), \deg(g)\} = [K(\mathtt{t}) : K(\alpha)] = 1 \quad \& \quad \alpha \in K(\mathtt{t}) \setminus K.$$

Existen por tanto $a, b, c, d \in K$ tales que $f(\mathtt{t}) = a\mathtt{t} + b$ y $g(\mathtt{t}) = c\mathtt{t} + d$ y el cociente $f/g \notin K$. Esto último equivale a que $a\mathtt{t} + b \neq r(c\mathtt{t} + d)$ para cada $r \in K$. Por tanto los vectores (a, b) y (c, d) de K^2 no son proporcionales, es decir, el determinante de la matriz

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

es no nulo. En consecuencia, si denotamos ϕ_A el único automorfismo de $K(\mathtt{t})|K$ que cumple $\phi_A(\mathtt{t}) = (a\mathtt{t} + b)/(c\mathtt{t} + d)$, la aplicación

$$\Psi : \mathrm{GL}_2(K) \to G(K(\mathtt{t}) : K),\ A \mapsto \phi_A$$

es sobreyectiva. Además es un homomorfismo, pues dados $i = 1, 2$,

$$A_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \quad \Longrightarrow \quad A_1A_2 = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix},$$

y denotando $\phi_i = \phi_{A_i}$ se cumple que

$$\begin{aligned}(\phi_1 \cdot \phi_2)(\mathtt{t}) &= \phi_2((a_1\mathtt{t} + b_1)/(c_1\mathtt{t} + d_1)) = (a_1\phi_2(\mathtt{t}) + b_1)/(c_1\phi_2(\mathtt{t}) + d_1) \\ &= (a_1(a_2\mathtt{t} + b_2)/(c_2\mathtt{t} + d_2) + b_1)/(c_1(a_2\mathtt{t} + b_2)/(c_2\mathtt{t} + d_2) + d_1) \\ &= ((a_1a_2 + b_1c_2)\mathtt{t} + a_1b_2 + b_1d_2)/((c_1a_2 + d_1c_2)\mathtt{t} + c_1b_2 + d_1d_2) \\ &= \phi_{A_1A_2}(\mathtt{t}).\end{aligned}$$

Esto implica que $\phi_1 \cdot \phi_2 = \phi_{A_1A_2}$, o lo que es lo mismo,

$$\Psi(A_1A_2) = \phi_{A_1A_2} = \phi_1 \cdot \phi_2 = \Psi(A_1) \cdot \Psi(A_2).$$

Por último, $A \in \ker \Psi$ si y sólo si $\Psi(\mathtt{t}) = \mathtt{t}$, esto es, $(a\mathtt{t} + b)/(c\mathtt{t} + d) = \mathtt{t}$, o lo que es lo mismo, $a\mathtt{t} + b = c\mathtt{t}^2 + d\mathtt{t}$. Esto significa que $b = c = 0$ y $a = d \in K \setminus \{0\}$, es decir, $A \in \mathcal{H}$. Ahora, por el Primer Teorema de isomorfía de grupos,

$$\mathrm{GL}_2(K)/\mathcal{H} = \mathrm{GL}_2(K)/\ker \Psi \cong \mathrm{im}\, \Psi = G(K(\mathtt{t}) : K).$$

□

1.b. Grupo de Galois de una extensión finita. En el resto de la sección estudiamos el grupo de Galois de las extensiones finitas, poniendo especial énfasis en las de característica 0.

Observaciones IV.1.4 (1) Sea $L|K$ una extensión algebraica y $\alpha \in L$ tal que $L = K(\alpha)$. Denotamos $f := P_{K,\alpha}$ el polinomio mínimo de α sobre K y sea $\phi \in G(L:K)$. Evidentemente $\phi(\alpha)$ determina ϕ, pero no todo elemento de L es imagen de α por un automorfismo de L que deja fijo K.

En efecto, dado $\beta \in K(\alpha)$, se deduce del Lema II.1.1 que existe un isomorfismo $\phi : K(\alpha) \to K(\beta)$ tal que $\phi|_K = \mathrm{id}_K$ y $\phi(\alpha) = \beta$ si y sólo si β es una raíz de f. Si éste es el caso se tiene

$$\deg(f) = [K(\alpha) : K] = [K(\alpha) : K(\beta)] \cdot [K(\beta) : K] = [K(\alpha) : K(\beta)] \deg(f),$$

luego $[K(\alpha) : K(\beta)] = 1$, es decir, $K(\alpha) = K(\beta)$, así que $\phi \in G(K(\alpha) : K)$. Por tanto, dado $\beta \in K(\alpha)$ existe un automorfismo $\phi \in G(K(\alpha) : K)$ tal que $\phi(\alpha) = \beta$ si y sólo si β es una raíz de f.

(2) De este modo, si $Z_{K(\alpha)}(f)$ es el conjunto de las raíces de f en $K(\alpha)$, la aplicación

$$G(K(\alpha) : K) \to Z_{K(\alpha)}(f),\ \phi \mapsto \phi(\alpha)$$

es biyectiva. En particular, el número de automorfismos de la extensión $K(\alpha)|K$ es menor o igual que su grado, ya que

$$\mathrm{ord}\left(G(K(\alpha) : K)\right) = \mathrm{Card}\left(Z_{K(\alpha)}(f)\right) \leq \deg(f) = [K(\alpha) : K]. \tag{1.1}$$

(3) Además, si $Z_{K(\alpha)}(f)$ tiene r elementos, el grupo $G(K(\alpha) : K)$ es isomorfo a un subgrupo del grupo de permutaciones $\mathcal{S}_r$. En efecto, como $\alpha \in Z_{K(\alpha)}(f)$, la restricción $\phi|_{Z_{K(\alpha)}(f)}$, que es una biyección de $Z_{K(\alpha)}(f)$, determina ϕ, es decir, la aplicación

$$G(K(\alpha) : K) \to \mathcal{S}_r,\ \phi \mapsto \phi|_{Z_{K(\alpha)}(f)}$$

es un homomorfismo inyectivo, luego $G(K(\alpha) : K)$ es isomorfo a su imagen, que es un subgrupo de $\mathcal{S}_r$.

(4) Con más generalidad, si $L := K(a_1, \ldots, a_r)|K$ es una extensión finitamente generada, cada automorfismo $\phi \in G(L : K)$ queda determinado por las imágenes $\phi(a_j)$ con $1 \leq j \leq r$.

(5) La desigualdad (1.1) del apartado (2) puede ser estricta. Consideremos, por ejemplo, $K := \mathbb{Q}$ y $\alpha := \sqrt[3]{p} \in \mathbb{R}$, donde p es un número primo. El polinomio mínimo de α sobre $\mathbb{Q}$ es $\mathtt{t}^3 - p$, que es irreducible en $\mathbb{Z}[\mathtt{t}]$, y por tanto en $\mathbb{Q}[\mathtt{t}]$, por el Criterio de Eisenstein. En consecuencia, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Sin embargo, si $\zeta := e^{2\pi i/3}$, las raíces de f en $\mathbb{C}$ son α, $\alpha\zeta$ y $\alpha\zeta^2$, ya que $\zeta^3 = 1$. Como $\mathbb{Q}(\alpha) \subset \mathbb{R}$, ni $\alpha\zeta$ ni $\alpha\zeta^2$ pertenecen a $\mathbb{Q}(\alpha)$, por lo que $Z_{\mathbb{Q}(\alpha)}(f) = \{\alpha\}$ consta de un único elemento.

Definición y Ejemplos IV.1.5 (1) Se dice que una extensión finita $L|K$ es *de Galois* si

$$[L : K] = \mathrm{ord}(G(L : K)).$$

(2) Por IV.1.4 (5), para todo número primo p la extensión $\mathbb{Q}(\sqrt[3]{p})|\mathbb{Q}$ no es de Galois.

(3) Sea K un cuerpo de característica distinta de 2. Entonces, toda extensión $L|K$ de grado 2 es de Galois. En efecto, tomando $\alpha \in L \setminus K$ resulta que $L = K(\alpha)$. El polinomio mínimo de α sobre K es mónico de grado 2, esto es, $P_{K,\alpha}(\mathtt{t}) = \mathtt{t}^2 - a\mathtt{t} + b \in K[\mathtt{t}]$, luego $a - \alpha \in K(\alpha)$ es raíz de $P_{K,\alpha}$. Si $a - \alpha \neq \alpha$ entonces $P_{K,\alpha}$ tiene dos raíces en $K(\alpha)$, por lo que $L|K$ es extensión de Galois, ya que

$$\mathrm{ord}(G(L : K)) = \mathrm{Card}\{\alpha, a - \alpha\} = 2 = [L : K].$$

De hecho este es el único caso posible porque si $a - \alpha = \alpha$ entonces $2\alpha = a \in K$ y, como $\mathrm{char}(K) \neq 2$, esto implica que $\alpha \in K$, que es falso.

Obtenemos a continuación una útil caracterización de las extensiones de Galois de característica 0.

Proposición IV.1.6 *Sea $L|K$ una extensión finita de cuerpos de característica 0. Las siguientes afirmaciones son equivalentes:*

(1) *La extensión $L|K$ es de Galois.*

(2) *Existe un polinomio irreducible $f \in K[\mathtt{t}]$ de grado $[L : K]$ tal que L es el cuerpo de descomposición de f sobre K.*

(3) *Existe un polinomio $f \in K[\mathtt{t}]$ tal que L es el cuerpo de descomposición de f sobre K.*

(4) *Si $g \in K[\mathtt{t}]$ es un polinomio irreducible de grado ≥ 1 que tiene una raíz en L, entonces g factoriza en $L[\mathtt{t}]$ como producto de factores de grado 1.*

Demostración. (1) $\Longrightarrow$ (2) Por el Teorema del elemento primitivo II.2.2, existe $\alpha \in L$ tal que $L = K(\alpha)$. Sea $f := P_{K,\alpha}$ el polinomio mínimo de α sobre K. Como la extensión $L|K$ es de Galois se tiene, por IV.1.4,

$$\deg(f) = [L : K] = \mathrm{ord}(G(L : K)) = \mathrm{Card}(Z_L(f)),$$

es decir, f tiene en L tantas raíces distintas como grado, por lo que contiene a un cuerpo de descomposición de f sobre K. Además, cada cuerpo de descomposición de f sobre K contiene a α porque $f(\alpha) = 0$, luego contiene a

$L = K(\alpha)$. En consecuencia, f es un polinomio irreducible en $K[\mathtt{t}]$ de grado $[L : K]$ y L es el cuerpo de descomposición de f sobre K.

La implicación (2) $\Longrightarrow$ (3) es obvia, así que probamos (3) $\Longrightarrow$ (4). Sea $g \in K[\mathtt{t}]$ un polinomio irreducible de grado ≥ 1 que tiene un raíz $\alpha \in L$. Se trata de demostrar que cualquier raíz β de g en un cierre algebraico de L también pertenece a L, y para ello basta ver que $[L(\beta) : L] = 1$. Como $K(\alpha) \subset L$ podemos escribir, por la transitividad del grado,

$$[L(\beta) : L] \cdot [L : K(\alpha)] \cdot [K(\alpha) : K] = [L(\beta) : K] = [L(\beta) : K(\beta)] \cdot [K(\beta) : K]$$

y como $P_{K,\alpha} = g = P_{K,\beta}$ se tiene $[K(\alpha) : K] = \deg(g) = [K(\beta) : K]$, luego la igualdad anterior se convierte en

$$[L(\beta) : L] \cdot [L : K(\alpha)] = [L(\beta) : K(\beta)],$$

luego todo se reduce a comprobar que $[L : K(\alpha)] = [L(\beta) : K(\beta)]$.

Como α y β son raíces del mismo polinomio irreducible $g \in K[\mathtt{t}]$ existe, por el Lema II.1.1, un isomorfismo $\phi : K(\alpha) \to K(\beta)$ tal que $\phi(\alpha) = \beta$ y $\phi|_K = \mathrm{id}_K$. Como L es un cuerpo de descomposición de f sobre K, se deduce que $L = L(\alpha)$ y $L(\beta)$ son cuerpos de descomposición de f sobre $K(\alpha)$ y $K(\beta)$, respectivamente. Esto implica, por II.1.2, que existe un isomorfismo $\Phi : L \to L(\beta)$ tal que $\Phi|_{K(\alpha)} = \phi$. Por tanto, $[L : K(\alpha)] = [L(\beta) : K(\beta)]$, como se quería demostrar.

(4) $\Longrightarrow$ (1) Por el Teorema del elemento primitivo existe un elemento $\alpha \in L$ tal que $L = K(\alpha)$, y como el polinomio mínimo $g := P_{K,\alpha}$ de α sobre K tiene una raíz $\alpha \in L$, factoriza en $L[\mathtt{t}]$ como producto de factores de grado 1. Además, puesto que $\mathrm{char}(K) = 0$, se sigue de II.1.3 (2) que g no tiene raíces múltiples en L, es decir, el conjunto $Z_L(g)$ de raíces de g en L tiene $\deg(g) = [L : K]$ elementos. Esto implica, por IV.1.4, que

$$\mathrm{ord}(G(L : K)) = \mathrm{Card}(Z_L(g)) = [L : K],$$

o sea, la extensión $L|K$ es de Galois. □

Corolario IV.1.7 *Sean $L|K$ una extensión de Galois de cuerpos de característica 0 y $E|K$ una subextensión de $L|K$. Entonces, también la extensión $L|E$ es de Galois.*

Demostración. Por la Proposición IV.1.6, L es un cuerpo de descomposición sobre K de un polinomio $f \in K[\mathtt{t}]$, luego también es un cuerpo de descomposición sobre E de $f \in E[\mathtt{t}]$. Empleando de nuevo la Proposición IV.1.6 deducimos que la extensión $L|E$ es de Galois. □

Observación IV.1.8 El ser extensión de Galois no tiene carácter transitivo. Para verlo denotamos $\sqrt[4]{2}$ el único número real positivo cuya potencia cuarta vale 2 y consideramos los cuerpos $K := \mathbb{Q}(\sqrt{2})$ y $L := \mathbb{Q}(\sqrt[4]{2})$. La extensión $L|\mathbb{Q}$ tiene grado 4, pues el polinomio $g(\mathtt{t}) := \mathtt{t}^4 - 2 \in \mathbb{Q}[\mathtt{t}]$ es irreducible, por el Criterio de Eisenstein, y no es de Galois, ya que g tiene en L una raíz $\alpha := \sqrt[4]{2}$, pero g no factoriza en $L[\mathtt{t}]$ en producto de factores de grado 1, pues $L \subset \mathbb{R}$ y, sin embargo, una raíz de g es $\alpha i \in \mathbb{C} \setminus \mathbb{R}$, donde $i := \sqrt{-1}$.

Sin embargo, las extensiones $K|\mathbb{Q}$ y $L|K$ tienen grado 2, luego son de Galois, como consecuencia de IV.1.5 (3). En efecto, el polinomio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$ es $\mathtt{t}^2-2$, de nuevo por el Criterio de Eisenstein, luego $[K : \mathbb{Q}] = \deg(\mathtt{t}^2-2) = 2$, mientras que $[L : K] = 2$ ya que

$$4 = [L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] = 2 \cdot [L : K]$$

Ejemplos IV.1.9 (1) El cuerpo $L := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ es un cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $f(\mathtt{t}) := (\mathtt{t}^2 - 2)(\mathtt{t}^2 - 3)$ luego, por la Proposición IV.1.6, la extensión $L|\mathbb{Q}$ es de Galois, y vamos a calcular su grupo de Galois $G(L : \mathbb{Q})$. Como su orden es, por I.2.4, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ se deduce del Ejemplo VI.1.7 (3) vol. I que es isomorfo al grupo cíclico $\mathbb{Z}_4$ de orden 4 o al producto $\mathbb{Z}_2 \times \mathbb{Z}_2$. Comprobemos que ningún elemento de $G(L : \mathbb{Q})$ tiene orden 4, lo que probará que $G(L : \mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. En efecto, si $\varphi \in G(L : \mathbb{Q})$ se deduce del Lema II.1.1 que $\varphi(\sqrt{2})$ y $\varphi(\sqrt{3})$ son raíces de los polinomios mínimos $\mathtt{t}^2 - 2$ y $\mathtt{t}^2 - 3$ de $\sqrt{2}$ y $\sqrt{3}$ sobre $\mathbb{Q}$, respectivamente. Por tanto $\varphi(\sqrt{2}) = \varepsilon\sqrt{2}$ y $\varphi(\sqrt{3}) = \delta\sqrt{3}$, donde $\varepsilon, \delta \in \{+1, -1\}$. Así,

$$\varphi^2(\sqrt{2}) = \varphi(\varepsilon\sqrt{2}) = \varepsilon\varphi(\sqrt{2}) = \varepsilon^2\sqrt{2} = \sqrt{2},$$

y análogamente $\varphi^2(\sqrt{3}) = \sqrt{3}$. Esto demuestra que $\varphi^2 = \mathrm{id}_L$, ya que todo elemento de L es de la forma $g(\sqrt{2}, \sqrt{3})$ para cierto polinomio $g \in \mathbb{Q}[\mathtt{x}, \mathtt{y}]$, luego $o(\varphi) \leq 2$ para cada $\varphi \in G(L : \mathbb{Q})$.

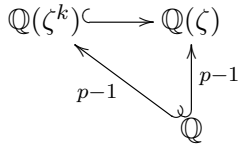
(2) Sean p un número primo impar y $\zeta := e^{2\pi i/p}$. Vamos a calcular el grupo de Galois $G(\mathbb{Q}(\zeta) : \mathbb{Q})$ de la extensión $\mathbb{Q}(\zeta)|\mathbb{Q}$. Vimos en el Ejemplo I.2.4 que el polinomio mínimo de ζ sobre $\mathbb{Q}$ es el polinomio ciclotómico $\Phi_p(\mathtt{t}) := \sum_{j=0}^{p-1} \mathtt{t}^j$, y vamos a demostrar que la extensión $\mathbb{Q}(\zeta)|\mathbb{Q}$ es de Galois y que su grupo de Galois $G(\mathbb{Q}(\zeta) : \mathbb{Q})$ es el grupo cíclico $\mathbb{Z}_{p-1}$ de orden $p - 1$.

Para lo primero comprobaremos que $\mathbb{Q}(\zeta)$ es un cuerpo de descomposición sobre $\mathbb{Q}$ de Φ_p. En efecto, para $1 \leq j \leq p-1$ la potencia ζ^j es también raíz de Φ_p, pues $\zeta^j \neq 1$ y

$$0 = (e^{2\pi i})^j - 1 = (\zeta^j)^p - 1 = (\zeta^j - 1)\Phi_p(\zeta^j).$$

En consecuencia, $\Phi_p(\mathtt{t}) = \prod_{j=1}^{p-1}(\mathtt{t} - \zeta^j)$ factoriza en $\mathbb{Q}(\zeta)[\mathtt{t}]$ como producto de factores de grado 1, por lo que $\mathbb{Q}(\zeta)$ es un cuerpo de descomposición de Φ_p sobre $\mathbb{Q}$.

Por otro lado, vimos en la Proposición VI.2.8, vol. I, que el grupo multiplicativo $\mathbb{Z}_p^*$ formado por los elementos no nulos de $\mathbb{Z}_p$ es cíclico, y consideramos un generador suyo $[k]_p := k + p\mathbb{Z}$. Como $\Phi_p(\zeta^k) = 0$, se deduce del Lema II.1.1 que existe un isomorfismo $\phi : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta^k)$ tal que $\phi(\zeta) = \zeta^k$. Pero $\mathbb{Q}(\zeta^k) = \mathbb{Q}(\zeta)$, pues Φ_p es el polinomio mínimo tanto de ζ como de ζ^k, así que, por la transitividad del grado aplicada a las extensiones



se deduce que $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta^k)] = 1$, esto es, $\mathbb{Q}(\zeta^k) = \mathbb{Q}(\zeta)$. En consecuencia, $\phi : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ es un elemento del grupo de Galois $G(\mathbb{Q}(\zeta) : \mathbb{Q})$, y para ver que este grupo es cíclico basta comprobar que el orden $o(\phi) = r$ de ϕ coincide con el orden $\mathrm{ord}(G(\mathbb{Q}(\zeta) : \mathbb{Q})) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ de su grupo de Galois.

Ahora bién, como ϕ^r es el automorfismo identidad, $\zeta = \phi^r(\zeta) = \zeta^{k^r}$, así que $\zeta^{k^r-1} = 1$, por lo que $k^r - 1 \in p\mathbb{Z}$, esto es, $([k]_p)^r = [1]_p$, luego r es múltiplo del orden de $[k]_p \in \mathbb{Z}_p^*$, que es $p - 1$ porque hemos elegido k de forma que $\mathbb{Z}_p^* = \langle [k]_p \rangle$. En particular,

$$r \geq p - 1 = \mathrm{ord}(G(\mathbb{Q}(\zeta) : \mathbb{Q})) \geq o(\phi) = r,$$

luego $o(\phi) = p - 1$.

1.c. Clausura de Galois. Para terminar esta sección introducimos la noción de *clausura de Galois* de una extensión finita $E|K$ de cuerpos. Hablando con cierta imprecisión se trata de "la menor" extensión de Galois $L|K$ que tiene a $E|K$ por subextensión. Por ello $E|K$ es su clausura de Galois si ella misma es una extensión de Galois.

Definición y Proposición IV.1.10 (1) Sea $E|K$ una extensión finita. Se dice que la extensión finita $L|K$ es una *clausura de Galois* de $E|K$ si $E|K$ es una subextensión de $L|K$, esta extensión es de Galois, y no existe ningún cuerpo intermedio $E \subset F \subsetneq L$ tal que la extensión $F|K$ sea de Galois.

(2) Toda extensión finita $E|K$ de cuerpos de característica 0 admite una clausura de Galois. Además, dos clausuras de Galois de $E|K$ son isomorfas.

Demostración. Por el Teorema del elemento primitivo existe $\alpha \in E$ tal que $E = K(\alpha)$, y sea L un cuerpo de descomposición sobre K del polinomio mínimo $P_{K,\alpha}$ de α sobre K. Como α es raíz de $P_{K,\alpha}$ pertenece a L, luego $E|K$ es una subextensión de $L|K$. Además $L|K$ es de Galois, por la Proposición IV.1.6. Sea F un cuerpo intermedio $E \subset F \subset L$ tal que la extensión $F|K$ es de Galois. Como $\alpha \in E \subset F$ el polinomio $P_{K,\alpha}$ factoriza en $F[\mathtt{t}]$ como producto de factores de grado 1,

$$P_{K,\alpha}(\mathtt{t}) := (\mathtt{t} - \alpha_1) \cdots (\mathtt{t} - \alpha_n), \;\; \alpha_1 = \alpha,$$

y por tanto, $L = K(\alpha_1, \ldots, \alpha_n) \subset F$, es decir, $F = L$. Por último, si $L_1|K$ y $L_2|K$ son clausuras de Galois de $E|K$ ambas son cuerpos de descomposición de $P_{K,\alpha}$ sobre K luego, por el Teorema II.1.2, las extensiones $L_1|K$ y $L_2|K$ son isomorfas. □

Ejemplo IV.1.11 Vimos en IV.1.5 que si $E := \mathbb{Q}(\sqrt[3]{2})$ la extensión $E|\mathbb{Q}$ no es de Galois. Vamos a determinar su clausura de Galois, que denotamos $L|\mathbb{Q}$.

El polinomio $f(\mathtt{t}) := \mathtt{t}^3 - 2$ es irreducible en $\mathbb{Q}[\mathtt{t}]$ y $\alpha := \sqrt[3]{2} \in E \subset L$ es una raíz de f, luego f factoriza en $L[\mathtt{t}]$ como producto de factores de grado 1. Por tanto, L debe contener a las raíces en $\mathbb{C}$ de f, que son $\alpha, \alpha\zeta$ y $\alpha\zeta^2$, donde $\zeta := e^{2\pi i/3}$, pues estos tres números son distintos y, como $\zeta^3 = 1$,

$$(\alpha\zeta)^3 = \alpha^3\zeta^3 = 2 \quad \& \quad (\alpha\zeta^2)^3 = \alpha^3\zeta^6 = 2.$$

Por tanto $L \subset L_f$ donde $L_f := \mathbb{Q}(\alpha, \alpha\zeta, \alpha\zeta^2)$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$. Por la Proposición IV.1.6, la extensión $L_f|\mathbb{Q}$ es de Galois, y por la minimalidad de $L|\mathbb{Q}$ entre las extensiones de Galois que tienen a $E|\mathbb{Q}$ por subextensión se deduce que $L = L_f$.

De hecho $L = \mathbb{Q}(\alpha, \zeta)$. En efecto, por un lado $\alpha \in L$ y $\zeta = \alpha\zeta/\alpha \in L$, lo que prueba que $\mathbb{Q}(\alpha, \zeta) \subset L$. Recíprocamente, $\alpha, \alpha\zeta, \alpha\zeta^2 \in \mathbb{Q}(\alpha, \zeta)$, lo que prueba la igualdad buscada. Determinamos ahora el grupo de Galois $G(L : \mathbb{Q})$ de $L|\mathbb{Q}$, para lo que calculamos antes $\mathrm{ord}(G(L : \mathbb{Q})) = [L : \mathbb{Q}]$. Nótese que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 3$, mientras que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$, pues el polinomio mínimo de ζ sobre $\mathbb{Q}$ es el polinomio ciclotómico $\Phi_2(\mathtt{t}) = \mathtt{t}^2 + \mathtt{t} + 1$ de grado 2, cuya irreducibilidad se probó en VI.2.7, vol. II. Como los grados 2 y 3 de las extensiones $\mathbb{Q}(\alpha)|\mathbb{Q}$ y $\mathbb{Q}(\zeta)|\mathbb{Q}$ son primos entre sí y, por el Ejemplo I.2.4,

$$[L : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta) : \mathbb{Q}] = 3 \cdot 2 = 6.$$

Por tanto $G(L : \mathbb{Q})$ es un grupo de orden 6, y se deduce del Ejemplo VI.2.9, vol. I que $G(L : \mathbb{Q})$ es isomorfo al grupo cíclico $\mathbb{Z}_6$ o al grupo simétrico $\mathcal{S}_3$.

Para decidir cuál es el caso es suficiente estudiar si $G(L:\mathbb{Q})$ es o no abeliano, pero vamos a describir completamente los elementos de este grupo. Señalamos en IV.1.4 (4) que cada automorfismo $\phi \in G(L:\mathbb{Q})$ está determinado por los valores $\phi(\alpha)$ y $\phi(\zeta)$. Además, se desprende del Lema II.1.1 que $\phi(\alpha)$ es raíz de $f := P_{\mathbb{Q},\alpha}$ y $\phi(\zeta)$ es raíz de $\Phi_2 = P_{\mathbb{Q},\zeta}$. Ya hemos señalado que las raíces de $P_{\mathbb{Q},\alpha}$ son $\alpha\zeta^j$ para $0 \le j \le 2$ mientras que las de $P_{\mathbb{Q},\zeta}$ son ζ^k con $1 \le k \le 2$. Como sabemos que $G(L:\mathbb{Q})$ tiene orden 6, deducimos que existen, exactamente, seis automorfismos $\phi_{jk} : L \to L$ cuya restricción a $\mathbb{Q}$ es la identidad y que están determinados por las condiciones:

$$\phi_{jk}(\alpha) = \alpha\zeta^j \quad \& \quad \phi_{jk}(\zeta) = \zeta^k.$$

Comprobemos ya que el grupo $G(L:\mathbb{Q})$ no es abeliano, lo que implica que es isomorfo a $\mathcal{S}_3$. Por ejemplo,

$$\begin{aligned}(\phi_{11}\cdot\phi_{02})(\alpha) &= \phi_{02}(\alpha\zeta) = \phi_{02}(\alpha)\cdot\phi_{02}(\zeta) = \alpha\zeta^2 \quad \&\\ (\phi_{02}\cdot\phi_{11})(\alpha) &= \phi_{11}(\phi_{02}(\alpha)) = \phi_{11}(\alpha) = \alpha\zeta,\end{aligned}$$

lo que demuestra que $\phi_{11}\cdot\phi_{02} \neq \phi_{02}\cdot\phi_{11}$.

2. Teorema fundamental de la teoría de Galois.

En esta sección enunciamos y probamos el Teorema fundamental de la teoría de Galois para extensiones de Galois $L|K$ de cuerpos de característica 0, cuya primera parte afirma que existe una biyección entre las subextensiones de $L|K$ y los subgrupos del grupo de Galois $G(L:K)$, y cuya segunda parte dice que la subextensión $E|K$ de $L|K$ es de Galois si y sólo si $G(L:E)$ es un subgrupo normal de $G(L:K)$. En el Capítulo V veremos el mismo resultado para extensiones de cuerpos finitos.

2.a. Cuerpo fijo por un grupo de automorfismos.

Definiciones y Proposición IV.2.1 (1) Dado un cuerpo L se denomina *subcuerpo fijo* asociado a un subgrupo H del grupo $\mathrm{Aut}(L)$ de automorfismos de L al conjunto

$$\mathrm{Fix}(H) := \{\alpha \in L :\ \phi(\alpha) = \alpha \ \ \forall\, \phi \in H\}.$$

Nótese que $\mathrm{Fix}(H)$ no es vacío, ya que $1 \in \mathrm{Fix}(H)$, y es un subcuerpo de L pues dados elementos no nulos $x, y \in \mathrm{Fix}(H)$ tanto $x-y$ como xy^{-1} pertenecen

a $\mathrm{Fix}(H)$, ya que para todo $\phi \in H$ se tiene

$$\phi(x-y) = \phi(x) - \phi(y) = x - y \quad \& \\ \phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = xy^{-1}.$$

(2) Se cumple que $H \subset G(L : \mathrm{Fix}(H))$, pues si $\phi \in H$ y $x \in \mathrm{Fix}(H)$ entonces $\phi(x) = x$.

(3) Si H es finito y $\mathrm{char}(L) = 0$, también es finita la extensión $L|\mathrm{Fix}(H)$ y además

$$[L : \mathrm{Fix}(H)] \leq \mathrm{ord}(H).$$

En efecto, escribimos $H := \{\phi_1, \ldots, \phi_n\}$ y vamos a demostrar en primer lugar que para cada $\alpha \in L$ el elemento $\sum_{i=1}^{n} \phi_i(\alpha) \in \mathrm{Fix}(H)$. En efecto, si $\phi \in H$ se cumple la igualdad

$$H = \{\phi_i \cdot \phi : \ 1 \leq i \leq n\},$$

por la Proposición I.1.3, vol. I. Ahora, para cada $\phi \in H$ se tiene

$$\phi\Big(\sum_{i=1}^{n} \phi_i(\alpha)\Big) = \sum_{i=1}^{n} \phi(\phi_i(\alpha)) = \sum_{i=1}^{n} (\phi_i \cdot \phi)(\alpha) = \sum_{j=1}^{n} \phi_j(\alpha).$$

Se trata de probar que $[L : \mathrm{Fix}(H)] \leq n$ y suponemos lo contrario. Existen por tanto $u_1, \ldots, u_{n+1} \in L$ que son $\mathrm{Fix}(H)$-linealmente independientes. Consideramos el sistema homogéneo de ecuaciones lineales con coeficientes en L

$$\begin{cases} \phi_1^{-1}(u_1)\mathtt{x}_1 + \cdots + \phi_1^{-1}(u_n)\mathtt{x}_n + \phi_1^{-1}(u_{n+1})\mathtt{x}_{n+1} = 0 \\ \quad \vdots \qquad\qquad\qquad \vdots \qquad\qquad \vdots \qquad\quad \vdots \\ \phi_n^{-1}(u_1)\mathtt{x}_1 + \cdots + \phi_n^{-1}(u_n)\mathtt{x}_n + \phi_n^{-1}(u_{n+1})\mathtt{x}_{n+1} = 0 \end{cases} \tag{2.2}$$

Como el rango de su matriz de coeficientes es $\leq n$, pues tiene n filas, y el número de incógnitas es $n+1$ se deduce del Teorema de Rouché que tiene una solución no nula $(x_1, \ldots, x_{n+1}) \in L^{n+1}$. Reordenando las variables si es preciso, y teniendo en cuenta que el sistema es homogéneo, podemos suponer que $x_{n+1} = 1$.

Si sustituimos $x_1, \ldots, x_n, x_{n+1} = 1$ en el sistema (2.2) y aplicamos ϕ_i a su fila i-ésima para $1 \leq i \leq n$, nos queda

$$\begin{cases} u_1\phi_1(x_1) + \cdots + u_n\phi_1(x_n) + u_{n+1} = 0 \\ \quad \vdots \qquad\qquad\qquad \vdots \qquad\qquad \vdots \qquad \vdots \\ u_1\phi_n(x_1) + \cdots + u_n\phi_n(x_n) + u_{n+1} = 0 \end{cases}$$

y sumando todas las ecuaciones tenemos

$$\lambda_1 u_1 + \cdots + \lambda_n u_n + n u_{n+1} = 0$$

donde, por lo visto anteriormente, $\lambda_j := \sum_{i=1}^{n} \phi_i(x_j) \in \mathrm{Fix}(H)$ para $1 \leq j \leq n$. Esto es imposible porque $n \neq 0$, ya que $\mathrm{Fix}(H))$ es un cuerpo de característica 0, y $u_1, \ldots, u_{n+1}$ son $\mathrm{Fix}(H)$-linealmente independientes.

(4) Si $\mathrm{char}(L) = 0$ y el subgrupo H es finito, entonces $L|\mathrm{Fix}(H)$ es una extensión de Galois y $G(L : \mathrm{Fix}(H)) = H$.

En efecto la extensión finita $L|\mathrm{Fix}(H)$ es simple, ya que $\mathrm{Fix}(H)$ tiene característica 0, luego aplicando (2), (3) y IV.1.4 (2) se tiene

$$[L : \mathrm{Fix}(H)] \leq \mathrm{ord}(H) \leq \mathrm{ord}(G(L : \mathrm{Fix}(H))) \leq [L : \mathrm{Fix}(H)].$$

Esto demuestra que $\mathrm{ord}(G(L : \mathrm{Fix}(H))) = [L : \mathrm{Fix}(H)]$, es decir, $L|\mathrm{Fix}(H)$ es una extensión de Galois y, además, $H = G(L : \mathrm{Fix}(H))$.

(5) Sea $L|K$ una extensión de modo que $\mathrm{char}(K) = 0$ y H es un subgrupo de $G(L : K)$. Por ello $K \subset \mathrm{Fix}(H)$ y para calcular el grado de la extensión $\mathrm{Fix}(H)|K$ basta observar que

$$[\mathrm{Fix}(H) : K] = \frac{[L : K]}{[L : \mathrm{Fix}(H)]} = \frac{[L : K]}{\mathrm{ord}(G(L : \mathrm{Fix}(H))} = \frac{[L : K]}{\mathrm{ord}(H)}.$$

Corolario IV.2.2 *Sea $H = G(L : K)$ el grupo de automorfismos de una extensión finita $L|K$ de cuerpos de característica 0. Entonces, las siguientes afirmaciones son equivalentes:*

(1) *La extensión $L|K$ es de Galois.*

(2) *Se tiene la igualdad $K = \mathrm{Fix}(H)$.*

Demostración. (1) $\Longrightarrow$ (2) Nótese que $K \subset F := \mathrm{Fix}(H) \subset L$ y que, como la extensión $L|K$ es de Galois, también $L|F$ lo es, por IV.2.1 (4). Como además $H = G(L : F)$ se tiene

$$\begin{aligned} \mathrm{ord}(G(L : K)) &= [L : K] = [L : F] \cdot [F : K] = \mathrm{ord}(G(L : F)) \cdot [F : K] \\ &= \mathrm{ord}(H) \cdot [F : K] = \mathrm{ord}(G(L : K)) \cdot [F : K] \end{aligned}$$

y, por tanto, $[F : K] = 1$ o, equivalentemente, $\mathrm{Fix}(H) = F = K$.

(2) $\Longrightarrow$ (1) Esta implicación se vió en IV.2.1 (4). □

2.b. Teorema fundamental de la teoría de Galois. A continuación demostraremos en dos etapas el Teorema fundamental de la Teoría de Galois para extensiones de Galois de cuerpos de característica 0.

Teorema IV.2.3 (Parte 1ª del Teorema fundamental) *Sea $L|K$ una extensión de Galois de cuerpos de característica 0. Entonces, las aplicaciones*

$$E|K \mapsto G(L:E) \quad \& \quad H \mapsto \mathrm{Fix}(H)|K$$

entre el conjunto de subextensiones de $L|K$ y el de subgrupos del grupo de Galois $G(L:K)$, son mutuamente inversas. Además,

$$[E:K] \cdot \mathrm{ord}(G(L:E)) = [L:K].$$

Demostración. Observamos que $G(L:E)$ es subgrupo de $G(L:K)$ para cada subextensión $E|K$ de $L|K$, porque si $\phi : L \to L$ es un automorfismo cuya restricción $\phi|_E$ es la identidad, entonces $\phi|_K = \mathrm{id}_K$ ya que $K \subset E$. Así, la aplicación

$$E|K \mapsto G(L:E)$$

está bien definida y comprobemos ahora que la aplicación $H \mapsto \mathrm{Fix}(H)|K$, donde H denota un subgrupo de $G(L:K)$, es su inversa.

En primer lugar hemos de probar que dados una subextensión $E|K$ de $L|K$, el subgrupo $H := G(L:E)$ de $G(L:K)$ y el subcuerpo $F := \mathrm{Fix}(H)$ de L, se tiene $F = E$. La inclusión $E \subset F$ es evidente, pues $\phi|_E = \mathrm{id}_E$ para cada $\phi \in H$. Además, por el Corolario IV.1.7, $L|E$ es una extensión de Galois, mientras que por IV.2.1 (4), $L|F$ es una extensión de Galois con grupo de Galois H, es decir, $G(L:F) = H = G(L:E)$. En consecuencia,

$$[L:E] = \mathrm{ord}(G(L:E)) = \mathrm{ord}(G(L:F)| = [L:F],$$

así que $[F:E] = [L:E]/[L:F] = 1$, luego $E = F$. Sean ahora H un subgrupo de $G(L:K)$ y $F := \mathrm{Fix}(H)$. Por IV.2.1 (4), $H = G(L:F)$, y queda probado que las aplicaciones

$$H \mapsto \mathrm{Fix}(H)|K \quad \& \quad E|K \mapsto G(L:E)$$

son mutuamente inversas. Por último, en IV.2.1 (5) se demostró la igualdad

$$[E:K] \cdot \mathrm{ord}(G(L:E)) = [L:K].$$

□

Teorema IV.2.4 (Parte 2ª del Teorema fundamental) *Sea $L|K$ una extensión de Galois de cuerpos de característica 0 y sea $E|K$ una subextensión de $L|K$. Las siguientes afirmaciones son equivalentes:*

(1) *$E|K$ es una subextensión de Galois de $L|K$.*

(2) *$\phi(E) \subset E$ para cada $\phi \in G(L:K)$.*

(3) *$G(L:E)$ es un subgrupo normal de $G(L:K)$.*

Además, si éste es el caso, $G(E:K) \cong G(L:K)/G(L:E)$.

Demostración. Comprobaremos que se cumple la siguiente cadena de implicaciones:

$$(1) \Longrightarrow (2) \Longrightarrow (3) \Longrightarrow (2) \Longrightarrow (1).$$

(1) $\Longrightarrow$ (2) Por el Teorema del elemento primitivo II.2.2 existe $\alpha \in E$ tal que $E = K(\alpha)$. Sea $f := P_{K,\alpha}$ el polinomio mínimo de α sobre K. Como la extensión $E|K$ es de Galois y f tiene una raíz en E entonces, por la Proposición IV.1.6, f factoriza en $E[\mathtt{t}]$ como producto de factores de grado 1.

Cada $\phi \in G(L:K)$ induce, por restricción, un isomorfismo $\phi|_E : E \to \phi(E)$ que es la identidad sobre K. Por el Lema II.1.1, $\beta := \phi(\alpha)$ es raíz de f en L y, como acabamos de señalar, pertenece a E. Por tanto, $\phi(E) = K(\beta) \subset E$.

(2) $\Longrightarrow$ (3) Denotamos $H := G(L:E)$ y hemos de comprobar que $\phi^{-1}H\phi \subset H$ para cada $\phi \in G(L:K)$, es decir, que $(\phi^{-1}\psi\phi)(\alpha) = \alpha$ para cada $\psi \in H$ y cada $\alpha \in E$. Pero $\phi^{-1}(\alpha) \in E$ ya que $\phi^{-1}(E) \subset E$, luego $\psi(\phi^{-1}(\alpha)) = \phi^{-1}(\alpha)$, por lo que

$$(\phi^{-1}\psi\phi)(\alpha) = \phi(\psi(\phi^{-1}(\alpha))) = \phi(\phi^{-1}(\alpha)) = \alpha.$$

(3) $\Longrightarrow$ (2) Dado $\phi \in G(L:K)$ tenemos que comprobar que $\phi(E) \subset E$ y para ello, puesto que la primera parte del Teorema fundamental IV.2.3 implica que $E = \mathrm{Fix}(H)$, donde $H := G(L:E)$, basta con demostrar que $\psi(\phi(\alpha)) = \phi(\alpha)$ para cada $\alpha \in E$ y cada $\psi \in H$. Pero esto es equivalente a probar que para cada $\psi \in H$ se cumple que $(\phi^{-1} \circ \psi \circ \phi)|_E = \mathrm{id}_E$, es decir, $\phi \cdot \psi \cdot \phi^{-1} \in G(L:E)$, lo que es cierto porque $G(L:E)$ es, por hipótesis, subgrupo normal de $G(L:K)$.

(2) $\Longrightarrow$ (1) Para probar que la extensión $E|K$ es de Galois tenemos que demostrar que $[E:K] = \mathrm{ord}(G(E:K))$. Como $\phi(E) \subset E$ para cada $\phi \in G(L:K)$, también $\phi^{-1}(E) \subset E$, ya que $\phi^{-1} \in G(L:K)$, y por tanto

$$E = \phi(\phi^{-1}(E)) \subset \phi(E) \subset E.$$

En conclusión, $\phi|_E \in G(E:K)$ para cada $\phi \in G(L:K)$. Por ello la aplicación

$$\Psi : G(L:K) \to G(E:K),\ \phi \mapsto \phi|_E$$

es un homomorfismo de grupos cuyo núcleo está formado por aquellos automorfismos de L cuya restricción a E es id_E, es decir, $\ker \Psi = G(L : E)$. Por el Primer teorema de isomorfia de grupos, II.2.4, vol. I,

$$\operatorname{im} \Psi \cong G(L : K)/G(L : E),$$

y como tanto $L|K$ como $L|E$ son extensiones de Galois,

$$\begin{aligned}[L : E] \cdot [E : K] = [L : K] &= \operatorname{ord}(G(L : K)) = \operatorname{ord}(G(L : E)) \cdot \operatorname{ord}(\operatorname{im} \Psi) \\ &\leq \operatorname{ord}(G(L : E)) \cdot \operatorname{ord}(G(E : K)) = [L : E] \cdot \operatorname{ord}(G(E : K)).\end{aligned} \tag{2.3}$$

Simplificando se tiene $[E : K] \leq \operatorname{ord}(G(E : K))$, y la desigualdad

$$\operatorname{ord}(G(E : K)) \leq [E : K]$$

se cumple por IV.1.4 (2), así que $[E : K] = \operatorname{ord}(G(E : K))$, lo que prueba que la extensión $E|K$ es de Galois. Además esto demuestra que la desigualdad en (2.3) es una igualdad, de donde $\operatorname{im} \Psi = G(E : K)$. Por ello, los grupos $G(E : K)$ y $G(L : K)/G(L : E)$ son isomorfos. □

Corolario IV.2.5 *Sean K un cuerpo de característica cero y $E_1|K$ y $E_2|K$ dos extensiones de Galois. Denotamos $\overline{K}$ un cierre algebraico de K que contiene a E_1 y E_2, $L := E_1 \cap E_2$ y F el menor subcuerpo de $\overline{K}$ que contiene a E_1 y E_2. Entonces la extensión $F|K$ es de Galois y se cumple la igualdad*

$$[F : K] \cdot [L : K] = [E_1 : K] \cdot [E_2 : K].$$

Demostración. Por IV.1.6 existen polinomios irreducibles $f_1, f_2 \in K[\mathtt{t}]$ tales que E_i es el cuerpo de descomposición de f_i sobre K para $i = 1, 2$. Factorizamos

$$f_1(\mathtt{t}) = (\mathtt{t} - \alpha_1) \cdots (\mathtt{t} - \alpha_r) \quad \& \quad f_2(\mathtt{t}) = (\mathtt{t} - \beta_1) \cdots (\mathtt{t} - \beta_s),$$

de modo que cada $\alpha_k \in E_1$ y cada $\beta_\ell \in E_2$. De hecho se tienen las igualdades

$$E_1 = K(\alpha_1, \ldots, \alpha_r) \quad \& \quad E_2 = K(\beta_1, \ldots, \beta_s),$$

lo que implica que F es el cuerpo de descomposición de $f_1 \cdot f_2$ sobre K, ya que

$$F = K(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s) \quad \& \quad f_1(\mathtt{t}) f_2(\mathtt{t}) = \prod_{i=1}^{r} (\mathtt{t} - \alpha_i) \cdot \prod_{j=1}^{s} (\mathtt{t} - \beta_j).$$

Se deduce de IV.1.6 que la extensión $F|K$ es de Galois. Para la segunda parte, y puesto que cada $E_i|K$ es una subextensión de Galois de $F|K$, se desprende de la segunda parte del Teorema fundamental de la teoría de Galois que existen subgrupos normales H_1 y H_2 del grupo $G := G(F:K)$ tales que $E_i = \mathrm{Fix}(H_i)$ para $i = 1, 2$, y $[F : E_i] = \mathrm{ord}(H_i)$. Además, puesto que $H_1 \cap H_2 \subset H_i$, cada

$$E_i = \mathrm{Fix}(H_i) \subset \mathrm{Fix}(H_1 \cap H_2) \subset F,$$

luego $\mathrm{Fix}(H_1 \cap H_2) = F = \mathrm{Fix}\{\mathrm{id}_F\}$, y por la primera parte del Teorema fundamental de la teoría de Galois, $H_1 \cap H_2 = \{\mathrm{id}_F\}$. Por otro lado, como H_1 y H_2 son subgrupos normales de G el producto H_1H_2 es subgrupo de G, por II.1.1 (3), vol. I, y de hecho $L = \mathrm{Fix}(H_1H_2)$. En efecto, como cada $H_i \subset H_1H_2$ se cumple $\mathrm{Fix}(H_1H_2) \subset \mathrm{Fix}(H_i) = E_i$, así que $\mathrm{Fix}(H_1H_2) \subset E_1 \cap E_2 = L$. Recíprocamente, sean $x \in L$ y $\varphi \in H_1H_2$. Existen por tanto $\varphi_1 \in H_1$ y $\varphi_2 \in H_2$ tales que $\varphi = \varphi_1 \cdot \varphi_2$, luego

$$\varphi(x) = \varphi_2(\varphi_1(x)) = \varphi_2(x) = x,$$

es decir, $x \in \mathrm{Fix}(H_1H_2)$. Como $\mathrm{ord}(H_1H_2) = \mathrm{ord}(H_1) \cdot \mathrm{ord}(H_2)$ se tiene,

$$\begin{aligned}
[E_1 : K] \cdot [E_2 : K] &= \frac{[F:K]}{[F:E_1]} \cdot \frac{[F:K]}{[F:E_2]} = \frac{[F:K]}{[F:\mathrm{Fix}(H_1)]} \cdot \frac{[F:K]}{[F:\mathrm{Fix}(H_2)]} \\
&= \frac{[F:K]}{\mathrm{ord}(H_1)} \cdot \frac{[F:K]}{\mathrm{ord}(H_2)} = \frac{[F:K] \cdot [F:K]}{\mathrm{ord}(H_1H_2)} \\
&= \frac{[F:K] \cdot [F:K]}{[F:\mathrm{Fix}(H_1H_2)]} = [F:K] \cdot \frac{[F:K]}{[F:L]} = [F:K] \cdot [L:K].
\end{aligned}$$

□

Empleamos a continuación el Teorema fundamental para calcular, en un par de casos muy sencillos, las subextensiones de una extensión de Galois dada.

Ejemplos IV.2.6 (1) Vimos en el Ejemplo IV.1.9 que si $L := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ la extensión $L|\mathbb{Q}$ es de Galois y su grupo de Galois $G(L:\mathbb{Q})$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Vamos a determinar las subextensiones propias de $L|\mathbb{Q}$. Todo subgrupo propio de $\mathbb{Z}_2 \times \mathbb{Z}_2$ tiene orden 2. Como $\mathbb{Z}_2 \times \mathbb{Z}_2$ tiene, exactamente, tres elementos distintos del neutro posee, exactamente, tres subgrupos propios, todos de orden 2. Por la primera parte del Teorema fundamental deducimos que $L|\mathbb{Q}$ tiene, exactamente, tres subextensiones propias $E|\mathbb{Q}$, todas de grado 2, pues

$$[E:\mathbb{Q}] = [L:\mathbb{Q}]/2 = 4/2 = 2.$$

Por simple inspección se advierte que $\sqrt{2}, \sqrt{3}$ y $\sqrt{6}$ pertenecen a L y ninguno de ellos es un número racional, luego

$$\mathbb{Q}(\sqrt{2})|\mathbb{Q}, \quad \mathbb{Q}(\sqrt{3})|\mathbb{Q} \quad \& \quad \mathbb{Q}(\sqrt{6})|\mathbb{Q}$$

son subextensiones propias de $L|\mathbb{Q}$ y, por lo anterior, son todas. Más aún, estas tres extensiones son de Galois. Un argumento es que tienen grado 2, y basta aplicar IV.1.5 (3). Otro modo de verlo es apelar a la segunda parte del Teorema fundamental, ya que al ser $G(L : \mathbb{Q})$ un grupo abeliano todos sus subgrupos son normales.

(2) En el Ejemplo IV.1.11 vimos que si $\alpha := \sqrt[3]{2}$ es el único número real cuyo cubo es 2 y $\zeta := e^{2\pi i/3}$, la extensión $L|\mathbb{Q}$ es de Galois, donde $L := \mathbb{Q}(\alpha, \zeta)$. Además probamos que $G(L : \mathbb{Q}) = \mathcal{S}_3$, el grupo simétrico de orden 6. Esto, junto con el Teorema fundamental, permite calcular elementos primitivos de las subextensiones de $L|\mathbb{Q}$.

El grupo $\mathcal{S}_3$ posee, exactamente, 3 subgrupos de orden 2, generados por las transposiciones $(1, 2)$, $(1, 3)$ y $(2, 3)$. Ninguno de ellos es normal, por lo que existen, exactamente, tres subextensiones de grado $6/2 = 3$ de $L|\mathbb{Q}$, y ninguna de ellas es de Galois. Como $\alpha, \alpha\zeta$ y $\alpha\zeta^2$ pertenecen a L y tienen a $\mathtt{t}^3 - 2$ por polinomio mínimo, las subextensiones de grado 3 de $L|\mathbb{Q}$ son

$$\mathbb{Q}(\alpha)|\mathbb{Q}, \quad \mathbb{Q}(\alpha\zeta)|\mathbb{Q} \quad \& \quad \mathbb{Q}(\alpha\zeta^2)|\mathbb{Q},$$

y ninguna de ellas es de Galois. Por otro lado, $\mathcal{S}_3$ posee un único subgrupo de orden 3, formado por la identidad y los 3-ciclos $(1, 2, 3)$ y $(1, 3, 2)$. En consecuencia existe una única subextensión de $L|\mathbb{Q}$ de grado $6/3 = 2$, que necesariamente es de Galois. Dicha subextensión es $\mathbb{Q}(\zeta)|\mathbb{Q}$, ya que

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(P_{\mathbb{Q},\zeta}) = \deg(\mathtt{t}^2 + \mathtt{t} + 1) = 2,$$

Ejercicios y problemas propuestos

Número IV.1 Sea α la raíz séptima real de 5. ¿Cuáles de las siguientes extensiones son de Galois?

$$\mathbb{Q}(\alpha)|\mathbb{Q}, \quad \mathbb{Q}(\sqrt{5}, \alpha)|\mathbb{Q}(\alpha), \quad \mathbb{Q}(\sqrt{-5})|\mathbb{Q} \quad \& \quad \mathbb{R}(\sqrt{-7})|\mathbb{R}.$$

Número IV.2 Sea $E := \mathbb{Q}(r)$, donde $r := \sqrt[4]{2}$ es el único número real positivo cuya potencia cuarta vale 2. ¿Existen números reales α y β tales que

$$\mathbb{Q}(\alpha) \neq E \neq \mathbb{Q}(\beta) \quad \& \quad E = \mathbb{Q}(\alpha, \beta)?$$

Número IV.3 Sean $E \subset \mathbb{R}$ un cuerpo que contiene a $\mathbb{Q}$ de modo que la extensión $E|\mathbb{Q}$ es de Galois, y $F := E(\sqrt{-1})$. ¿Se puede asegurar que la extensión $F|\mathbb{Q}$ es también de Galois?

Número IV.4 Sean $L|K$ una extensión algebraica y $\phi : L \to L$ un homomorfismo de cuerpos tal que $\phi|_K = \mathrm{id}_K$. Demostrar que $\phi \in G(L : K)$, esto es, que ϕ es un automorfismo.

Número IV.5 Sean K un cuerpo de característica 0 y $E|K$ y $F|K$ dos subextensiones de Galois de la extensión $L|K$. Demostrar que $(E \cap F)|K$ es extensión de Galois.

Número IV.6 Sean $L|K$ una extensión de Galois y $\alpha \in L$ tal que el único automorfismo de L que deja fijo α es la identidad. Demostrar que $L = K(\alpha)$.

Número IV.7 Sean K un cuerpo y $\mathtt{t}$ una indeterminada sobre K.

(1) Demostrar que las siguientes afirmaciones son equivalentes, en cuyo caso se dice que K posee la *propiedad de la extensión:*

(1.1) Cada automorfismo de $K(\mathtt{t})$ es extensión de un automorfismo de K.

(1.2) Para cada automorfismo $\varphi : K(\mathtt{t}) \to K(\mathtt{t})$ se cumple que $\varphi(K) = K$.

(1.3) Para cada automorfismo $\varphi : K(\mathtt{t}) \to K(\mathtt{t})$ se cumple que $\varphi(K) \subset K$.

(2) Sea K un cuerpo en el que cada uno de sus elementos es, bien un cuadrado bien el opuesto de un cuadrado. Demostrar que K posee la propiedad de la extensión. Deducir que los cuerpos algebraicamente cerrados tienen la propiedad de la extensión.

(3) Sea K un cuerpo en el que el polinomio $f(\mathtt{t}) := \mathtt{t}^2 + 1$ no tiene raíces. Sea $i := \sqrt{-1}$ una raíz de f en un cierre algebraico de K, y supongamos que $K(i)$ es un cuerpo algebraicamente cerrado. Probar que cada elemento de K es, un cuadrado o el opuesto de un cuadrado y, por tanto, posee la propiedad de la extensión. Deducir que $G(\mathbb{R}(\mathtt{t}) : \mathbb{R}) = \mathrm{Aut}(\mathbb{R}(\mathtt{t}))$.

(4) Demostrar que toda extensión algebraica de $\mathbb{Q}$ posee la propiedad de la extensión.

(5) Encontrar un cuerpo que no posee la propiedad de la extensión.

Número IV.8 Sea $L|K$ una extensión de Galois y consideremos, para cada automorfismo $\sigma \in G(L : K)$, el homomorfismo de anillos

$$\widehat{\sigma} : L[\mathtt{t}] \to L[\mathtt{t}],\ \sum_{i=0}^{d} a_i \mathtt{t}^i \mapsto \sum_{i=0}^{d} \sigma(a_i)\mathtt{t}^i.$$

(1) Probar que un polinomio $h \in L[\mathtt{t}]$ pertenece a $K[\mathtt{t}]$ si y sólo si $\widehat{\tau}(h) = h$ para cada $\tau \in G(L : K)$.

(2) Demostrar que para cada $g \in L[\mathtt{t}]$ se cumple que $\widehat{g} := \prod_{\sigma \in G(L:K)} \widehat{\sigma}(g) \in K[\mathtt{t}]$.

(3) Sean $f(\mathtt{t}) = \mathtt{t}^n + \sum_{j=0}^{n-1} b_j \mathtt{t}^j \in L[\mathtt{t}]$ un polinomio mónico y $L = K(b_0, \ldots, b_{n-1})$. Demostrar que si $\sigma, \tau \in G(L : K)$ son distintos, entonces $\widehat{\sigma}(f) \neq \widehat{\tau}(f)$, y probar que si $\widehat{f}$ es irreducible en $K[\mathtt{t}]$, entonces f es irreducible en $L[\mathtt{t}]$.

(4) Probar que para cada $n \in \mathbb{Z}^+$ el polinomio $f_n(\mathtt{t}) = \mathtt{t}^n - \sqrt{2}$ es irreducible en $\mathbb{Q}(\sqrt{2})[\mathtt{t}]$.

Número IV.9 Dada una extensión de Galois $L|K$ de cuerpos de característica 0 denotamos $G := G(L:K)$ su grupo de Galois y fijamos $u \in L$. Definimos el polinomio

$$f(\mathtt{t}) := \prod_{\phi \in G} (\mathtt{t} - \phi(u)).$$

(1) Probar que f pertenece a $K[\mathtt{t}]$ y es potencia del polinomio mínimo de u sobre K.

(2) Probar que f es irreducible en $K[\mathtt{t}]$ si y sólo si u es elemento primitivo de $L|K$.

Número IV.10 Sean K un cuerpo, $f \in K[\mathtt{t}]$ un polinomio de grado n y E un cuerpo de descomposición de f sobre K en el que f posee n raíces distintas $\xi_1, \ldots, \xi_n$. Demostrar que para cada polinomio $p \in K[\mathtt{t}]$ existe otro $g \in K[\mathtt{t}]$ de grado n del que son raíces $\{p(\xi_i) : 1 \le i \le n\}$.

Número IV.11 Sean $\alpha := e^{\pi i/3}$ y β una raíz del polinomio $f(\mathtt{t}) := \mathtt{t}^4 - 6\mathtt{t}^2 + 6$. Encontrar generadores de la clausura de Galois $L|\mathbb{Q}$ de las siguientes extensiones y calcular en cada caso el grado de $L|\mathbb{Q}$:

$$\mathbb{Q}(\sqrt[4]{3})|\mathbb{Q}, \quad \mathbb{Q}(\alpha)|\mathbb{Q}, \quad \mathbb{Q}(\beta)|\mathbb{Q} \quad \& \quad \mathbb{Q}(\sqrt[5]{2})|\mathbb{Q}.$$

Número IV.12 Sean $A := \mathbb{Z}[\sqrt{2}]$, $\xi := e^{\pi i/5}$, donde $i := \sqrt{-1} \in \mathbb{C}$, y $L \subset \mathbb{C}$ un cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^{10} - 2$. Se pide:

(1) Hallar el polinomio mínimo de ξ sobre $\mathbb{Q}$ y estudiar si es irreducible en $A[\mathtt{t}]$.

(2) Encontrar el polinomio mínimo de $\sqrt[10]{2}$ sobre $\mathbb{Q}$ y factorizarlo en producto de polinomios irreducibles en el anillo $A[\mathtt{t}]$.

(3) Calcular el grado $n := [L:\mathbb{Q}]$ de la extensión $L|\mathbb{Q}$.

(4) Probar que para cada divisor positivo d de n la extensión $L|\mathbb{Q}$ admite alguna subextensión de grado d.

(5) ¿Cuántas subextensiones $E|\mathbb{Q}$ de $L|\mathbb{Q}$ tienen grado 8? ¿Cuántas tienen grado 5?

(6) ¿Es abeliano el grupo de Galois $G(L:\mathbb{Q})$?

Número IV.13 (1) Sea G un grupo abeliano de orden ocho tal que el orden máximo de los elementos de G es cuatro. Demostrar que G es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_4$ y calcular cuántos subgrupos tiene de cada orden.

(2) Sean $\xi := e^{\pi i/10}$, $\eta := \xi^4$, $i := \sqrt{-1}$ y $u := \eta + \eta^{-1}$. Calcular el polinomio mínimo de u sobre $\mathbb{Q}$ y decidir si el cuerpo $\mathbb{Q}(u)$ contiene a i.

(3) Demostrar que $\mathbb{Q}(\xi) = \mathbb{Q}(i, \eta)$, que $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{5})$ y que $[\mathbb{Q}(\xi) : \mathbb{Q}] = 8$. Calcular el polinomio mínimo de ξ sobre $\mathbb{Q}$.

(4) Probar que el grupo de Galois $G(\mathbb{Q}(\xi) : \mathbb{Q})$ es abeliano y encontrar generadores sobre $\mathbb{Q}$ de las subextensiones de $\mathbb{Q}(\xi)|\mathbb{Q}$.

(5) Sea E el cuerpo de descomposición sobre $\mathbb{Q}(\xi)$ del polinomio $f(\mathtt{t}) := \mathtt{t}^4 - 5$. Probar que la extensión $E|\mathbb{Q}$ es de Galois, calcular su grado y decidir si $G(E:\mathbb{Q})$ es o no abeliano.

Número IV.14 Sean $p \in \mathbb{Z}$ primo y L un cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^4 - p$. Probar que el grupo de Galois $G(L : \mathbb{Q})$ es isomorfo al grupo diedral $\mathcal{D}_4$ de orden 8 y calcular elementos primitivos de todas las subextensiones $E|\mathbb{Q}$ de $L|\mathbb{Q}$.

Número IV.15 (1) Probar que $h(\mathtt{t}) := \mathtt{t}^4 + 1$ es un polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$.

(2) Sea L un cuerpo de descomposición de h sobre $\mathbb{Q}$. Encontrar un elemento primitivo de la extensión $L|\mathbb{Q}$.

(3) ¿Cuál es el orden del grupo de Galois $G(L : \mathbb{Q})$? Demostrar que es abeliano y calcular sus coeficientes de torsión.

(4) Encontrar elementos primitivos de todas las subextensiones no triviales de $L|\mathbb{Q}$ y determinar cuáles son de Galois.

Número IV.16 (1) Probar que los polinomios $g(\mathtt{t}) := \mathtt{t}^2+4$, $h(\mathtt{t}) := \mathtt{t}^3+4$ y $f(\mathtt{t}) := \mathtt{t}^6+4$ son irreducibles en $\mathbb{Q}[\mathtt{t}]$.

(2) Demostrar que $L := \mathbb{Q}(\sqrt{3}, i, \sqrt[3]{2})$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$.

(3) Calcular el grado de la extensión $L|\mathbb{Q}$.

(4) ¿Cuál es el orden del grupo de Galois $G(L : \mathbb{Q})$? Probar que es un grupo diedral.

(5) Encontrar generadores de todas las subextensiones no triviales de $L|\mathbb{Q}$ y determinar cuáles son de Galois.

Número IV.17 Sean K un cuerpo de característica 0 tal que todo polinomio de $K[\mathtt{t}]$ de grado impar tiene alguna raíz en K, y $L|K$ una extensión de Galois. Demostrar que el orden del grupo de Galois $G(L : K)$ es potencia de 2.

Número IV.18 Sean $\overline{K}$ un cierre algebraico de un cuerpo K de característica 0 y un automorfismo $\sigma \in G(\overline{K} : K)$. Probar que el conjunto

$$E := \{x \in \overline{K} : \sigma(x) = x\}$$

es un subcuerpo de $\overline{K}$ que contiene a K y que toda extensión finita $L|E$ es de Galois y cíclica, esto es, su grupo de Galois $G(L : E)$ es un grupo cíclico.

Número IV.19 Sean E_1 y E_2 dos subcuerpos de $\mathbb{C}$ tales que las extensiones $E_1|\mathbb{Q}$ y $E_2|\mathbb{Q}$ son de Galois y $G(E_1 : \mathbb{Q}) \cong \mathbb{Z}_6 \cong G(E_2 : \mathbb{Q})$. Supongamos además que $[E_1 \cap E_2 : \mathbb{Q}] = 2$.

(1) Sea F el menor subcuerpo de $\mathbb{C}$ que contiene a E_1 y E_2. ¿Es de Galois la extensión $F|\mathbb{Q}$? ¿Cuál es su grado?

(2) Demostrar que el grupo de Galois $G(F : \mathbb{Q})$ es abeliano. Calcular sus coeficientes de torsión. ¿Cuántas subextensiones propias y no triviales tiene $F|\mathbb{Q}$?

CAPÍTULO V

Cuerpos finitos

En la primera sección de este capítulo se estudian las extensiones de cuerpos finitos, demostrando para dichas extensiones algunos resultados obtenidos en los capítulos anteriores para cuerpos de característica 0. En la sección segunda se demuestra la *Ley de reciprocidad cuadrática,* que permite estudiar la resolubilidad de ecuaciones de grado dos en una variable sobre los cuerpos $\mathbb{Z}_p$. Para cada cuerpo K denotamos $K^* := K \setminus \{0\}$ y $K^{*2} := \{x^2 : x \in K^*\}$.

1. Extensiones de cuerpos finitos

Comenzamos demostrando que el número de elementos de cualquier cuerpo finito es una potencia de su característica y que dos cuerpos finitos con el mismo número de elementos son isomorfos. Calculamos después, para cada primo p y cada entero positivo n, el número de polinomios mónicos e irreducibles de grado n con coeficientes en el cuerpo con p elementos.

A continuación obtenemos para extensiones de cuerpos finitos varios resultados (algunos de ellos más fuertes) probados en los capítulos precedentes para extensiones finitas de cuerpos de característica 0. Por ejemplo, toda extensión finita de cuerpos finitos es simple, el grupo de Galois $G(L : K)$ de una extensión de cuerpos finitos $L|K$ es cíclico y su orden coincide con el grado $[L : K]$ de la extensión. De esto se desprende el Teorema fundamental de la teoría de Galois para estas extensiones, V.1.13.

1.a. Número de elementos de un cuerpo finito. Nuestro primer objetivo es demostrar que el número de elementos de un cuerpo finito es una potencia de sus característica.

Observaciones V.1.1 (1) Sean p un número primo y $f \in \mathbb{Z}_p[\mathtt{t}]$ un polinomio irreducible de grado n. El cociente $L := \mathbb{Z}_p[\mathtt{t}]/(f)$ es un $\mathbb{Z}_p$-espacio vectorial

de dimensión n luego es isomorfo, como $\mathbb{Z}_p$-espacio vectorial, a $\mathbb{Z}_p^n$, por lo que $\mathrm{Card}(L) = p^n$.

(2) Vamos a demostrar que si K es un cuerpo finito con q elementos, el anillo $K[\mathtt{t}]$ contiene un polinomio irreducible f de grado 2, lo que por el apartado anterior prueba que el cuerpo $L := K[\mathtt{t}]/(f)$ tiene q^2 elementos. En particular, aplicando esto con $K = \mathbb{Z}_p$ y $q = p$, deducimos la existencia de un cuerpo con p^2 elementos.

Por ser $K[\mathtt{t}]$ un DFU, los polinomios mónicos reducibles de grado 2 en $K[\mathtt{t}]$ son los productos $(\mathtt{t} - a)(\mathtt{t} - b)$, donde $a, b \in K$. Si $a = b$ hay q polinomios de esta forma, mientras que el número de ellos con $a \neq b$ es $\binom{q}{2}$, puesto que $(\mathtt{t}-a)(\mathtt{t}-b) = (\mathtt{t}-b)(\mathtt{t}-a)$. Así, el número de polinomios mónicos reducibles de grado 2 en $K[\mathtt{t}]$ es $q + \binom{q}{2}$, luego el de polinomios mónicos irreducibles de grado 2 en $K[\mathtt{t}]$ es

$$q^2 - q - \binom{q}{2} = \binom{q}{2} \geq 1.$$

(3) En el Corolario V.1.5 probaremos que fijados un número primo p y un entero positivo n existe un polinomio irreducible $f \in \mathbb{Z}_p[\mathtt{t}]$ de grado n, por lo que el cuerpo $L := \mathbb{Z}_p[\mathtt{t}]/(f)$ tiene, exactamente, p^n elementos.

(4) Vimos en el Ejemplo I.1.2 que si L es un cuerpo finito existe un número primo p tal que $\mathbb{Z}_p$ es el cuerpo primo de L y $L|\mathbb{Z}_p$ es una extensión finita por ser L finito. Si $n := [L : \mathbb{Z}_p]$, el cuerpo L es isomorfo, como $\mathbb{Z}_p$-espacio vectorial, a $\mathbb{Z}_p^n$ por lo que $\mathrm{Card}(L) = p^n$.

(5) Sean L un cuerpo finito y $n \geq 1$ un entero. Entonces, existen un entero $m \geq n$ y un polinomio mónico e irreducible $f \in L[\mathtt{t}]$ de grado m. En efecto, como L es finito con, digamos, q elementos, el anillo $L[\mathtt{t}]$ contiene q^d polinomios mónicos de grado d, luego el número de polinomios mónicos e irreducibles de $L[\mathtt{t}]$ de grado menor o igual que n es finito. Sin embargo, vimos en el Lema VI.2.1, vol. II, que $L[\mathtt{t}]$ contiene infinitos polinomios mónicos e irreducibles, luego el grado m de alguno de ellos es mayor que n. Nótese que el cociente $L[\mathtt{t}]/(f)$ es un L-espacio vectorial de dimensión m, luego $\mathrm{Card}(L) = q^m$.

La existencia y unicidad del cuerpo de descomposición tiene interesantes consecuencias al tratar con cuerpos finitos, que recogemos en los siguientes resultados.

Teorema V.1.2 *Sea $f(\mathtt{t}) := \mathtt{t}^{p^n} - \mathtt{t} \in \mathbb{Z}_p[\mathtt{t}]$ donde p es un número primo, y n es un entero positivo. Entonces,*

(1) *Cada cuerpo de descomposición de f sobre $\mathbb{Z}_p$ tiene p^n elementos y todos ellos son raíces del polinomio f.*

(2) *Dos cuerpos con p^n elementos son isomorfos.*

Demostración. (1) Sea L un cuerpo de descomposición de f sobre $\mathbb{Z}_p$. Todas las raíces de f en L son simples, pues $f'(\mathtt{t}) = p^n\mathtt{t}^{p^n-1} - 1 = -1$ y $f(\mathtt{t})$ son primos entre sí en $\mathbb{Z}_p[\mathtt{t}]$. Vamos a demostrar que el conjunto $F := \{\alpha_1, \ldots, \alpha_{p^n}\}$ formado por las raíces de f en L es un subcuerpo de L. Es suficiente comprobar que $x - y,\ xy^{-1} \in F$ para cada par de elementos $x, y \in F$ con $y \neq 0$. Ahora bien, se deduce de VI.2.7 (3) vol. II, que

$$(x-y)^{p^n} = x^{p^n} + (-1)^{p^n}y^{p^n} = x - y \quad \& \quad (xy^{-1})^{p^n} = x^{p^n}(y^{p^n})^{-1} = xy^{-1},$$

y por tanto, $x - y$ y xy^{-1} son raíces de f, o lo que es lo mismo, elementos de F. El cálculo anterior es también válido si $p = 2$, pues entonces $-1 = 1$.

Como F es un cuerpo de característica p, contiene a $\mathbb{Z}_p$. Así, $F|\mathbb{Z}_p$ es una extensión de cuerpos y el polinomio $f \in \mathbb{Z}_p[\mathtt{t}]$ factoriza en $F[\mathtt{t}]$ en producto de factores de grado 1. Por la minimalidad del cuerpo de descomposición deducimos que $L \subset F$, luego $F = L$.

(2) Por la unicidad, salvo isomorfía, del cuerpo de descomposición de un polinomio sobre un cuerpo dado, Teorema II.1.2, basta probar que si F es un cuerpo con p^n elementos, entonces F es un cuerpo de descomposición sobre $\mathbb{Z}_p$ del polinomio $f(\mathtt{t}) := \mathtt{t}^{p^n} - \mathtt{t}$.

Ahora bien, el conjunto $F^* := F \setminus \{0\}$ es un grupo multiplicativo de orden $p^n - 1$, luego $\alpha^{p^n-1} = 1$ para cada $\alpha \in F^*$. Esto implica que $\alpha^{p^n} - \alpha = 0$, igualdad ésta que también cumple $\alpha = 0$. Por tanto, $f(\mathtt{t}) = \prod_{\alpha\in F}(\mathtt{t} - \alpha)$, lo que demuestra que F es un cuerpo de descomposición de f sobre $\mathbb{Z}_p$. □

Observaciones V.1.3 (1) La segunda parte del Teorema anterior afirma que si p es un número primo y n es un entero positivo podemos hablar del *cuerpo finito con p^n elementos,* que en adelante denotaremos por $\mathbb{F}_{p^n}$; en particular $\mathbb{F}_p := \mathbb{Z}_p$.

(2) Se deduce de I.1.2 (5) y V.1.1 (4) que $\mathbb{F}_p \subset \mathbb{F}_{p^n}$ y $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

(3) Si $\mathbb{F}_{q_1}|\mathbb{F}_{q_2}$ es una extensión de cuerpos finitos existen un número primo p y enteros positivos m y n tales que m divide a n y $q_2 = p^m$ y $q_1 = p^n$.

En efecto, por ser $\mathbb{F}_{q_2}$ finito su característica es $\mathrm{char}(\mathbb{F}_{q_2}) = p$ para algún número primo p. Esto implica que $\mathbb{F}_p \subset \mathbb{F}_{q_2} \subset \mathbb{F}_{q_1}$, luego tanto $\mathbb{F}_{q_2}$ como

$\mathbb{F}_{q_1}$ son $\mathbb{F}_p$-espacios vectoriales de dimensión finita, digamos $[\mathbb{F}_{q_2} : \mathbb{F}_p] = m$ y $[\mathbb{F}_{q_1} : \mathbb{F}_p] = n$. Por la Proposición I.1.6,

$$n = [\mathbb{F}_{q_1} : \mathbb{F}_p] = [\mathbb{F}_{q_1} : \mathbb{F}_{q_2}] \cdot [\mathbb{F}_{q_2} : \mathbb{F}_p] = [\mathbb{F}_{q_1} : \mathbb{F}_{q_2}] \cdot m,$$

luego m divide a n. Además, $\mathbb{F}_{q_2}$ es isomorfo a $\mathbb{F}_p^m$ como $\mathbb{F}_p$-espacio vectorial, luego tiene p^m elementos, o sea, $q_2 = p^m$, y $\mathbb{F}_{q_1}$ es isomorfo a $\mathbb{F}_p^n$, así que tiene $q_1 = p^n$ elementos.

(4) Si m y n son enteros positivos y m divide a n, entonces $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. En efecto, por el Teorema V.1.2 (1), basta probar que toda raíz α del polinomio $f(\mathtt{t}) := \mathtt{t}^{p^m} - \mathtt{t}$ también es raíz de $g(\mathtt{t}) := \mathtt{t}^{p^n} - \mathtt{t}$. Nótese que si $d := n/m$ se tiene $p^n = p^{md} = (p^m)^d$, y argumentamos por inducción sobre d. Si $d = 1$ nada hay que probar, y si suponemos $d \geq 2$ y probada nuestra afirmación para $d - 1$, es decir, $\alpha^{p^{m(d-1)}} = \alpha$, entonces $g(\alpha) = 0$, pues

$$\alpha^{p^n} = \alpha^{p^{md}} = \alpha^{p^{m(d-1)+m}} = \alpha^{p^{m(d-1)}p^m} = \left(\alpha^{p^{m(d-1)}}\right)^{p^m} = \alpha^{p^m} = \alpha.$$

Corolario V.1.4 *Sean p un número primo, n un entero positivo y consideremos el conjunto*

$$D(n) := \{d \in \mathbb{Z}^+ : d \text{ divide a } n\}.$$

Entonces, el polinomio $\mathtt{t}^{p^n} - \mathtt{t} \in \mathbb{F}_p[\mathtt{t}]$ es el producto de todos los polinomios mónicos e irreducibles de $\mathbb{F}_p[\mathtt{t}]$ cuyo grado $d \in D(n)$.

Demostración. Para cada $d \in D(n)$ denotamos Σ_d el conjunto de polinomios mónicos e irreducibles de $\mathbb{F}_p[\mathtt{t}]$ de grado d. Sea $\Sigma := \bigsqcup_{d \in D(n)} \Sigma_d$. Denotamos $h(\mathtt{t}) := \mathtt{t}^{p^n} - \mathtt{t}$ y hemos de probar que $h = \prod_{f \in \Sigma} f$.

Para demostrar que el producto $\prod_{f \in \Sigma} f$ divide a h en el dominio de factorización única $\mathbb{F}_p[\mathtt{t}]$ es suficiente demostrar que cada $f \in \Sigma$ divide a h. El polinomio f tiene una raíz $\alpha := \mathtt{t} + (f)$ en el cuerpo finito $L := \mathbb{F}_p[\mathtt{t}]/(f)$, y de hecho (f) es el núcleo del homomorfismo evaluación

$$\mathrm{ev}_\alpha : \mathbb{F}_p[\mathtt{t}] \to L,\ g \mapsto g(\alpha).$$

Por tanto, para probar que f divide a h en $\mathbb{F}_p[\mathtt{t}]$ es suficiente demostrar que $h \in \ker \mathrm{ev}_\alpha$, esto es, que $h(\alpha) = 0$, o lo que es igual, $\alpha \in \mathbb{F}_{p^n}$. Si $\deg(f) = d$, entonces, como $d|n$, se deduce de V.1.3 (4) que $\alpha \in L := \mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$, como queríamos demostrar.

Recíprocamente, vamos a probar que h divide a $\prod_{f \in \Sigma} f$ en $\mathbb{F}_p[\mathtt{t}]$. Observamos que $h' = -1$, luego h carece de factores irreducibles múltiples en $\mathbb{F}_p[\mathtt{t}]$.

Así, como este anillo es un DFU, es suficiente demostrar que cada factor irreducible y mónico g de h en $\mathbb{F}_p[\mathtt{t}]$ pertenece a la familia Σ, es decir, que su grado divide a n.

Sea v una raíz de g en un cuerpo de descomposición de g. Como g divide a h también $h(v) = 0$, y esto significa que $v \in \mathbb{F}_{p^n}$. Por tanto $\mathbb{F}_p \subset \mathbb{F}_p(v) \subset \mathbb{F}_{p^n}$ y $[\mathbb{F}_p(v) : \mathbb{F}_p] = \deg(g)$, ya que al ser mónico e irreducible, g es el polinomio mínimo de v sobre $\mathbb{F}_p$. Por tanto,

$$\begin{aligned} n = [\mathbb{F}_{p^n} : \mathbb{F}_p] &= [\mathbb{F}_{p^n} : \mathbb{F}_p(v)] \cdot [\mathbb{F}_p(v) : \mathbb{F}_p] \\ &= [\mathbb{F}_{p^n} : \mathbb{F}_p(v)] \cdot \deg(P_{\mathbb{F}_p,v}) = [\mathbb{F}_{p^n} : \mathbb{F}_p(v)] \cdot \deg(g), \end{aligned}$$

lo que prueba que $\deg(g)$ divide a n, como queríamos demostrar. □

Corolario V.1.5 *Sean p un número primo y $n > 1$ un número entero. Denotemos N_n^p el número de polinomios irreducibles en $\mathbb{F}_p[\mathtt{t}]$ mónicos de grado n y $D(n) := \{d \in \mathbb{Z}^+ : d \text{ divide a } n\}$. Entonces,*

(1) $\sum_{d\in D(n)} dN_d^p = p^n$.

(2) *Se llama* función de Möbius $\mu : \mathbb{N} \to \{-1, 0, 1\}$, véase el Ejercicio VI.18, vol. I, *a la definida del modo siguiente:*

$$\mu(1) = 1, \ \ \mu(n) = (-1)^r \ \textit{si } n \textit{ es producto de } r \textit{ números primos distintos } \&$$

$$\mu(n) = 0 \ \textit{si } n \textit{ es múltiplo del cuadrado de un número primo.}$$

Entonces, $nN_n^p = \sum_{d\in D(n)} \mu(n/d)p^d$.

(3) *Existe al menos un polinomio irreducible en $\mathbb{F}_p[\mathtt{t}]$ de grado n.*

Demostración. (1) Para cada $d \in D(n)$ denotamos Σ_d el conjunto de polinomios mónicos e irreducibles de $\mathbb{F}_p[\mathtt{t}]$ de grado d y $\Sigma := \bigsqcup_{d\in D(n)} \Sigma_d$. Por el Corolario V.1.4,

$$\mathtt{t}^{p^n} - \mathtt{t} = \prod_{f\in\Sigma} f,$$

y contando grados en ambos miembros resulta,

$$\begin{aligned} p^n = \deg(\mathtt{t}^{p^n} - \mathtt{t}) = \deg\Big(\prod_{f\in\Sigma} f\Big) &= \sum_{f\in\Sigma} \deg(f) \\ &= \sum_{d\in D(n)} \sum_{f\in\Sigma_d} \deg(f) = \sum_{d\in D(n)} dN_d^p. \end{aligned} \tag{1.1}$$

(2) La Fórmula de inversión que obtuvimos en el Ejercicio VI.19, vol. I. (1), afirma que si $\phi : \mathbb{N} \to \mathbb{Z}$ y $\Phi : \mathbb{N} \to \mathbb{Z}$, $n \mapsto \sum_{d\in D(n)} \phi(d)$, entonces

$$\phi(n) = \sum_{d\in D(n)} \mu(n/d)\Phi(d).$$

Consideremos la función $\phi(n) := nN_n^p$. Con estas notaciones, la igualdad (1.1) se lee

$$p^n = \sum_{d\in D(n)} dN_d^p = \sum_{d\in D(n)} \phi(d) = \Phi(n),$$

y aplicándole la Fórmula de inversión se obtiene la igualdad buscada

$$nN_n^p = \phi(n) = \sum_{d\in D(n)} \mu(n/d)\Phi(d) = \sum_{d\in D(n)} \mu(n/d)p^d.$$

(3) Basta demostrar que $nN_n^p > 0$. Denotemos $D'(n) := D(n) \setminus \{n\}$. Entonces,

$$nN_n^p = \sum_{d\in D(n)} \mu(n/d)p^d = p^n + \sum_{d\in D'(n)} \mu(n/d)p^d \geq p^n - \sum_{d\in D'(n)} p^d$$

$$\geq p^n - \sum_{d=1}^{n-1} p^d = p^n - \frac{p^n - p}{p-1} = \frac{p(p^n - 2p^{n-1} + 1)}{p-1} = \frac{p(p^{n-1}(p-2)+1)}{p-1} > 0.$$

□

Ejemplos V.1.6 (1) Empleamos el apartado (2) del Corolario V.1.5 para calcular los números N_2^p y N_3^p de polinomios mónicos e irreducibles en $\mathbb{F}_p[\mathtt{t}]$ de grados 2 y 3. Se tiene,

$$N_2^p = \frac{\mu(2)p + \mu(1)p^2}{2} = \frac{p^2 - p}{2} = \frac{p(p-1)}{2} = \binom{p}{2},$$

el mismo resultado obtenido en V.1.1 (3). Por otro lado,

$$N_3^p = \big(\mu(3)p + \mu(1)p^3\big)/3 = (p^3 - p)/3 = (p-1)p(p+1)/3.$$

Nuestro siguiente objetivo es demostrar que si K es un cuerpo finito, toda extensión finita $L|K$ es simple. Antes necesitamos un resultado auxiliar con interés en sí mismo.

Proposición V.1.7 *Todo subgrupo del grupo multiplicativo K^* formado por los elementos no nulos de un cuerpo finito K es cíclico.*

Demostración. Vimos en I.1.9, vol. I, que todo subgrupo de un grupo cíclico es cíclico, luego basta probar que K^* es cíclico. Como K^* es un grupo abeliano finito tiene *exponente,* esto es, existe $a \in K^*$ cuyo orden $m \in \mathbb{Z}^+$ es múltiplo del orden de cada elemento de K^*. Denotamos $n = \mathrm{ord}(K^*)$ y probaremos que $m = n$, por lo que K^* es el grupo cíclico generado por a. Desde luego $m \leq n$, y además $x^m = 1$ para cada elemento de K^*. Esto último se expresa diciendo que el polinomio $\mathtt{t}^m - 1$ tiene a todos los elementos de K^* por raíces luego, por la Proposición V.2.2 vol. II, $n \leq m$, y con ello $m = n$. □

Corolario V.1.8 (Elemento primitivo) *Sean K un cuerpo finito y $L|K$ una extensión finita. Entonces existe $\theta \in L$ tal que $L = K(\theta)$.*

Demostración. Sea m el número elementos de K. Esto implica que también L es finito, pues si $n := [L : K]$ es el grado de la extensión, el cuerpo L tiene m^n elementos. Por la Proposición V.1.7 el grupo multiplicativo $L^* := L \setminus \{0\}$ es cíclico, y consideramos un generador suyo θ. Esto significa que todo elemento de L es potencia de θ, y en particular $L \subset K(\theta)$. Como la inclusión $K(\theta) \subset L$ es obvia, se tiene $L = K(\theta)$. □

1.b. Teoría de Galois para extensiones de cuerpos finitos.

Definición y Observaciones V.1.9 (1) Sean p un número primo, L un cuerpo de característica p y $\phi : \mathbb{F}_p \to L$ un homomorfismo de cuerpos. De la igualdad $[k]_p = [1]_p + \overset{k)}{\cdots} + [1]_p$ se desprende que

$$\phi([k]_p) = \phi([1]_p) + \overset{k)}{\cdots} + \phi([1]_p) = [1]_p + \overset{k)}{\cdots} + [1]_p = [k]_p.$$

En particular la identidad es el único automorfismo de $\mathbb{F}_p$, y para cada extensión de cuerpos $L|\mathbb{F}_p$ se cumple que $\mathrm{Aut}(L) = G(L : \mathbb{F}_p)$. En efecto, para cada $\phi \in \mathrm{Aut}(L)$ su restricción $\phi|_{\mathbb{F}_p} : \mathbb{F}_p \to L$ cumple que $\phi(x) = x$ para cada $x \in \mathbb{F}_p$, esto es, $\phi \in G(L : \mathbb{F}_p)$.

(2) La aplicación $\phi : L \to L$, $x \mapsto x^p$ se denomina *automorfismo de Frobenius,* y es un automorfismo de la extensión $L|\mathbb{F}_p$. En efecto, según vimos en VI.2.7, vol. II, el número combinatorio $\binom{p}{k}$ es múltiplo de p para $1 \leq k \leq p-1$, luego dados $x, y \in L$,

$$\phi(x+y) = (x+y)^p = \sum_{j=0}^{p} \binom{p}{k} x^{p-k} y^k = x^p + y^p = \phi(x) + \phi(y) \quad \&$$
$$\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y).$$

Es útil conocer que $\phi^m(x) = x^{p^m}$ para cada $x \in L$ y cada entero $m > 0$, donde $\phi^m = \phi \overset{m)}{\cdots} \phi$. Lo probamos por inducción sobre m, siendo obvio el caso $m = 1$. Si lo admitimos para $m-1$, entonces

$$\phi^m(x) = \phi(\phi^{m-1}(x)) = \phi\big(x^{p^{m-1}}\big) = \big(x^{p^{m-1}}\big)^p = x^{p^{m-1}\cdot p} = x^{p^m}.$$

Proposición V.1.10 *Sean $L|K$ una extensión de cuerpos finitos y $f \in K[\mathtt{t}]$ un polinomio irreducible que posee una raíz en L. Entonces f factoriza en $L[\mathtt{t}]$ como producto de factores de grado* 1.

Demostración. Si $p := \mathrm{char}(K)$ y $n := [L : \mathbb{F}_p]$, sabemos por el Teorema V.1.2 que $L = \mathbb{F}_{p^n}$. Podemos suponer que f es mónico y sea $\alpha \in L$ una raíz de f. Así α es algebraico sobre K y como la extensión $K|\mathbb{F}_p$ es algebraica por ser finita, α es también algebraico sobre $\mathbb{F}_p$. Además, el polinomio mínimo $g := P_{\mathbb{F}_p,\alpha}$ de α sobre $\mathbb{F}_p$ pertenece a $K[\mathtt{t}]$ y tiene a α por raíz, luego es múltiplo en $K[\mathtt{t}]$ de $f := P_{K,\alpha}$. Nótese que $\mathbb{F}_p \subset \mathbb{F}_p(\alpha) \subset L$, luego por la transitividad del grado,

$$n = [L : \mathbb{F}_p] = [L : \mathbb{F}_p(\alpha)] \cdot [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [L : \mathbb{F}_p(\alpha)] \cdot \deg(g).$$

Como $\deg(g)|n$ se deduce del Corolario V.1.4 que g divide a $h := \mathtt{t}^{p^n} - \mathtt{t}$ en $\mathbb{F}_p[\mathtt{t}]$, luego g divide a h en $K[\mathtt{t}]$. Como ya habíamos señalado que f divide a g en $K[\mathtt{t}]$ concluimos que f divide a h en $K[\mathtt{t}]$, por lo que las raíces de f en un cierre algebraico de $\mathbb{F}_p$ lo son de h. Como las raíces de h son los elementos del cuerpo $\mathbb{F}_{p^n} = L$, concluimos que f factoriza en $L[\mathtt{t}]$ como producto de factores de grado 1. □

Teorema V.1.11 *Cada extensión de cuerpos finitos $L|K$ es de Galois y el grupo de Galois $G(L : K)$ es cíclico, generado por una potencia del automorfismo de Frobenius de L.*

Demostración. Si denotamos $p := \mathrm{char}(K) = \mathrm{char}(L)$ se deduce de V.1.3 que existen enteros positivos m y n tales que m divide a n y $K := \mathbb{F}_{p^m}$ es el cuerpo con p^m elementos, mientras que $L := \mathbb{F}_{p^n}$ es el cuerpo con p^n elementos. Denotamos $\phi : L \to L$, $x \mapsto x^p$ el automorfismo de Frobenius, y vamos a demostrar en primer lugar que su orden es $o(\phi) = n$.

Por un lado $\phi^n = \mathrm{id}_L$, pues L está formado por las raíces del polinomio $\mathtt{t}^{p^n} - \mathtt{t}$ luego, en virtud de V.1.9 (2), $\phi^n(x) = x^{p^n} = x$ para cada $x \in L$. Esto demuestra que $\ell := o(\phi) \leq n$. Además, $\phi^\ell = \mathrm{id}_L$ por lo que $x = \phi^\ell(x) = x^{p^\ell}$

para cada $x \in L$, es decir, x es raíz del polinomio $\mathtt{t}^{p^\ell} - \mathtt{t}$. Esto implica, por el Teorema V.1.2, que x pertenece al cuerpo $\mathbb{F}_{p^\ell}$ con p^ℓ elementos, por lo que $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^\ell}$, luego $n \leq \ell$, así que $o(\phi) = n$.

Probemos que $\phi^m \in G(L:K)$ es decir, la restrición $\phi^m|_K$ es la identidad. En efecto, para todo $x \in K = \mathbb{F}_{p^m}$ se tiene, por V.1.9 (2) y el Teorema V.1.2, $x = x^{p^m} = \phi^m(x)$. Para terminar, denotamos $d := n/m$ y, utilizando el Lema I.2.6, vol. I y que por el Teorema del elemento primitivo V.1.8 la extensión $L|K$ es simple, se deduce de IV.1.4 (2) que

$$\begin{aligned} d = n/m = o(\phi)/\operatorname{mcd}(o(\phi), m) &= o(\phi^m) \\ &\leq \operatorname{ord}(G(L:K)) \leq [L:K] = [L:\mathbb{F}_p]/[K:\mathbb{F}_p] = n/m = d. \end{aligned}$$

Esto demuestra que $G(L:K) = \langle \phi^m \rangle$ y que $\operatorname{ord}(G(L:K)) = [L:K]$, así que la extensión $L|K$ es de Galois y el grupo $G(L:K)$ es cíclico. □

Corolario V.1.12 (1) *Sea $H := G(L:K)$ el grupo de automorfismos de una extensión $L|K$ de cuerpos finitos. Entonces $K = \operatorname{Fix}(H)$.*

(2) *Se cumple la igualdad* $\operatorname{ord}(G(L:K)) = [L:K]$.

Demostración. (1) Sea $p = \operatorname{char}(K)$. Por el Teorema V.1.11, $H = \langle \phi^m \rangle$ para cierto entero no negativo m, donde $\phi : L \to L$, $x \mapsto x^p$ es el automorfismo de Frobenius, y $\operatorname{Card}(K) = p^m$. Así, un elemento $x \in L$ pertenece a $\operatorname{Fix}(H)$ si y sólo si $\phi^m(x) = x$, lo que por V.1.9 significa que $x^{p^m} = x$, y esto equivale a que $x \in \mathbb{F}_{p^m} = K$.

(2) Con las notaciones anteriores,

$$\begin{aligned} \operatorname{ord}(G(L:K)) = o(\phi^m) = o(\phi)/\operatorname{mcd}(o(\phi), m) &= n/m \\ = [L:\mathbb{F}_p]/[K:\mathbb{F}_p] &= [L:K]. \end{aligned}$$

□

Terminamos esta seción formulando el Teorema fundamental de la Teoría de Galois para extensiones de cuerpos finitos.

Teorema V.1.13 *Sea $L|K$ una extensión de cuerpos finitos. Las aplicaciones*

$$E|K \to G(L:E) \quad \& \quad H \mapsto \operatorname{Fix}(H)|K$$

entre el conjunto de subextensiones de $L|K$ y el de subgrupos del grupo de Galois $G(L:K)$, son mutuamente inversas. Además,

$$G(E:K) \cong G(L:K)/G(L:E),$$

y en particular $[E:K]\cdot \mathrm{ord}(G(L:E)) = [L:K]$.

Demostración. Si p es la característica de K existen, por el Teorema V.1.2 y la Observación V.1.3, enteros positivos m y n tales que m divide a n y $K := \mathbb{F}_{p^m}$ y $L := \mathbb{F}_{p^n}$ son los cuerpos con p^m y p^n elementos, respectivamente. Además, si $\phi : L \to L$, $x \mapsto x^p$ es el automorfismo de Frobenius, hemos visto en el Teorema V.1.11 que para cada subextensión $E|K$ de $L|K$, donde $E := \mathbb{F}_{p^r}$, el grupo $G(L:E) = \langle \phi^r \rangle$ es cíclico de orden n/r y $E = \mathrm{Fix}(G(L:E))$.

Recíprocamente, todo subgrupo H del grupo cíclico $G(L:K) = \langle \phi^m \rangle$ es cíclico, por la Proposición I.1.9, vol. I, generado por ϕ^{md} para cierto divisor d de $n := o(\phi^m)$, luego

$$\mathrm{Fix}(H) = \{x \in L : x = \phi^{md}(x) = x^{p^{md}}\} = \mathbb{F}_{p^{md}} \subset \mathbb{F}_{p^{mn}}.$$

Como la extensión $L|\mathrm{Fix}(H)$ es de Galois, el orden del grupo $G(L:\mathrm{Fix}(H))$ es $[L:\mathrm{Fix}(H)] = mn/md = n/d = \mathrm{ord}(H)$. Por tanto, H y $G(L:\mathrm{Fix}(H))$ son subgrupos del mismo orden del grupo cíclico $G(L:K)$, luego coinciden, en virtud de I.2.8, vol. I. Además, el grupo cociente $G(L:K)/G(L:E)$ es cíclico por serlo $G(L:K)$, y también es cíclico $G(E:K)$, luego para probar que son isomorfos basta probar que sus órdenes coinciden. Por ser de Galois las tres extensiones involucradas, y la transitividad del grado,

$$\begin{aligned}\mathrm{ord}(G(L:K)/G(L:E)) &= \mathrm{ord}(G(L:K))/\,\mathrm{ord}(G(L:E))\\ &= [L:K]/[L:E] = [E:K] = \mathrm{ord}(G(E:K)).\end{aligned}$$

En particular,

$$\begin{aligned}[E:K]\cdot \mathrm{ord}(G(L:E)) &= \mathrm{ord}(G(E:K))\cdot \mathrm{ord}(G(L:E))\\ &= \mathrm{ord}(G(L:K)) = [L:K].\end{aligned}$$

□

2. Restos cuadráticos en cuerpos finitos

En esta sección presentamos la solución obtenida por Gauss al problema de decidir si, fijados un primo p y un entero n, la clase $n \bmod p$ es un cuadrado en el cuerpo $\mathbb{F}_p$ con p elementos. La solución viene dada por la llamada *Ley de reciprocidad cuadrática.* En un apéndice presentamos el Teorema de Chevalley-Warning, que el lector necesitará para resolver los tres últimos ejercicios propuestos en este capítulo.

2.a. Ley de reciprocidad cuadrática.

Lema V.2.1 *Sea K un cuerpo finito. Se cumplen las siguientes propiedades.*

(1) *Si K tiene característica 2, todos sus elementos son un cuadrado en K.*

(2) *Si la característica de K es impar, entonces K^{*2} es un subgrupo de índice 2 del grupo multiplicativo K^*.*

(3) *Si la característica de K es impar y ζ es un generador del grupo cíclico K^*, entonces ζ no es el cuadrado de un elemento de K.*

Demostración. (1) Como $\mathrm{char}(K) = 2$ la aplicación $\phi : K \to K,\ x \to x^2$ es su automorfismo de Frobenius, luego es sobreyectivo, o sea, cada elemento de K es un cuadrado.

(2) El homomorfismo de grupos $\psi : K^* \to K^*$, $x \mapsto x^2$, cuya imagen es K^{*2}, tiene por núcleo al subgrupo formado por los elementos $x \in K^*$ tales que $x^2 = 1$, esto es, $\ker \psi = \{-1, +1\}$. Por el Primer Teorema de isomorfía de grupos, $K^*/\ker\psi \cong \mathrm{im}\,\psi = K^{*2}$, luego

$$[K^* : K^{*2}] = \mathrm{ord}(K^*)/\,\mathrm{ord}(K^{*2}) = \mathrm{ord}(\ker\psi) = 2.$$

(3) El cardinal q de K es potencia de $\mathrm{char}(K)$, luego es impar. Si $\zeta := \xi^2$ para un $\xi \in K^*$, entonces $K^* = \langle\zeta\rangle \subset \langle\xi\rangle \subset K^*$, luego $o(\xi) = q - 1$ es par, y por el Lema I.2.6, vol. I,

$$q - 1 = \mathrm{ord}(K^*) = o(\zeta) = o(\xi^2) = o(\xi)/\,\mathrm{mcd}(o(\xi), 2) = (q-1)/2,$$

lo que es falso. □

Lema V.2.2 (Euler) *Sea K un cuerpo con q elementos y sea $a \in K^*$. El polinomio $\mathtt{t}^2 - a$ tiene una raíz en K si y sólo si $a^{(q-1)/2} = 1$.*

Demostración. Supongamos primero que existe $x \in K$ tal que $x^2 = a$. Como $a \neq 0$ también $x \in K^*$, y el orden $o(x)$ de x divide, por la Fórmula de Lagrange, al orden de K^*, que es $q - 1$. Por tanto, $a^{(q-1)/2} = x^{q-1} = 1$.

Recíprocamente, puesto que por la Proposición V.1.7 el grupo multiplicativo K^* es cíclico, existen un generador ζ de K^* y un entero no negativo k tales que $a := \zeta^k$. Entonces, $k(q-1)/2$ es múltiplo de $q - 1 = o(\zeta)$ pues

$$\zeta^{k(q-1)/2} = (\zeta^k)^{(q-1)/2} = a^{(q-1)/2} = 1,$$

luego k es par. Por tanto, existe $\ell \in \mathbb{Z}$ tal que $k := 2\ell$, y así $a = \zeta^k = \zeta^{2\ell} = x^2$, donde $x := \zeta^\ell \in K$. □

Corolario V.2.3 *Si p es un número primo impar, el polinomio $\mathtt{t}^2+1$ tiene alguna raíz en $\mathbb{F}_p$ si y sólo si $p-1$ es múltiplo de 4.*

Demostración. Por el Criterio de Euler V.2.2, -1 es un cuadrado en $\mathbb{F}_p$ si y sólo si $(-1)^{(p-1)/2}=1$, o sea, $(p-1)/2$ es par, esto es, $4|(p-1)$. □

El Criterio de Euler es poco eficiente, si p es grande, para determinar si un polinomio del tipo $\mathtt{t}^2-a$ tiene alguna raíz en $\mathbb{F}_p$. Para obtener un procedimiento más útil se introduce el llamado *símbolo de Legendre.* Denotaremos $[n]_p\in\mathbb{F}_p$ la clase $\mathsf{mod}\ p$ del entero $n\in\mathbb{Z}$.

Definición y Proposición V.2.4 (Símbolo de Legendre) (1) Para cada número primo impar p y cada entero n primo con p definimos el *símbolo de Legendre de n respecto de p* como

$$\left(\frac{n}{p}\right)=\begin{cases}+1 & \text{si } \mathtt{t}^2-[n]_p=0 \text{ tiene raíz en } \mathbb{F}_p,\\ -1 & \text{si } \mathtt{t}^2-[n]_p=0 \text{ no tiene raíz en } \mathbb{F}_p.\end{cases}$$

Si el polinomio $\mathtt{t}^2-[n]_p=0$ tiene solución en $\mathbb{F}_p$ decimos que n es un *resto cuadrático* $\mathsf{mod}\ p$, y que no lo es en caso contrario. Se deduce del apartado (2) en V.2.1 que entre los enteros $1\le k\le p-1$ la mitad son restos cuadráticos $\mathsf{mod}\, p$ y la otra mitad no lo son.

(2) Sean p un primo impar y n,m dos enteros primos con p. Se cumple que:

(2.1) $\left(\frac{n^2}{p}\right)=1$. En particular, $\left(\frac{1}{p}\right)=1$.

(2.2) *Si $n\equiv m\ \mathsf{mod}\, p$, entonces* $\left(\frac{n}{p}\right)=\left(\frac{m}{p}\right)$.

(2.3) $\left(\frac{n}{p}\right)\equiv n^{(p-1)/2}\ \mathsf{mod}\, p$.

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

(2.5) *Si k es un entero no negativo,* $\left(\frac{n^k}{p}\right)=\left(\frac{n}{p}\right)^k$.

(2.6) $\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}=\begin{cases}+1 & \text{si } \ p\equiv 1 \ \mathsf{mod}\, 4,\\ -1 & \text{si } \ p\equiv 3 \ \mathsf{mod}\, 4.\end{cases}$

Demostración. (2.1) Este apartado es evidente pues n^2 es un residuo cuadrático $\mathsf{mod}\, p$ porque $[n^2]_p=[n]_p^2$.

(2.2) Si $n \equiv m \bmod p$, entonces $[n]_p = [m]_p$, luego los polinomios $\mathtt{t}^2 - [n]_p$ y $\mathtt{t}^2 - [m]_p$ coinciden y, por tanto,

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

(2.3) Por el Pequeño Teorema de Fermat, $[n]_p^{p-1} = [1]_p \bmod p$. Si $q := (p-1)/2$ resulta

$$\left([n]_p^q - [1]_p\right) \cdot \left([n]_p^q + [1]_p\right) = [n]^{2q} - [1]_p = [n]_p^{p-1} - [1]_p = [0]_p = 0_{\mathbb{F}_p},$$

y como $\mathbb{F}_p$ es un cuerpo, uno de los dos factores es nulo, es decir, $n^{(p-1)/2} \equiv \pm 1 \bmod p$. Por el Criterio de Euler V.2.2, $[n]_p$ es un cuadrado en $\mathbb{F}_p$ si y sólo si $n^{(p-1)/2} \equiv 1 \bmod p$, luego

$$\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \bmod p.$$

(2.4) El producto mn es primo con p por serlo m y n luego, por el apartado anterior,

$$\left(\frac{nm}{p}\right) \equiv (nm)^{(p-1)/2} = (n^{(p-1)/2})(m^{(p-1)/2}) \equiv \left(\frac{n}{p}\right) \cdot \left(\frac{m}{p}\right) \bmod p,$$

y como los números involucrados en esta igualdad son 1 y -1, resulta que

$$\left(\frac{nm}{p}\right) - \left(\frac{n}{p}\right)\left(\frac{m}{p}\right) \in p\mathbb{Z} \cap \{-2, 0, 2\}.$$

Como p es un primo impar se deduce que la resta anterior es nula, esto es,

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

(2.5) Argumentamos por inducción sobre k. El caso $k = 0$ se ha probado en (2.2). Supongamos que $k \geq 1$ y el resultado probado para $k-1$. Denotemos $m := n^{k-1}$, que es primo con p y, por el apartado (2.4) y la hipótesis de inducción,

$$\left(\frac{n^k}{p}\right) = \left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right) \cdot \left(\frac{m}{p}\right) = \left(\frac{n}{p}\right) \cdot \left(\frac{n^{k-1}}{p}\right) = \left(\frac{n}{p}\right) \cdot \left(\frac{n}{p}\right)^{k-1} = \left(\frac{n}{p}\right)^k.$$

(2.6) Este apartado es consecuencia inmediata de (2.3) aplicado a $n := -1$ y el hecho de que p es un primo impar. □

Corolario V.2.5 *Si p es un primo impar, entonces* $\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)=0$.

Demostración. Por la Proposición VI.2.8, vol. I, el grupo $\mathbb{F}_p^*$ es cíclico, luego tiene un generador $[m]_p := \zeta \in \mathbb{F}_p^*$. Hemos probado en V.2.1 (3) que ζ no es un cuadrado en $\mathbb{F}_p$, esto es, $\left(\frac{m}{p}\right) = -1$. Como

$$\{[1]_p, \dots, [p-1]_p\} = \mathbb{F}_p^* = \langle\zeta\rangle = \{[m]_p, \dots, [m]_p^{p-1}\},$$

al sumar, teniendo en cuenta que p es impar y empleando V.2.4 (2.5),

$$\sum_{n=1}^{p-1}\left(\frac{n}{p}\right) = \sum_{k=1}^{p-1}\left(\frac{m^k}{p}\right) = \sum_{k=1}^{p-1}\left(\frac{m}{p}\right)^k = \sum_{k=1}^{p-1}(-1)^k = 0.$$

□

Lema V.2.6 (Gauss) *Sean p un número primo impar, n un entero positivo primo con p y k el número de elementos del conjunto*

$$S := \{n, 2n, 3n, \dots, (p-1)n/2\}$$

cuyos restos al dividir entre p son mayores que $p/2$. Entonces, $\left(\frac{n}{p}\right) = (-1)^k$.

Demostración. Como n y p son primos entre sí el conjunto

$$\widehat{S} := \{[nx]_p : \ 1 \le x \le (p-1)/2\}$$

tiene $(p-1)/2$ elementos. En efecto, en caso contrario existirían números enteros $1 \le x < y \le (p-1)/2$ tales que p divide a $n(y-x)$. Como p y n son primos entre sí esto implica que $y-x$ es múltiplo de p, lo que es falso ya que $1 \le y-x < (p-1)/2$.

Como $p/2 \in \mathbb{Q} \setminus \mathbb{Z}$, el resto de la división entre p de cada elemento de S es distinto de $p/2$. Por ello, si $r_1, \dots, r_\ell$ son aquellos restos de la división entre p de los elementos de S tales que $0 < r_i < p/2$ y $s_1, \dots, s_k$ son aquellos restos tales que $p/2 < s_j < p$, se cumple que $\ell + k = \mathrm{Card}(\widehat{S}) = (p-1)/2$. Además,

$$0 < r_1, \dots, r_\ell,\ p - s_1, \dots, p - s_k < p/2,$$

y los enteros $r_1, \dots, r_\ell,\ p - s_1, \dots, p - s_k$ son distintos dos a dos, es decir, $p - s_j \neq r_i$ para cualesquiera i, j. En caso contrario existen i, j tales que

$p - s_j = r_i$ o lo que es lo mismo, $r_i + s_j = p$. Por definición de los r_i, s_j existen enteros $1 \leq u, v \leq (p-1)/2$ tales que $un \equiv r_i \bmod p$ y $vn \equiv s_j \bmod p$. De este modo

$$(u+v)n \equiv un + vn \equiv r_i + s_j \equiv 0 \bmod p.$$

Como n es primo con p, deducimos que $u + v \equiv 0 \bmod p$, y esto es imposible ya que $2 \leq u + v \leq p - 1$. Así,

$$\{r_1, \ldots, r_\ell,\ p - s_1, \ldots,\ p - s_k\} = \{1 \leq x \leq (p-1)/2,\, x \in \mathbb{Z}\}. \tag{2.2}$$

Por tanto, el producto de los elementos del conjunto de la izquierda coincide con el de los elementos del conjunto de la derecha, y en consecuencia

$$\big((p-1)/2\big)! \equiv \prod_{i=1}^{\ell} r_i \cdot \prod_{j=1}^{k} (p - s_j) \equiv (-1)^k \prod_{i=1}^{\ell} r_i \prod_{j=1}^{k} s_j \bmod p.$$

Pero los números $r_1, \ldots, r_\ell,\ s_1, \ldots, s_k$ son congruentes $\bmod p$, aunque posiblemente en distinto orden, con $n, 2n, \ldots, (p-1)n/2$ y, por tanto,

$$\big((p-1)/2\big)! \equiv (-1)^k \prod_{i=1}^{\ell} r_i \prod_{j=1}^{k} s_j \equiv (-1)^k n^{(p-1)/2} \big((p-1)/2\big)! \bmod p.$$

Como p no divide al producto $\big((p-1)/2\big)! = \prod_{j=1}^{(p-1)/2} j$ se deduce, simplificando el factor $\big((p-1)/2\big)!$ en la igualdad anterior,

$$(-1)^k n^{(p-1)/2} \equiv 1 \bmod p \quad \Longleftrightarrow \quad n^{(p-1)/2} \equiv (-1)^k \bmod p.$$

En virtud de V.2.4 (2.3) concluimos que

$$\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \equiv (-1)^k \bmod p,$$

por lo que $\left(\frac{n}{p}\right) = (-1)^k$. □

Corolario V.2.7 *Dado un primo impar p, el polinomio $\mathtt{t}^2 - 2$ tiene alguna raíz en $\mathbb{F}_p$ si y sólo si $8|(p-1)$ o $8|(p+1)$. De hecho, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.*

Demostración. Por el Lema V.2.6, $\left(\frac{2}{p}\right) = (-1)^k$, donde k es el número de enteros en el conjunto

$$S := \{2, 2 \cdot 2, 3 \cdot 2, \ldots, (p-1) \cdot 2/2\}$$

cuyos restos al dividir entre p son mayores que $p/2$. Cada $x \in S$ es menor que p, luego coincide con el resto de su división entre p. Por tanto, k es el número de enteros positivos pares $x := 2y$ tales que $p/2 < x < p$. Como p es impar estas desigualdades equivalen a

$$(p+1)/2 \leq 2y \leq p-1 \quad \Longleftrightarrow \quad (p+1)/4 \leq y \leq (p-1)/2.$$

Escribimos las desigualdades anteriores según la forma del primo impar p, que es una de las siguientes:

$$p := 8z+1,\ p := 8z+3,\ p := 8z+5 \quad \& \quad p := 8z+7$$

con $z \in \mathbb{Z}$. Se tiene:

(1) Si $p := 8z+1 \quad \Longrightarrow \quad 2z + 1/2 \leq y \leq 4z \quad \Longrightarrow \quad k = 4z - 2z = 2z.$

(2) Si $p := 8z+3 \quad \Longrightarrow \quad 2z+1 \leq y \leq 4z+1,$ es decir

$$k = (4z+1) - (2z+1) + 1 = 2z+1.$$

(3) Si $p := 8z+5 \quad \Longrightarrow \quad 2z + 3/2 \leq y \leq 4z+2,$ es decir

$$k = (4z+2) - (2z+1) = 2z+1.$$

(4) Si $p := 8z+7 \quad \Longrightarrow \quad 2z+2 \leq y \leq 4z+3,$ es decir

$$k = (4z+3) - (2z+2) + 1 = 2(z+1).$$

Por tanto, k es par si y sólo si $p \equiv \pm 1 \bmod 8$, y como $\left(\frac{2}{p}\right) = (-1)^k$ resulta que el polinomio $\mathtt{t}^2 - 2 = 0$ tiene alguna raíz en $\mathbb{F}_p$ si y sólo si $p \equiv \pm 1 \bmod 8$, lo que demuestra la primera parte. Para la segunda observamos que si $p := 8z \pm 1$ entonces

$$(p^2-1)/8 = \big((8z \pm 1)^2 - 1\big)/8 = 8z^2 \pm 2z = 2z(4z \pm 1),$$

que es un entero par, mientras que si $p := 8z \pm 3$ entonces

$$(p^2-1)/8 = \big((8z \pm 3)^2 - 1\big)/8 = 8z^2 \pm 6z + 1 = 2z(4z \pm 3) + 1,$$

que es un entero impar. Esto demuestra que k y $(p^2-1)/8$ tienen la misma paridad, y por tanto $\left(\frac{2}{p}\right) = (-1)^k = (-1)^{(p^2-1)/8}$. □

Teorema V.2.8 (Ley de reprocidad cuadrática de Gauss) *Si p y q son números primos distintos se tiene*

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{(p-1)(q-1)/4}.$$

Demostración. Desarrollamos la prueba en tres etapas.

Paso 1. Si n es un entero impar primo con p y denotamos $\rho:=\sum_{j=1}^{(p-1)/2}[jn/p]$, entonces

$$\left(\frac{n}{p}\right)=(-1)^{\rho}.$$

En efecto, como en la prueba del Lema V.2.6, consideramos el conjunto de números enteros

$$S:=\{n,2n,3n,\ldots,(p-1)n/2\}$$

y denotamos $r_1,\ldots,r_\ell$ aquellos restos de la división entre p de los elementos de S tales que $0<r_i<p/2$, y $s_1,\ldots,s_k$ los restos de la división entre p de los elementos de S tales que $p/2<s_j<p$.

Para todo $1\le j\le(p-1)/2$ el cociente de la división euclídea de jn entre p es la parte entera $[jn/p]$ de jn/p. Si el resto de dicha división es menor que $p/2$, entonces es uno de los enteros $r_1,\ldots,r_\ell$, mientras que si es mayor que $p/2$, entonces es uno de los enteros $s_1,\ldots,s_k$. Sumando los números jn con $1\le j\le(p-1)/2$ tenemos

$$\sum_{j=1}^{(p-1)/2}jn=\sum_{j=1}^{(p-1)/2}[jn/p]\,p+\sum_{i=1}^{\ell}r_i+\sum_{i=1}^{k}s_i. \tag{2.3}$$

Por otro lado, la igualdad (2.2) de la demostración del Lema de Gauss V.2.6, afirma que

$$\{r_1,\ldots,r_\ell,p-s_1,\ldots,p-s_k\}=\{1\le j\le(p-1)/2,\,j\in\mathbb{Z}\}. \tag{2.4}$$

Entonces,

$$\sum_{j=1}^{(p-1)/2}j=\sum_{i=1}^{\ell}r_i+\sum_{i=1}^{k}(p-s_i)=kp+\sum_{i=1}^{\ell}r_i-\sum_{i=1}^{k}s_i, \tag{2.5}$$

y restando las expresiones (2.3) y (2.5) deducimos que

$$(n-1)\sum_{j=1}^{(p-1)/2}j=p\Big(\sum_{j=1}^{(p-1)/2}[jn/p]-k\Big)+2\sum_{i=1}^{k}s_i.$$

Como p y n son impares necesariamente $\rho := \sum_{j=1}^{(p-1)/2} [jn/p]$ y k tienen la misma paridad, y se desprende del Lema V.2.6 que

$$(-1)^\rho = (-1)^k = \left(\frac{n}{p}\right).$$

Paso 2. Si p y q son dos primos impares distintos, entonces

$$(p-1)(q-1)/4 = \sum_{\ell=1}^{(p-1)/2} [\ell q/p] + \sum_{\ell=1}^{(q-1)/2} [\ell p/q]\,. \tag{2.6}$$

Para demostrar esta igualdad observamos en primer lugar que el miembro de la izquierda es el número de puntos con coordenadas enteras situados en el interior del rectángulo $\mathcal{R} \subset \mathbb{R}^2$ de vértices $(0,0)$, $(0,q/2)$, $(p/2,0)$ y $(p/2,q/2)$.

Vamos a contar de otro modo el número de puntos con coordenadas enteras en el interior del rectángulo $\mathcal{R}$. Consideramos la diagonal

$$T := \{(x,y) \in \mathbb{R}^2 : qx = py\}$$

de $\mathcal{R}$ que pasa por los vértices $(0,0)$ y $(p/2,q/2)$. Como p y q son primos entre sí, los puntos con coordenadas enteras situados en la recta T son los de la forma (pu,qu) con $u \in \mathbb{Z}$ y, por tanto, ninguno está en el interior del rectángulo $\mathcal{R}$. Para $1 \le \ell \le (p-1)/2$ los puntos del interior de $\mathcal{R}$ situados debajo de T son

$$\{(\ell,k) :\ 1 \le k < q\ell/p\}.$$

El número de ellos es $[\ell q/p]$, por lo que el número de puntos con coordenadas enteras en el interior de $\mathcal{R}$ por debajo de la diagonal T es $\sum_{\ell=1}^{(p-1)/2} [\ell q/p]$. Argumentando por simetría, el número de puntos con coordenadas enteras en el interior de $\mathcal{R}$ situados por encima de la diagonal T es $\sum_{\ell=1}^{(q-1)/2} [\ell p/q]$, y sumando resulta la igualdad (2.6).

Paso 3. Para terminar, sean $\rho_1 := \sum_{\ell=1}^{(p-1)/2} [\ell q/p]$ y $\rho_2 := \sum_{\ell=1}^{(q-1)/2} [\ell p/q]$. Entonces, por lo visto en los pasos 1 y 2 se tiene

$$(-1)^{(p-1)(q-1)/4} = (-1)^{\rho_1+\rho_2} = (-1)^{\rho_1}(-1)^{\rho_2} = \left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right).$$

□

La Ley de reciprocidad cuadrática se puede reformular del modo siguiente:

Teorema V.2.9 *Sean p y q primos impares distintos. Entonces,*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{si } \ p \equiv 1 \bmod 4 \ \text{ o } \ q \equiv 1 \bmod 4, \\ -\left(\frac{q}{p}\right) & \text{si } \ p \equiv q \equiv 3 \bmod 4. \end{cases}$$

Demostración. Basta observar que $(p-1)(q-1)/4$, que es par si al menos uno de los dos enteros p o q es del tipo $4k+1$, es impar si $p := 4k+3$ y $q := 4\ell+3$. Esto es obvio pues entonces $(p-1)/2 = 2k+1$ y $(q-1)/2 = 2\ell+1$ son impares, luego lo es su producto $(p-1)(q-1)/4$. □

Ejemplo V.2.10 Si $p \neq 3$ es un primo impar, entonces

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \bmod 3, \\ -1 & \text{si } p \equiv 2 \bmod 3. \end{cases}$$

En efecto, en primer lugar, por V.2.4 (2.4) y (2.6), tenemos

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{3}{p}\right) & \text{si } p \equiv 1 \bmod 4, \\ -\left(\frac{3}{p}\right) & \text{si } p \equiv 3 \bmod 4. \end{cases}$$

Por la Ley de reciprocidad cuadrática,

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{si } p \equiv 1 \bmod 4, \\ -\left(\frac{p}{3}\right) & \text{si } p \equiv 3 \bmod 4. \end{cases}$$

Al sustituir en la igualdad anterior concluimos que $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$ en todos los casos, y como 1 es el único residuo cuadrático no nulo $\bmod 3$ resulta

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \bmod 3, \\ -1 & \text{si } p \equiv 2 \bmod 3. \end{cases}$$

Euler no pudo probar la Ley de reciprocidad cuadrática, pero conjeturó que era cierta, demostró algunos casos particulares y la formuló del modo siguiente.

Teorema V.2.11 (Euler) *Sean n un entero positivo y p, q primos impares tales que $p \equiv \pm q \bmod 4n$. Entonces*

$$\left(\frac{n}{p}\right) = \left(\frac{n}{q}\right).$$

Demostración. En primer lugar, afirmamos que basta con probar el caso en el que n es primo. En efecto, si $n = 1$ no hay nada que probar, con lo que podemos suponer que $n \geq 2$. Escribimos $n := p_1 \cdots p_r$ donde $p_1, \ldots, p_r$ son números primos no necesariamente distintos. Como cada p_j divide a n se tiene $p \equiv \pm q \bmod 4p_j$ para $1 \leq j \leq r$. Así, si damos por probado el caso primo, tenemos

$$\left(\frac{p_j}{p}\right) = \left(\frac{p_j}{q}\right) \quad \text{para } 1 \leq j \leq r,$$

y por V.2.4 (2.4) y (2.6), resulta

$$\left(\frac{n}{p}\right) = \prod_{j=1}^{r} \left(\frac{p_j}{p}\right) = \prod_{j=1}^{r} \left(\frac{p_j}{q}\right) = \left(\frac{n}{q}\right).$$

Por tanto suponemos en lo sucesivo que n es un número primo, y distinguimos dos casos.

Caso 1. Suponemos que $n = 2$. Entonces la hipótesis dice que $p \equiv \pm q \bmod 8$, es decir, $p = \varepsilon q + 8t$, donde $\varepsilon = \pm 1$ y $t \in \mathbb{Z}$. Por el Corolario V.2.7 se tiene

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^{(q^2+16\varepsilon qt+64t^2-1)/8} = (-1)^{(q^2-1)/8} = \left(\frac{2}{q}\right).$$

Caso 2. Suponemos ahora que n es un primo impar. Por la Ley de reciprocidad cuadrática V.2.8 tenemos

$$\begin{aligned} \left(\frac{n}{p}\right) \cdot \left(\frac{n}{q}\right) \cdot \left(\frac{p}{n}\right) \cdot \left(\frac{q}{n}\right) &= \left(\frac{n}{p}\right) \cdot \left(\frac{p}{n}\right) \cdot \left(\frac{n}{q}\right) \cdot \left(\frac{q}{n}\right) \\ &= (-1)^{\frac{(p-1)(n-1)}{4} + \frac{(q-1)(n-1)}{4}} = (-1)^{\frac{(n-1)(p+q-2)}{4}}. \end{aligned} \tag{2.7}$$

Como $p \equiv \pm q \bmod 4n$ o, equivalentemente, $p = \varepsilon q + 4nt$, donde $\varepsilon = \pm 1$ y $t \in \mathbb{Z}$, tenemos $p + q - 2 = (\varepsilon + 1)q + 4nt - 2$, y por V.2.4 (2.4),

$$\left(\frac{p}{n}\right) = \left(\frac{\varepsilon q + 4nt}{n}\right) = \left(\frac{\varepsilon q}{n}\right) = \left(\frac{\varepsilon}{n}\right) \cdot \left(\frac{q}{n}\right) \quad \Longrightarrow \quad \left(\frac{\varepsilon}{n}\right) = \left(\frac{p}{n}\right) \cdot \left(\frac{q}{n}\right),$$

por lo que la igualdad (2.7) se reescribe así:

$$\left(\frac{n}{p}\right) \cdot \left(\frac{n}{q}\right) \cdot \left(\frac{\varepsilon}{n}\right) = (-1)^{\frac{(n-1)((\varepsilon+1)q+4nt-2)}{4}}. \tag{2.8}$$

Ahora distinguimos dos subcasos:

Subcaso 2.1 Si $\varepsilon = 1$, entonces

$$(n-1)\big((\varepsilon+1)q + 4nt - 2\big) = 2(n-1)(2nt+q-1)$$

es múltiplo de 8, porque n y q son impares, y deducimos de (2.8) y V.2.4 (2.2)

$$\left(\frac{n}{p}\right) = \left(\frac{n}{q}\right).$$

Subcaso 2.2 Si $\varepsilon = -1$, entonces

$$(n-1)\big((\varepsilon+1)q + 4nt - 2\big) = 2(n-1)(2nt-1),$$

y por (2.8) y V.2.4 (2.6), se tiene

$$\left(\frac{n}{p}\right)\cdot\left(\frac{n}{q}\right)\cdot\left(\frac{-1}{n}\right) = (-1)^{\frac{(n-1)(2nt-1)}{2}} = (-1)^{\frac{(n-1)}{2}} = \left(\frac{-1}{n}\right),$$

y simplificando el factor $\left(\frac{-1}{n}\right)$ obtenemos finalmente $\left(\frac{n}{p}\right) = \left(\frac{n}{q}\right)$. □

Ejemplo V.2.12 Si $p = 31,\ q = 3$ y $n = 7$, se cumple que $p \equiv q \bmod 4n$ y, por el Teorema V.2.11,

$$\left(\frac{7}{31}\right) = \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1,$$

es decir, la clase $[7]_{31}$ es un cuadrado en el cuerpo $\mathbb{F}_{31}$.

Observación V.2.13 Sean p un primo impar y $n \neq \pm 1$ un entero no divisible por p. Supongamos que $n = \pm 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, donde los primos p_i son impares y distintos dos a dos y cada k_i es un entero no negativo. Como el símbolo de Legendre tiene, por la Proposición V.2.4, carácter multiplicativo, tenemos

$$\left(\frac{n}{p}\right) = \left(\frac{\pm 1}{p}\right)\cdot\left(\frac{2}{p}\right)^{k_0}\cdot\left(\frac{p_1}{p}\right)^{k_1}\cdots\left(\frac{p_r}{p}\right)^{k_r}.$$

Por tanto, para determinar $\left(\frac{n}{p}\right)$ sólo tenemos que calcular los símbolos de Legendre $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ y $\left(\frac{p_i}{p}\right)$. Hemos calculado $\left(\frac{-1}{p}\right)$ y $\left(\frac{2}{p}\right)$ en V.2.4 (2.6) y el Corolario V.2.7, respectivamente. Para calcular $\left(\frac{p_i}{p}\right)$ se emplea la Ley de reciprocidad cuadrática, que permite sustituir $\left(\frac{p_i}{p}\right)$ por otro símbolo con "denominador" menor. Tras sucesivas inversiones y divisiones, el cálculo se reduce a las cantidades conocidas $\left(\frac{-1}{p}\right)$ y $\left(\frac{2}{p}\right)$. □

Ejercicios y problemas propuestos

Número V.1 Sean $\omega := e^{2\pi i/3}$ y $A := \{a + b\omega : a, b \in \mathbb{Z}\}$.

(1) Comprobar que el polinomio mínimo $f := P_{\mathbb{Q},\omega}$ de ω sobre $\mathbb{Q}$ tiene coeficientes enteros y demostrar que A es un subanillo de $\mathbb{C}$ cerrado respecto de la conjugación de números complejos.

(2) Demostrar que la función

$$\|\cdot\| : A \to \mathbb{N},\ a + b\omega \mapsto a^2 + b^2 - ab$$

es una norma que dota al anillo A de estructura de dominio euclídeo. ¿Cuáles son las unidades de A?

(3) Sea $p \in \mathbb{Z}$ un número primo y denotemos $\widehat{f}$ la imagen de f por el epimorfismo canónico $\mathbb{Z}[\mathtt{t}] \to \mathbb{Z}_p[\mathtt{t}]$ que transforma $\mathtt{t}$ en $\mathtt{t}$ y cada $k \in \mathbb{Z}$ en su clase $\widehat{k} = k \bmod p$. Sea $\mathfrak{a}$ el ideal de $\mathbb{Z}_p[\mathtt{t}]$ generado por $\widehat{f}$. Demostrar que la aplicación

$$\varphi : A \to \mathbb{Z}_p[\mathtt{t}]/\mathfrak{a},\ a + b\omega \mapsto (\widehat{a} + \widehat{b}\mathtt{t}) + \mathfrak{a}$$

es un epimorfismo de anillos. Calcular un generador del núcleo de φ.

(4) Probar que un número primo $p \in \mathbb{Z}$ es irreducible en A si y sólo si $p \equiv 2 \bmod 6$ o $p \equiv 5 \bmod 6$.

(5) ¿Cuántos elementos tiene el cuerpo $K := A/2A$?

Número V.2 Probar que el polinomio $f(\mathtt{t}) := \mathtt{t}^3 + 2\mathtt{t} + 2 \in \mathbb{F}_3[\mathtt{t}]$ es irreducible y sea u una raíz de f en una extensión de $\mathbb{F}_3$. Hallar las raíces cúbicas de $u + 2$ en $\mathbb{F}_3(u)$.

Número V.3 (1) Sea $A := \mathbb{Z}[i]$ el anillo de los enteros de Gauss. Demostrar que el cociente $E := A/7A$ es un cuerpo finito y calcular cuántos elementos tiene.

(2) Determinar el cuerpo primo K de E y un elemento primitivo ξ de la extensión $E|K$. Calcular el polinomio mínimo de ξ sobre K.

Número V.4 (1) Sean $p \in \mathbb{Z}$ primo y $f \in \mathbb{F}_p[\mathtt{t}]$. Probar que $(f(\mathtt{t}))^p = f(\mathtt{t}^p)$ y que si α es raíz de f entonces también lo es α^{p^n} para cada $n \in \mathbb{Z}^+$.

(2) Hallar los polinomios mínimos de β^2 y β^3 sobre $\mathbb{F}_2$ sabiendo que $\beta^4 + \beta + 1 = 0$.

Número V.5 Sea K un cuerpo finito con q elementos. Determinar el número de polinomios mónicos e irreducibles de grado 3 en $K[\mathtt{t}]$.

Número V.6 Sean $p \in \mathbb{Z}$ un número primo mayor que 3 y L_f un cuerpo de descomposición del polinomio $f(\mathtt{t}) := \mathtt{t}^p - 3$ sobre $\mathbb{F}_p$. Calcular el grado $[L_f : \mathbb{F}_p]$.

Número V.7 ¿Son isomorfos los cuerpos de descomposición sobre el cuerpo $\mathbb{F}_3$ de los polinomios

$$f(\mathtt{t}) := \mathtt{t}^3 + 2\mathtt{t} + 1 \quad \& \quad g(\mathtt{t}) := \mathtt{t}^3 + \mathtt{t}^2 + \mathtt{t} + 2?$$

Si lo son, definir un isomorfismo entre ellos.

Número V.8 (1) Factorizar $\mathtt{t}^{16} - \mathtt{t}$ como producto de polinomios irreducibles en $\mathbb{F}_2[\mathtt{t}]$.

(2) Factorizar como producto de polinomios irreducibles en $\mathbb{F}_3[\mathtt{t}]$ el polinomio $\mathtt{t}^9 - \mathtt{t}$.

Número V.9 Escribir las tablas de sumar y multiplicar del cuerpo de 9 elementos.

Número V.10 Sean p y q dos números primos. Calcular el número de polinomios mónicos e irreducibles en $\mathbb{F}_p[\mathtt{t}]$ de grados 4, 6 y q.

Número V.11 Sea F un cuerpo finito de característica $p > 0$. Describir su cierre algebraico y demostrar que es un cuerpo numerable y no finito.

Número V.12 Demostrar que toda raíz α del polinomio $f(\mathtt{t}) := \mathtt{t}^3 + \mathtt{t} + 1 \in \mathbb{F}_2[\mathtt{t}]$ en un cierre algebraico de $\mathbb{F}_2$ es un generador del grupo multiplicativo $\mathbb{F}_{2^3}^*$ formado por los elementos no nulos del cuerpo con 8 elementos.

Número V.13 Sean K un cuerpo finito y $\mathtt{t}$ una indeterminada sobre K. Demostrar que para cada automorfismo $\varphi : K(\mathtt{t}) \to K(\mathtt{t})$ se cumple que $\varphi(K) = K$.

Número V.14 Sean p un número primo, K un cuerpo finito de característica p y α una raíz del polinomio $f(\mathtt{t}) := \mathtt{t}^p - \mathtt{t} - a \in K[\mathtt{t}]$, donde $a \in K^* := K \setminus \{0\}$.

(1) Demostrar que $K(\alpha)$ es cuerpo de descomposición de f sobre K y expresar en función de α las restantes raíces de f.

(2) Probar que si no es trivial el grupo de Galois $G(K(\alpha) : K)$ es cíclico de orden p.

(3) Demostrar que si f es reducible en $K[\mathtt{t}]$ entonces factoriza en $K[\mathtt{t}]$ como producto de factores de grado 1.

(4) Demostrar que si $a \in \mathbb{F}_p \setminus \{0\}$ entonces f es irreducible en $\mathbb{F}_p[\mathtt{t}]$.

Número V.15 Sean K un cuerpo con 2^{10} elementos y $\alpha \in K^*$ un generador del grupo multiplicativo $K^* := K \setminus \{0\}$. Hallar un elemento primitivo de cada subextensión de $K|\mathbb{F}_2$.

Número V.16 Demostrar que $f(\mathtt{t}) := \mathtt{t}^4 + 1$ es irreducible como polinomio en $\mathbb{Z}[\mathtt{t}]$ pero es reducible en $\mathbb{F}_p[\mathtt{t}]$ para cada primo p.

Número V.17 ¿Tiene alguna raíz el polinomio $f(\mathtt{t}) := \mathtt{t}^2 - [7]_{23} \in \mathbb{F}_{23}[\mathtt{t}]$ en el cuerpo $\mathbb{F}_{23}$?

Número V.18 ¿Tiene alguna raíz en el cuerpo finito $\mathbb{F}_{97}$ con 97 elementos el polinomio $f(\mathtt{t}) := \mathtt{t}^2 - [2002]_{97} \in \mathbb{F}_{97}[\mathtt{t}]$?

Número V.19 ¿Existe algún número entero x tal que $x^2 + 4x + 3 \equiv 7 \bmod 11$?

Número V.20 Sean $K := \mathbb{F}_{31}$ y $f(\mathtt{x}, \mathtt{y}) := 317\mathtt{x}^2 - 151\mathtt{xy} + 40\mathtt{y}^2$. Decidir si existe algún punto $(a, b) \in K^2$ con alguna coordenada no nula en el que se anula la forma cuadrática f.

Número V.21 ¿Para qué primos p tiene $[-7]_p$ raíz cuadrada en el cuerpo $\mathbb{F}_p$?

Número V.22 Calcular, para cada primo impar p, el símbolo de Legendre $\left(\frac{3}{p}\right)$.

Número V.23 (1) Sea p un primo tal que $q := 2p + 1$ es primo y $p \equiv 3 \bmod 4$. Demostrar que $2^p \equiv 1 \bmod q$.

(2) ¿Es primo el número $2^{59} - 1$?

Número V.24 ¿Para qué primos p existen $x, y \in \mathbb{Z}$ tales que $p = x^2 + 7y^2$?

Número V.25 (1) Sean p un primo impar, $a \in \mathbb{Z} \setminus p\mathbb{Z}$ y $k \geq 2$ un entero. Demostrar que el número de soluciones de la ecuación $\mathtt{x}^2 \equiv a \bmod p$ coincide con el número de soluciones de la ecuación $\mathtt{x}^2 \equiv a \bmod p^k$.

(2) Encontrar las soluciones de la ecuación $\mathtt{x}^2 \equiv 14 \bmod 625$.

Número V.26 Sean K un cuerpo finito de característica distinta de 2 y tres elementos $a, b, c \in K^*$. Demostrar que existen $x, y \in K$ tales que $c = ax^2 + by^2$.

Número V.27 Sea p un número primo. Determinar el número de puntos del conjunto

$$X := \{(x, y, z) \in \mathbb{F}_p^3 : x^2 + y^2 + z^2 = 0\}.$$

Número V.28 (Teorema de Erdös-Ginzburg-Ziv) Sean p un número primo y números enteros $a_1, \ldots, a_{2p-1}$. Probar que existe un subconjunto I de $\{1, \ldots, 2p-1\}$ con p elementos tal que $\sum_{i \in I} a_i \equiv 0 \bmod p$.

CAPÍTULO VI

Grupo de Galois de algunos polinomios

En la primera sección de este capítulo se introduce la noción de grupo de Galois de un polinomio $f \in K[\mathtt{t}]$ donde K es un cuerpo de característica 0 y probamos que la irreducibilidad de f equivale a que dicho grupo sea un subgrupo transitivo del grupo de permutaciones de sus raíces. Tres son los resultados fundamentales en esta sección. Vemos primero que para cada número primo p el grupo simétrico $\mathcal{S}_p$ es el grupo de Galois de un polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$ de grado p. Después calculamos el grupo de Galois de los polinomios ciclotómicos, y los empleamos para demostrar una forma débil del Teorema del número primo de Dirichlet. Esto nos permite ver que $\mathbb{Z}_n$ es el grupo de Galois sobre $\mathbb{Q}$ de algún polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$ de grado n.

En la sección segunda se introduce la acción natural del grupo simétrico $\mathcal{S}_n$ sobre el anillo de polinomios en n variables, lo que nos permite estudiar el grupo de Galois del polinomio general de grado n y presentar un procedimiento algorítmico para determinar el *grupo de Galois de los polinomios de grado* ≤ 5 con coeficientes en un cuerpo de característica 0.

1. Grupo de Galois de un polinomio.

Definición y Observaciones VI.1.1 (1) Para cada $f \in K[\mathtt{t}]$ sea L_f un cuerpo de descomposición de f sobre K. Se define el *grupo de Galois* $G_K(f)$ *de* f *sobre* K como el grupo $G_K(f) := G(L_f : K)$ de K-automorfismos de L_f.

(2) Vimos en el Teorema II.1.2 que el cuerpo de descomposición de un polinomio es único salvo K-isomorfismo, por lo que la definición del grupo $G_K(f)$ es consistente, salvo isomorfía. Se desprende de IV.1.4 que si $Z_{L_f}(f)$ denota el conjunto de raíces de f en L_f, el grupo $G_K(f)$ es isomorfo a un subgrupo del grupo de biyecciones de $Z_{L_f}(f)$, pues cada automorfismo $\phi \in G_K(f)$ queda

determinado por su restricción $\phi|_{Z_{L_f}(f)}$. Así, si $Z_{L_f}(f)$ tiene n elementos, la aplicación

$$G_K(f) \to \mathrm{Biy}(Z_{L_f}(f)) = \mathcal{S}_n,\ \phi \mapsto \phi|_{Z_{L_f}(f)}$$

es un homomorfismo inyectivo, luego $G_K(f)$ es isomorfo a su imagen, que es un subgrupo de $\mathcal{S}_n$.

(3) En particular, y puesto que $\mathrm{char}(K) = 0$, podemos aplicar II.1.3 (2) y deducir que si f es irreducible en $K[\mathtt{t}]$ entonces todas sus raíces son simples, y en consecuencia, $\mathrm{Card}(Z_{L_f}(f)) = \deg(f) = n$ y $G_K(f)$ es un subgrupo de $\mathcal{S}_n$. Vía esta identificación, y si $Z_{L_f}(f) = \{\alpha_1, \ldots, \alpha_n\}$, se tiene $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ para cada $\sigma \in G_K(f)$ y cada $1 \leq i \leq n$.

Proposición VI.1.2 (1) *Un polinomio $f \in K[\mathtt{t}]$ de grado n es irreducible en $K[\mathtt{t}]$ si y sólo si su grupo de Galois $G_K(f)$ es un subgrupo* transitivo *de $\mathcal{S}_n$, es decir, para $1 \leq i, j \leq n$ existe $\sigma \in G_K(f)$ tal que $\sigma(\alpha_i) = \alpha_j$.*

(2) *En particular, si $f \in K[\mathtt{t}]$ es irreducible y $\deg(f) = n$, entonces el orden de su grupo de Galois $G_K(f)$ es múltiplo de n.*

Demostración. (1) Supongamos que f es irreducible en $K[\mathtt{t}]$. Entonces, por el Lema II.1.1, como los polinomios mínimos de α_i y α_j sobre K coinciden, pues ambos son f, existe un K-isomorfismo $\psi : K(\alpha_i) \to K(\alpha_j)$ tal que $\psi(\alpha_i) = \alpha_j$. Como $L_f(\alpha_i) = L_f = L_f(\alpha_j)$ es el cuerpo de descomposición de f sobre $K(\alpha_i)$ y sobre $K(\alpha_j)$, se deduce del Lema II.1.2 que existe un automorfismo $\sigma : L_f \to L_f$ tal que $\sigma|_{K(\alpha_i)} = \psi$, y por tanto, $\sigma(\alpha_i) = \psi(\alpha_i) = \alpha_j$.

Recíprocamente, suponemos que $G_K(f)$ es transitivo y sea $g \in K[\mathtt{t}]$ un factor irreducible y mónico de f. Todo se reduce a probar que $f = g$ y, como las raíces de f en L_f son simples, es suficiente demostrar que toda raíz $\alpha \in L_f$ de f lo es también de g. Tomamos una raíz $\beta \in L_f$ de g. Por ser $G_K(f)$ un grupo transitivo existe $\sigma \in G_K(f)$ tal que $\sigma(\beta) = \alpha$ y, como $g = \sum_{j=0}^{d} a_j \mathtt{t}^j \in K[\mathtt{t}]$, cada $\sigma(a_j) = a_j$ y se tiene

$$g(\alpha) = g(\sigma(\beta)) = \sum_{j=0}^{d} \sigma(a_j)\sigma(\beta)^j = \sigma\big(\sum_{j=0}^{d} a_j \beta^j\big) = \sigma(g(\beta)) = \sigma(0) = 0.$$

(2) Este apartado se deduce del anterior y el Corolario IV.1.9, vol. I. □

Definiciones y Observaciones VI.1.3 (1) Vimos en I.1.7, vol. I, que para cada entero positivo n el conjunto

$$\mathcal{U}_n := \{\zeta \in \mathbb{C} : \zeta^n = 1\}$$

es un subgrupo cíclico del grupo multiplicativo $\mathbb{C}^*$ formado por los números complejos no nulos, llamado *grupo de las raíces n-ésimas de la unidad.* Análogamente, si K es un cuerpo de característica 0 todas las raíces del polinomio $f(\mathtt{t}) := \mathtt{t}^n - 1$ en un cierre algebraico $\overline{K}$ de K son simples ya que la única raíz de su derivada $f'(\mathtt{t}) = n\mathtt{t}^{n-1}$ es 0, (salvo para $n = 1$, en cuyo caso f' es 1), que no es raíz de f. En consecuencia,

$$\mathcal{U}_n(\overline{K}) := \{\zeta \in \overline{K} : \ \zeta^n = 1\}$$

es un subgrupo cíclico de orden n del grupo multiplicativo $\overline{K}^* := \overline{K} \setminus \{0\}$.

(2) Se dice que $\zeta \in \mathcal{U}_n(\overline{K})$ es una *raíz primitiva* n-ésima de la unidad si $\mathcal{U}_n(\overline{K}) = \langle\zeta\rangle$, es decir, si el orden $o(\zeta)$ de ζ como elemento de $\mathcal{U}_n(\overline{K})$ es n. Denotamos $\varphi : \mathbb{N} \to \mathbb{N}$ la función de Euler, VI.2.1 vol. I. El número de raíces primitivas n-ésimas de la unidad es $\varphi(n)$, pues vimos en VI.2.6, vol. I, que $\varphi(n)$ es el número de generadores de cada grupo cíclico de orden n. Denotaremos $\mathcal{P}_n$ el conjunto de raíces primitivas n-ésimas de la unidad, sin referencia expresa al cuerpo $\overline{K}$ al que pertenecen.

Comenzamos calculando el grupo de Galois del polinomio más sencillo: $\mathtt{t}^n - a$. Entre otras cosas, utilizaremos este resultado en el Capítulo VII para estudiar la resolubilidad de ecuaciones polinómicas por radicales.

Lema VI.1.4 *Sean K un cuerpo de característica 0 y $f(\mathtt{t}) := \mathtt{t}^n - 1 \in K[\mathtt{t}]$, donde n es un entero positivo.*

(1) *El grupo de Galois $G_K(f)$ es abeliano.*

(2) *Supongamos que f factoriza en $K[\mathtt{t}]$ en producto de factores de grado 1. Sean $a \in K$ y $g(\mathtt{t}) := \mathtt{t}^n - a$. Entonces, el grupo de Galois $G_K(g)$ es abeliano.*

Demostración. (1) Sea $\zeta \in \mathcal{U}_n(\overline{K})$ una raíz primitiva n-ésima de la unidad. Así, $L_f := K(\zeta)$ es un cuerpo de descomposición de f sobre K, por lo que los K-automorfismos de L_f están determinados por la imagen de ζ que, por el Lema II.1.1, será ζ^k para cierto $1 \leq k \leq n$. Así, dados $\sigma_1, \sigma_2 \in G_K(f)$ existen k, ℓ tales que $\sigma_1(\zeta) = \zeta^k$ y $\sigma_2(\zeta) = \zeta^\ell$. En consecuencia,

$$(\sigma_2 \cdot \sigma_1)(\zeta) = \sigma_1(\zeta^\ell) = \zeta^{k\ell} = \zeta^{\ell k} = (\sigma_1 \cdot \sigma_2)(\zeta),$$

lo que implica que $\sigma_1 \cdot \sigma_2 = \sigma_2 \cdot \sigma_1$ así que $G_K(f)$ es un grupo abeliano.

(2) Para $a = 0$ el cuerpo K es cuerpo de descomposición de g sobre K, por lo que el grupo $G_K(g)$ es trivial. Suponemos en lo que sigue que $a \neq 0$ y, puesto que f factoriza en $K[\mathtt{t}]$ en producto de factores de grado 1, existe un generador $\zeta \in K$ del grupo $\mathcal{U}_n(\overline{K})$. Elegimos una raíz $\alpha \in \overline{K}$ de g. Entonces, para $0 \leq j \leq n-1$ se tiene

$$g(\alpha\zeta^j) = (\alpha\zeta^j)^n - a = \alpha^n(\zeta^n)^j - a = a - a = 0.$$

Como $\alpha\zeta^j \neq \alpha\zeta^k$ si $0 \leq j < k \leq n-1$ ya que $\alpha \neq 0$, se deduce que

$$g(\mathtt{t}) = \prod_{j=0}^{n-1} (\mathtt{t} - \alpha\zeta^j).$$

Por tanto, un cuerpo de descomposición de g sobre K es $L_g := K(\alpha, \zeta) = K(\alpha)$, luego cada elemento del grupo de Galois $G_K(g)$ queda determinado por la imagen de α que, por el Lema II.1.1, es un elemento de la forma $\alpha\zeta^j$ para cierto $0 \leq j \leq n-1$. De este modo, si $\sigma_1, \sigma_2 \in G_K(g)$ existen exponentes $0 \leq j < k \leq n-1$ tales que $\sigma_1(\alpha) = \alpha\zeta^j$ y $\sigma_2(\alpha) = \alpha\zeta^k$, y por tanto, como $\sigma_1(\zeta) = \sigma_2(\zeta) = \zeta \in K$,

$$(\sigma_2 \cdot \sigma_1)(\alpha) = \sigma_1(\alpha\zeta^k) = \sigma_1(\alpha)\sigma_1(\zeta)^k = \alpha\zeta^j\zeta^k = \alpha\zeta^{j+k}.$$

Así, $(\sigma_1 \cdot \sigma_2)(\alpha) = \alpha\zeta^{k+j} = (\sigma_2 \cdot \sigma_1)(\alpha)$, y por ello $\sigma_1 \cdot \sigma_2 = \sigma_2 \cdot \sigma_1$, por lo que $G_K(g)$ es abeliano. □

1.a. $\mathcal{S}_p$ como grupo de Galois. En esta subsección probamos que si p es primo el grupo simétrico $\mathcal{S}_p$ es el grupo de Galois de un polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$ de grado p. Para verlo emplearemos el siguiente lema, que es básico para calcular el grupo de Galois de algunos polinomios con coeficientes racionales.

Lema VI.1.5 *Sean $L|\mathbb{Q}$ una subextensión de Galois de $\mathbb{C}|\mathbb{Q}$ y denotemos*

$$\sigma : \mathbb{C} \to \mathbb{C},\ a + \sqrt{-1}b \mapsto a - \sqrt{-1}b \quad \forall\ a, b \in \mathbb{R}.$$

(1) *Se cumple la igualdad $\sigma(L) = L$. Por tanto $\tau := \sigma|_L$ es un elemento del grupo de Galois $G(L : \mathbb{Q})$ cuyo cuerpo fijo es $L \cap \mathbb{R}$.*

(2) *El automorfismo τ es la identidad si $L \subset \mathbb{R}$ y tiene orden 2 en caso contrario.*

Demostración. (1) Como $\sigma \circ \sigma = \mathrm{id}_{\mathbb{C}}$, para probar que $\sigma(L) = L$ es suficiente demostrar la inclusión $\sigma(L) \subset L$, pues en tal caso $L = \sigma(\sigma(L)) \subset \sigma(L) \subset L$. Para cada $\alpha \in L$ sea $P_{\mathbb{Q},\alpha}(\mathtt{t}) := \sum_{j=0}^{d} a_j \mathtt{t}^j$ el polinomio mínimo de α sobre $\mathbb{Q}$. Como $P_{\mathbb{Q},\alpha}(\alpha) = 0$ se tiene

$$0 = \sigma(0) = \sigma(P_{\mathbb{Q},\alpha}(\alpha)) = \sigma\Big(\sum_{j=0}^{d} a_j \alpha^j\Big) = \sum_{j=0}^{d} a_j (\sigma(\alpha))^j = P_{\mathbb{Q},\alpha}(\sigma(\alpha)),$$

es decir, $\sigma(\alpha)$ es una raíz de $P_{\mathbb{Q},\alpha}$. Como $L|\mathbb{Q}$ es una extensión de Galois y el polinomio irreducible $P_{\mathbb{Q},\alpha} \in \mathbb{Q}[\mathtt{t}]$ tiene una raíz $\alpha \in L$ se deduce de la Proposición IV.1.6 que también $\sigma(\alpha) \in L$, así que $\sigma(L) \subset L$. Además, $\mathrm{Fix}(\tau) = L \cap \mathrm{Fix}(\sigma) = L \cap \mathbb{R}$.

(2) La igualdad $\tau = \mathrm{id}_L$ equivale a que $L = \mathrm{Fix}(\tau) = L \cap \mathbb{R}$, esto es, $L \subset \mathbb{R}$. Por ello si $L \not\subset \mathbb{R}$, y puesto que $\tau \circ \tau = \mathrm{id}_L$, se sigue que $o(\tau) = 2$. □

Corolario VI.1.6 *Sea $f \in \mathbb{Q}[\mathtt{t}]$ un polinomio irreducible de grado $n \geq 3$ que tiene, exactamente, dos raíces en $\mathbb{C} \setminus \mathbb{R}$. Entonces el grupo de Galois $G_{\mathbb{Q}}(f)$ de f sobre $\mathbb{Q}$ contiene, como subgrupo de $\mathcal{S}_n$, una transposición. En particular, si $p = n$ es primo, entonces $G_{\mathbb{Q}}(f) = \mathcal{S}_p$.*

Demostración. Como $\mathbb{C}$ es algebraicamente cerrado contiene un cuerpo de descomposición L_f de f sobre $\mathbb{Q}$. Además, $L_f \not\subset \mathbb{R}$, luego por el Lema anterior VI.1.5, la restricción $\tau := \sigma|_{L_f}$ de la conjugación compleja $\sigma : \mathbb{C} \to \mathbb{C}$ es un elemento de orden 2 del grupo de Galois $G_{\mathbb{Q}}(f) = G(L_f : \mathbb{Q})$, cuyo cuerpo fijo es $L_f \cap \mathbb{R}$. Sean $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ las raíces de f en $\mathbb{C}$. Podemos suponer que $\alpha_1, \alpha_2 \in \mathbb{C} \setminus \mathbb{R}$ y que $\alpha_3, \ldots, \alpha_n \in \mathbb{R}$. Así, $\alpha_3, \ldots, \alpha_n \in \mathrm{Fix}(\tau)$, mientras que α_1, α_2 son conjugadas una de la otra, por lo que $\tau(\alpha_1) = \alpha_2$ y $\tau(\alpha_2) = \alpha_1$. Por tanto, interpretando $G_{\mathbb{Q}}(f)$ como subgrupo de $\mathcal{S}_n$ vía el homomorfismo inyectivo

$$G_{\mathbb{Q}}(f) \hookrightarrow \mathcal{S}_n,\ \sigma \mapsto \sigma|_{\{\alpha_1,\ldots,\alpha_n\}},$$

la involución τ se identifica con la transposición $(1,2) \in \mathcal{S}_n$.

Para la segunda parte, supongamos que $n = p$ es primo. En la Proposición VI.1.2 demostramos que $G_{\mathbb{Q}}(f)$ es un subgrupo transitivo de $\mathcal{S}_p$. Como además contiene una transposición, la igualdad $G_{\mathbb{Q}}(f) = \mathcal{S}_p$ se deduce de la Proposición III.2.7 vol. I. □

Ejemplo VI.1.7 Para cada número primo $p \geq 3$ existe un polinomio irreducible $f \in \mathbb{Q}[\mathtt{t}]$ de grado p cuyo grupo de Galois sobre $\mathbb{Q}$ es el grupo simétrico

$\mathcal{S}_p$. Para demostrarlo es suficiente, a la vista del Corolario anterior VI.1.6, encontrar, para cada entero $n \geq 3$, un polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$ de grado n y con, exactamente, dos raíces en $\mathbb{C}\setminus\mathbb{R}$. Denotamos $k := n-2 \geq 1$ e introducimos el polinomio auxiliar

$$g(\mathtt{t}) := (\mathtt{t}^2+4)\prod_{j=1}^{k}(\mathtt{t}-2j),$$

que tiene grado n y cumple las siguientes propiedades:

(i) Salvo el coeficiente director que vale 1, todos los coeficientes de g son pares y su término independiente es múltiplo de 4.

(ii) Para $1 \leq \ell \leq k-1$ el valor máximo de $|g|$ en el intervalo $I_\ell := [2\ell, 2\ell+2]$ es $M_\ell > 4$ y su signo en I_ℓ es constante, de valor $(-1)^{k-\ell} = (-1)^{n-\ell}$. En efecto, se cumple

$$\begin{aligned} M_\ell \geq |g(2\ell+1)| &= \left|(2\ell+1)^2+4\right| \cdot \prod_{j=1}^{k} |(2\ell+1-2j)| \\ &= \left|(2\ell+1)^2+4\right| \cdot \prod_{j=1}^{k} |2(\ell-j)+1| \geq \left|(2\ell+1)^2+4\right| > 4. \end{aligned}$$

Como g no se anula en ningún punto de I_ℓ, su signo en dicho intervalo es constante, por el teorema de Bolzano, y concide con el de $g(2\ell+1)$, que es

$$g(2\ell+1) = \big((2\ell+1)^2+4\big)\cdot\prod_{j=1}^{k}(2\ell+1-2j) = \big((2\ell+1)^2+4\big)\cdot\prod_{j=1}^{k}\big(2(\ell-j)+1\big).$$

Por tanto, el signo de g en I_ℓ es $(-1)^{k-\ell} = (-1)^{n-\ell}$.

Para cada número racional $r \in (0,2]$ consideramos el polinomio

$$h_r(\mathtt{t}) := g(\mathtt{t}) - r \in \mathbb{Q}[\mathtt{t}],$$

que tiene al menos $n-2$ raíces reales. En efecto, $h_r(2\ell) = g(2\ell) - r = -r < 0$ para $1 \leq \ell \leq k-1$, y ya hemos señalado que el signo de $g(2\ell+1)$ es $(-1)^{n-\ell}$. Distinguimos dos casos.

(1) Si n es par entonces $g(2\ell+1) > 0$ si ℓ es par y, por el terorema de Bolzano, h_r tiene al menos dos raíces reales en $I_\ell = [2\ell, 2\ell+2]$ para $1 \leq \ell \leq k-1 = n-3$,

con ℓ par. Como hay $(n-4)/2$ enteros pares entre 1 y $n-3$, deducimos que h_r tiene al menos $n-4$ raíces reales en el intervalo $(4, 2n-6)$. Por otra parte

$$h_r(0) = g(0) - r = 4 \cdot \prod_{j=1}^{n-2}(-2j) - r = 4(-1)^{n-2} \cdot \prod_{j=1}^{n-2} 2j - r > 0$$

y, por tanto, como $h_r(2) = -r < 0$, se deduce del teorema de Bolzano que h_r tiene una raíz en el intervalo $(0, 2)$. Además, $h_r(2k) = -r < 0$ y

$$h_r(2k+1) = \big((2k+1)^2 + 4\big) \cdot \prod_{j=1}^{k}(2(k-j)+1) - r > 4 - r > 0,$$

luego h_r tiene alguna raíz más en el intervalo $(2k, 2k+1) = (2n-4, 2n-3)$. De este modo, h_r tiene, al menos, $n-2$ raíces en $\mathbb{R}$.

(2) Si n es impar entonces $g(2\ell+1) > 0$ si ℓ es impar y, por el teorema de Bolzano, h_r tiene al menos dos raíces reales en los intervalos $I_\ell = [2\ell, 2\ell+2]$ con $1 \le \ell \le k-1 = n-3$ y ℓ impar. Como hay $(n-3)/2$ enteros impares entre 1 y $n-3$, deducimos que h_r tiene al menos $n-3$ raíces reales en el intervalo $(2, 2n-4)$. Además, $h_r(2k) = -r < 0$ y

$$h_r(2k+1) = \big((2k+1)^2 + 4\big) \cdot \prod_{j=1}^{k}(2(k-j)+1) - r > 4 - r > 0,$$

con lo que h_r tiene alguna raíz más en el intervalo $(2k, 2k+1) = (2n-4, 2n-3)$.

En conclusión, con independencia de la paridad de n, el polinomio h_r tiene al menos $n-2$ raíces en $\mathbb{R}$.

Si h_r tiene alguna raíz real más entonces tiene n raíces reales y, por tanto, g toma el valor r en n puntos reales distintos. Como $r \in (0, 2]$ es positivo y g se anula sólo en $n-2$ puntos, para aumentar el número de raíces al *trasladar la grafica de g hacia abajo r unidades*, tiene que ocurrir que g alcance un mínimo local en un punto $u \in \mathbb{R}$ tal que $0 < g(u) < r$. Como los puntos en los que g tiene un mínimo local son raíces de su derivada g', que es un polinomio, existe a lo sumo un número finito de puntos $u \in \mathbb{R}$ en los que se anula la derivada y tales que $g(u) > 0$. Sea

$$m := \text{mín}\{g(u) : u \in \mathbb{R},\ g'(u) = 0,\ g(u) > 0\}.$$

Así, elegimos $0 < r < \text{mín}\{2, m\}$ y el polinomio h_r tiene, exactamente, $n-2$ raíces en $\mathbb{R}$. Por último tomamos un primo $p > 2$ con $0 < r = 2/p < \text{mín}\{2, m\}$.

Por lo que acabamos de ver, el polinomio $f := ph_r - 2$ tiene, exactamente, $n-2$ raíces en $\mathbb{R}$ y es irreducible en $\mathbb{Z}[\mathtt{t}]$ como consecuencia del Criterio de Eisenstein VI.2.6, vol. II, ya que el número primo 2 divide a todos los coeficientes de f menos al coeficiente director y 4 no divide al término independiente. Por el Lema de Gauss, f es también irreducible $\mathbb{Q}[\mathtt{t}]$ y es el polinomio buscado.

Corolario VI.1.8 *Para cada grupo finito G existen una extensión finita $K|\mathbb{Q}$ y una extensión de Galois $L|K$ tales que el grupo de Galois $G(L : K)$ es isomorfo a G.*

Demostración. Sean $n := \mathrm{ord}(G)$ el orden del grupo G y p un número primo mayor que n. Por el Teorema de Cayley, III.1.2, vol. I., G es subgrupo del grupo de permutaciones $\mathcal{S}_n$, que a su vez es subgrupo de $\mathcal{S}_p$. En virtud del Corolario VI.1.6 y el Ejemplo VI.1.7, existe una extensión de Galois $L|\mathbb{Q}$ cuyo grupo de Galois es $\mathcal{S}_p$, y consideramos el cuerpo fijo $K := \mathrm{Fix}(G)$. Como la extensión $L|\mathbb{Q}$ es de Galois también $L|K$ lo es, y por el Teorema fundamental de la Teoría de Galois, IV.2.3, $G(L : K) = G(L : \mathrm{Fix}(G)) = G$. □

1.b. Grupo de Galois de los polinomios ciclotómicos. Introducimos ahora los polinomios ciclotómicos, calculamos su grupo de Galois, obtenemos una forma débil del Teorema del número primo de Dirichlet y probamos que $\mathbb{Z}_n = G_{\mathbb{Q}}(f)$ para cierto polinomio irreducible $f \in \mathbb{Q}[\mathtt{t}]$ de grado n.

Definición y Observaciones VI.1.9 (1) Para cada $n \geq 1$ consideramos el polinomio

$$\Phi_n(\mathtt{t}) := \prod_{\zeta \in \mathcal{P}_n} (\mathtt{t} - \zeta) \in \mathbb{C}[\mathtt{t}].$$

El polinomio mónico Φ_n recibe el nombre de n-ésimo *polinomio ciclotómico.* Si $n = p$ es un número primo la única raíz p-ésima de la unidad que no es primitiva es 1, luego

$$\Phi_p(\mathtt{t}) = \prod_{\zeta \in \mathcal{P}_p} (\mathtt{t} - \zeta) = \frac{\mathtt{t}^p - 1}{\mathtt{t} - 1} = \sum_{j=0}^{p-1} \mathtt{t}^j,$$

que coincide con la definición de p-ésimo polinomio ciclotómico dada en VI.2.7, vol. II.

(2) Ya hemos señalado que $\mathrm{Card}(\mathcal{P}_n) = \varphi(n)$, donde φ es la función de Euler. En consecuencia, $\deg(\Phi_n) = \varphi(n)$. Además, se deduce directamente de la definición que todas las raíces de Φ_n en $\mathbb{C}$ son simples.

(3) Sean $d > 0$ un divisor de n y $\zeta \in \mathcal{U}_n$. Ésta es raíz primitiva d-ésima de la unidad si y sólo si $o(\zeta) = d$, donde $o(\zeta)$ es el orden de ζ como elemento de $\mathcal{U}_n$.

(4) Denotemos $D(n) := \{d \geq 1 : d|n\}$ el conjunto formado por los divisores positivos de n. Por la Fórmula de Lagrange, $o(\zeta) \in D(n)$ para cada $\zeta \in \mathcal{U}_n$. Por tanto, $\mathcal{U}_n = \bigsqcup_{d \in D(n)} \mathcal{P}_d$, es decir, toda raíz n-ésima de la unidad es raíz primitiva d-ésima de la unidad para un único divisor d de n. En consecuencia,

$$\mathtt{t}^n - 1 = \prod_{\zeta \in \mathcal{U}_n} (\mathtt{t} - \zeta) = \prod_{d \in D(n)} \prod_{\zeta \in \mathcal{P}_d} (\mathtt{t} - \zeta) = \prod_{d \in D(n)} \Phi_d(\mathtt{t}). \tag{1.1}$$

Proposición VI.1.10 *Para cada entero $n \geq 1$ el polinomio $\Phi_n \in \mathbb{Z}[\mathtt{t}]$, y si $n \geq 2$ su término independiente vale* 1.

Demostración. El resultado es obvio para $n = 1$ ya que $\Phi_1(\mathtt{t}) = \mathtt{t} - 1$. Argumentamos por inducción sobre n y denotamos $D'(n) := D(n) \setminus \{n\}$. Así, escribimos la fórmula (1.1) anterior como

$$\mathtt{t}^n - 1 = \prod_{d \in D(n)} \Phi_d(\mathtt{t}) = \Phi_n(\mathtt{t}) \cdot \prod_{d \in D'(n)} \Phi_d(\mathtt{t}) = \Phi_n(\mathtt{t}) \cdot p(\mathtt{t}) \tag{1.2}$$

y, por la hipótesis de inducción, $\Phi_d \in \mathbb{Z}[\mathtt{t}]$ para cada $d \in D'(n)$. Por tanto, $p \in \mathbb{Z}[\mathtt{t}]$ y, como es mónico por serlo cada polinomio ciclotómico, existen polinomios $q, r \in \mathbb{Z}[\mathtt{t}]$ tales que $\deg(r) < \deg(p)$ y $\mathtt{t}^n - 1 = pq + r$. Esta igualdad es también una división euclídea en el dominio euclídeo $\mathbb{C}[\mathtt{t}]$, pero otra división euclídea de $\mathtt{t}^n - 1$ entre p en $\mathbb{C}[\mathtt{t}]$ es $\mathtt{t}^n - 1 = p(\mathtt{t}) \cdot \Phi_n(\mathtt{t}) + 0$. Por la unicidad del cociente y el resto, deducimos que $r = 0$ y $\Phi_n = q \in \mathbb{Z}[\mathtt{t}]$.

También empleamos la inducción para probar que $\Phi_n(0) = 1$. El caso $n = 2$ es obvio pues $\Phi_2(\mathtt{t}) = \mathtt{t} + 1$. Suponemos el resultado probado para cada entero m con $2 \leq m < n$ y escribimos la igualdad (1.2) como

$$\mathtt{t}^n - 1 = \prod_{d \in D(n)} \Phi_d(\mathtt{t}) = (\mathtt{t} - 1) \cdot \Phi_n(\mathtt{t}) \cdot \prod_{d \in D''(n)} \Phi_d(\mathtt{t}),$$

donde $D''(n) = D'(n) \setminus \{1\}$. Por la hipótesis de inducción $\Phi_d(0) = 1$ para cada $d \in D''(n)$, así que $-1 = (-1) \cdot \Phi_n(0) \cdot 1$, es decir, $\Phi_n(0) = 1$. □

Teorema VI.1.11 *Para cada $n \geq 1$ el polinomio ciclotómico $\Phi_n \in \mathbb{Z}[\mathtt{t}]$ es irreducible en $\mathbb{Q}[\mathtt{t}]$ y el grupo de Galois $G_{\mathbb{Q}}(\Phi_n)$ de Φ_n sobre $\mathbb{Q}$ es isomorfo al grupo $\mathbb{Z}_n^*$ de las unidades del anillo $\mathbb{Z}_n$.*

Demostración. Para demostrar la irreduciblidad de Φ_n en $\mathbb{Q}[\mathtt{t}]$ es suficiente probar que lo es en $\mathbb{Z}[\mathtt{t}]$. Supongamos lo contrario, esto es, existen polinomios mónicos $f, g \in \mathbb{Z}[\mathtt{t}]$ de grado mayor o igual que 1 tales que f es irreducible en $\mathbb{Z}[\mathtt{t}]$ y $\Phi_n = fg$. En particular, f es irreducible en $\mathbb{Q}[\mathtt{t}]$ y elegimos una raíz ζ de f en $\mathbb{C}$. Como ζ es una raíz primitiva n-ésima de la unidad genera el grupo $\mathcal{U}_n$. En particular las restantes raíces de Φ_n, que son raíces n-ésimas de la unidad, son potencias de ζ, luego $\mathbb{Q}(\zeta)$ es un cuerpo de descomposición de Φ_n sobre $\mathbb{Q}$. Veamos que:

Si un número primo p no divide a n, y $\xi \in \mathbb{C}$ es raíz de f, entonces ξ^p es también raíz de f.

En efecto, supongamos, por reducción al absurdo, que $f(\xi^p) \neq 0$. Obsérvese que $\xi^p \in \mathcal{U}_n$ y, de hecho, ξ^p es raíz primitiva n-ésima de la unidad, ya que $o(\xi^p) = o(\xi)/\operatorname{mcd}(p,n) = n$. Esto implica que $\Phi_n(\xi^p) = 0$, luego $g(\xi^p) = 0$. Sea $h(\mathtt{t}) := g(\mathtt{t}^p) \in \mathbb{Z}[\mathtt{t}]$. Como f es mónico se puede dividir h entre f en $\mathbb{Z}[\mathtt{t}]$ y existen un cociente $q \in \mathbb{Z}[\mathtt{t}]$ y un resto $r \in \mathbb{Z}[\mathtt{t}]$ tales que $h = fq + r$ y $\deg(r) < \deg(f)$. Ésta es también una división en el dominio euclídeo $\mathbb{Q}[\mathtt{t}]$. Pero, como $f = P_{\mathbb{Q},\xi}$ y $h(\xi) = g(\xi^p) = 0$, el polinomio h es múltiplo en $\mathbb{Q}[\mathtt{t}]$ de f. Por la unicidad de la división, $r = 0$, luego $q \in \mathbb{Z}[\mathtt{t}]$ y $h = fq$.

El epimorfismo $\mathbb{Z} \mapsto \mathbb{Z}_p,\ x \to [x]_p$ induce otro, llamado *reducción* $\bmod p$,

$$\Psi : \mathbb{Z}[\mathtt{t}] \to \mathbb{Z}_p[\mathtt{t}],\ u(\mathtt{t}) := \sum_{k=0}^{m} a_k \mathtt{t}^k \mapsto \sum_{k=0}^{m} [a_k]_p \mathtt{t}^k.$$

Escribimos $g(\mathtt{t}) := \sum_{j=0}^{\ell} b_j \mathtt{t}^j$, por lo que $h(\mathtt{t}) = \sum_{j=0}^{\ell} b_j \mathtt{t}^{jp}$. Para $0 \leq j \leq \ell$ se cumple, por el Pequeño Teorema de Fermat, la igualdad $[b_j]_p^p = [b_j]_p$, luego

$$\Psi(g)^p = \Big(\sum_{j=0}^{\ell} [b_j]_p \mathtt{t}^j \Big)^p = \sum_{j=0}^{\ell} [b_j]_p^p \mathtt{t}^{jp} = \sum_{j=0}^{\ell} [b_j]_p \mathtt{t}^{jp} = \Psi(h).$$

Por tanto, $\Psi(f) \cdot \Psi(q) = \Psi(h) = \Psi(g)^p$. Sea $q_1 \in \mathbb{Z}[\mathtt{t}]$ cuya imagen $\Psi(q_1)$ es un factor irreducible de $\Psi(f)$ en $\mathbb{Z}_p[\mathtt{t}]$. Como $\Psi(f)$ divide a $\Psi(h) = \Psi(g)^p$ se deduce que $\Psi(q_1)$ divide a $\Psi(g)^p$, por lo que $\Psi(q_1) | \Psi(g)$. Esto implica que $\Psi(q_1)^2$ divide a $\Psi(f) \cdot \Psi(g) = \Psi(\Phi_n)$, que a su vez divide a $\Psi(\mathtt{t}^n - 1)$. Por tanto, $\Psi(\mathtt{t}^n - 1) = \Psi(\mathtt{t})^n - 1$ tiene un factor múltiple, o lo que es lo mismo, $\Psi(\mathtt{t}^n - 1)$ y su derivada $n\Psi(\mathtt{t})^{n-1}$ tienen un factor en común. Como p y n son primos entre sí el polinomio $n\Psi(\mathtt{t})^{n-1}$ es no nulo y su único factor irreducible en $\mathbb{Z}[\mathtt{t}]$ es $\Psi(\mathtt{t})$. Por tanto, $\Psi(\mathtt{t})$ ha de dividir a $\Psi(\mathtt{t})^n - 1$, lo cual es falso. En consecuencia, ξ^p no es raíz de g, luego lo es de f.

Como $\deg(g) \geq 1$ existe $\eta \in \mathbb{C}$ tal que $g(\eta) = 0$, por lo que $\Phi_n(\eta) = 0$. Así η es una raíz primitiva n-ésima de la unidad, luego existe un entero $s \geq 1$ primo con n tal que $\eta = \zeta^s$. Escribimos $s = p_1 \cdots p_\ell$, donde cada p_i es un número primo que no divide a n. Como ζ es raíz de f se deduce de lo que acabamos de probar que ζ^{p_1} es también raíz de f y reiterando el proceso concluimos que $\eta = \zeta^{p_1 \cdots p_\ell}$ es raíz de f.

De este modo, f y g comparten una raíz, lo que significa que el polinomio ciclotómico Φ_n tiene una raíz múltiple en $\mathbb{C}$, y esto contradice VI.1.9 (2). Así, concluimos que Φ_n es irreducible en $\mathbb{Z}[\mathtt{t}]$.

Para terminar, veamos que el grupo de Galois $G_{\mathbb{Q}}(\Phi_n)$ es isomorfo al grupo $\mathbb{Z}_n^*$. Las raíces de Φ_n son las raíces primitivas n-ésimas de la unidad, que son $\zeta^{m_1}, \zeta^{m_2}, \ldots, \zeta^{m_t}$ donde $t := \varphi(n)$ y $1 = m_1 < m_2 < \cdots < m_t < n$ son los enteros entre 1 y $n-1$ primos con n. Por ello, el grupo de Galois $G_{\mathbb{Q}}(\Phi_n)$ es el conjunto de $\mathbb{Q}$-automorfismos $\{\tau_k : 1 \leq k \leq t\}$ de $\mathbb{Q}(\zeta)$ inducidos por las asignaciones $\tau_k : \zeta \mapsto \zeta^{m_k}$. El isomorfismo buscado es

$$\gamma : G_{\mathbb{Q}}(\Phi_n) \to \mathbb{Z}_n^*, \ \tau_k \mapsto [m_k]_n,$$

donde $[m_k]_n$ es la clase de $m_k \ \mathsf{mod}\, n$. En efecto, γ es una aplicación bien definida porque $\mcd(m_k, n) = 1$, esto es, $[m_k]_n \in \mathbb{Z}_n^*$, para $1 \leq k \leq t$. Además γ es homomorfismo, puesto que

$$(\tau_k \cdot \tau_\ell)(\zeta) = \tau_\ell(\tau_k(\zeta)) = \tau_\ell(\zeta^{m_k}) = (\tau_\ell(\zeta))^{m_k} = (\zeta^{m_\ell})^{m_k} = \zeta^{m_k m_\ell}.$$

La irreducibilidad de Φ_n implica que es el polinomio mínimo sobre $\mathbb{Q}$ de cualquiera de sus raíces, así que los grupos $G_{\mathbb{Q}}(\Phi_n)$ y $\mathbb{Z}_n^*$ tienen el mismo orden pues si $\varphi : \mathbb{N} \to \mathbb{N}$ es la función de Euler,

$$\mathrm{ord}\left(G_{\mathbb{Q}}(\Phi_n)\right) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(P_{\mathbb{Q},\zeta}) = \deg(\Phi_n) = \varphi(n) = \mathrm{ord}(\mathbb{Z}_n^*).$$

Por tanto sólo falta ver que γ es sobreyectiva, lo que es obvio porque las clases $m_k \ \mathsf{mod}\, n$ son distintas dos a dos. □

1.c. Método de cálculo de polinomios ciclotómicos. A continuación presentamos un procedimiento para calcular explícitamente los coeficientes de los polinomios ciclotómicos y algunas propiedades que permiten efectuar dicho cálculo de modo más eficiente.

Observaciones VI.1.12 (1) Dados primos distintos $p_1, \ldots, p_r$ y números enteros $\alpha_i \geq 1$, sea $n := p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Entonces,

$$\Phi_n(\mathtt{t}) = \Phi_{p_1 \cdots p_r}(\mathtt{t}^{p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}}).$$

En efecto, veamos en primer lugar que ambos miembros son polinomios del mismo grado. El de $\Phi_n(\mathtt{t})$ es $\varphi(n)$, donde $\varphi : \mathbb{N} \to \mathbb{N}$ es la función de Euler, mientras que el de $q(\mathtt{t}) := \Phi_{p_1 \cdots p_r}(\mathtt{t}^{p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}})$ es, en virtud de la Proposición VI.2.2 vol. I,

$$\deg(q) = \varphi(p_1 \cdots p_r) \prod_{i=1}^{r} p_i^{\alpha_i - 1} = \prod_{i=1}^{r} (p_i - 1) p_i^{\alpha_i - 1} = \varphi(n).$$

Además, tanto q como Φ_n son mónicos y Φ_n es, por el Teorema VI.1.11, irreducible en $\mathbb{Q}[\mathtt{t}]$. Sea ζ un raíz de Φ_n, que por tanto es una raíz primitiva n-ésima de la unidad. Basta probar que $q(\zeta) = 0$. Visto esto, q es múltiplo de $P_{\mathbb{Q},\zeta} = \Phi_n$ en $\mathbb{Q}[\mathtt{t}]$ y, como ambos son mónicos y tienen el mismo grado, coinciden.

Denotamos $m := \prod_{i=1}^{r} p_i^{\alpha_i - 1}$ y $s := p_1 \cdots p_r$, que cumplen $ms = n$. Nótese que ζ^m es raíz s-ésima de la unidad, pues $(\zeta^m)^s = \zeta^{ms} = \zeta^n = 1$. De hecho ζ^m es raíz primitiva s-ésima de la unidad, pues

$$o(\zeta^m) = o(\zeta)/\operatorname{mcd}(n, m) = n/m = s,$$

por lo que $\Phi_s(\zeta^m) = 0$, esto es $q(\zeta) = 0$.

(2) En particular, tomando $r = 1$, $p_1 = p$ y $\alpha_1 = \alpha$ resulta que si p es un número primo y α es un entero positivo, entonces $\Phi_{p^\alpha}(\mathtt{t}) = \Phi_p(\mathtt{t}^{p^{\alpha-1}})$.

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

En efecto, tanto $\Phi_{2n}(\mathtt{t})$ como $\Phi_n(-\mathtt{t})$ son polinomios mónicos e irreducibles en $\mathbb{Q}[\mathtt{t}]$, luego para demostrar que coinciden es suficiente probar que comparten alguna raíz $\xi \in \mathbb{C}$, pues en tal caso ambos son el polinomio mínimo de ξ sobre $\mathbb{Q}$. Tomamos una raíz cualquiera $\xi \in \mathbb{C}$ de Φ_{2n} y vamos a demostrar que $\Phi_n(-\xi) = 0$, para lo que hemos de ver que $-\xi$ es raíz primitiva n-ésima de la unidad. Nótese que

$$0 = \xi^{2n} - 1 = (\xi^n - 1)(\xi^n + 1),$$

y $\xi^n \neq 1$, ya que $o(\xi) = 2n$. Esto implica que $\xi^n = -1$ y, como n es impar,

$$(-\xi)^n = (-1)^n \xi^n = -\xi^n = 1.$$

Por tanto, $-\xi$ es raíz n-ésima de la unidad y para ver que es primitiva es suficiente demostrar que su orden, como elemento del grupo $\mathbb{C}^*$, es n. Puesto que $-\xi = (-1)\xi = \xi^n \cdot \xi = \xi^{n+1}$ y $2n = 2(n+1) - 2$, resulta

$$\begin{aligned} o(-\xi) = o(\xi^{n+1}) &= o(\xi)/\operatorname{mcd}(o(\xi), n+1) = 2n/\operatorname{mcd}(2n, n+1) \\ &= 2n/\operatorname{mcd}(2, n+1) = 2n/2 = n. \end{aligned}$$

(4) Sean n un entero positivo y p un número primo que no divide a n. Entonces

$$\Phi_n(\mathtt{t}) \cdot \Phi_{pn}(\mathtt{t}) = \Phi_n(\mathtt{t}^p).$$

Demostramos esta igualdad por inducción cuando n recorre los enteros positivos que no son múltiplos de p. Para $n = 1$ se tiene

$$\Phi_1(\mathtt{t}) \cdot \Phi_p(\mathtt{t}) = (\mathtt{t} - 1) \cdot (\mathtt{t}^{p-1} + \mathtt{t}^{p-2} + \cdots + \mathtt{t} + 1) = \mathtt{t}^p - 1 = \Phi_1(\mathtt{t}^p).$$

Si $n > 1$ y puesto que p es primo y $n \notin p\mathbb{Z}$, el conjunto $D(pn)$ de divisores positivos de pn es la unión disjunta $D(pn) = D(n) \sqcup pD(n)$, donde $D(n)$ es el conjunto de divisores positivos de n. En consecuencia, por VI.1.9 (4),

$$\begin{aligned}\mathtt{t}^{pn} - 1 = \prod_{d \in D(pn)} \Phi_d(\mathtt{t}) &= \prod_{d \in D(n)} \Phi_d(\mathtt{t}) \cdot \prod_{d \in D(n)} \Phi_{pd}(\mathtt{t}) \\ &= \Phi_{pn}(\mathtt{t}) \cdot \prod_{d \in D(n)} \Phi_d(\mathtt{t}) \cdot \prod_{d \in D'(n)} \Phi_{pd}(\mathtt{t}),\end{aligned}$$

donde $D'(n) := D(n) \setminus \{n\}$. Reagrupando términos reescribimos esto como

$$\mathtt{t}^{pn} - 1 = \Phi_{pn}(\mathtt{t}) \cdot \Phi_n(\mathtt{t}) \cdot \prod_{d \in D'(n)} \big(\Phi_d(\mathtt{t}) \cdot \Phi_{pd}(\mathtt{t})\big). \tag{1.3}$$

Cada divisor $d \in D'(n)$ de n no es múltiplo de p luego, por la hipótesis de inducción,

$$\Phi_d(\mathtt{t}) \cdot \Phi_{pd}(\mathtt{t}) = \Phi_d(\mathtt{t}^p) \quad \forall\ d \in D'(n),$$

lo que sustituido en la igualdad (1.3) nos proporciona

$$\mathtt{t}^{pn} - 1 = \Phi_{pn}(\mathtt{t}) \cdot \Phi_n(\mathtt{t}) \cdot \prod_{d \in D'(n)} \Phi_d(\mathtt{t}^p). \tag{1.4}$$

Por otro lado, si denotamos $\mathtt{x} := \mathtt{t}^p$ se tiene

$$\mathtt{t}^{pn} - 1 = \mathtt{x}^n - 1 = \prod_{d \in D(n)} \Phi_d(\mathtt{x}) = \Phi_n(\mathtt{x}) \cdot \prod_{d \in D'(n)} \Phi_d(\mathtt{x}) = \Phi_n(\mathtt{t}^p) \cdot \prod_{d \in D'(n)} \Phi_d(\mathtt{t}^p), \tag{1.5}$$

e igualando las expresiones de $\mathtt{t}^{pn} - 1$ obtenidas en (1.4) y (1.5) llegamos a

$$\Phi_{pn}(\mathtt{t}) \cdot \Phi_n(\mathtt{t}) \cdot \prod_{d \in D'(n)} \Phi_d(\mathtt{t}^p) = \mathtt{t}^{pn} - 1 = \Phi_n(\mathtt{t}^p) \cdot \prod_{d \in D'(n)} \Phi_d(\mathtt{t}^p).$$

Simplificando resulta finalmente $\Phi_{pn}(\mathtt{t}) \cdot \Phi_n(\mathtt{t}) = \Phi_n(\mathtt{t}^p)$, como pretendíamos.

(5) Dados enteros positivos m y n tales que todo divisor primo de m lo es de n se cumple que $\Phi_{mn}(\mathtt{t}) = \Phi_n(\mathtt{t}^m)$. En efecto, por la hipótesis sobre m y n existen números primos $p_1, \ldots, p_k, p_{k+1}, \ldots, p_\ell$ y enteros positivos $r_1, \ldots, r_k, s_1, \ldots, s_k, s_{k+1}, \ldots, s_\ell$ tales que

$$m = \prod_{j=1}^{k} p_j^{r_j} \quad \& \quad n = \prod_{j=1}^{\ell} p_j^{s_j}.$$

Si denotamos $q := \prod_{j=1}^{\ell} p_j$, hemos probado en el primer apartado que

$$\Phi_n(\mathtt{t}) = \Phi_q(\mathtt{t}^{p_1^{s_1-1}\cdots p_\ell^{s_\ell-1}}).$$

Por tanto, puesto que $mn = p_1^{r_1+s_1}\cdots p_k^{r_k+s_k}\cdot p_{k+1}^{s_{k+1}}\cdots p_\ell^{s_\ell}$, aplicando (1) de nuevo,

$$\begin{aligned}\Phi_n(\mathtt{t}^m) &= \Phi_q(\mathtt{t}^{m\cdot p_1^{s_1-1}\cdots p_\ell^{s_\ell-1}}) \\ &= \Phi_q(\mathtt{t}^{p_1^{r_1+s_1-1}\cdots p_k^{r_k+s_k-1}\cdot p_{k+1}^{s_{k+1}-1}\cdots p_\ell^{s_\ell-1}}) = \Phi_{mn}(\mathtt{t}).\end{aligned}$$

(6) Vamos a calcular los polinomios ciclotómicos Φ_{40} y Φ_{225}. Empleando el apartado anterior con $m = 4$ y $n = 10$ se tiene $\Phi_{40}(\mathtt{t}) = \Phi_{10}(\mathtt{t}^4)$. Además $\Phi_2(\mathtt{t})\cdot\Phi_{10}(\mathtt{t}) = \Phi_2(\mathtt{t}^5)$, por el apartado (4), es decir, $(\mathtt{t}+1)\cdot\Phi_{10}(\mathtt{t}) = \mathtt{t}^5+1$, por lo que

$$\Phi_{10}(\mathtt{t}) = \mathtt{t}^4 - \mathtt{t}^3 + \mathtt{t}^2 - \mathtt{t} + 1.$$

En consecuencia,

$$\Phi_{40}(\mathtt{t}) = \Phi_{10}(\mathtt{t}^4) = \mathtt{t}^{16} - \mathtt{t}^{12} + \mathtt{t}^8 - \mathtt{t}^4 + 1.$$

Para calcular Φ_{225} empleamos el apartado (5) con $n = m = 15$, lo que nos proporciona la igualdad $\Phi_{225}(\mathtt{t}) = \Phi_{15}(\mathtt{t}^{15})$. Por el apartado (4) se tiene

$$\Phi_3(\mathtt{t})\cdot\Phi_{15}(\mathtt{t}) = \Phi_3(\mathtt{t}^5) \quad \& \quad \Phi_3(\mathtt{t}) = \mathtt{t}^2 + \mathtt{t} + 1,$$

por lo que

$$\Phi_{15}(\mathtt{t}) = \frac{\Phi_3(\mathtt{t}^5)}{\Phi_3(\mathtt{t})} = \frac{\mathtt{t}^{10}+\mathtt{t}^5+1}{\mathtt{t}^2+\mathtt{t}+1} = \mathtt{t}^8 - \mathtt{t}^7 + \mathtt{t}^5 - \mathtt{t}^4 + \mathtt{t}^3 - \mathtt{t} + 1,$$

y finalmente,

$$\Phi_{225}(\mathtt{t}) = \Phi_{15}(\mathtt{t}^{15}) = \mathtt{t}^{120} - \mathtt{t}^{105} + \mathtt{t}^{75} - \mathtt{t}^{60} + \mathtt{t}^{45} - \mathtt{t}^{15} + 1.$$

1.d. Forma débil del Teorema del número primo de Dirichlet. El *Teorema del número primo de Dirichlet* afirma que dados números enteros no nulos n y a primos entre sí existen infinitos números primos $p \equiv a \bmod n$. En esta subsección probaremos una forma débil de dicho teorema; la que resulta de hacer $a = 1$, y que emplearemos después para demostrar que el grupo cíclico de orden n es el grupo de Galois sobre $\mathbb{Q}$ de un polinomio irreducible de grado n. Veamos antes un lema auxiliar.

Lema VI.1.13 *Sean k y n dos enteros positivos.*

(1) *Los enteros n y $\Phi_n(kn)$ son primos entre sí.*

(2) *Existe un entero $m_0 > 1$ tal que $|\Phi_n(mn)| > 1$ para todo entero $m \geq m_0$.*

(3) *Si un número primo p_0 divide a $\Phi_n(k)$ pero no a n, entonces $p_0 - 1$ es múltiplo de n.*

Demostración. (1) Sea $D'(n)$ el conjunto de divisores positivos de n menores que n y consideremos los polinomios

$$f(\mathtt{t}) := \mathtt{t}^n - 1 \quad \& \quad p(\mathtt{t}) := \prod_{d \in D'(n)} \Phi_d(\mathtt{t}),$$

que según vimos en VI.1.9 cumplen la igualdad $f(\mathtt{t}) = \Phi_n(\mathtt{t}) \cdot p(\mathtt{t})$.

Si $\operatorname{mcd}(n, \Phi_n(kn)) \neq 1$ existe un número primo q_0 que divide a n y a $\Phi_n(kn)$. Consideremos el homomorfismo reducción $\bmod q_0$ definido por

$$\Psi : \mathbb{Z}[\mathtt{t}] \to \mathbb{Z}_{q_0}[\mathtt{t}], \sum_{j=0}^{\ell} a_j \mathtt{t}^j \mapsto \sum_{j=0}^{\ell} [a_j]_{q_0} \mathtt{t}^j. \tag{1.6}$$

Al actuar el homomorfismo Ψ sobre los dos miembros de la igualdad $f = \Phi_n \cdot p$ resulta $\Psi(f) = \Psi(\Phi_n) \cdot \Psi(p)$, y al evaluar en $\mathtt{t} = [0]_{q_0} = [kn]_{q_0}$ se obtiene la siguiente contradicción:

$$\begin{aligned}[-1]_{q_0} = \Psi(f)([0]_{q_0}) = \Psi(f)([kn]_{q_0}) = \Psi(\Phi_n)([kn]_{q_0}) \cdot \Psi(p)([kn]_{q_0}) \\ = [\Phi_n(kn)]_{q_0} \cdot \Psi(p)([kn]_{q_0}) = [0]_{q_0}.\end{aligned}$$

(2) El polinomio producto

$$g(\mathtt{t}) := \Phi_n(n\mathtt{t}) \cdot (\Phi_n(n\mathtt{t}) - 1) \cdot (\Phi_n(n\mathtt{t}) + 1)$$

no es nulo porque no lo es ninguno de los factores, luego tiene un número finito de raíces reales. Tomamos $m_0 \in \mathbb{Z}$ mayor que todas ellas y así, para todo

$m \geq m_0$ resulta que $g(m) \neq 0$, lo que en particular implica que $\Phi_n(nm)$ es un número entero distinto de 0, de 1 y de -1, es decir, $|\Phi_n(nm)| > 1$ para todo $m \geq m_0$.

(3) Con las notaciones del primer apartado, $k^n - 1 = f(k) = \Phi_n(k) \cdot p(k) \in p_0\mathbb{Z}$ y, en particular, k no es múltiplo de p_0. Así $[k]_{p_0} \in \mathbb{Z}_{p_0}^*$, y vamos a probar que el orden de $[k]_{p_0} \in \mathbb{Z}_{p_0}^*$ es n. Visto esto, $n = o([k]_{p_0}) | \operatorname{ord}(\mathbb{Z}_{p_0}^*) = p_0 - 1$, por la Fórmula de Lagrange, que es lo que queremos demostrar.

Hemos probado que $k^n - 1 \in p_0\mathbb{Z}$, o sea, $[k]_{p_0}^n = [1]_{p_0}$, luego $e := o([k]_{p_0}) \leq n$ y suponemos, por reducción al absurdo, que la desigualdad es estricta. En tal caso e es un divisor propio de n, y por tanto, si $D(e)$ es el conjunto de divisores positivos de e, existe un polinomio $h \in \mathbb{Z}[\mathtt{t}]$ tal que

$$\mathtt{t}^n - 1 = \Phi_n(\mathtt{t}) \cdot \prod_{d \in D'(n)} \Phi_d(\mathtt{t}) = \Phi_n(\mathtt{t}) \cdot \prod_{d \in D(e)} \Phi_d(\mathtt{t}) \cdot h(\mathtt{t}) = \Phi_n(\mathtt{t}) \cdot (\mathtt{t}^e - 1) \cdot h(\mathtt{t}).$$

Sea $\Psi_1 : \mathbb{Z}[\mathtt{t}] \to \mathbb{Z}_{p_0}[\mathtt{t}]$ la reducción $\mathsf{mod}\, p_0$. Entonces,

$$\widehat{f}(\mathtt{t}) := \mathtt{t}^n - [1]_{p_0} = \Psi_1(\mathtt{t}^n - 1) = \Psi_1(\Phi_n) \cdot (\mathtt{t}^e - [1]_{p_0}) \cdot \Psi_1(h),$$

y esto implica que $x := [k]_{p_0} \in \mathbb{Z}_{p_0}$ es raíz múltiple de $\widehat{f}$, ya que

$$\Psi_1(\Phi_n)(x) = [\Phi_n(k)]_{p_0} = [0]_{p_0} \quad \& \quad x^e - [1]_{p_0} = [k]_{p_0}^e - [1]_{p_0} = [0]_{p_0}.$$

Esto es una contradicción ya que, como k y n no son múltiplos de p_0,

$$\widehat{f}'(x) = nx^{n-1} = [nk^{n-1}]_{p_0} \neq [0]_{p_0}.$$

□

Teorema VI.1.14 (Forma débil del Teorema del número primo) *Dado un entero positivo n existen infinitos números primos $p \equiv 1 \,\mathsf{mod}\, n$.*

Demostración. La prueba consiste en aplicar repetidas veces el Lema anterior VI.1.13. En efecto, por el apartado (2) existe un entero positivo m_0 tal que $|\Phi_n(m_0 n)| > 1$, por lo que $\Phi_n(m_0 n)$ tiene algún divisor primo p_1. Por el apartado (1) del Lema VI.1.13, p_1 no divide a n, y esto implica, por el apartado (3), que $p_1 \equiv 1 \,\mathsf{mod}\, n$. Para terminar es suficiente demostrar que si $p_1, \ldots, p_s$ son primos distintos tales que $p_j \equiv 1 \,\mathsf{mod}\, n$ para $1 \leq j \leq s$, existe otro número primo p_{s+1} distinto de los anteriores tal que $p_{s+1} \equiv 1 \,\mathsf{mod}\, n$.

Definimos $m := p_1 \cdots p_s \cdot n$ y, por el Lema VI.1.13 (2), existe un entero positivo ℓ tal que $|\Phi_m(\ell m)| > 1$. Elegimos como p_{s+1} un divisor primo cualquiera

de $\Phi_m(\ell m)$. Se deduce de VI.1.13 (1) que p_{s+1} no divide a m, luego $p_{s+1} \neq p_j$ para todo $1 \leq j \leq s$. Además, por el apartado (3), $p_{s+1} - 1$ es múltiplo de m, luego de n, esto es, $p_{s+1} \equiv 1 \bmod n$. □

Corolario VI.1.15 *Para cada entero positivo n existe un polinomio irreducible $f \in \mathbb{Q}[\mathtt{t}]$ de grado n cuyo grupo de Galois $G_{\mathbb{Q}}(f)$ es isomorfo a $\mathbb{Z}_n$.*

Demostración. Por el Teorema VI.1.14, existe un primo p tal que $p - 1 \in n\mathbb{Z}$, luego $p = sn + 1$ para cierto $s \in \mathbb{Z}$. Sea $\zeta \in \mathbb{C}$ una raíz primitiva p-ésima de la unidad. Sabemos por el Teorema VI.1.11 que $L := \mathbb{Q}(\zeta)$ es un cuerpo de descomposición del polinomio ciclotómico $\Phi_p(\mathtt{t}) = \mathtt{t}^{p-1} + \cdots + \mathtt{t} + 1$ y que $G_{\mathbb{Q}}(\Phi_p) = G(L : \mathbb{Q})$ es isomorfo al grupo $\mathbb{Z}_p^*$ de las unidades del anillo $\mathbb{Z}_p$, que es cíclico y de orden $p - 1$. Existe, por tanto, un subgrupo H de $G_{\mathbb{Q}}(\Phi_p)$ de orden s, necesariamente normal, y si denotamos $E := \mathrm{Fix}(H)$, resulta que $H = G(L : E)$. Por la segunda parte del Teorema fundamental de la teoría de Galois, IV.2.4, $E|\mathbb{Q}$ es una extensión de Galois cuyo grupo de Galois es

$$G(E : \mathbb{Q}) \cong G(L : \mathbb{Q})/G(L : E) = G_{\mathbb{Q}}(\Phi_p)/H \cong \mathbb{Z}_n,$$

ya que todo cociente de un grupo cíclico es también cíclico y

$$\mathrm{ord}\big(G(E : \mathbb{Q})\big) = \mathrm{ord}\big(G_{\mathbb{Q}}(\Phi_p)/H\big) = \mathrm{ord}\big(G_{\mathbb{Q}}(\Phi_p)\big)/\,\mathrm{ord}(H) = (p-1)/s = n.$$

Si α es un elemento primitivo de $E|\mathbb{Q}$, su polinomio mínimo $f := P_{\mathbb{Q},\alpha}$ sobre $\mathbb{Q}$ cumple lo requerido. En efecto, por un lado

$$\deg(f) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [E : \mathbb{Q}] = \mathrm{ord}(G(E : \mathbb{Q})) = n.$$

Por otro, como $E|\mathbb{Q}$ es una extensión de Galois y $\alpha \in E$ es una raíz del polinomio irreducible $f \in \mathbb{Q}[\mathtt{t}]$, este polinomio factoriza en $E[\mathtt{t}]$ como producto de factores de grado 1. En particular $E = \mathbb{Q}(\alpha)$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$, por lo que $G_{\mathbb{Q}}(f) = G(E : \mathbb{Q}) \cong \mathbb{Z}_n$. □

2. Ecuación general de grado n. Resolventes

En esta sección presentamos la acción natural del grupo $\mathcal{S}_n$ sobre el anillo de polinomios $K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$, mediante la que calculamos el grupo de Galois de la ecuación general de grado n. Estudiamos también el concepto de *resolvente universal* y sus propiedades, que nos permite obtener en la sección siguiente

un procedimiento algorítmico para calcular el grupo de Galois de cada polinomio de grado ≤ 5. Para agilizar la lectura hemos decidido postponer al final del capítulo las demostraciones de los resultados más técnicos acerca de estas resolventes.

2.a. Acción de $\mathcal{S}_n$ sobre $K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$. Comenzamos introduciendo el polinomio general de grado n. Denotamos $\mathtt{s}_1, \ldots, \mathtt{s}_n \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ las formas simétricas elementales en n variables.

Definición VI.2.1 Dados un cuerpo K e indeterminadas $\mathtt{x}_1, \ldots, \mathtt{x}_n$ sobre K se llama *polinomo general de grado n* "sobre" K, aunque debería decirse sobre $K(\mathtt{s}_1, \ldots, \mathtt{s}_n)$, a

$$g_n(\mathtt{t}) := \mathtt{t}^n + \sum_{k=1}^{n} (-1)^k \mathtt{s}_k \mathtt{t}^{n-k} = (\mathtt{t} - \mathtt{x}_1) \cdots (\mathtt{t} - \mathtt{x}_n),$$

donde cada $\mathtt{s}_k := \mathtt{s}_k(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ es la forma simétrica elemental de grado k en n variables.

El primer resultado importante de esta sección es el siguiente.

Teorema VI.2.2 (Abel) *Sean $\mathtt{x}_1, \ldots, \mathtt{x}_n$ indeterminadas sobre un cuerpo K. Entonces, la extensión*

$$K(\mathtt{x}_1, \ldots, \mathtt{x}_n) | K(\mathtt{s}_1, \ldots, \mathtt{s}_n)$$

es de Galois y su grupo de Galois es $\mathcal{S}_n$. En particular, el grupo de Galois $G_{K(\mathtt{s}_1, \ldots, \mathtt{s}_n)}(g_n)$ del polinomio general de grado n es $\mathcal{S}_n$.

Definición y Observaciones VI.2.3 (1) Sea G un subgrupo del grupo $\mathcal{S}_n$, y consideramos la acción sobre el anillo $K[\mathtt{x}] := K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ de polinomios en n variables definida mediante el homomorfismo inyectivo de grupos

$$G \hookrightarrow \mathrm{Biy}(K[\mathtt{x}]),\ \sigma \mapsto \widetilde{\sigma},$$

donde para cada $\mathtt{p} \in K[\mathtt{x}]$ y cada $\sigma \in G$ se define

$$\widetilde{\sigma}(\mathtt{p})(\mathtt{x}_1, \ldots, \mathtt{x}_n) := \mathtt{p}(\mathtt{x}_{\sigma(1)}, \ldots, \mathtt{x}_{\sigma(n)}).$$

Nótese que para cada $\sigma \in \mathcal{S}_n$, la biyección $\widetilde{\sigma} : K[\mathtt{x}] \to K[\mathtt{x}]$ es el único homomorfismo de anillos que fija los elementos de K y cumple $\widetilde{\sigma}(\mathtt{x}_i) = \mathtt{x}_{\sigma(i)}$ para

$1 \leq i \leq n$. Se trata efectivamente de una acción, ya que dadas permutaciones $\sigma, \tau \in G$,

$$(\widetilde{\sigma}\widetilde{\tau})(\mathtt{x}_i) = \widetilde{\tau}(\widetilde{\sigma}(\mathtt{x}_i)) = \widetilde{\tau}(\mathtt{x}_{\sigma(i)}) = \mathtt{x}_{\tau(\sigma(i))} = \mathtt{x}_{(\sigma\tau)(i)} = \widetilde{\sigma\tau}(\mathtt{x}_i), \tag{2.7}$$

y por ello $(\widetilde{\sigma}\widetilde{\tau})(\mathtt{p}) = \widetilde{\sigma\tau}(\mathtt{p})$ para cada $\mathtt{p} \in K[\mathtt{x}]$, luego $\widetilde{\sigma}\widetilde{\tau} = \widetilde{\sigma\tau}$. Como para toda acción, denotamos el estabilizador de $\mathtt{p} \in K[\mathtt{x}]$ mediante

$$\mathrm{Stab}_G(\mathtt{p}) := \{\sigma \in G : \widetilde{\sigma}(\mathtt{p}) = \mathtt{p}\}.$$

(2) Se deduce del Corolario IV.1.8, vol. I, que para cada polinomio $\mathtt{p} \in K[\mathtt{x}]$ y cada permutación $\sigma \in \mathcal{S}_n$,

$$\sigma^{-1}\,\mathrm{Stab}_{\mathcal{S}_n}(\mathtt{p})\sigma = \mathrm{Stab}_{\mathcal{S}_n}(\widetilde{\sigma}(\mathtt{p})). \tag{2.8}$$

(3) Esta acción permite interpretar $\mathcal{S}_n$ como grupo de K-automorfismos del cuerpo $K(\mathtt{x}) := K(\mathtt{x}_1, \ldots, \mathtt{x}_n)$, identificando cada permutación $\sigma \in \mathcal{S}_n$ con el único K-automorfismo

$$\widetilde{\sigma} : K(\mathtt{x}_1, \ldots, \mathtt{x}_n) \to K(\mathtt{x}_1, \ldots, \mathtt{x}_n)$$

que cumple $\widetilde{\sigma}(\mathtt{x}_i) = \mathtt{x}_{\sigma(i)}$ para $1 \leq i \leq n$. Es obvio que el homomorfismo

$$\mathcal{S}_n \to G(K(\mathtt{x}_1, \ldots, \mathtt{x}_n) : K),\ \sigma \mapsto \widetilde{\sigma}$$

es inyectivo. En el Lema siguiente calculamos el cuerpo fijo $\mathrm{Fix}(\mathcal{S}_n) \subset K(\mathtt{x})$. Antes observamos que para cada polinomio $g \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$, el producto

$$\mathtt{u} := \prod_{\sigma \in \mathcal{S}_n} \widetilde{\sigma}(g)$$

pertenece a $\mathrm{Fix}(\mathcal{S}_n)$ pues para todo $\tau \in \mathcal{S}_n$ se tiene $\mathcal{S}_n = \{\sigma\tau : \sigma \in \mathcal{S}_n\}$, luego

$$\widetilde{\tau}(\mathtt{u}) = \widetilde{\tau}\Big(\prod_{\sigma \in \mathcal{S}_n} \widetilde{\sigma}(g)\Big) = \prod_{\sigma \in \mathcal{S}_n} \widetilde{\tau}(\widetilde{\sigma}(g)) = \prod_{\sigma \in \mathcal{S}_n} \widetilde{\sigma\tau}(g) = \prod_{\alpha \in \mathcal{S}_n} \widetilde{\alpha}(g) = \mathtt{u}.$$

Lema VI.2.4 *Sean* $\mathtt{s}_1, \ldots, \mathtt{s}_n \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ *las formas simétricas elementales en* n *variables. Entonces* $\mathrm{Fix}(\mathcal{S}_n) = K(\mathtt{s}_1, \ldots, \mathtt{s}_n)$.

Demostración. Es obvio que cada forma simétrica $\mathtt{s}_j$ pertenece a $\mathrm{Fix}(\mathcal{S}_n)$. Recíprocamente, sean $f, g \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ no nulos tales que $f/g \in \mathrm{Fix}(\mathcal{S}_n)$. Multiplicamos el numerador y el denominador de esta fracción por el producto

$$h := \prod_{\sigma \in \mathcal{S}_n \setminus \{\mathrm{id}\}} \widetilde{\sigma}(g),$$

de modo que $f/g = (fh)/(gh)$. Por lo visto en VI.2.3 (3), el denominador

$$\mathtt{u} := gh = \prod_{\sigma \in \mathcal{S}_n} \widetilde{\sigma}(g) \in \mathrm{Fix}(\mathcal{S}_n),$$

luego $\mathtt{v} := fh = (f/g)(gh) \in \mathrm{Fix}(\mathcal{S}_n)$ y es un polinomio. Se deduce del Teorema VII.1.16, vol. II, que existen polinomios $\mathtt{p}, \mathtt{q} \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ tales que

$$\mathtt{v}(\mathtt{x}_1, \ldots, \mathtt{x}_n) = \mathtt{p}(\mathtt{s}_1, \ldots, \mathtt{s}_n) \quad \& \quad \mathtt{u}(\mathtt{x}_1, \ldots, \mathtt{x}_n) = \mathtt{q}(\mathtt{s}_1, \ldots, \mathtt{s}_n),$$

y, en consecuencia,

$$f/g = fh/gh = \mathtt{v}/\mathtt{u} = \mathtt{p}(\mathtt{s}_1, \ldots, \mathtt{s}_n)/\mathtt{q}(\mathtt{s}_1, \ldots, \mathtt{s}_n) \in K(\mathtt{s}_1, \ldots, \mathtt{s}_n).$$

Demostración de VI.2.2. La extensión $K(\mathtt{x}_1, \ldots, \mathtt{x}_n)|K(\mathtt{s}_1, \ldots, \mathtt{s}_n)$ es finita porque es finitamente generada y algebraica, ya que $g_n(\mathtt{x}_j) = 0$. Por el Lema VI.2.4, $K(\mathtt{s}_1, \ldots, \mathtt{s}_n) = \mathrm{Fix}(\mathcal{S}_n)$, lo que por IV.2.1 (4) implica que la extensión

$$K(\mathtt{x}_1, \ldots, \mathtt{x}_n)|K(\mathtt{s}_1, \ldots, \mathtt{s}_n)$$

es de Galois y su grupo de Galois es $\mathcal{S}_n$. □

2.b. Resolventes. Introducimos a continuación la noción de resolvente de un polinomio, que resultará esencial en el cálculo del grupo de Galois de todo polinomio de grado menor o igual que 5.

Definición y Observaciones VI.2.5 (1) Denotamos $\mathtt{x} := (\mathtt{x}_1, \ldots, \mathtt{x}_n)$ y sea $\mathtt{p} := \mathtt{p}(\mathtt{x}) \in K[\mathtt{x}]$. Sea $O_{\mathtt{p}} := \{\widetilde{\tau}(\mathtt{p}) : \tau \in \mathcal{S}_n\}$ la órbita de $\mathtt{p}$ bajo la acción del grupo simétrico $\mathcal{S}_n$ descrita en VI.2.3. Según se prueba en la Proposición IV.1.7, vol. I., la aplicación

$$\mathcal{S}_n/\mathcal{R}_{\mathrm{Stab}_{\mathcal{S}_n}(\mathtt{p})} \to O_{\mathtt{p}},\ \mathrm{Stab}_{\mathcal{S}_n}(\mathtt{p})\tau \mapsto \widetilde{\tau}(\mathtt{p}) \tag{2.9}$$

es una biyección bien definida. Se denomina *resolvente universal de* $\mathtt{p}$ al polinomio

$$R_{\mathtt{p}}(\mathtt{t}) := \prod_{\mathtt{q} \in O_{\mathtt{p}}} (\mathtt{t} - \mathtt{q}(\mathtt{x})) \in K[\mathtt{x}, \mathtt{t}]. \tag{2.10}$$

(2) Vamos a comprobar que la resolvente $R_{\mathtt{p}}(\mathtt{t}) \in K[\mathtt{s}_1, \ldots, \mathtt{s}_n][\mathtt{t}]$. Veamos primero que

$$K[\mathtt{x}] \cap K(\mathtt{s}_1, \ldots, \mathtt{s}_n) = K[\mathtt{s}_1, \ldots, \mathtt{s}_n].$$

Es obvio que el miembro de la izquierda contiene al de la derecha. Recíprocamente, sea $f \in K[\mathtt{x}]$ un polinomio que se escribe como cociente,

$$f(\mathtt{x}) = f_1(\mathtt{s}_1, \dots, \mathtt{s}_n)/f_2(\mathtt{s}_1, \dots, \mathtt{s}_n)$$

para ciertos polinomios $f_1, f_2 \in K[\mathtt{x}]$ primos entre sí. Esto implica que el polinomio f es simétrico, y el Teorema de los polinomios simétricos, VII.1.16, vol. II, asegura que existe un polinomio $h \in K[\mathtt{x}]$ tal que $f(\mathtt{x}) = h(\mathtt{s}_1, \dots, \mathtt{s}_n)$. En consecuencia,

$$f_1(\mathtt{s}_1, \dots, \mathtt{s}_n) = f_2(\mathtt{s}_1, \dots, \mathtt{s}_n)h(\mathtt{s}_1, \dots, \mathtt{s}_n),$$

y por el Lema VII.1.15 vol. II, $f_1(\mathtt{x}) = f_2(\mathtt{x})h(\mathtt{x})$. Como $\mathrm{mcd}(f_1, f_2) = 1$ esto implica que $f_2 \in K$, luego $f(\mathtt{x}) = f_1(\mathtt{s}_1, \dots, \mathtt{s}_n)/f_2 \in K[\mathtt{s}_1, \dots, \mathtt{s}_n]$.

Por tanto, basta demostrar que $R_{\mathtt{p}}(\mathtt{t}) \in K(\mathtt{s}_1, \dots, \mathtt{s}_n)[\mathtt{t}]$. Nótese que cada polinomio $\mathtt{q}$ de la órbita $O_{\mathtt{p}}$ de $\mathtt{p}$ pertenece a $K(\mathtt{x}_1, \dots, \mathtt{x}_n)$, que es el cuerpo descomposición sobre $E := K(\mathtt{s}_1, \dots, \mathtt{s}_n)$ del polinomio general de grado n

$$g_n(\mathtt{t}) = (\mathtt{t} - \mathtt{x}_1) \cdots (\mathtt{t} - \mathtt{x}_n).$$

Por el Teorema de Abel VI.2.2 la extensión $K(\mathtt{x}_1, \dots, \mathtt{x}_n)|E$ es de Galois con grupo de Galois $\mathcal{S}_n$, o sea, $E = \mathrm{Fix}(\mathcal{S}_n)$, luego para ver que $R_{\mathtt{p}} \in E[\mathtt{t}]$ es suficiente probar que sus coeficientes quedan fijos bajo la acción de cada permutación $\sigma \in \mathcal{S}_n$. Los coeficientes de $R_{\mathtt{p}}$ son las formas simétricas elementales evaluadas en los elementos $\mathtt{q} \in O_{\mathtt{p}}$, por lo que basta comprobar que $\widetilde{\sigma}(O_{\mathtt{p}}) = O_{\mathtt{p}}$ para cada $\sigma \in \mathcal{S}_n$. Pero esto es evidente, ya que

$$\begin{aligned} \widetilde{\sigma}(O_{\mathtt{p}}) &= \{\widetilde{\sigma}(\widetilde{\tau}(\mathtt{p})) : \tau \in \mathcal{S}_n\} = \{\widetilde{\tau}\widetilde{\sigma}(\mathtt{p}) : \tau \in \mathcal{S}_n\} \\ &= \{\widetilde{\tau\sigma}(\mathtt{p}) : \tau \in \mathcal{S}_n\} = \{\widetilde{\alpha}(\mathtt{p}) : \alpha \in \mathcal{S}_n\} = O_{\mathtt{p}}. \end{aligned} \tag{2.11}$$

(3) Nótese, además, que si $\mathtt{q} \in O_{\mathtt{p}}$, entonces $O_{\mathtt{p}} = O_{\mathtt{q}}$, y por ello $R_{\mathtt{p}} = R_{\mathtt{q}}$.

Ejemplo VI.2.6 (1) Consideramos $\mathtt{x} := (\mathtt{x}_1, \dots, \mathtt{x}_n)$ y los polinomios

$$\delta(\mathtt{x}) := \prod_{1 \le i < j \le n} (\mathtt{x}_i - \mathtt{x}_j) \in K[\mathtt{x}] \quad \& \quad \Delta(\mathtt{x}) := \delta(\mathtt{x})^2.$$

Para cada permutación $\sigma \in \mathcal{S}_n$ se tiene

$$(\widetilde{\sigma}(\delta))^2 = \prod_{1 \le i < j \le n} (\mathtt{x}_{\sigma(i)} - \mathtt{x}_{\sigma(j)})^2 = \prod_{1 \le i < j \le n} (\mathtt{x}_i - \mathtt{x}_j)^2 = \delta^2 = \Delta,$$

luego $\widetilde{\sigma}(\delta) \in \{\delta, -\delta\}$. Además, $\widetilde{\mathrm{id}}(\delta) = \delta$ mientras que $\widetilde{\sigma}(\delta) = -\delta$ donde $\sigma := (1,2)$. Por tanto la órbita $O_\delta = \{\delta, -\delta\}$ de δ bajo la acción del grupo simétrico $\mathcal{S}_n$ consta de, exactamente, dos elementos. En consecuencia,

$$R_\delta(\mathtt{t}) := \prod_{\mathtt{q}\in O_\delta} (\mathtt{t}-\mathtt{q}(\mathtt{x})) = (\mathtt{t}-\delta(\mathtt{x}))(\mathtt{t}+\delta(\mathtt{x})) = \mathtt{t}^2-\delta(\mathtt{x})^2 = \mathtt{t}^2-\Delta(\mathtt{x}). \quad (2.12)$$

Por VI.2.5 (1), $[\mathcal{S}_n : \mathrm{Stab}_{\mathcal{S}_n}(\delta)] = \mathrm{Card}(O_\delta) = 2$, luego $\mathrm{Stab}_{\mathcal{S}_n}(\delta)$ es subgrupo de índice 2 de $\mathcal{S}_n$, así que $\mathrm{Stab}_{\mathcal{S}_n}(\delta) = \mathcal{A}_n$, por el Corolario III.2.6 y la Proposición III.2.8, vol. I.

Ejemplo VI.2.7 (Resolvente cúbica) (1) Sean $\mathtt{p}_1 := (\mathtt{x}_1 + \mathtt{x}_2)(\mathtt{x}_3 + \mathtt{x}_4)$ y vamos a calcular la resolvente $R_{\mathtt{p}_1} \in K[\mathtt{s}_1, \mathtt{s}_2, \mathtt{s}_3, \mathtt{s}_4, \mathtt{t}]$, donde $\mathtt{s}_1, \mathtt{s}_2, \mathtt{s}_3, \mathtt{s}_4$ son las formas simétricas elementales en cuatro indeterminadas. Para ello determinamos antes el estabilizador $\mathrm{Stab}_{\mathcal{S}_4}(\mathtt{p}_1)$. Consideremos las transposiciones $\sigma_1 := (2,3)$ y $\sigma_2 := (2,4)$. Los polinomios

$$\mathtt{p}_2 := \widetilde{\sigma}_1(\mathtt{p}_1) = (\mathtt{x}_1 + \mathtt{x}_3)(\mathtt{x}_2 + \mathtt{x}_4) \quad \& \quad \mathtt{p}_3 := \widetilde{\sigma}_2(\mathtt{p}_1) = (\mathtt{x}_1 + \mathtt{x}_4)(\mathtt{x}_2 + \mathtt{x}_3)$$

son distintos entre sí y distintos de $\mathtt{p}_1$, luego $\mathrm{Card}(O_{\mathtt{p}_1}) \geq 3$ pues dicha órbita contiene a $\mathtt{p}_1, \mathtt{p}_2$ y $\mathtt{p}_3$. Por otro lado, es inmediato comprobar que

$$\{\tau_1 := \mathrm{id},\ \tau_2 := (1,2),\ \tau_3 := (3,4),\ \tau_4 := \tau_2\tau_3,\ \tau_5 := (1,3,2,4)\} \subset \mathrm{Stab}_{\mathcal{S}_4}(\mathtt{p}_1).$$

Por tanto, $\mathrm{Stab}_{\mathcal{S}_4}(\mathtt{p}_1)$ es un subgrupo de $\mathcal{S}_4$ con al menos 5 elementos y que contiene un subgrupo $\{\tau_1, \tau_2, \tau_3, \tau_4\}$ de orden 4, luego $\mathrm{ord}(\mathrm{Stab}_{\mathcal{S}_4}(\mathtt{p}_1)) \geq 5$ y es múltiplo de 4, así que $\mathrm{ord}(\mathrm{Stab}_{\mathcal{S}_4}(\mathtt{p}_1)) \geq 8$. En consecuencia,

$$3 \leq \mathrm{Card}(O_{\mathtt{p}_1}) = [\mathcal{S}_4 : \mathrm{Stab}_{\mathcal{S}_4}(\mathtt{p}_1)] \leq 24/8 = 3,$$

de donde $\mathrm{Card}(O_{\mathtt{p}_1}) = 3$, por lo que $O_{\mathtt{p}_1} = \{\mathtt{p}_1, \mathtt{p}_2, \mathtt{p}_3\}$. Esto implica que

$$\begin{aligned} R_{\mathtt{p}_1}(\mathtt{t}) :&= \prod_{i=1}^{3}(\mathtt{t} - \mathtt{p}_i(\mathtt{x})) = \mathtt{t}^3 - (\mathtt{p}_1(\mathtt{x}) + \mathtt{p}_2(\mathtt{x}) + \mathtt{p}_3(\mathtt{x}))\mathtt{t}^2 \\ &+ (\mathtt{p}_1(\mathtt{x})\mathtt{p}_2(\mathtt{x}) + \mathtt{p}_1(\mathtt{x})\mathtt{p}_3(\mathtt{x}) + \mathtt{p}_2(\mathtt{x})\mathtt{p}_3(\mathtt{x}))\mathtt{t} - \mathtt{p}_1(\mathtt{x})\mathtt{p}_2(\mathtt{x})\mathtt{p}_3(\mathtt{x}) \quad (2.13) \\ &= \mathtt{t}^3 - 2\mathtt{s}_2\mathtt{t}^2 + (\mathtt{s}_2^2 + \mathtt{s}_1\mathtt{s}_3 - 4\mathtt{s}_4)\mathtt{t} \\ &+ (\mathtt{s}_4\mathtt{s}_1^2 + \mathtt{s}_3^2 - \mathtt{s}_1\mathtt{s}_2\mathtt{s}_3) \in K[\mathtt{s}_1, \mathtt{s}_2, \mathtt{s}_3, \mathtt{s}_4, \mathtt{t}]. \end{aligned}$$

(2) Es inmediato comprobar que para $i = 1, 2, 3$ el grupo de Klein

$$V := \{\rho_1 := \mathrm{id},\ \rho_2 := (1,2)(3,4),\ \rho_3 := (1,3)(2,4),\ \rho_4 := (1,4)(2,3)\}$$

está contenido en el estabilizador $\mathrm{Stab}_{\mathcal{S}_4}(\mathtt{p}_i)$. Además, $\mathrm{Stab}_{\mathcal{S}_4}(\mathtt{p}_1)$ tiene orden 8 y el ciclo $(1,3,2,4) \in \mathrm{Stab}_{\mathcal{S}_4}(\mathtt{p}_1) \setminus \mathrm{Stab}_{\mathcal{S}_4}(\mathtt{p}_2)$, luego

$$V = \bigcap_{i=1}^{3} \mathrm{Stab}_{\mathcal{S}_4}(\mathtt{p}_i).$$

(3) Es útil observar que los discriminantes de los polinomios

$$f(\mathtt{t}) := \prod_{i=1}^{4}(\mathtt{t} - \mathtt{x}_i) \quad \& \quad R_{\mathtt{p}_1}(\mathtt{t}) := \prod_{i=1}^{3}(\mathtt{t} - \mathtt{p}_i(\mathtt{x}))$$

coinciden. En efecto, por el Teorema VII.2.10, vol. II, tenemos

$$\begin{aligned}\Delta(R_{\mathtt{p}_1}) &= (\mathtt{p}_1 - \mathtt{p}_2)^2 \cdot (\mathtt{p}_1 - \mathtt{p}_3)^2 \cdot (\mathtt{p}_2 - \mathtt{p}_3)^2 \\ &= (\mathtt{x}_1 - \mathtt{x}_4)^2(\mathtt{x}_2 - \mathtt{x}_3)^2(\mathtt{x}_1 - \mathtt{x}_3)^2(\mathtt{x}_2 - \mathtt{x}_4)^2(\mathtt{x}_1 - \mathtt{x}_2)^2(\mathtt{x}_3 - \mathtt{x}_4)^2 = \Delta(f).\end{aligned}$$

2.c. Especialización de las resolventes. A lo largo de esta subsección supondremos que $\mathrm{char}(K) = 0$.

Definiciones y Proposición VI.2.8 (1) Sea $f \in K[\mathtt{t}]$ un polinomio irreducible de grado n. Sea $L_f \subset \overline{K}$ un cuerpo de descomposición de f sobre K y sean $\alpha_1, \ldots, \alpha_n \in L_f$ las n raíces distintas de f en $\overline{K}$. Denotamos $G_K(f) = G(L_f : K)$, abreviamos $\alpha := (\alpha_1, \ldots, \alpha_n)$ y $\mathtt{x} := (\mathtt{x}_1, \ldots, \mathtt{x}_n)$ y consideramos el único K-homomorfismo $\mathrm{ev}_\alpha : K(\mathtt{x}) \to L_f$ que cumple $\mathrm{ev}_\alpha(\mathtt{x}_i) = \alpha_i$ para $1 \leq i \leq n$. Denotamos también $\mathrm{ev}_\alpha : K(\mathtt{x})[\mathtt{t}] \to L_f[\mathtt{t}]$ su única extensión que fija la variable $\mathtt{t}$. Nótese que si

$$f(\mathtt{t}) := (\mathtt{t} - \alpha_1) \cdots (\mathtt{t} - \alpha_n) = \mathtt{t}^n + \sum_{k=1}^{n}(-1)^k c_k \mathtt{t}^{n-k},$$

y g_n denota el polinomio general de grado n, que introdujimos en la Definición VI.2.1, se tiene $f = \mathrm{ev}_\alpha(g_n)$, por lo que $c_k = \mathrm{ev}_\alpha(\mathtt{s}_k)$ para $1 \leq k \leq n$.

Dado $\mathtt{p} \in K[\mathtt{x}]$ denotamos $\mathtt{p}(\alpha) = \mathrm{ev}_\alpha(\mathtt{p}) \in L_f$, y para cada permutación $\sigma \in G_K(f) \subset \mathcal{S}_n$ tiene sentido $\sigma(\mathtt{p}(\alpha)) \in L_f$.

(2) Dados $\sigma \in G_K(f)$ y $\mathtt{p} \in K[\mathtt{x}]$ se tiene $\widetilde{\sigma}(\mathtt{p})(\alpha) = \sigma(\mathtt{p}(\alpha))$.

(3) Sea $\mathtt{p} \in K[\mathtt{x}]$. Se denomina *resolvente de* $\mathtt{p}$ *especializada en* f al polinomio

$$R_{f,\mathtt{p}}(\mathtt{t}) := \prod_{\mathtt{q} \in O_\mathtt{p}} (\mathtt{t} - \mathtt{q}(\alpha)) \in K[\mathtt{t}], \tag{2.14}$$

que se obtiene al evaluar $R_{\mathtt{p}}$ en $\mathtt{x}_i := \alpha_i$ para $1 \leq i \leq n$, o sea, $R_{f,\mathtt{p}} = \mathrm{ev}_\alpha(R_{\mathtt{p}})$.

(3.1) Cada raíz $\mathtt{q}(\alpha)$ de $R_{f,\mathtt{p}}$ pertenece a $L_f = K(\alpha_1, \ldots, \alpha_n)$, puesto que $\mathtt{q} \in O_{\mathtt{p}} \subset K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$.

(3.2) Para cada $\sigma \in \mathcal{S}_n$ se tiene $\mathrm{Stab}_{G_K(f)}(\widetilde{\sigma}(\mathtt{p})) \subset G(L_f : K(\widetilde{\sigma}(\mathtt{p})(\alpha)))$.

(3.3) Si $\sigma \in \mathcal{S}_n$ y $\sigma G_K(f)\sigma^{-1} \subset \mathrm{Stab}_{\mathcal{S}_n}(\mathtt{p})$, entonces $\widetilde{\sigma}(\mathtt{p})(\alpha) \in K$.

(3.4) Sea $\sigma \in \mathcal{S}_n$ una permutación tal que $\widetilde{\sigma}(\mathtt{p})(\alpha) \in K$ y es raíz simple de $R_{f,\mathtt{p}}$. Entonces, $\sigma G_K(f)\sigma^{-1} \subset \mathrm{Stab}_{\mathcal{S}_n}(\mathtt{p})$.

Corolario VI.2.9 *Sean $f \in K[\mathtt{t}]$ un polinomio irreducible de grado n y cuyo discriminante se denota $\Delta(f) \in K$. Entonces, el grupo de Galois $G_K(f)$ está contenido en $\mathcal{A}_n$ si y sólo si $\Delta(f)$ es el cuadrado de un elemento de K.*

Demostración. Observamos que si $\alpha_1, \ldots, \alpha_n$ son las raíces de f en un cuerpo de descomposición sobre K y denotamos

$$\delta(\mathtt{x}) := \prod_{1 \leq i < j \leq n} (\mathtt{x}_i - \mathtt{x}_j)$$

y $\delta(\alpha) = \mathrm{ev}_\alpha(\delta)$, entonces $\delta(\alpha)^2 = \Delta(f)$. Además $R_{f,\delta}(\mathtt{t}) = \mathtt{t}^2 - \Delta(f)$, en virtud de VI.2.6, luego $\pm\delta(\alpha)$ son las raíces de $R_{f,\delta}$. Ambas raíces son simples pues $\Delta(f) \neq 0$ ya que f es irreducible en $K[\mathtt{t}]$. Vimos en VI.2.6 que $\mathrm{Stab}_{\mathcal{S}_n}(\delta) = \mathcal{A}_n$. Aplicando (3.3) y (3.4) en VI.2.8 con $\sigma := \mathrm{id}$ y $\mathtt{p} := \delta$ se tiene

$$G_K(f) \subset \mathcal{A}_n \iff G_K(f) \subset \mathrm{Stab}_{\mathcal{S}_n}(\delta) \iff \pm\delta(\alpha) \in K,$$

y esto último significa, exactamente, que $\Delta(f)$ es un cuadrado en K. □

3. Grupo de Galois de los polinomios de grado ≤ 4

El objetivo de esta sección es determinar, a partir únicamente de sus coeficientes, el grupo de Galois $G_K(f)$ de cada polinomio $f \in K[\mathtt{t}]$ con $\deg(f) \leq 5$.

3.a. Grupo de Galois de un polinomio de grado ≤ 2.

Observaciones VI.3.1 Sea $f \in K[\mathtt{t}]$ un polinomio con coeficientes en K.

(1) Si $\deg(f) = 1$, entonces $L_f = K$, así que $G_K(f) = G(K : K) = \{\mathrm{id}_K\}$.

(2) Si $\deg(f) = 2$ y $\alpha, \beta \in L_f$ son las raíces de f en $\overline{K}$, se tiene

$$f(\mathtt{t}) := (\mathtt{t} - \alpha)(\mathtt{t} - \beta) = \mathtt{t}^2 - (\alpha + \beta)\mathtt{t} + \alpha\beta \in K[\mathtt{t}].$$

Por el Teorema VII.2.10, vol. II, el discriminante de f es $\Delta(f) = (\alpha - \beta)^2$, y distinguimos dos casos según que $\Delta(f)$ sea o no un cuadrado en K.

(2.1) Si $\Delta(f)$ es un cuadrado en K, entonces $\alpha - \beta \in K$ y como $\alpha + \beta \in K$, tanto α como β pertenecen a K, luego $L_f = K$ y$G_K(f) = G(K : K) = \{\mathrm{id}_K\}$.

(2.2) Si $\Delta(f)$ no es un cuadrado en K, entonces $\alpha - \beta \notin K$. En particular f es irreducible en $K[\mathtt{t}]$, y se desprende del Corolario VI.2.9 que $G_K(f)$ es un subgrupo no trivial de $\mathcal{S}_2 = \mathbb{Z}_2$. Así, el grupo de Galois de f sobre K es $G_K(f) = G(L_f : K) \cong \mathbb{Z}_2$ en este caso.

3.b. Grupo de Galois de un polinomio de grado 3. Sea $f \in K[\mathtt{t}]$ un polinomio mónico de grado 3. Denotamos $\alpha_1, \alpha_2, \alpha_3$ las raíces de f en $\overline{K}$ y fijamos una raíz cuadrada $\delta(\alpha)$ del discriminante $\Delta(f)$ de f en $\overline{K}$.

Proposición VI.3.2 *Entonces, el grupo de Galois $G_K(f)$ es el dado por la siguiente tabla:*

	$\delta(\alpha) \in K$	$\delta(\alpha) \notin K$
f es reducible en $K[\mathtt{t}]$	$\{1\}$	$\mathbb{Z}_2$
f es irreducible en $K[\mathtt{t}]$	$\mathbb{Z}_3$	$\mathcal{S}_3$

Demostración. Recordemos que, salvo el signo, podemos suponer que

$$\delta(\alpha) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3).$$

El caso $\delta(\alpha) = 0$ requiere un tratamiento aparte. Esto significa que alguna de las raíces de f es múltiple y, como $\mathrm{char}(K) = 0$, se deduce de II.1.3 que f es reducible en $K[\mathtt{t}]$. Como $\deg(f) = 3$ esto implica que alguna de las raíces de f pertenece al cuerpo K. Además, si α_1 es raíz múltiple de f, resulta que

$$\mathtt{t}^3 - (2\alpha_1 + \alpha_3)\mathtt{t}^2 + (\alpha_1^2 + 2\alpha_1\alpha_3)\mathtt{t} - \alpha_1^2\alpha_3 = f(\mathtt{t}) \in K[\mathtt{t}].$$

Como α_1 o α_3 pertenecen a K y $2\alpha_1 + \alpha_3 \in K$ deducimos que $\alpha_1, \alpha_3 \in K$, luego $L_f = K(\alpha_1, \alpha_3) = K$ y $G_K(f)$ es el grupo trivial. Suponemos en lo que

sigue que $\delta(\alpha) \neq 0$, y comprobemos que $L_f = K(\alpha_i, \delta(\alpha))$ para $i = 1, 2, 3$. Por supuesto, es suficiente verlo para $i = 1$. Por la Regla de Ruffini el polinomio f es múltiplo de $\mathtt{t} - \alpha_1$ en $K(\alpha_1)[\mathtt{t}]$, y como sus otras dos raíces son α_2 y α_3 resulta que $f(\mathtt{t}) := (\mathtt{t} - \alpha_1)h(\mathtt{t})$, donde

$$h(\mathtt{t}) := (\mathtt{t} - \alpha_2)(\mathtt{t} - \alpha_3) = \mathtt{t}^2 - (\alpha_2 + \alpha_3)\mathtt{t} + \alpha_2\alpha_3 \in K(\alpha_1)[\mathtt{t}].$$

Como $h(\alpha_1) \in K(\alpha_1)$ y $0 \neq \delta(\alpha) = \pm h(\alpha_1)(\alpha_2 - \alpha_3)$, la resta $\alpha_2 - \alpha_3$ pertenece a $K(\alpha_1, \delta(\alpha))$. Pero $\alpha_2 + \alpha_3 \in K(\alpha_1)$ luego $\alpha_2, \alpha_3 \in K(\alpha_1, \delta(\alpha))$. Por tanto,

$$K(\alpha_1, \delta(\alpha)) \subset K(\alpha_1, \alpha_2, \alpha_3) = L_f \subset K(\alpha_1, \delta(\alpha)),$$

así que $L_f = K(\alpha_1, \delta(\alpha))$. Distinguimos ahora dos casos:

(1) Si f es reducible en $K[\mathtt{t}]$ podemos suponer que $\alpha_1 \in K$. Así $L_f = K(\delta(\alpha))$, luego si $\delta(\alpha) \in K$, entonces $L_f = K$, por lo que $G_K(f) = \{1\}$, mientras que si $\delta(\alpha) \notin K$, entonces $G_K(f) = \mathbb{Z}_2$, ya que $P_{K,\delta(\alpha)} = \mathtt{t}^2 - \Delta(f)$ y

$$\mathrm{ord}(G_K(f)) = [L_f : K] = [K(\delta(\alpha)) : K] = 2.$$

(2) Si f es irreducible en $K[\mathtt{t}]$ el grupo $G_K(f)$ es, por VI.1.2, subgrupo de $\mathcal{S}_3$ y su orden es múltiplo de 3, luego es $\mathcal{A}_3$ o $\mathcal{S}_3$. Por VI.2.9, si $\delta(\alpha) \in K$ entonces $G_K(f) = \mathcal{A}_3 = \mathbb{Z}_3$, y si $\delta(\alpha) \notin K$ entonces $G_K(f) = \mathcal{S}_3$. □

3.c. Grupo de Galois de un polinomio de grado 4.

Sea

$$f(\mathtt{t}) := \mathtt{t}^4 + a\mathtt{t}^3 + b\mathtt{t}^2 + c\mathtt{t} + d \in K[\mathtt{t}]$$

un polinomio mónico e irreducible en $K[\mathtt{t}]$ de grado 4. Denotamos $\alpha_1, \alpha_2, \alpha_3$ y α_4 las raíces de f en $\overline{K}$ y fijamos una raíz cuadrada $\delta := \delta(\alpha) \in \overline{K}$ del discriminante $\Delta(f)$ de f. Sean $R_{\mathtt{p}}$ la resolvente cúbica introducida en VI.2.7 y denotemos $g := R_{f,\mathtt{p}} = \mathrm{ev}_\alpha(R_{\mathtt{p}})$, que es

$$g(\mathtt{t}) := \mathtt{t}^3 - 2b\mathtt{t}^2 + (b^2 + ac - 4d)\mathtt{t} + (da^2 + c^2 - abc) \in K[\mathtt{t}].$$

Proposición VI.3.3 El grupo de Galois $G_K(f)$ es el dado por la siguiente tabla:

	g es reducible en $K[\mathtt{t}]$		g es irreducible en $K[\mathtt{t}]$	
	$\delta \in K$	$\delta \notin K$	$\delta \in K$	$\delta \notin K$
f es reducible en $K(\delta)[\mathtt{t}]$	–	$\mathbb{Z}_4$	–	–
f es irreducible en $K(\delta)[\mathtt{t}]$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathcal{D}_4$	$\mathcal{A}_4$	$\mathcal{S}_4$

donde $\mathcal{D}_4$ es el grupo diedral de orden 8, $\mathcal{A}_4$ el grupo alternado de orden 12 y $\mathcal{S}_4$ el grupo simétrico de orden 24.

Demostración. Se deduce de VI.2.7 que las raíces de g en $\overline{K}$ son

$$\beta_1 := (\alpha_1+\alpha_2)(\alpha_3+\alpha_4),\ \beta_2 := (\alpha_1+\alpha_3)(\alpha_2+\alpha_4)\ \&\ \beta_3 := (\alpha_1+\alpha_4)(\alpha_2+\alpha_3).$$

Sean $F := K(\beta_1, \beta_2, \beta_3)$ y el subgrupo de $\mathcal{S}_4$

$$V := \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

(1) Vamos a demostrar que

$$G_F(f) = G_K(f) \cap V \quad \& \quad G(F:K) \cong G_K(f)/G_F(f). \tag{3.15}$$

En el Ejemplo VI.2.7 introdujimos los polinomios

$$\mathtt{p}_1 := (\mathtt{x}_1+\mathtt{x}_2)(\mathtt{x}_3+\mathtt{x}_4), \quad \mathtt{p}_2 := (\mathtt{x}_1+\mathtt{x}_3)(\mathtt{x}_2+\mathtt{x}_4) \quad \& \quad \mathtt{p}_3 := (\mathtt{x}_1+\mathtt{x}_4)(\mathtt{x}_2+\mathtt{x}_3),$$

que cumplen $\beta_i = \mathtt{p}_i(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ y, por VI.2.5 (3), $g = R_{f,\mathtt{p}_i}$ para $i = 1, 2, 3$. Como f es irreducible en $K[\mathtt{t}]$ su discriminante $\Delta(f)$ es no nulo y, por el apartado (3) en el Ejemplo VI.2.7, $\Delta(g) = \Delta(f) \neq 0$, luego las raíces β_1, β_2 y β_3 de g son simples. Estamos en condiciones de aplicar VI.2.8 (3.4) al grupo de Galois $G_F(f)$.

En efecto, cada β_i es raíz simple del polinomio $g = R_{f,\mathtt{p}_i}$, así que en virtud de VI.2.8 (3.4) y el Ejemplo VI.2.7 (2)

$$G_F(f) \subset \bigcap_{i=1}^{3} \mathrm{Stab}_{\mathcal{S}_4}(\mathtt{p}_i) = V.$$

Según demostramos en el Ejemplo III.1.17, vol. I, V es un subgrupo normal de $\mathcal{S}_4$ que, por el Teorema de estructura de los grupos abelianos finitos, es

isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ pues tiene orden 4 y ninguno de sus elementos tiene orden 4. Por otro lado es obvio que

$$G_F(f) = G(L_f : F) \subset G(L_f : K) = G_K(f),$$

luego $G_F(f) \subset G_K(f) \cap V$. La inclusión recíproca es clara. En efecto, la extensión $L_f|F$ es de Galois por serlo $L_f|K$. Además, cada $\beta_i \in \mathrm{Fix}(G_K(f) \cap V)$, luego $F \subset \mathrm{Fix}(G_K(f) \cap V)$, así que

$$G_K(f) \cap V = G(L_f|\,\mathrm{Fix}(G_K(f) \cap V)) \subset G(L_f|F) = G_F(f).$$

Más aún, como $G_K(f) \cap V$ es subgrupo normal de $G_K(f)$, ya que $V \lhd \mathcal{S}_4$, se deduce de la segunda parte del Teorema fundamental, IV.2.4, que también es de Galois la extensión $F|K$ y su grupo de Galois es

$$G(F : K) \cong G(L_f : K)/G(L_f : F) = G_K(f)/(G_K(f) \cap V) = G_K(f)/G_F(f).$$

(2) Hemos señalado en el Ejemplo VI.2.7 (3) que $\Delta(f) = \Delta(g)$, luego δ es una raíz cuadrada de $\Delta(g)$. Además, como se demostró en VI.3.2 al estudiar el grupo de Galois de los polinomios de grado 3, se cumplen las igualdades

$$F = K(\beta_1, \beta_2, \beta_3) = K(\beta_j, \delta), \tag{3.16}$$

para $j = 1, 2, 3$. Nuestro objetivo es demostrar que para $i = 1, 2, 3, 4$

$$L_f = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = K(\alpha_i, \beta_1, \beta_2, \beta_3) = F(\alpha_i) \tag{3.17}$$

y, por tanto, $L_f = K(\alpha_i, \beta_j, \delta)$, para $1 \leq i \leq 4$ y $1 \leq j \leq 3$.

Observemos que $4 \big| \,\mathrm{ord}(G_K(f)) = [L_f : K]$, en virtud de la Proposición VI.1.2. Distinguimos dos casos:

(2.1) Si f es irreducible en $F[\mathtt{t}]$ entonces $G_F(f) = V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ y $L_f = F(\alpha_i)$.

En efecto, por la Proposición VI.1.2 el orden del grupo $G_F(f)$ es múltiplo de 4. Por otro lado, hemos demostrado en (3.15) que $G_F(f) \subset V$, luego $\mathrm{ord}(G_F(f)) \leq \mathrm{ord}(V) = 4$. Por tanto, $G_F(f) = V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ en este caso, y en consecuencia $L_f = F(\alpha_i)$ para $1 \leq i \leq 4$, ya que

$$[L_f : F] = \mathrm{ord}(G_F(f)) = 4 = \deg(f) = \deg(P_{F,\alpha_i}) = [F(\alpha_i) : F].$$

(2.2) Si f es reducible en $F[\mathtt{t}]$, entonces $[L_f : F] = 2$ o $[L_f : F] = 4$. En efecto, vimos en (3.15) que $G_F(f)$ es subgrupo de V, luego

$$[L_f : F] = \mathrm{ord}(G_F(f))|\,\mathrm{ord}(V) = 4,$$

y basta probar que $L_f \neq F$.

En caso contrario $G_K(f) = G(L_f : K) = G(F : K) = G_K(g)$ es el grupo de Galois de un polinomio de grado 3, por lo que su orden divide a 6, y por tanto no es múltiplo de 4, y ya hemos señalado que esto es falso.

(2.2.1) Vamos a probar que f es el producto de dos polinomios irreducibles en $F[\mathtt{t}]$ de grado 2. En caso contrario un factor irreducible $f_1 \in F[\mathtt{t}]$ de f tendría grado 3 y alguna de las α_i es raíz de f_1, por lo que $f_1 = P_{F,\alpha_i}$. Así,

$$[L_f : F] = [L_f : F(\alpha_i)] \cdot [F(\alpha_i) : F] = [L_f : F(\alpha_i)] \cdot \deg(f_1) = [L_f : F(\alpha_i)] \cdot 3.$$

Esto es imposible pues hemos visto que $[L_f : F]$ divide a 4.

Si f tuviese dos factores irreducibles de grado 1 en $F[\mathtt{t}]$, podemos suponer que son $\mathtt{t} - \alpha_1$ y $\mathtt{t} - \alpha_2$, es decir, $\alpha_1, \alpha_2 \in F$, y el cociente

$$f(\mathtt{t})/(\mathtt{t} - \alpha_1)(\mathtt{t} - \alpha_2) = (\mathtt{t} - \alpha_3)(\mathtt{t} - \alpha_4) = \mathtt{t}^2 - (\alpha_3 + \alpha_4)\mathtt{t} + \alpha_3\alpha_4 \in F[\mathtt{t}].$$

Por tanto $\gamma_1 := \alpha_3 + \alpha_4 \in F$ y, por otro lado,

$$\alpha_1\alpha_2 + \alpha_3\alpha_4 + \alpha_1\alpha_3 + \alpha_2\alpha_4 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) = \beta_3 \in F.$$

Como α_1, α_2 y $\alpha_3\alpha_4$ pertenecen a F, también $\gamma_2 := \alpha_1\alpha_3 + \alpha_2\alpha_4 \in F$. Resulta entonces

$$\begin{cases} \alpha_3 + \alpha_4 = \gamma_1 \\ \alpha_1\alpha_3 + \alpha_2\alpha_4 = \gamma_2, \end{cases}$$

e interpretamos estas igualdades como un sistema de ecuaciones lineales en las incógnitas α_3 y α_4, que es compatible determinado porque $\alpha_1 \neq \alpha_2$. Por tanto, al despejar, resulta que $\alpha_3, \alpha_4 \in F$, lo que significa que $F = L_f$, que es una contradicción.

Queda pues probado que f factoriza en $F[\mathtt{t}]$ en producto de dos polinomios irreducibles f_1 y f_2 de grado 2 y, renombrando los índices si es preciso, podemos suponer que

$$f_1(\mathtt{t}) := (\mathtt{t} - \alpha_1)(\mathtt{t} - \alpha_2) \in F[\mathtt{t}] \quad \& \quad f_2(\mathtt{t}) := (\mathtt{t} - \alpha_3)(\mathtt{t} - \alpha_4) \in F[\mathtt{t}].$$

Veamos que también en este caso se cumple que $L_f = F(\alpha_i)$. Basta hacerlo para $i = 1$, y denotamos $E := F(\alpha_1)$. Nótese que $\gamma_1 = \alpha_3 + \alpha_4 \in F \subset E$, por ser un coeficiente de f_2. Además, $\alpha_1 + \alpha_2 \in F \subset E$, por lo que también $\alpha_2 \in E$, y $\alpha_3\alpha_4 \in F \subset E$. Como

$$\alpha_1\alpha_2 + \alpha_3\alpha_4 + \alpha_1\alpha_3 + \alpha_2\alpha_4 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) = \beta_3 \in F \subset E,$$

la suma $\gamma_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4 \in E$. Podemos interpretar lo anterior como un sistema de ecuaciones lineales con coeficientes en E e incógnitas α_3 y α_4:

$$\begin{cases} \alpha_3 + \alpha_4 = \gamma_1 \\ \alpha_1\alpha_3 + \alpha_2\alpha_4 = \gamma_2. \end{cases}$$

Este sistema es compatible determinado pues $\alpha_1 \neq \alpha_2$, así que $\alpha_3, \alpha_4 \in E$, lo que significa que $F(\alpha_1) = E = L_f$, como queríamos probar. Además,

$$\begin{aligned} \mathrm{ord}(G_K(f) \cap V) &= [L_f : F] = [E : F] = [F(\alpha_1) : F] \\ &= \deg(P_{F,\alpha_1}) = \deg(f_1) = 2. \end{aligned}$$

(3) Procedemos ya a demostrar que la tabla del enunciado es correcta.

(3.1) Si g es reducible en $K[\mathtt{t}]$ podemos suponer que $\beta_1 \in K$ luego,

$$\begin{aligned} L_f = K(\alpha_i, \beta_1, \delta) = K(\alpha_i, \delta) \quad \forall\ 1 \leq i \leq 4 \quad \& \\ F = K(\beta_1, \beta_2, \beta_3) = K(\beta_1, \delta) = K(\delta). \end{aligned}$$

(3.1.1) Si además $\delta \in K$, entonces $L_f = K(\alpha_i)$, $F = K$ y f es irreducible en $F[\mathtt{t}] = K[\mathtt{t}]$. Por tanto, en virtud de (2.1),

$$G_K(f) = G_F(f) = G_K(f) \cap V = V \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

(3.1.2) Si $\delta \notin K$, distinguimos dos subcasos:

(i) Si f es reducible en $K(\delta)[\mathtt{t}] = F[\mathtt{t}]$ hemos visto que $\mathrm{ord}(G_K(f) \cap V) = 2$ y f es el producto de dos factores irreducibles en $F[\mathtt{t}]$ de grado 2. De este modo,

$$\mathrm{ord}(G_K(f)) = [L_f : K] = [L_f : F]\cdot[F : K] = [F(\alpha_i) : F]\cdot[K(\delta) : K] = 2\cdot 2 = 4,$$

y como $G_K(f)$ es un subgrupo transitivo de orden 4 del grupo de permutaciones $\mathcal{S}_4$ y es distinto de V, no es isomorfo, por III.2.7, vol. I, a $\mathbb{Z}_2 \times \mathbb{Z}_2$ y, por tanto, es isomorfo a $\mathbb{Z}_4$.

(ii) Si f es irreducible en $K(\delta)[\mathtt{t}] = F[\mathtt{t}]$, entonces

$$\mathrm{ord}(G_K(f)) = [L_f : K] = [L_f : F]\cdot[F : K] = [F(\alpha_i) : F]\cdot[K(\delta) : K] = 4\cdot 2 = 8,$$

luego $G_K(f) \cong \mathcal{D}_4$, pues probamos en V.1.8 (5), vol. I, que todos los subgrupos de orden 8 de $\mathcal{S}_4$ son isomorfos al grupo diedral $\mathcal{D}_4$. En lo que sigue suponemos que

(3.2) El polinomio g es irreducible en $K[\mathtt{t}]$, luego $g = P_{K,\beta_1}$, y distinguimos dos subcasos:

(3.2.1) Si $\delta \in K$ entonces $F = K(\beta_1, \delta) = K(\beta_1)$, luego $[F : K] = \deg(g) = 3$, así que

$$[L_f : F] \cdot 3 = [L_f : F] \cdot [F : K] = [L_f : K] \\ = [L_f : K(\alpha_1)] \cdot [K(\alpha_1) : K] = [L_f : K(\alpha_1)] \cdot 4,$$

de donde se deduce que $12 = 3 \cdot 4$ divide a $[L_f : K]$. Como además

$$[L_f : K] = [K(\alpha_1, \beta_1) : K] = [F(\alpha_1) : F] \cdot [F : K] \leq 4 \cdot 3,$$

concluimos que $\mathrm{ord}(G_K(f)) = [L_f : K] = 12$ y, por tanto, $G_K(f) \cong \mathcal{A}_4$, pues $\mathcal{A}_4$ es el único subgrupo de orden 12 de $\mathcal{S}_4$, según probamos en III.2.8, vol. I. Hay que señalar que en este caso f es irreducible en $K(\delta)[\mathtt{t}] = K[\mathtt{t}]$.

(3.2.2) Si $\delta \notin K$, y puesto que $\delta^2 = \Delta(g)$, se deduce de VI.3.2 que

$$G(F : K) = G_K(g) \cong \mathcal{S}_3$$

y, por tanto, $[F : K] = \mathrm{ord}(G_K(g)) = 6$. Como $G(L_f : F) = G_K(f) \cap V$ y

$$[L_f : F] = \mathrm{ord}\left(G_K(f) \cap V\right) = 2r, \text{ donde } r = 1, 2,$$

$$[L_f : K] = [L_f : F] \cdot [F : K] = [L_f : F] \cdot 6 = 12r.$$

En consecuencia, el orden del grupo $G_K(f)$ es 12 o 24, y como es un subgrupo de $\mathcal{S}_4$, bien $G_K(f) \cong \mathcal{A}_4$ o $G_K(f) \cong \mathcal{S}_4$. Lo primero contradice el Corolario VI.2.9, así que $G_K(f)$ es isomorfo a $\mathcal{S}_4$. Además, $V \subset G_K(f)$, de donde deducimos que f es irreducible en $F[\mathtt{t}]$, luego es irreducible en $K(\delta)[\mathtt{t}]$. □

Observaciones VI.3.4 (1) En la Proposición anterior no se trata el caso de los polinomios de grado 4 reducibles en $K[\mathtt{t}]$ porque la casuística se multiplica y la tabla se complica grandemente, mientras que la naturaleza del problema es muy sencilla. En efecto, sea f un polinomio de grado 4 reducible en $K[\mathtt{t}]$.

(1.1) Si f tiene alguna raíz $\alpha \in K$, entonces $f(\mathtt{t}) := (\mathtt{t} - \alpha)h(\mathtt{t})$ donde $h \in K[\mathtt{t}]$ es un polinomio de grado 3. Se cumple que $G_K(f) = G_K(h)$, pues los cuerpos de descomposición de f y h sobre K coinciden, y para conocer $G_K(h)$ basta aplicar la Proposición VI.3.2 al polinomio h.

(1.2) Si f no tiene raíces en K, entonces $f = h_1 h_2$ donde $h_1, h_2 \in K[\mathtt{t}]$ son polinomios irreducibles en $K[\mathtt{t}]$ de grado 2, digamos $h_i(\mathtt{t}) = \mathtt{t}^2 - a_i\mathtt{t} + b_i$ para $i = 1, 2$. Sean α_i, β_i las raíces de h_i en $\overline{K}$ para $i = 1, 2$. Como $\alpha_i + \beta_i = a_i$, cada $\beta_i = a_i - \alpha_i \in K(\alpha_i)$, luego

$$L_f = K(\alpha_1, \beta_1, \alpha_2, \beta_2) = K(\alpha_1, \alpha_2).$$

Si $\alpha_2 \in K(\alpha_1)$ se tiene

$$\mathrm{ord}(G_K(f)) = [L_f : K] = [K(\alpha_1) : K] = \deg(P_{K,\alpha_1}) = \deg(h_1) = 2$$

luego $G_K(f) \cong \mathbb{Z}_2$, mientras que si $\alpha_2 \notin K(\alpha_1)$, entonces

$$\mathrm{ord}(G_K(f)) = [K(\alpha_1)(\alpha_2) : K(\alpha_1)] \cdot [K(\alpha_1) : K] = 2 \cdot 2 = 4.$$

De hecho $G_K(f) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, ya que $G_K(f)$ carece de elementos de orden 4 pues cada $\sigma \in G_K(f)$ cumple $\sigma^2(\alpha_i) = \alpha_i$ para $i = 1, 2$. Esto es evidente si $\sigma(\alpha_i) = \alpha_i$, mientras que si $\sigma(\alpha_i) \neq \alpha_i$ entonces $\sigma(\alpha_i) = \beta_i$, y por tanto

$$\sigma^2(\alpha_i) = \sigma(\beta_i) = \sigma(a_i - \alpha_i) = a_i - \sigma(\alpha_i) = a_i - \beta_i = \alpha_i.$$

(2) En los Ejercicios de este Capítulo se presentan ejemplos, para $K = \mathbb{Q}$, en los que los grupos de Galois de polinomios de grados 3 y 4 toman todos los valores proporcionados por las tablas anteriores.

4. Grupo de Galois de los polinomios de grado 5.

Terminamos el capítulo calculando $G_K(f)$ para cada $f \in K[\mathtt{t}]$ irreducible de grado 5, para lo que introducimos la denominada *resolvente séxtica.*

Observaciones VI.4.1 (1) Sea $f \in K[\mathtt{t}]$ de grado 5. Si es reducible existen $f_1, f_2 \in K[\mathtt{t}]$ de grado menor o igual que 4 tales que $f := f_1 f_2$, y el cálculo de $G_K(f)$ se reduce al de los grupos $G_K(f_1)$ y $G_K(f_2)$ que ya hemos analizado. Supondremos en lo sucesivo que f es irreducible en $K[\mathtt{t}]$, lo que por VI.1.2 equivale a que $G_K(f)$ es subgrupo transitivo de $\mathcal{S}_5$. Por el Ejemplo A.7, vol. I., $G_K(f)$ es isomorfo a uno de los cinco grupos siguientes:

$$\mathbb{Z}_5,\ \mathcal{D}_5,\ \mathcal{A}_5,\ \mathcal{S}_5 \ \ \& \ \ \mathcal{F}_5.$$

Vimos en el Apéndice A.2 vol. I que el grupo afín $\mathcal{F}_5$ está generado por los ciclos $\sigma = (1, 2, 3, 4, 5)$ y $\tau = (1, 2, 4, 3)$ y que $\mathcal{D}_5 = \mathcal{F}_5 \cap \mathcal{A}_5$. En particular,

(2) Los subgrupos transitivos de $\mathcal{S}_5$ contenidos en $\mathcal{A}_5$ son $\mathbb{Z}_5, \mathcal{D}_5$ y $\mathcal{A}_5$.

(3) Los subgrupos transitivos de $\mathcal{S}_5$ contenidos en $\mathcal{F}_5$ son $\mathbb{Z}_5, \mathcal{D}_5$ y $\mathcal{F}_5$.

4.a. Resolvente séxtica. Introducimos la resolvente séxtica, que emplearemos para determinar el grupo de Galois de los polinomios de grado 5.

Definición y Proposición VI.4.2 (1) Sean $\mathtt{x} := (\mathtt{x}_1, \mathtt{x}_2, \mathtt{x}_3, \mathtt{x}_4, \mathtt{x}_5)$ y el polinomio homogéneo de grado 2

$$\mathtt{q}(\mathtt{x}) := \mathtt{x}_1\mathtt{x}_2 + \mathtt{x}_2\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_1 - \mathtt{x}_1\mathtt{x}_3 - \mathtt{x}_3\mathtt{x}_5 - \mathtt{x}_5\mathtt{x}_2 - \mathtt{x}_2\mathtt{x}_4 - \mathtt{x}_4\mathtt{x}_1.$$

Explicamos la definición de este polinomio. Etiquetamos consecutivamente los vértices de un pentágono con los números $1, 2, 3, 4$ y 5. Este pentágono tiene cinco aristas, que unen vértices consecutivos, y cinco diagonales que unen vértices no consecutivos. En la fórmula que define el polinomio $\mathtt{q}$ asignamos signo positivo a los cinco monomios $\mathtt{x}_i\mathtt{x}_j$ si el par de índices (i, j) corresponde a los vértices de una arista y asignamos signo negativo a los cinco monomios $\mathtt{x}_i\mathtt{x}_j$ si el par de índices (i, j) corresponde a los vértices de una diagonal. Consideremos el polinomio $\mathtt{p} := \mathtt{q}^2 \in K[\mathtt{x}]$ y calculemos la resolvente $R_{\mathtt{p}}(\mathtt{t})$.

(2) Comenzamos probando que $\mathrm{Stab}_{\mathcal{S}_5}(\mathtt{p}) = \mathcal{F}_5$. Escribimos $\mathtt{q} := \mathtt{q}_1 - \mathtt{q}_2$, donde

$$\begin{aligned} \mathtt{q}_1(\mathtt{x}) &:= \mathtt{x}_1\mathtt{x}_2 + \mathtt{x}_2\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_1 \quad \& \\ \mathtt{q}_2(\mathtt{x}) &:= \mathtt{x}_1\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_2 + \mathtt{x}_2\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_1. \end{aligned}$$

Entonces,

$$\begin{aligned} \widetilde{\sigma}(\mathtt{q}_1) &= \mathtt{x}_2\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_1 + \mathtt{x}_1\mathtt{x}_2 = \mathtt{q}_1, \\ \widetilde{\sigma}(\mathtt{q}_2) &= \mathtt{x}_2\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_1 + \mathtt{x}_1\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_2 = \mathtt{q}_2, \\ \widetilde{\tau}(\mathtt{q}_1) &= \mathtt{x}_2\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_1 + \mathtt{x}_1\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_2 = \mathtt{q}_2, \\ \widetilde{\tau}(\mathtt{q}_2) &= \mathtt{x}_2\mathtt{x}_1 + \mathtt{x}_1\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_2 = \mathtt{q}_1, \end{aligned}$$

y en consecuencia $\widetilde{\sigma}(\mathtt{q}) = \mathtt{q}$ y $\widetilde{\tau}(\mathtt{q}) = -\mathtt{q}$. Por ello $\widetilde{\sigma}(\mathtt{p}) = \mathtt{p}$ y $\widetilde{\tau}(\mathtt{p}) = \mathtt{p}$, lo que prueba la inclusión $\mathcal{F}_5 \subset \mathrm{Stab}_{\mathcal{S}_5}(\mathtt{p})$. Si el contenido fuese estricto el orden de $\mathrm{Stab}_{\mathcal{S}_5}(\mathtt{p})$ sería un múltiplo propio de $20 = \mathrm{ord}(\mathcal{F}_5)$ que divide a $120 = \mathrm{ord}(\mathcal{S}_5)$. Pero $\mathcal{S}_5$ no tiene subgrupos de orden 40, según se prueba en IV.1.6 vol. I, y se demuestra en III.2.6, vol. I que su único subgrupo de orden 60 es $\mathcal{A}_5$. Vimos en el Apéndice A.2 vol. I que $\mathcal{F}_5 \not\subset \mathcal{A}_5$, luego debería darse la igualdad $\mathrm{Stab}_{\mathcal{S}_5}(\mathtt{p}) = \mathcal{S}_5$, es decir, el polinomio $\mathtt{p}$ debería ser simétrico. Sin embargo esto es falso. En efecto, la transposición $\alpha := (1, 2)$ cumple

$$\begin{aligned} \widetilde{\alpha}(\mathtt{p}) = (&\mathtt{x}_1\mathtt{x}_2 + \mathtt{x}_1\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_2 \\ &- \mathtt{x}_2\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_1 + \mathtt{x}_1\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_2)^2 \end{aligned}$$

Al desarrollar el cuadrado aparece el monomio $-2\mathtt{x}_2\mathtt{x}_3\mathtt{x}_4\mathtt{x}_5$, mientras que el monomio que aparece en $\mathtt{p}$ es $2\mathtt{x}_2\mathtt{x}_3\mathtt{x}_4\mathtt{x}_5$, luego $\widetilde{\alpha}(\mathtt{p}) \neq \mathtt{p}$.

(3) Consideremos los 3-ciclos $\tau_1 := (1,2,3)$, $\tau_2 := (2,3,4)$, $\tau_3 := (3,4,5)$, $\tau_4 := (1,4,5)$ y $\tau_5 := (1,2,5)$ y la permutación identidad, que denotamos $\tau_0 := \mathrm{id}$. Demostramos en el Apéndice A.2, vol. I, que estas permutaciones son representantes de las clases de congruencia por la izquierda definidas por $\mathcal{F}_5$ en $\mathcal{S}_5$. Se deduce de VI.2.5 (1) que la órbita de $\mathtt{p}$ bajo la acción del grupo simétrico $\mathcal{S}_5$ es

$$O_{\mathtt{p}} = \{\widetilde{\tau}_i(\mathtt{p}) := \mathtt{p}_i : 0 \leq i \leq 5\},$$

por lo que la resolvente universal de Galois de $\mathtt{p}$ es

$$R_{\mathtt{p}}(\mathtt{t}) := \prod_{i=0}^{5}(\mathtt{t} - \mathtt{p}_i(\mathtt{x})) \in K[\mathtt{s}_1, \mathtt{s}_2, \mathtt{s}_3, \mathtt{s}_4, \mathtt{s}_5, \mathtt{t}],$$

donde $\mathtt{s}_1, \mathtt{s}_2, \mathtt{s}_3, \mathtt{s}_4$ y $\mathtt{s}_5$ son las formas simétricas elementales en 5 indeterminadas.

(4) Para calcular los coeficientes de la resolvente $R_{\mathtt{p}}$ procedemos como sigue. Denotamos $\mathtt{q}_i := \widetilde{\tau}_i(\mathtt{q})$ y consideramos el polinomio auxiliar

$$\widehat{R}_{\mathtt{p}}(\mathtt{t}) := \prod_{i=0}^{5}(\mathtt{t} - \mathtt{q}_i(\mathtt{x})),$$

que está relacionado con $R_{\mathtt{p}}$ como sigue. Como $\mathtt{p} = \mathtt{q}^2$, para $0 \leq i \leq 5$ se tiene

$$\mathtt{p}_i = \widetilde{\tau}_i(\mathtt{p}) = \widetilde{\tau}_i(\mathtt{q}^2) = (\widetilde{\tau}_i(\mathtt{q}))^2 = \mathtt{q}_i^2,$$

y en consecuencia,

$$R_{\mathtt{p}}(\mathtt{t}^2) = \prod_{i=0}^{5}(\mathtt{t}^2 - \mathtt{q}_i(\mathtt{x})^2) = \prod_{i=0}^{5}(\mathtt{t} - \mathtt{q}_i(\mathtt{x})) \cdot \prod_{i=0}^{5}(\mathtt{t} + \mathtt{q}_i(\mathtt{x})) = \widehat{R}_{\mathtt{p}}(\mathtt{t}) \cdot \widehat{R}_{\mathtt{p}}(-\mathtt{t}).$$

Vamos a determinar los coeficientes de $\widehat{R}_{\mathtt{p}}(\mathtt{t})$; esto nos proporciona los del polinomio $R_{\mathtt{p}}(\mathtt{t}^2)$, a partir de los cuales se obtienen los de $R_{\mathtt{p}}(\mathtt{t})$. Comenzamos calculando

$$\begin{aligned}
\mathtt{q}_0(\mathtt{x}) &= \mathtt{x}_1\mathtt{x}_2 + \mathtt{x}_2\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_1 - \mathtt{x}_1\mathtt{x}_3 - \mathtt{x}_3\mathtt{x}_5 - \mathtt{x}_5\mathtt{x}_2 - \mathtt{x}_2\mathtt{x}_4 - \mathtt{x}_4\mathtt{x}_1,\\
\mathtt{q}_1(\mathtt{x}) &= \mathtt{x}_2\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_1 + \mathtt{x}_1\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_2 - \mathtt{x}_2\mathtt{x}_1 - \mathtt{x}_1\mathtt{x}_5 - \mathtt{x}_5\mathtt{x}_3 - \mathtt{x}_3\mathtt{x}_4 - \mathtt{x}_4\mathtt{x}_2,\\
\mathtt{q}_2(\mathtt{x}) &= \mathtt{x}_1\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_2 + \mathtt{x}_2\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_1 - \mathtt{x}_1\mathtt{x}_4 - \mathtt{x}_4\mathtt{x}_5 - \mathtt{x}_5\mathtt{x}_3 - \alpha_3\mathtt{x}_2 - \mathtt{x}_2\mathtt{x}_1,\\
\mathtt{q}_3(\mathtt{x}) &= \mathtt{x}_1\mathtt{x}_2 + \mathtt{x}_2\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_1 - \mathtt{x}_1\mathtt{x}_4 - \mathtt{x}_4\mathtt{x}_3 - \mathtt{x}_3\mathtt{x}_2 - \mathtt{x}_2\mathtt{x}_5 - \mathtt{x}_5\mathtt{x}_1,\\
\mathtt{q}_4(\mathtt{x}) &= \mathtt{x}_4\mathtt{x}_2 + \mathtt{x}_2\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_1 + \mathtt{x}_1\mathtt{x}_4 - \mathtt{x}_4\mathtt{x}_3 - \mathtt{x}_3\mathtt{x}_1 - \mathtt{x}_1\mathtt{x}_2 - \mathtt{x}_2\mathtt{x}_5 - \mathtt{x}_5\mathtt{x}_4,\\
\mathtt{q}_5(\mathtt{x}) &= \mathtt{x}_2\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_1 + \mathtt{x}_1\mathtt{x}_2 - \mathtt{x}_2\mathtt{x}_3 - \mathtt{x}_3\mathtt{x}_1 - \mathtt{x}_1\mathtt{x}_5 - \mathtt{x}_5\mathtt{x}_4 - \mathtt{x}_4\mathtt{x}_2,
\end{aligned}$$

Empleando un programa de cálculo simbólico se obtienen, a partir de estas expresiones, los coeficientes del polinomio $\widehat{R}_{\mathtt{p}}(\mathtt{t})$, y resulta

$$\widehat{R}_{\mathtt{p}}(\mathtt{t}) := \mathtt{t}^6 + \mathtt{a}_2\mathtt{t}^4 + \mathtt{a}_4\mathtt{t}^2 + \mathtt{a}_6 - 2^5\delta(\mathtt{x})\mathtt{t}, \tag{4.18}$$

donde $\mathtt{a}_2 := 8\mathtt{s}_1\mathtt{s}_3 - 3\mathtt{s}_2^2 - 20\mathtt{s}_4$, $\delta(\mathtt{x}) = \prod_{1\le i<j\le 5}(\mathtt{x}_i - \mathtt{x}_j)$ es una raíz cuadrada del discriminante

$$\Delta(\mathtt{x}) = \prod_{1\le i<j\le 5} (\mathtt{x}_i - \mathtt{x}_j)^2$$

y los coeficientes $\mathtt{a}_4$ y $\mathtt{a}_6$ son los siguientes:

$$\begin{aligned}\mathtt{a}_4 := {} & 3\mathtt{s}_2^4 - 16\mathtt{s}_1\mathtt{s}_2^2\mathtt{s}_3 + 16\mathtt{s}_1^2\mathtt{s}_3^2 + 16\mathtt{s}_2\mathtt{s}_3^2 + 16\mathtt{s}_1^2\mathtt{s}_2\mathtt{s}_4 - 8\mathtt{s}_2^2\mathtt{s}_4 - 112\mathtt{s}_1\mathtt{s}_3\mathtt{s}_4 \\ & + 240\mathtt{s}_4^2 - 64\mathtt{s}_1^3\mathtt{s}_5 + 240\mathtt{s}_1\mathtt{s}_2\mathtt{s}_5 - 400\mathtt{s}_3\mathtt{s}_5 \quad \&\end{aligned} \tag{4.19}$$

$$\begin{aligned}\mathtt{a}_6 : = {} & 8\mathtt{s}_1\mathtt{s}_2^4\mathtt{s}_3 - \mathtt{s}_2^6 - 16\mathtt{s}_1^2\mathtt{s}_2^2\mathtt{s}_3^2 - 16\mathtt{s}_2^3\mathtt{s}_3^2 + 64\mathtt{s}_1\mathtt{s}_2\mathtt{s}_3^3 - 64\mathtt{s}_3^4 - 16\mathtt{s}_1^2\mathtt{s}_2^3\mathtt{s}_4 \\ & + 28\mathtt{s}_2^4\mathtt{s}_4 + 64\mathtt{s}_1^3\mathtt{s}_2\mathtt{s}_3\mathtt{s}_4 - 112\mathtt{s}_1\mathtt{s}_2^2\mathtt{s}_3\mathtt{s}_4 - 128\mathtt{s}_1^2\mathtt{s}_3^2\mathtt{s}_4 + 224\mathtt{s}_2\mathtt{s}_3^2\mathtt{s}_4 \\ & - 64\mathtt{s}_1^4\mathtt{s}_4^2 + 224\mathtt{s}_1^2\mathtt{s}_2\mathtt{s}_4^2 - 176\mathtt{s}_2^2\mathtt{s}_4^2 - 64\mathtt{s}_1\mathtt{s}_3\mathtt{s}_4^2 + 320\mathtt{s}_4^3 + 48\mathtt{s}_1\mathtt{s}_2^3\mathtt{s}_5 \\ & - 192\mathtt{s}_1^2\mathtt{s}_2\mathtt{s}_3\mathtt{s}_5 - 80\mathtt{s}_2^2\mathtt{s}_3\mathtt{s}_5 + 640\mathtt{s}_1\mathtt{s}_3^2\mathtt{s}_5 + 384\mathtt{s}_1^3\mathtt{s}_4\mathtt{s}_5 - 640\mathtt{s}_1\mathtt{s}_2\mathtt{s}_4\mathtt{s}_5 \\ & - 1600\mathtt{s}_3\mathtt{s}_4\mathtt{s}_5 - 1600\mathtt{s}_1^2\mathtt{s}_5^2 + 4000\mathtt{s}_2\mathtt{s}_5^2.\end{aligned}$$

Denotando $\delta := \delta(\mathtt{x})$, la resolvente séxtica universal $R_{\mathtt{p}}(\mathtt{t})$ cumple

$$\begin{aligned}R_{\mathtt{p}}(\mathtt{t}^2) = \widehat{R}_{\mathtt{p}}(\mathtt{t})\cdot\widehat{R}_{\mathtt{p}}(-\mathtt{t}) = {} & (\mathtt{t}^6 + \mathtt{a}_2\mathtt{t}^4 + \mathtt{a}_4\mathtt{t}^2 + \mathtt{a}_6 - 2^5\delta\mathtt{t})\cdot \\ & (\mathtt{t}^6 + \mathtt{a}_2\mathtt{t}^4 + \mathtt{a}_4\mathtt{t}^2 + \mathtt{a}_6 + 2^5\delta\mathtt{t}) = (\mathtt{t}^6 + \mathtt{a}_2\mathtt{t}^4 + \mathtt{a}_4\mathtt{t}^2 + \mathtt{a}_6)^2 - 2^{10}\Delta\mathtt{t}^2,\end{aligned}$$

de donde se deduce la igualdad que buscamos:

$$R_{\mathtt{p}}(\mathtt{t}) = (\mathtt{t}^3 + \mathtt{a}_2\mathtt{t}^2 + \mathtt{a}_4\mathtt{t} + \mathtt{a}_6)^2 - 2^{10}\Delta(\mathtt{x})\mathtt{t}. \tag{4.20}$$

Teorema VI.4.3 *Sean $f \in K[\mathtt{t}]$ un polinomio irreducible de grado 5 y $R_{f,\mathtt{p}}$ la resolvente séxtica especializada en f. Entonces,*

(1) *El grupo de Galois $G_K(f)$ de f es subgrupo del grupo alternado $\mathcal{A}_5$, o lo que es igual, es isomorfo a $\mathbb{Z}_5$, $\mathcal{D}_5$ o $\mathcal{A}_5$, si y sólo si el discriminante $\Delta(f)$ de f es un cuadrado en K.*

(2) *El grupo de Galois $G_K(f)$ de f es conjugado a un subgrupo de $\mathcal{F}_5$ si y sólo si $R_{f,\mathtt{p}}$ posee una raíz en K.*

(3) *El grupo de Galois $G_K(f)$ es isomorfo a $\mathbb{Z}_5$ si y sólo si para cada raíz u de f en $\overline{K}$ el cuerpo $K(u)$ es cuerpo de descomposición de f sobre K.*

Demostración. (1) Este apartado se deduce directamente del Corolario VI.2.9.

(2) Denotamos $\alpha := (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ una 5-upla formada por las raíces $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ y α_5 de f en $\overline{K}$. Vimos en VI.4.2 (2) que $\mathrm{Stab}_{\mathcal{S}_5}(\mathtt{p}) = \mathcal{F}_5$, luego en virtud de VI.2.8 (3.3) & (3.4), y puesto que las raíces de la resolvente de $\mathtt{p}$ especializada en f son simples en virtud de la igualdad (4.20) y la irreducibilidad de f, el grupo $G_K(f)$ es conjugado a un subgrupo de $\mathcal{F}_5$ si y sólo si existe $\sigma \in \mathcal{S}_5$ tal que $\sigma(\mathtt{p}(\alpha))$ pertenece a K. Pero por (2.14) y VI.2.8 (2), $\sigma(\mathtt{p}(\alpha)) = \widetilde{\sigma}(\mathtt{p})(\alpha)$ es una raíz de $R_{f,\mathtt{p}}$, y todas las raíces de la resolvente $R_{f,\mathtt{p}}$ son de esa forma.

(3) Sean L_f un cuerpo de descomposición de f sobre K y $u \in \overline{K}$ una raíz de f. Entonces, como $[K(u) : K] = \deg(P_{K,u}) = \deg(f) = 5$, tenemos

$$\begin{aligned} G_K(f) \cong \mathbb{Z}_5 \quad &\Longleftrightarrow \quad \mathrm{ord}(G_K(f)) = 5 \quad \Longleftrightarrow \quad [L_f : K] = 5 \\ &\Longleftrightarrow \quad [L_f : K(u)] = \frac{[L_f : K]}{[K(u) : K]} = 1 \quad \Longleftrightarrow \quad L_f = K(u), \end{aligned}$$

es decir, $K(u)$ es cuerpo de descomposición de f sobre K. □

Corolario VI.4.4 *Sea $f \in \mathbb{Q}[\mathtt{t}]$ un polinomio irreducible de grado 5 cuyo grupo de Galois es $\mathbb{Z}_5$. Entonces f tiene 5 raíces reales.*

Demostración. Como f tiene grado impar posee alguna raíz real u, y $\mathbb{Q}(u)$ es cuerpo de descomposición de f sobre $\mathbb{Q}$, ya que si L_f denota un cuerpo de descomposición de f sobre $\mathbb{Q}$, la inclusión $\mathbb{Q}(u) \subset L_f$ es evidente y como f es el polinomio mínimo de u sobre $\mathbb{Q}$,

$$[L_f : \mathbb{Q}(u)] = \frac{[L_f : \mathbb{Q}]}{[\mathbb{Q}(u) : \mathbb{Q}]} = \frac{\mathrm{ord}(G_K(f))}{\deg(P_{\mathbb{Q},u})} = \frac{\mathrm{ord}(\mathbb{Z}_5)}{\deg(f)} = \frac{5}{5} = 1,$$

es decir, $L_f = \mathbb{Q}(u)$. Por tanto, las cinco raíces de f en $\mathbb{C}$, que son distintas pues f es irreducible, pertenecen a $L_f = \mathbb{Q}(u) \subset \mathbb{R}$. □

4.b. Grupo de Galois de un polinomio irreducible de grado 5. En esta sección determinamos el grupo de Galois de una quíntica irreducible en función de su discriminante y su resolvente séxtica.

Proposición VI.4.5 Sean $f \in K[\mathtt{t}]$ un polinomio irreducible de grado 5, $L_f \subset \overline{K}$ un cuerpo de descomposición de f contenido en un cierre algebraico

$\overline{K}$ de K, y sean $u \in \overline{K}$ una de sus raíces, $\delta \in \overline{K}$ una raíz cuadrada de su discriminante $\Delta(f)$ y $R_{f,\mathtt{p}}$ la resolvente séxtica especializada en f. Entonces, su grupo de Galois $G_K(f)$ es el dado por la siguiente tabla.

$\delta \in K$	$R_{f,\mathtt{p}}$ tiene una raíz en K	$L_f = K(u)$	$G_K(f)$
NO	NO	–	$\mathcal{S}_5$
SI	NO	–	$\mathcal{A}_5$
NO	SI	–	$\mathcal{F}_5$
SI	SI	NO	$\mathcal{D}_5$
SI	SI	SI	$\mathbb{Z}_5$

Demostración. Como f es irreducible en $K[\mathtt{t}]$ su grupo de Galois $G_K(f)$ es, necesariamente, uno de los cinco grupos de la tabla, pues éstos son los únicos subgrupos transitivos de $\mathcal{S}_5$. Supongamos primero que $R_{f,\mathtt{p}}$ posee alguna raíz en K. Esto implica, por el Teorema VI.4.3 (2), que $G_K(f)$ es conjugado a un subgrupo de $\mathcal{F}_5$, luego es isomorfo a $\mathbb{Z}_5, \mathcal{D}_5$ o $\mathcal{F}_5$.

Si $\delta \notin K$ entonces el grupo $G_K(f)$ no está contenido en $\mathcal{A}_5$, por el Corolario VI.2.9, luego $G_K(f)$ es isomorfo a $\mathcal{F}_5$. Por el contrario, si $\delta \in K$ entonces $G_K(f) \subset \mathcal{A}_5$, así que es isomorfo al grupo cíclico de orden 5 o al diedral de orden 10 y para distinguir ambos casos apelamos al apartado (3) en el Teorema VI.4.3: el grupo es cíclico si y sólo si $K(u)$ es un cuerpo de descomposición de f sobre K.

Por último, si $R_{f,\mathtt{p}}$ no posee alguna raíz en K se sigue del Teorema VI.4.3 que $G_K(f)$ es isomorfo a $\mathcal{S}_5$ o $\mathcal{A}_5$ y para dilucidar en qué caso estamos basta emplear el Corolario VI.2.9, pues $G_K(f) = \mathcal{A}_5$ si y sólo si $\delta \in K$. □

Aunque la tabla anterior permite determinar el grupo de Galois de las quínticas irreducibles, exponemos a continuación un resultado adicional.

Teorema VI.4.6 *Sean $f \in K[\mathtt{t}]$ un polinomio irreducible de grado 5 y $R_{f,\mathtt{p}}$ la resolvente séxtica de Galois especializada en f. Las siguientes afirmaciones son equivalentes:*

(1) *La resolvente $R_{f,\mathtt{p}}$ es irreducible en $K[\mathtt{t}]$.*

(2) *El grupo de Galois $G_K(f)$ es el grupo alternado $\mathcal{A}_5$ o el grupo simétrico $\mathcal{S}_5$.*

Demostración. (1) $\Longrightarrow$ (2) Sean $\alpha := (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ una 5-upla formada por las raíces de f en $\overline{K}$ y $\omega := \mathtt{p}(\alpha) \in \overline{K}$, que es una raíz de $R_{f,\mathtt{p}} \in K[\mathtt{t}]$. Como estamos suponiendo que este polinomio es irreducible en $K[\mathtt{t}]$ es el polinomio mínimo de ω sobre K, luego $[K(\omega) : K] = \deg(R_{f,\mathtt{p}}) = 6$. Señalamos en VI.2.8 (3.1) que $\omega \in L_f$, luego $K \subset K(\omega) \subset L_f$. Por tanto,

$$\mathrm{ord}(G_K(f)) = [L_f : K] = [L_f : K(\omega)] \cdot [K(\omega) : K] = 6 \cdot [L_f : K(\omega)] \in 6\mathbb{Z}.$$

En consecuencia, $G_K(f)$ es un subgrupo transitivo de $\mathcal{S}_5$ cuyo orden es múltiplo de 6, lo que por el Ejemplo A.7, vol. I. implica que $G_K(f) = \mathcal{A}_5$ o $G_K(f) = \mathcal{S}_5$.

(2) $\Longrightarrow$ (1) Consideremos $\tau_0 := \mathrm{id}$ y los 3-ciclos

$$\tau_1 := (1,2,3),\ \tau_2 := (2,3,4),\ \tau_3 := (3,4,5),\ \tau_4 := (1,4,5) \quad \& \quad \tau_5 := (1,2,5).$$

Por VI.4.2 y VI.2.8, la resolvente séxtica especializada está definida por

$$R_{f,\mathtt{p}}(\mathtt{t}) = \prod_{i=0}^{5} (\mathtt{t} - \tau_i(\omega)).$$

Hay que demostrar que $R_{f,\mathtt{p}}$ coincide con el polinomio mínimo $P_{K,\omega} \in K[\mathtt{t}]$ de ω sobre K, pues esto implica su irreduciblidad. Comenzamos probando que $R_{f,\mathtt{p}}$ es potencia de $P_{K,\omega} \in K[\mathtt{t}]$. Desde luego este polinomio divide a $R_{f,\mathtt{p}}$, luego factoriza en $L_f[\mathtt{t}]$ en producto de factores de grado 1, pues $R_{f,\mathtt{p}}$ lo hace. Sean $\omega_1 := \omega, \omega_2, \ldots, \omega_d$ las raíces en $\overline{K}$ de $P_{K,\omega}$, esto es,

$$P_{K,\omega}(\mathtt{t}) := \prod_{j=1}^{d} (\mathtt{t} - \omega_j).$$

Por supuesto las raíces de $P_{K,\omega}$ son raíces de $R_{f,\mathtt{p}}$, y la clave consiste en observar que toda raíz de $R_{f,\mathtt{p}}$ lo es de $P_{K,\omega}$. Para ello escribimos

$$P_{K,\omega}(\mathtt{t}) := \sum_{k=0}^{d} c_k \mathtt{t}^k \in K[\mathtt{t}],$$

y, fijada una raíz $\tau_i(\omega)$ de $R_{f,\mathtt{p}}$ se tiene $\tau_i(\omega) = \tau_i(\mathtt{p}(\alpha)) = \widetilde{\tau}_i(\mathtt{p})(\alpha)$, en virtud de VI.2.8 (2). En consecuencia,

$$\begin{aligned} P_{K,\omega}(\tau_i(\omega)) &= \sum_{k=0}^{d} c_k \tau_i(\omega)^k = \sum_{k=0}^{d} c_k (\widetilde{\tau}_i(\mathtt{p})(\alpha))^k = \tau_i\Big(\sum_{k=0}^{d} c_k (\mathtt{p}(\alpha))^k\Big) \\ &= \tau_i\Big(\sum_{k=0}^{d} c_k \omega^k\Big) = \tau_i(P_{K,\omega}(\omega)) = \tau_i(0) = 0. \end{aligned}$$

Definimos en $X := \{\tau_0, \tau_1, \tau_2, \tau_3, \tau_4, \tau_5\}$ la relación de equivalencia $\tau_i \mathcal{R} \tau_j$ si $\tau_j(\omega) = \tau_i(\omega)$ esto es, si $\tau_i^{-1}\tau_j \in H := G(L_f : K(\omega))$, y observamos que todas las clases de equivalencia $[\tau_i]$, con $0 \leq i \leq 5$, tienen el mismo número de elementos. En efecto, la aplicación

$$\psi : [\tau_0] \to [\tau_i],\ \tau \mapsto \tau_i \cdot \tau$$

es una biyección bien definida, pues si $\tau \in [\tau_0]$, entonces $\tau \mathcal{R} \tau_0$, esto es, $\tau^{-1} \in H$, luego $(\tau_i \cdot \tau)^{-1}\tau_i = \tau^{-1} \in H$, es decir, $\tau_i \cdot \tau \in [\tau_i]$. La aplicación ψ es inyectiva por la propiedad cancelativa, y es también sobreyectiva, pues dada $\tau_j \in [\tau_i]$ existe $\tau := \tau_i^{-1}\tau_j \in [\tau_0]$ tal que $\psi(\tau) = \tau_j$.

Nótese que $d = \deg(P_{K,\omega}) = \mathrm{Card}(X/\mathcal{R})$, pues las raíces de $P_{K,\omega}$ y $R_{f,\mathtt{p}}$ son las mismas, y si m es el número de elementos común de las clases de equivalencia de $X/\mathcal{R}$ se tiene $6 = md$. En consecuencia, si $\tau_{i_1}, \ldots, \tau_{i_d}$ son representantes de las d clases de equivalencia del cociente $X/\mathcal{R}$ resulta que $\{\omega_1, \ldots, \omega_d\} = \{\tau_{i_1}(\omega), \ldots, \tau_{i_d}(\omega)\}$, por lo que

$$R_{f,\mathtt{p}}(\mathtt{t}) = \prod_{j=1}^{d}(\mathtt{t} - \tau_{i_j}(\omega))^m = \Big(\prod_{j=1}^{d}(\mathtt{t} - \tau_{i_j}(\omega))\Big)^m = \Big(\prod_{j=1}^{d}(\mathtt{t} - \omega_j)\Big)^m = P_{K,\omega}^m(\mathtt{t}).$$

Por tanto $R_{f,\mathtt{p}} = P_{K,\omega}^m$ y, además, $6 = md = m\deg(P_{K,\omega})$, luego $d \in \{1, 2, 3, 6\}$. Hay que comprobar que $m = 1$, para lo que basta probar que ninguno de los otros tres casos puede darse.

Si $m = 6$ entonces $\deg(P_{K,\omega}) = 1$, así que $\omega \in K$ es raíz de $R_{f,\mathtt{p}}$. Esto contradice la Tabla VI.4.1, ya que $\mathcal{A}_5 \subset G_K(f)$. Supongamos que $m = 2$. Entonces $P_{K,\omega}$ es un polinomio mónico de grado 3 y, manteniendo las notaciones del Ejemplo VI.4.2, y denotando $a_i := \mathtt{a}_i(\alpha)$, se tiene

$$(\mathtt{t}^3 + a_2\mathtt{t}^2 + a_4\mathtt{t} + a_6)^2 - 2^{10}\Delta(f)\mathtt{t} = R_{f,\mathtt{p}}(\mathtt{t}) = P_{K,\omega}^2(\mathtt{t}).$$

Si abreviamos $h(\mathtt{t}) := \mathtt{t}^3 + a_2\mathtt{t}^2 + a_4\mathtt{t} + a_6$ resulta que

$$(h(\mathtt{t}) - P_{K,\omega}(\mathtt{t})) \cdot (h(\mathtt{t}) + P_{K,\omega}(\mathtt{t})) = h^2(\mathtt{t}) - P_{K,\omega}^2(\mathtt{t}) = 2^{10}\Delta(f)\mathtt{t},$$

que es imposible pues $\Delta(f) \neq 0$, ya que f es irreducible en $K[\mathtt{t}]$ y $h + P_{K,\omega}$ tiene grado 3. Supongamos por último que $m = 3$. Entonces $\deg(P_{K,\omega}) = 2$, es decir, existen $a, b \in K$ tales que $P_{K,\omega}(\mathtt{t}) = \mathtt{t}^2 + a\mathtt{t} + b$, y por tanto,

$$(\mathtt{t}^3 + a_2\mathtt{t}^2 + a_4\mathtt{t} + a_6)^2 - 2^{10}\Delta(f)\mathtt{t} = R_{f,\mathtt{p}}(\mathtt{t}) = P_{K,\omega}(\mathtt{t})^3 = (\mathtt{t}^2 + a\mathtt{t} + b)^3. \quad (4.21)$$

Igualando los coeficientes de grado $0, 2, 3, 4$ y 5 de ambos miembros se obtiene:

$$\begin{cases} a_6^2 & & & = & b^3 & & \\ a_4^2 & + & 2a_2a_6 & = & 3b^2 & + & 3a^2b \\ 2a_6 & + & 2a_2a_4 & = & 6ab & + & a^3 \\ a_2^2 & + & 2a_4 & = & 3b & + & 3a^2 \\ 2a_2 & & & = & 3a & & \end{cases}$$

Despejamos $a_2 = 3a/2$ y remplazamos este valor en la penúltima igualdad:

$$2a_4 = 3b + 3a^2 - 9a^2/4 = 3b + 3a^2/4 \quad \Longrightarrow \quad a_4 = 3b/2 + 3a^2/8. \tag{4.22}$$

Sustituyendo los valores de a_2 y a_4 en la tercera igualdad resulta

$$2a_6 = 6ab + a^3 - 3a(3b/2 + 3a^2/8) = a(12b - a^2)/8, \tag{4.23}$$

y al introducir los valores obtenidos en la primera igualdad se tiene

$$4b^3 = 4a_6^2 = (2a_6)^2 = a^2(12b - a^2)^2/64 \quad \Longrightarrow \quad 256b^3 = a^2(12b - a^2)^2. \tag{4.24}$$

Nótese que $b \neq 0$, pues $P_{K,\omega}$ es irreducible, y denotamos $s := a^2/b$. Al sustituir en (4.24) obtenemos $256b^3 = bs(12b - bs)^2 = b^3s(12 - s)^2$, y simplificando el factor b^3, se tiene $256 = s(12 - s)^2$, es decir,

$$s^3 - 24s^2 + 144s - 256 = 0.$$

A simple vista se observa que $s = 4$ es solución de esta ecuación y de hecho, mediante la Regla de Ruffini se obtiene

$$(s - 4)^2(s - 16) = s^3 - 24s^2 + 144s - 256 = 0,$$

luego $s = 4$ o $s = 16$. Vamos a comprobar que la segunda posibilidad no puede darse. En efecto, si $s = 16$ entonces $a^2 = 16b$, y por tanto,

$$a_2 = 3a/2, \quad a_4 = 3b/2 + 3a^2/8 = 15b/2 \quad \& \quad a_6 = a(12b - a^2)/16 = -ab/4.$$

Al sustituir estos valores en la segunda de las igualdades iniciales se obtiene

$$225b^2/4 - 3a^2b/4 = 3b^2 + 3a^2b = 51b^2,$$

o sea, $225b^2/4 - 12b^2 = 51b^2$, esto es, $225 = 4 \cdot 63$, que es falso.

Por tanto, $a^2 = 4b$, y sustituyendo este valor en (4.22) y (4.23) se sigue que $a_4 = 3b$ y $2a_6 = ab$. Igualando los coeficientes de $\mathtt{t}$ en los dos miembros de (4.21) resulta

$$2a_4a_6 - 2^{10}\Delta(f) = 3ab^2 \quad \Longrightarrow \quad 2^{10}\Delta(f) = 2a_4a_6 - 3ab^2 = 3ab^2 - 3ab^2 = 0,$$

que es falso pues, al ser $\mathrm{char}(K) = 0$ y f irreducible, $\Delta(f)$ es no nulo. □

4.c. Realización de los grupos. Terminamos esta sección mostrando ejemplos de polinomios irreducibles $f \in \mathbb{Q}[\mathtt{t}]$ de grado 5 cuyos grupos de Galois son $\mathbb{Z}_5$, $\mathcal{D}_5$, $\mathcal{F}_5$, $\mathcal{A}_5$ y $\mathcal{S}_5$.

Ejemplos VI.4.7 (1) Buscamos un polinomio irreducible $f \in \mathbb{Z}[\mathtt{t}]$ de grado 5 cuyo grupo de Galois $G_{\mathbb{Q}}(f) = \mathbb{Z}_5$, para lo que empleamos la estrategia diseñada en el Corolario VI.1.15. Sea $\zeta := e^{2\pi i/11}$, que es una raíz primitiva undécima de la unidad.

Para $1 \leq k \leq 10$ denotamos $\sigma_k \in G(\mathbb{Q}(\zeta) : \mathbb{Q})$ el único $\mathbb{Q}$-automorfismo que cumple $\sigma_k(\zeta) = \zeta^k$. Entonces, el grupo de Galois de la extensión $\mathbb{Q}(\zeta)|\mathbb{Q}$ es $G(\mathbb{Q}(\zeta) : \mathbb{Q}) = \{\sigma_k : 1 \leq k \leq 10\}$, pues el conjunto de raíces del polinomio mínimo de ζ sobre $\mathbb{Q}$, que es el ciclotómico Φ_{11}, es $\{\zeta^k : 1 \leq k \leq 10\}$.

Si H es un subgrupo de $G(\mathbb{Q}(\zeta) : \mathbb{Q})$ de orden 2, cuyo cuerpo fijo denotamos $E := \mathrm{Fix}(H)$, el grupo de Galois $G(E : \mathbb{Q})$ es $\mathbb{Z}_5$, por lo que el polinomio mínimo $f := P_{\mathbb{Q},\alpha}$, donde α es un elemento primitivo de la extensión $E|\mathbb{Q}$, tiene grado 5 y su grupo de Galois tiene orden 5, luego es $\mathbb{Z}_5$. Comenzamos por tanto calculando H. Nótese que $\zeta^{11} = 1$, luego $\zeta^{10} = \zeta^{-1}$, así que $\sigma_{10} \neq \mathrm{id}_E$ pero $\sigma_{10}^2 = \mathrm{id}_E$ ya que

$$\sigma_{10}^2(\zeta) = \sigma_{10}(\zeta^{-1}) = \big(\sigma_{10}(\zeta)\big)^{-1} = (\zeta^{-1})^{-1} = \zeta.$$

Vamos a determinar qué elementos $x := \sum_{j=0}^{9} a_j\zeta^j \in \mathbb{Q}(\zeta)$ quedan fijos por el automorfismo $\sigma = \sigma_{10}$. Como $\sigma(\zeta) = \zeta^{10} = -\sum_{j=0}^{9}\zeta^j$ y $10j \equiv 11 - j \bmod 11$ se tiene

$$\sigma(x) = \sigma\Big(\sum_{j=0}^{9} a_j\zeta^j\Big) = \sum_{j=0}^{9} a_j\zeta^{10j} = \sum_{j=0}^{9} a_j\zeta^{11-j} = \sum_{j=2}^{9} a_{11-j}\zeta^j + a_0 - a_1\sum_{j=0}^{9}\zeta^j$$
$$= (a_0 - a_1) - a_1\zeta + \sum_{j=2}^{p}(a_{11-j} - a_1)\zeta^j.$$

Como $1, \zeta, \ldots, \zeta^9$ son $\mathbb{Q}$-linealmente independientes, la condición $x = \sigma(x)$ equivale a que

$$\begin{cases} a_0 = a_0 - a_1 \\ a_1 = -a_1 \\ a_j = a_{11-j} - a_1 \quad \text{para } 2 \leq j \leq 9 \end{cases}$$

o, equivalentemente, $a_1 = 0$ y $a_j = a_{11-j}$ para todo $2 \leq j \leq 9$, esto es

$$E = \mathrm{Fix}(H) = \Big\{a_0 + \sum_{j=2}^{5} a_j(\zeta^j + \zeta^{11-j}) : \ a_0, a_j \in \mathbb{Q}\Big\}. \tag{4.25}$$

En particular, eligiendo $a_0 = a_3 = a_4 = a_5 = 0$ y $a_2 = 1$ se deduce que $\alpha := \zeta^2 + \zeta^9 \in E$ y sólo falta demostrar que $E = \mathbb{Q}(\alpha)$ y calcular el polinomio $f := P_{\mathbb{Q},\alpha}$. Para lo primero es suficiente, a la vista de (4.25), comprobar que $\zeta^j + \zeta^{11-j} \in \mathbb{Q}(\alpha)$ para $3 \leq j \leq 5$. Nótese que

$$\alpha^2 = \zeta^4 + \zeta^{18} + 2\zeta^{11} = \zeta^4 + \zeta^7 + 2 \quad \Longrightarrow \quad \zeta^4 + \zeta^7 = \alpha^2 - 2 \in \mathbb{Q}(\alpha).$$

Por otro lado, teniendo en cuenta que $\zeta^{11} = 1$, al multiplicar resulta

$$\alpha^3 = \alpha^2 \cdot \alpha = (\zeta^4 + \zeta^7 + 2) \cdot (\zeta^2 + \zeta^9) = \zeta^6 + 3\zeta^9 + 3\zeta^2 + \zeta^5,$$

es decir, $\zeta^5 + \zeta^6 = \alpha^3 - 3\alpha \in \mathbb{Q}(\alpha)$. Para demostrar que $E = \mathbb{Q}(\alpha)$ sólo falta comprobar que $\zeta^3 + \zeta^8 \in \mathbb{Q}(\alpha)$, para lo que basta calcular

$$\alpha^4 = (\zeta^4 + \zeta^7 + 2)^2 = \zeta^8 + \zeta^3 + 4 + 2(1 + 2\zeta^4 + 2\zeta^7),$$

y despejando,

$$\zeta^3 + \zeta^8 = \alpha^4 - 4(\alpha^2 - 2) - 6 = \alpha^4 - 4\alpha^2 + 2 \in \mathbb{Q}(\alpha).$$

Por último, hemos de calcular el polinomio mínimo f de α sobre $\mathbb{Q}$. Como

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [E : \mathbb{Q}] = \operatorname{ord}(G(\mathbb{Q}(\zeta) : \mathbb{Q}))/\operatorname{ord}(H) = 10/2 = 5,$$

todo se reduce a encontrar un polinomio en $\mathbb{Q}[\mathtt{t}]$ de grado 5 que tenga a α por raíz. Para ello calculamos primero

$$\begin{aligned}\alpha^5 = (\zeta^2 + \zeta^9)^5 &= \zeta^{10} + 5(\zeta^{17} + \zeta^{38}) + 10(\zeta^{24} + \zeta^{31}) + \zeta^{45} \\ &= (\zeta^{10} + \zeta) + 5(\zeta^6 + \zeta^5) + 10(\zeta^2 + \zeta^9).\end{aligned}$$

Despejamos el sumando

$$\zeta^{10} + \zeta = \alpha^5 - 5(\alpha^3 - 3\alpha) - 10\alpha = \alpha^5 - 5\alpha^3 + 5\alpha$$

y, finalmente,

$$\begin{aligned}-1 = \sum_{j=1}^{10} \zeta^j &= (\zeta^{10} + \zeta) + (\zeta^9 + \zeta^2) + (\zeta^8 + \zeta^3) + (\zeta^7 + \zeta^4) + (\zeta^6 + \zeta^5) \\ &= (\alpha^5 - 5\alpha^3 + 5\alpha) + \alpha + (\alpha^4 - 4\alpha^2 + 2) + (\alpha^2 - 2) + (\alpha^3 - 3\alpha) \\ &= \alpha^5 + \alpha^4 - 4\alpha^3 - 3\alpha^2 + 3\alpha,\end{aligned}$$

luego $f(\mathtt{t}) := \mathtt{t}^5 + \mathtt{t}^4 - 4\mathtt{t}^3 - 3\mathtt{t}^2 + 3\mathtt{t} + 1$ es un polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$ cuyo grupo de Galois $G_{\mathbb{Q}}(f)$ es $\mathbb{Z}_5$.

(2) Comprobaremos a continuación que el polinomio $f(\mathtt{t}) := \mathtt{t}^5 - 5\mathtt{t} + 12$ es irreducible en $\mathbb{Q}[\mathtt{t}]$ y $G_{\mathbb{Q}}(f) = \mathcal{D}_5$. En primer lugar,

$$f(\mathtt{t}-2) = (\mathtt{t}-2)^5 - 5(\mathtt{t}-2) + 12 = \mathtt{t}^5 - 10\mathtt{t}^4 + 40\mathtt{t}^3 - 80\mathtt{t}^2 + 75\mathtt{t} - 10$$

es irreducible en $\mathbb{Z}[\mathtt{t}]$, por el Criterio de Eisenstein, luego lo es en $\mathbb{Q}[\mathtt{t}]$, así que también f lo es. Su resolvente séxtica es

$$\begin{aligned} R_{f,\mathtt{p}}(\mathtt{t}) = {} & \mathtt{t}^6 + 200\mathtt{t}^5 + 22000\mathtt{t}^4 + 1120000\mathtt{t}^3 \\ & + 28000000\mathtt{t}^2 - 66016000000\mathtt{t} + 1600000000, \end{aligned}$$

que tiene a $100 \in \mathbb{Q}$ por raíz. Además $\Delta(f) = 5^6 \cdot 4^6$, luego $\delta = 5^3 \cdot 4^3 \in \mathbb{Q}$. Atendiendo a la tabla de la Proposición VI.4.5 el grupo $G_{\mathbb{Q}}(f)$ es cíclico o diedral y, a la vista del Corolario VI.4.4, para comprobar que $G_{\mathbb{Q}}(f) = \mathcal{D}_5$ es suficiente demostrar que f posee alguna raíz en $\mathbb{C} \setminus \mathbb{R}$. Ahora bien, la derivada

$$f'(\mathtt{t}) = 5(\mathtt{t}^4 - 1) = 5(\mathtt{t}^2 - 1)(\mathtt{t}^2 + 1)$$

tiene, exactamente, dos raíces reales, y el Teorema de Rolle implica que f tiene, a lo sumo, tres raíces reales.

(3) Sea p un número primo. El polinomio $f(\mathtt{t}) := \mathtt{t}^5 - p$ es irreducible en $\mathbb{Q}[\mathtt{t}]$, por el criterio de Eisenstein, y si $u := \sqrt[5]{p} \in \mathbb{R}$ es la única raíz real de f y $\zeta := e^{2\pi i/5}$, las raíces de f en $\mathbb{C}$ son los números $\{u\zeta^i : 0 \leq i \leq 4\}$.

Por tanto, un cuerpo de descomposición de f sobre $\mathbb{Q}$ es $L_f := \mathbb{Q}(u, \zeta)$. Como $[\mathbb{Q}(u) : \mathbb{Q}] = \deg(f) = 5$ y $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(P_{\mathbb{Q},\zeta}) = \deg(\Phi_5) = 4$, donde Φ_5 es el quinto polinomio ciclotómico, y $\mathrm{mcd}(4, 5) = 1$, se tiene

$$\mathrm{ord}(G_{\mathbb{Q}}(f)) = [L_f : \mathbb{Q}] = [\mathbb{Q}(u, \zeta) : \mathbb{Q}] = 5 \cdot 4 = 20,$$

de donde se deduce que $G_{\mathbb{Q}}(f) = \mathcal{F}_5$.

(4) Vimos en VII.2.12, vol. II que el discriminante del polinomio $\mathtt{t}^5 + a\mathtt{t} + b$ es $2^8a^5 + 5^5b^4$. En particular, el discriminante del polinomio $f(\mathtt{t}) := \mathtt{t}^5 + 20\mathtt{t} + 16$ es $\Delta(f) = (2^8 \cdot 5^3)^2$, que es el cuadrado de un número racional.

Vamos a demostrar que f es irreducible en $\mathbb{Q}[\mathtt{t}]$ y que $G_{\mathbb{Q}}(f) = \mathcal{A}_5$. Para lo primero es suficiente probar que su reducción $\overline{f} \in \mathbb{F}_3[\mathtt{t}]$ es un polinomio irreducible en $\mathbb{F}_3[\mathtt{t}]$. Desde luego $\overline{f}(\mathtt{t}) = \mathtt{t}^5 + 2\mathtt{t} + 1$ no tiene raíces en $\mathbb{F}_3$, pues $\overline{f}(0) = \overline{f}(1) = \overline{f}(2) = 1$, luego si $\overline{f}$ fuese reducible existirían $a, b, c \in \mathbb{F}_3$ tales que $c \neq 0$ y

$$\mathtt{t}^5 + 2\mathtt{t} + 1 = (\mathtt{t}^3 + a\mathtt{t}^2 + b\mathtt{t} + c)(\mathtt{t}^2 - a\mathtt{t} + c),$$

e igualando los coeficientes de ambos miembros se tiene

$$\left\{\begin{array}{rcl} c & = & a^2-b \\ a(b-c) & = & c \\ c(b-a) & = & 2 \end{array}\right.$$

La segunda ecuación implica que $a \neq 0$, luego $a^2 = 1$, y sustituyendo este valor en la primera nos proporciona $c = 1 - b$. Al remplazar este valor en la segunda ecuación resulta $a(2b-1) = 1-b$. Esto implica que $a = 2$, pues si $a = 1$ se tiene $2b - 1 = 1 - b$, que es imposible. Por ello $1 - b = 2(2b-1) = b - 2$, es decir, $b = 0$ y $c = 1$, que no satisfacen la tercera ecuación.

Para probar que $G_{\mathbb{Q}}(f) = \mathcal{A}_5$ sólo falta comprobar, empleando la tabla VI.4.5, que la resolvente séxtica $R_{f,\mathtt{p}}$ especializada en f no tiene ninguna raíz racional. Como la resolvente

$$R_{f,\mathtt{p}}(\mathtt{t}) = (\mathtt{t}^3 - 400\mathtt{t}^2 + 96000\mathtt{t} + 2560000)^2 - (2^8 \cdot 5^3)^2\mathtt{t}$$

es un polinomio mónico, si tuviera raíces racionales las tendría enteras, que serían divisores del término independiente. Con paciencia se comprueba que ninguno de ellos es raíz de $R_{f,\mathtt{p}}$, así que $G_{\mathbb{Q}}(f) = \mathcal{A}_5$.

(5) Por último empleamos el Corolario VI.1.6 para demostrar que el grupo de Galois $G_{\mathbb{Q}}(f)$ del polinomio $f(\mathtt{t}) := \mathtt{t}^5 - 10\mathtt{t} - 2$ es $\mathcal{S}_5$, para lo que hemos de ver que f tiene, exactamente, dos raíces en $\mathbb{C} \setminus \mathbb{R}$.

Su derivada $f'(\mathtt{t}) = 5\mathtt{t}^4 - 10$ tiene, exactamente, 2 raíces reales, luego el número de raíces reales de f es, por el Teorema de Rolle, a lo sumo 3. Además,

$$f(-2) = -14 < 0, \quad f(-1) = 7 > 0, \quad f(0) = -2 < 0 \quad \& \quad f(2) = 10 > 0,$$

lo que por el Teorema de Bolzano garantiza que f tiene, al menos, tres raíces reales. Por tanto, el número de raíces de f en $\mathbb{R}$ es 3, y como f tiene 5 raíces complejas distintas por ser irreducible, se deduce que el número de raíces de f en $\mathbb{C} \setminus \mathbb{R}$ es 2.

Demostración de VI.2.8. (2) Comprobemos que $\widetilde{\sigma}(\mathtt{p})(\alpha) = \sigma(\mathtt{p}(\alpha))$ para todo $\sigma \in G_K(f)$ y $\mathtt{p} \in K[\mathtt{x}]$. En efecto, escribimos $\mathtt{p}(\mathtt{x}) := \sum_\nu a_\nu \mathtt{x}^\nu \in K[\mathtt{x}]$ donde $\nu := (\nu_1, \ldots, \nu_n)$ y $\mathtt{x}^\nu := \mathtt{x}_1^{\nu_1} \cdots \mathtt{x}_n^{\nu_n}$, y denotamos $\mathtt{q} := \widetilde{\sigma}(\mathtt{p})$. Resulta así

$$\mathtt{q}(\mathtt{x}) = \sum_\nu a_\nu \mathtt{x}_{\sigma(1)}^{\nu_1} \cdots \mathtt{x}_{\sigma(n)}^{\nu_n} \quad \Longrightarrow \quad \mathtt{q}(\alpha) = \sum_\nu a_\nu \alpha_{\sigma(1)}^{\nu_1} \cdots \alpha_{\sigma(n)}^{\nu_n},$$

y por otro lado

$$\sigma(\mathtt{p}(\alpha)) = \sigma\Big(\sum_{\nu} a_\nu \alpha_1^{\nu_1}\cdots\alpha_n^{\nu_n}\Big) = \sum_{\nu} a_\nu \sigma(\alpha_1)^{\nu_1}\cdots\sigma(\alpha_n)^{\nu_n}$$
$$= \sum_{\nu} a_\nu \alpha_{\sigma(1)}^{\nu_1}\cdots\alpha_{\sigma(n)}^{\nu_n} = \mathtt{q}(\alpha) = \widetilde{\sigma}(\mathtt{p})(\alpha).$$

(3) Debemos justificar que $R_{f,\mathtt{p}}$ pertenece a $K[\mathtt{t}]$. Nótese que cada $\mathtt{q}(\alpha) \in L_f$, por lo que $R_{f,\mathtt{p}} \in L_f[\mathtt{t}]$. Como $K = \mathrm{Fix}(G_K(f))$ y los coeficientes de $R_{f,\mathtt{p}}$ son las formas simétricas elementales evaluadas en los elementos del conjunto $Q := \{\mathtt{q}(\alpha),\, \mathtt{q} \in O_{\mathtt{p}}\}$, basta probar que $\sigma(Q) = Q$ para cada $\sigma \in G_K(f)$.

Es suficiente comprobar que $\sigma(Q) \subset Q$ pues aplicando esto para la permutación σ^{-1} se tiene $\sigma^{-1}(Q) \subset Q$, luego

$$Q = \sigma(\sigma^{-1}(Q)) \subset \sigma(Q) \subset Q.$$

Pero dado $\mathtt{q} \in O_{\mathtt{p}}$ y $\mathtt{q}(\alpha) \in Q$ se tiene $\widetilde{\sigma}(\mathtt{q}) = \mathtt{q}_1 \in O_p$ y, por el apartado (2),

$$\sigma(\mathtt{q}(\alpha)) = \widetilde{\sigma}(\mathtt{q})(\alpha) = \mathtt{q}_1(\alpha) \in Q.$$

(3.1) Cada raíz $\mathtt{q}(\alpha)$ de $R_{f,\mathtt{p}}$ pertenece a $L_f = K(\alpha_1,\ldots,\alpha_n)$, puesto que $\mathtt{q} \in O_{\mathtt{p}} \subset K[\mathtt{x}_1,\ldots,\mathtt{x}_n]$.

(3.2) Para cada $\sigma \in \mathcal{S}_n$ se tiene $\mathrm{Stab}_{G_K(f)}(\widetilde{\sigma}(\mathtt{p})) \subset G(L_f : K(\widetilde{\sigma}(\mathtt{p})(\alpha)))$.

En efecto, cada $\tau \in \mathrm{Stab}_{G_K(f)}(\widetilde{\sigma}(\mathtt{p}))$ es un K-automorfismo de L_f y se cumple $\widetilde{\tau}(\widetilde{\sigma}(\mathtt{p})) = \widetilde{\sigma}(\mathtt{p})$. Entonces, $\tau \in G(L_f : K(\widetilde{\sigma}(\mathtt{p})(\alpha)))$, porque

$$\tau(\widetilde{\sigma}(\mathtt{p})(\alpha)) = \widetilde{\tau}(\widetilde{\sigma}(\mathtt{p})(\alpha) = \widetilde{\sigma\tau}(\mathtt{p})(\alpha) = \widetilde{\sigma}\widetilde{\tau}(\mathtt{p})(\alpha) = \widetilde{\tau}(\widetilde{\sigma}(\mathtt{p}))(\alpha) = \widetilde{\sigma}(\mathtt{p})(\alpha).$$

(3.3) Si $\sigma \in \mathcal{S}_n$ y $\sigma G_K(f)\sigma^{-1} \subset \mathrm{Stab}_{\mathcal{S}_n}(\mathtt{p})$, entonces $\widetilde{\sigma}(\mathtt{p})(\alpha) \in K$. En efecto, empleando la igualdad (2.8) en VI.2.3 y la hipótesis resulta

$$G_K(f) \subset \sigma^{-1}\,\mathrm{Stab}_{\mathcal{S}_n}(\mathtt{p})\sigma = \mathrm{Stab}_{\mathcal{S}_n}(\widetilde{\sigma}(\mathtt{p})).$$

Se tiene entonces, utilizando la inclusión (3.2) que acabamos de probar,

$$G(L_f : K) = G_K(f) = G_K(f) \cap \mathrm{Stab}_{\mathcal{S}_n}(\widetilde{\sigma}(\mathtt{p}))$$
$$= \mathrm{Stab}_{G_K(f)}(\widetilde{\sigma}(\mathtt{p})) \subset G(L_f : K(\widetilde{\sigma}(\mathtt{p})(\alpha))) \subset G(L_f : K),$$

y por tanto $G(L_f : K) = G(L_f : K(\widetilde{\sigma}(\mathtt{p})(\alpha)))$. Como $L_f|K$ es una extensión de Galois se deduce que $\widetilde{\sigma}(\mathtt{p})(\alpha) \in K$ pues, por el Teorema fundamental,

$$K(\widetilde{\sigma}(\mathtt{p})(\alpha)) = \mathrm{Fix}(G(L_f : K(\widetilde{\sigma}(\mathtt{p})(\alpha)))) = \mathrm{Fix}(G(L_f : K)) = K.$$

(3.4) Si $\sigma \in \mathcal{S}_n$ es una permutación tal que $\widetilde{\sigma}(\mathtt{p})(\alpha) \in K$ y es raíz simple de $R_{f,\mathtt{p}}$ se tiene $\sigma G_K(f)\sigma^{-1} \subset \mathrm{Stab}_{\mathcal{S}_n}(\mathtt{p})$.

En efecto, suponemos, por reducción al absurdo, que $\sigma G_K(f)\sigma^{-1}$ no está contenido en $\mathrm{Stab}_{\mathcal{S}_n}(\mathtt{p})$, es decir, existe $\tau \in G_K(f)$ tal que $\sigma\tau\sigma^{-1} \notin \mathrm{Stab}_{\mathcal{S}_n}(\mathtt{p})$. Esto significa, por la igualdad (2.8) en VI.2.3, que

$$\tau \notin \sigma^{-1}\,\mathrm{Stab}_{\mathcal{S}_n}(\mathtt{p})\sigma = \mathrm{Stab}_{\mathcal{S}_n}(\widetilde{\sigma}(\mathtt{p})),$$

luego tanto $\mathtt{q}_1 := \widetilde{\sigma}(\mathtt{p})$ como $\mathtt{q}_2 := \widetilde{\tau}(\widetilde{\sigma}(\mathtt{p})) = \widetilde{\tau}(\mathtt{q}_1)$ pertenecen a la órbita $O_{\mathtt{p}}$ y son distintos. De la definición de resolvente de Galois (2.10) se deduce que

$$R_{f,\mathtt{p}}(\mathtt{t}) = \prod_{\mathtt{q}\in O_{\mathtt{p}}} (\mathtt{t}-\mathtt{q}(\alpha)) = (\mathtt{t}-\mathtt{q}_1(\alpha))(\mathtt{t}-\mathtt{q}_2(\alpha))\cdot \prod_{\mathtt{q}\in O_{\mathtt{p}}\setminus\{\mathtt{q}_1,\mathtt{q}_2\}} (\mathtt{t}-\mathtt{q}(\alpha)). \quad (4.26)$$

Por el apartado (2) se tiene $\mathtt{q}_1(\alpha) = \widetilde{\sigma}(\mathtt{p})(\alpha) \in K$, luego $\tau(\mathtt{q}_1(\alpha)) = \mathtt{q}_1(\alpha)$, pues $\tau \in G_K(f)$. Así, de nuevo por el apartado (2),

$$\mathtt{q}_2(\alpha) = \widetilde{\tau}(\mathtt{q}_1)(\alpha) = \tau(\mathtt{q}_1(\alpha)) = \mathtt{q}_1(\alpha),$$

lo que por la igualdad (4.26) implica que la multiplicidad de $\mathtt{q}_1(\alpha)$ como raíz de $R_{f,\mathtt{p}}$ es al menos 2, contra la hipótesis. □

Ejercicios y problemas propuestos

Número VI.1 Sean m y n enteros positivos primos entre sí y ζ_m, $\zeta_n \in \mathbb{C}$ raíces primitivas m-ésima y n-ésima de la unidad, respectivamente. Probar la igualdad $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

Número VI.2 (1) Hallar el polinomio ciclotómico Φ_9 y su grupo de Galois $G_{\mathbb{Q}}(\Phi_9)$.

(2) Sea $L \subset \mathbb{C}$ un cuerpo de descomposición de Φ_9 sobre $\mathbb{Q}$. Expresar como extensiones simples las subextensiones de $L|\mathbb{Q}$ y en cada caso encontrar el polinomio mínimo sobre $\mathbb{Q}$ de un elemento primitivo.

Número VI.3 Sean n y k dos números enteros positivos tales que, o bien n es impar o bien tanto n como k son pares. Utilizar, si se desea, el Teorema del número primo de Dirichlet para demostrar que existen números enteros u, v tales que

$$\mathrm{mcd}(u,n) = \mathrm{mcd}(v,n) = 1 \quad \& \quad k = u + v.$$

Número VI.4 ¿Es finito el conjunto formado por los números primos p para los que existe algún entero n tal que $p|(n^2+1)$?

Número VI.5 (1) Probar que un primo impar $p \equiv \pm 1 \bmod 5$ si y sólo si 5 es un resto cuadrático $\bmod p$.

(2) Sea p un primo impar. Probar que alguno de los números 2, 5 y 10 es un resto cuadrático $\bmod p$.

(3) Demostrar que existen infinitos números primos impares p tales que 2, 5 y 10 son restos cuadráticos $\bmod p$ y encontrar uno de ellos.

Número VI.6 Sea $L_f \subset \mathbb{C}$ un cuerpo de descomposición sobre $\mathbb{Q}$ de un polinomio irreducible $f \in \mathbb{Q}[\mathtt{t}]$. Probar que si $[L_f : \mathbb{Q}]$ es impar entonces $L_f \subset \mathbb{R}$.

Número VI.7 Sean K un cuerpo de característica 0 y $f \in K[\mathtt{t}]$ un polinomio irreducible cuyo grupo de Galois $G_K(f)$ es cíclico. Probar que el discriminante $\Delta(f)$ es el cuadrado de un elemento de K si y sólo si el orden de $G_K(f)$ es impar.

Número VI.8 Sean K un cuerpo de característica 0 y $f \in K[\mathtt{t}]$ un polinomio irreducible de grado 3. Sea L_f un cuerpo de descomposición de f sobre K. ¿Qué se puede decir acerca del número de extensiones $L_f|E$ de grado 2, donde $K \subset E \subset L_f$?

Número VI.9 Sean u, v y w las raíces en $\mathbb{C}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^3 - 3\mathtt{t} + 1$. Sean $a := u^2v^2$, $b := u^2w^2$ y $c := v^2w^2$.

(1) Hallar los coeficientes de $g(\mathtt{t}) := (\mathtt{t} - a)(\mathtt{t} - b)(\mathtt{t} - c)$. ¿Es g irreducible en $\mathbb{Q}[\mathtt{t}]$?

(2) Calcular el discriminante de g y el grupo de Galois $G_{\mathbb{Q}}(g)$.

Número VI.10 Calcular la resolvente cúbica g de $f(\mathtt{t}) := \mathtt{t}^4 - 2\mathtt{t}^2 - 1$ y el grupo de Galois $G_{\mathbb{Q}}(g)$.

Número VI.11 Sean K un cuerpo de característica 0 y para cada $s \in K$ consideramos el polinomio

$$f_s(\mathtt{t}) := \mathtt{t}^3 - s\mathtt{t}^2 + (s-3)\mathtt{t} + 1 \in K[\mathtt{t}].$$

(1) Probar que f_s es reducible en $K[\mathtt{t}]$ si y sólo si existe $u \in K$ tal que $u^3 - 3u + 1 = su(u-1)$.

(2) Calcular el discriminante $\Delta(f_s)$ de f_s y demostrar que es el cuadrado de un elemento de K. Deducir que f_s tiene alguna raíz múltiple en un cierre algebraico $\overline{K}$ de K si y sólo si $s^2 - 3s + 9 = 0$, y que en tal caso $f_s(\mathtt{t}) = (\mathtt{t} - s/3)^3$.

(3) Sea $s \in K$ tal que f_s es irreducible en $K[\mathtt{t}]$. Calcular el grupo de Galois $G_K(f_s)$ y demostrar que si α es una raíz de f_s en $\overline{K}$, las otras dos raíces de f_s en $\overline{K}$ se pueden expresar como cocientes de expresiones polinómicas en α cuyos coeficientes no dependen de s.

(4) Sea $L|K$ una extensión de Galois de grado 3. Demostrar que existen $\alpha \in L$ y $s \in K$ tales que $L = K(\alpha)$ y el polinomio mínimo de α sobre K es

$$P_{K,\alpha}(\mathtt{t}) := f_s(\mathtt{t}) = \mathtt{t}^3 - s\mathtt{t}^2 + (s-3)\mathtt{t} + 1.$$

Número VI.12 Encontrar polinomios $f \in \mathbb{Q}[\mathtt{t}]$ de grado 3 cuyo grupo de Galois $G_{\mathbb{Q}}(f)$ coincida con los que aparecen en la tabla de la Proposición VI.3.2.

Número VI.13 Encontrar una extensión $K|\mathbb{Q}$ de grado 2 y un polinomio $f \in \mathbb{Q}[\mathtt{t}]$ de grado 3 tales que f es irreducible en $K[\mathtt{t}]$ y los grupos de Galois $G_{\mathbb{Q}}(f)$ y $G_K(f)$ no sean isomorfos.

Número VI.14 Sean p un número primo y supongamos que el grupo de Galois $G_{\mathbb{Q}}(f)$ es cíclico, donde $f(\mathtt{t}) := \mathtt{t}^3 - p\mathtt{t} + p$. Demostrar que $p \equiv 1 \bmod 3$.

Número VI.15 Sean K un cuerpo de característica 0 y $f \in K[\mathtt{t}]$ un polinomio de grado 4 cuyo grupo de Galois $G_K(f)$ es el grupo alternado $\mathcal{A}_4$. ¿Cuál es el grupo de Galois sobre K de la resolvente cúbica g del polinomio f?

Número VI.16 Sean $K \subset \mathbb{R}$ un cuerpo y $f \in K[\mathtt{t}]$ un polinomio irreducible de grado 4 que tiene, exactamente, dos raíces reales. Probar que su grupo de Galois $G_K(f)$ es $\mathcal{D}_4$ o $\mathcal{S}_4$.

Número VI.17 Sean $p > 5$ un número primo y $f_p(\mathtt{t}) := \mathtt{t}^4 + p\mathtt{t} + p \in \mathbb{Q}[\mathtt{t}]$. Determinar el grupo de Galois $G_{\mathbb{Q}}(f_p)$.

Número VI.18 Sean K un cuerpo de característica 0 y $E|K$ una extensión de grado 4. Demostrar que las siguientes afirmaciones son equivalentes:

(1) $E|K$ es de Galois y $G(E:K) = \mathbb{Z}_4$.

(2) Existen un elemento primitivo α de la extensión $E|K$ y $a \in K^* := K \setminus \{0\}$, $s, u \in K$ tales que el polinomio mínimo de α sobre K adopta una de las siguientes formas:

$$P_{K,\alpha}(\mathtt{t}) = \mathtt{t}^4 - 4u(4s^2+1)\mathtt{t}^2 + 4u^2(4s^2+1), \text{ o bien } P_{K,\alpha}(\mathtt{t}) = \mathtt{t}^4 - a,$$

la segunda tan sólo en el caso en que -1 es un cuadrado en K.

Número VI.19 Sea $E|K$ una extensión de cuerpos de grado 4. Demostrar que las siguientes afirmaciones son equivalentes:

(1) $E|K$ es de Galois y $G(E:K) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

(2) Existen un elemento primitivo α de la extensión $E|K$ y $s, u \in K$ tales que

$$P_{K,\alpha}(\mathtt{t}) = \mathtt{t}^4 - 2(s+u)\mathtt{t}^2 + (s-u)^2.$$

Número VI.20 Calcular el grupo de Galois $G_{\mathbb{Q}}(f_i)$ para $i = 1, 2$, donde

$$f_1(\mathtt{t}) := \mathtt{t}^4 + 3\mathtt{t}^3 - 3\mathtt{t} - 2 \quad \& \quad f_2(\mathtt{t}) := \mathtt{t}^4 + \mathtt{t}^2 - 2\mathtt{t} + 1.$$

Número VI.21 Encontrar polinomios irreducibles $f \in \mathbb{Q}[\mathtt{t}]$ de grado 4 cuyo grupo de Galois $G_{\mathbb{Q}}(f)$ coincida con los que aparecen en la tabla de la Proposición VI.3.3.

Número VI.22 Sean K un cuerpo de característica 0 y $a, b \in K$ tales que el polinomio $f(\mathtt{t}) := \mathtt{t}^4 + a\mathtt{t}^2 + b$ es irreducible en $K[\mathtt{t}]$. Hallar, en función de los valores de a y b, el grupo de Galois de f sobre K.

Número VI.23 Sean $f_1(\mathtt{t}) := \mathtt{t}^4 - 2\mathtt{t}^2 + 2$, $f_2(\mathtt{t}) := \mathtt{t}^3 + 9\mathtt{t} + 18$, L_i el cuerpo de descomposición de f_i sobre $\mathbb{Q}$ y L el menor subcuerpo de $\mathbb{C}$ que contiene a L_1 y L_2.

(1) Probar que el grupo de Galois $G_{\mathbb{Q}}(f_1)$ es isomorfo al grupo diedral $\mathcal{D}_4$ de orden 8.

(2) Sean v y w dos raíces de f_1 en L_1 que no son opuestas. Calcular el polinomio mínimo de w sobre $\mathbb{Q}(v)$.

(3) Probar que f_2 tiene tres raíces distintas u_1, u_2 y u_3 en L_2, que el grupo de Galois $G_{\mathbb{Q}}(f_2) \cong \mathcal{S}_3$ y que $G_{L_1}(f_2)$ es isomorfo a $\mathbb{Z}_3$.

(4) Demostrar que $[L : \mathbb{Q}] = 24$.

(5) Probar que $L_1|\mathbb{Q}$ es la única subextensión de $L|\mathbb{Q}$ de grado 8.

(6) Demostrar que $\mathbb{Q}(u_i)|\mathbb{Q}$, con $i = 1, 2, 3$ son todas las subextensiones de grado 3 de la extensión $L|\mathbb{Q}$.

(7) Demostrar que existe un único automorfismo $\rho \in G(L : \mathbb{Q})$ tal que $\rho(v) = w$, $\rho(w) = -v$ y $\rho(u_1) = u_2$. Calcular el grado $[F : \mathbb{Q}]$, donde $F = \mathrm{Fix}(\rho)$ es el cuerpo fijo de ρ.

(8) Hallar un elemento primitivo θ de la extensión $F|\mathbb{Q}$ y el polinomio mínimo de θ sobre $\mathbb{Q}$.

Número VI.24 (1) Hallar un polinomio irreducible $f \in \mathbb{Q}[\mathtt{t}]$ de grado 4 tal que $G_{\mathbb{Q}}(f) = \mathcal{D}_4$ mientras que $G_{\mathbb{Q}(i)}(f) = \mathbb{Z}_2 \times \mathbb{Z}_2$, donde $i := \sqrt{-1}$.

(2) Encontrar un polinomio irreducible $f \in \mathbb{Q}[\mathtt{t}]$ de grado 4 cuyo grupo de Galois sobre $\mathbb{Q}$ sea el grupo cíclico $\mathbb{Z}_4$ mientras que $G_{\mathbb{Q}(\sqrt{2})}(f) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Número VI.25 Sean $K := \mathbb{Q}(\sqrt{-3})$ y $f(\mathtt{t}) := (\mathtt{t}^3 - 2)(\mathtt{t}^2 - 5)$. Hallar el grupo de Galois $G_K(f)$.

Número VI.26 Sean p un número primo, $f(\mathtt{t}) := \mathtt{t}^5 - p$ y $L_f \subset \mathbb{C}$ un cuerpo de descomposición de f sobre el cuerpo $\mathbb{Q}$ de los números racionales.

(1) Determinar el grupo de Galois $G_{\mathbb{Q}}(f)$ de f sobre $\mathbb{Q}$.

(2) ¿Contiene $G_{\mathbb{Q}}(f)$ alguna transposición visto como subgrupo de $\mathcal{S}_5$?

(3) ¿Es abeliano el grupo $G_{\mathbb{Q}}(f)$?

(4) Calcular, para cada divisor n del orden del grupo $G_{\mathbb{Q}}(f)$, el número de elementos de orden n.

(5) Encontrar un elemento primitivo de cada subextensión propia de Galois de $L_f|\mathbb{Q}$.

Número VI.27 Denotemos $\mathtt{x} := (\mathtt{x}_1, \mathtt{x}_2, \mathtt{x}_3, \mathtt{x}_4, \mathtt{x}_5)$ y consideremos el polinomio

$$\mathtt{q}(\mathtt{x}) := \mathtt{x}_1\mathtt{x}_2 + \mathtt{x}_2\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_1 - \mathtt{x}_1\mathtt{x}_3 - \mathtt{x}_3\mathtt{x}_5 - \mathtt{x}_5\mathtt{x}_2 - \mathtt{x}_2\mathtt{x}_4 - \mathtt{x}_4\mathtt{x}_1.$$

Calcular el estabilizador $\mathrm{Stab}_{\mathcal{S}_5}(\mathtt{q})$ para la acción de $\mathcal{S}_5$ sobre $K[\mathtt{x}]$ introducida en VI.2.3.

Número VI.28 Hallar el grupo de Galois de $f(\mathtt{t}) := \mathtt{t}^5 - 2$ sobre $K := \mathbb{Q}(\sqrt{5})$.

Número VI.29 Sean $a, b \in \mathbb{Q}$ tales que $f(\mathtt{t}) := \mathtt{t}^5 + a\mathtt{t}^3 + (a^2/5)\mathtt{t} + b$ es irreducible en $\mathbb{Q}[\mathtt{t}]$. Calcular el grupo de Galois de f sobre $\mathbb{Q}$.

Número VI.30 Sean K un cuerpo de característica cero, $K_1|K$ una extensión de Galois y $f \in K[\mathtt{t}]$.

(1) Demostrar que el grupo de Galois $G_{K_1}(f)$ de f sobre el cuerpo K_1 es isomorfo a un subgrupo normal H del grupo de Galois $G_K(f)$ de f sobre K.

(2) Probar que el cociente $G_K(f)/H$ es isomorfo a un cociente del grupo $G(K_1 : K)$.

CAPÍTULO VII

Aplicaciones de la teoría de Galois

En la primera sección de este capítulo estudiamos la resolubilidad mediante radicales de ecuaciones polinómicas. En la sección segunda abordamos algunos problemas sobre constructibilidad con regla y compás; en particular, para probar que es imposible la cuadratura del círculo emplearemos la transcendencia de π, que se demuestra en el Apéndice B. Por simplicidad fijamos a lo largo del capítulo un cuerpo K de característica 0 y un cierre algebraico suyo $\overline{K}$.

1. Resolubilidad por radicales

El objetivo principal de esta sección es enunciar y demostrar el Teorema de Abel-Galois que permite decidir qué ecuaciones polinómicas en una variable son *resolubles por radicales* sobre un cuerpo dado y demostrar que la ecuación polinómica general de grado n es resoluble por radicales si y sólo si $n \leq 4$. Este teorema afirma lo siguiente.

Teorema VII.1.1 (Galois) *Un polinomio $f \in K[\mathtt{t}]$ de grado ≥ 1 es resoluble por radicales si y sólo si el grupo de Galois $G_K(f)$ de f sobre K es resoluble.*

Formalizamos a continuación el significado de la resolubilidad por radicales de un polinomio y desarrollamos los preliminares necesarios para demostrar el teorema anterior.

Definiciones y Observaciones VII.1.2 (1) Una extensión $E|K$ se dice *radical* si existen $\alpha_1, \ldots, \alpha_n \in \overline{K}$ tales que $E = K(\alpha_1, \ldots, \alpha_n)$, α_1 es raíz de un polinomio de la forma $\mathtt{t}^{\ell_1} - a_1 \in K[\mathtt{t}]$ y α_i es, para $2 \leq i \leq n$, raíz de un polinomio del tipo $\mathtt{t}^{\ell_i} - a_i \in K(\alpha_1, \ldots, \alpha_{i-1})[\mathtt{t}]$.

(2) En la definición anterior se puede suponer que los exponentes ℓ_i son primos. En efecto, si $\ell_1 = p_1 m_1$ donde p_1 es primo y $m_1 > 1$ denotamos $\beta_1 := \alpha_1^{m_1}$, que

es raíz del polinomio $\mathtt{t}^{p_1} - a_1$ y cumple que α_1 es raíz de $\mathtt{t}^{m_1} - \beta_1 \in K(\alpha_1)[\mathtt{t}]$ y $E = K(\beta_1, \alpha_1, \ldots, \alpha_n)$. Como $m_1 < \ell_1$, basta continuar el proceso.

(3) Una extensión $L|K$ es *quasiradical* si es subextensión de una extensión radical $E|K$. Se desprende directamente de la definición que toda subextensión $F|K$ de una extensión quasiradical es también quasiradical.

(4) Existen extensiones quasiradicales que no son radicales. Por ejemplo, si denotamos $\zeta := e^{2\pi i/7}$ y $E = \mathbb{Q}(\zeta)$, la extensión $E|\mathbb{Q}$ es radical porque ζ es raíz del polinomio $\mathtt{t}^7 - 1$. Sea $\alpha := \zeta + 1/\zeta \in E \cap \mathbb{R}$, cuyo polinomio mínimo sobre $\mathbb{Q}$ es $f(\mathtt{t}) := \mathtt{t}^3 + \mathtt{t}^2/2 - \mathtt{t}/2 - 1/8$. Como las raíces de este polinomio no son expresables mediante radicales *reales,* la extensión $\mathbb{Q}(\alpha)|\mathbb{Q}$ no es radical. Sin embargo es quasiradical porque $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta)$.

(5) Si las extensiones $F|K$ y $E|F$ son radicales, entonces también la extensión $E|K$ es radical.

En efecto, existen $\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n \in \overline{K}$ tales que

$$F = K(\alpha_1, \ldots, \alpha_m) \quad \& \quad E = F(\alpha_{m+1}, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n),$$

de modo que α_1 es raíz de un polinomio $\mathtt{t}^{\ell_1} - a_1 \in K[\mathtt{t}]$, para $2 \leq i \leq m$ existe $a_i \in K(\alpha_1, \ldots, \alpha_{i-1})$ tal que α_i es raíz de un polinomio de la forma $\mathtt{t}^{\ell_i} - a_i$, α_{m+1} es raíz de un polinomio $\mathtt{t}^{\ell_{m+1}} - a_{m+1} \in F[\mathtt{t}] = K(\alpha_1, \ldots, \alpha_m)[\mathtt{t}]$, y para $2 \leq j \leq n - m$, α_{m+j} es raíz de un polinomio de la forma

$$\mathtt{t}^{\ell_{m+j}} - a_{m+j} \in F(\alpha_{m+1}, \ldots, \alpha_{m+j-1})[\mathtt{t}] = K(\alpha_1, \ldots, \alpha_{m+j-1})[\mathtt{t}].$$

Esto demuestra que la extensión $E|K$ es radical.

(6) Si las extensiones $F|K$ y $L|F$ son quasiradicales, entonces también la extensión $L|K$ es quasiradical.

En efecto, sean $E_1|K$ y $E|F$ extensiones radicales tales que $F|K$ es subextensión de $E_1|K$ y $L|F$ lo es de $E|F$. En particular existen $\beta_1, \ldots, \beta_n \in \overline{K}$ tales que $E := F(\beta_1, \ldots, \beta_n)$, de modo que β_1 es raíz de $\mathtt{t}^{\ell_1} - b_1 \in F[\mathtt{t}]$ y, para $2 \leq i \leq n$, β_i es raíz de un polinomio de la forma $\mathtt{t}^{\ell_i} - b_i \in F(\beta_1, \ldots, \beta_{i-1})[\mathtt{t}]$.

Como la extensión $E_1|K$ es radical, existen $\alpha_1, \ldots, \alpha_m \in \overline{K}$ tales que α_1 es raíz de un polinomio de la forma $\mathtt{t}^{r_1} - a_1 \in K[\mathtt{t}]$, para $2 \leq i \leq m$, α_i es raíz de un polinomio de la forma $\mathtt{t}^{r_i} - a_i \in K(\alpha_1, \ldots, \alpha_{i-1})[\mathtt{t}]$ y $E_1 = K(\alpha_1, \ldots, \alpha_m)$. En consecuencia,

$$L \subset E = F(\beta_1, \ldots, \beta_n) \subset E_1(\beta_1, \ldots, \beta_n) = K(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n) := E_2,$$

luego $L|K$ es subextensión de la extensión radical $E_2|K$, por lo que es quasiradical.

Definición y Observación VII.1.3 (1) Sea $f \in K[\mathtt{t}]$ un polinomio de grado ≥ 1 y consideremos un cuerpo de descomposición $L_f \subset \overline{K}$ de f sobre K. Se dice que f es *resoluble por radicales sobre* K si la extensión $L_f|K$ es quasiradical, es decir, si todas las raíces de f en $\overline{K}$ se obtienen mediante expresiones que involucran una cantidad finita de elementos de K y las operaciones $+$, $-$, $\cdot$, $/$ y $\sqrt[\ell]{\cdot}$ para ciertos enteros positivos $\ell \geq 2$.

(2) El polinomio $f(\mathtt{t}) := \mathtt{t}^6 - 6\mathtt{t}^3 + 7$ es resoluble por radicales sobre $\mathbb{Q}$. En efecto, si $t \in \mathbb{C}$ es raíz de f, su cubo $x := t^3$ es raíz del polinomio de segundo grado $g(\mathtt{t}) := \mathtt{t}^2 - 6\mathtt{t} + 7 \in \mathbb{Q}[\mathtt{t}]$. En consecuencia, $x = x_1 := 3 + \sqrt{2}$ o $x = x_2 := 3 - \sqrt{2}$. Informalmente, esto implica que las raíces de f en un cierre algebraico $\overline{\mathbb{Q}} \subset \mathbb{C}$ de $\mathbb{Q}$ son $\sqrt[3]{3 \pm \sqrt{2}}$, donde el símbolo $\sqrt[3]{\cdot}$ denota las tres raíces cúbicas complejas de todo número complejo no nulo. Por tanto, el polinomio f es resoluble por radicales sobre $\mathbb{Q}$.

Más formalmente, hemos de probar que si $L_f \subset \mathbb{C}$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$, la extensión $L_f|\mathbb{Q}$ es quasiradical. Sea $\zeta := e^{2\pi i/3}$, que es una raíz primitiva cúbica de la unidad. Entonces, si r_1 y r_2 son las raíces cúbicas reales de x_1 y x_2 se tiene

$$L_f = \mathbb{Q}(r_1, r_1\zeta, r_1\zeta^2, r_2, r_2\zeta, r_2\zeta^2) = \mathbb{Q}(r_1, r_2, \zeta).$$

Nótese que $\alpha_1 := \sqrt{2}$ es raíz del polinomio $\mathtt{t}^2 - 2 \in \mathbb{Q}[\mathtt{t}]$, mientras que $\alpha_2 := \zeta$ es raíz de $\mathtt{t}^3 - 1 \in \mathbb{Q}[\mathtt{t}] \subset \mathbb{Q}(\alpha_1)[\mathtt{t}]$. Además, $\alpha_3 := r_1$ y $\alpha_4 := r_2$ son raíces, respectivamente, de los polinomios

$$\mathtt{t}^3 - (3 + \alpha_1) \in \mathbb{Q}(\alpha_1, \alpha_2)[\mathtt{t}] \quad \& \quad \mathtt{t}^3 - (3 - \alpha_1) \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)[\mathtt{t}].$$

Por tanto $L_f|\mathbb{Q}$ es subextensión de la extensión radical $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)|\mathbb{Q}$, por lo que $L_f|\mathbb{Q}$ es una extensión quasiradical.

(3) El resultado fundamental de este capítulo se debe a Galois y relaciona la resolubilidad por radicales sobre K de un polinomio $f \in K[\mathtt{t}]$ con la resolubilidad del grupo de Galois $G_K(f)$. Para la noción de grupo resoluble y algunas propiedades básicas, véase §2 del Capítulo V, vol. I. Veamos antes un lema acerca de extensiones radicales.

Lema VII.1.4 *La clausura de Galois $F|K$ de una extensión quasiradical $L|K$ es también una extensión quasiradical. Además, si $L|K$ es radical también $F|K$ lo es.*

Demostración. Probaremos, simultáneamente, ambas partes del enunciado. Si $L|K$ es quasiradical existen $\alpha_1, \ldots, \alpha_n \in \overline{K}$ tales que α_1 es raíz de un polinomio

del tipo $\mathtt{t}^{\ell_1} - a_1 \in K[\mathtt{t}]$ y, para $2 \leq i \leq n$, α_i es raíz de un polinomio de la forma $\mathtt{t}^{\ell_i} - a_i \in K(\alpha_1, \ldots, \alpha_{i-1})[\mathtt{t}]$ de modo que $L \subset E_0 := K(\alpha_1, \ldots, \alpha_n)$.

Para $1 \leq i \leq n$ sea $f_i := P_{K,\alpha_i}$ y $f := \prod_{i=1}^n f_i \in K[\mathtt{t}]$. Denotamos E_1 un cuerpo de descomposición de f sobre K. La extensión $E_1|K$ es de Galois, por IV.1.6, y como $L \subset E_0 \subset E_1$ y $F|K$ es la clausura de Galois de $L|K$, se deduce que $F \subset E_1$. Además, si la extensión $L|K$ es radical entonces $L = E_0$, y por tanto $F = E_1$. Por esto basta probar que la extensión $E_1|K$ es radical.

Como $\mathrm{char}(K) = 0$ y f_i es irreducible en $K[\mathtt{t}]$, tiene en su cuerpo de descomposición tantas raíces como grado. Denotamos $d_i := \deg(f_i)$ y sean $\beta_{i1} := \alpha_i, \beta_{i2}, \ldots, \beta_{id_i}$ las raíces de f_i en E_1. Se cumple que

$$E_1 = K(\beta_{ij} : \ 1 \leq i \leq n, \ 1 \leq j \leq d_i),$$

y todo se reduce a probar que cada β_{ij} es raíz de un polinomio del tipo

$$\mathtt{t}^{\ell_i} - a_{ij} \in K(\beta_{kj} : \ 1 \leq k \leq i-1, \ 1 \leq j \leq d_k)[\mathtt{t}].$$

Como α_i y β_{ij} son raíces del mismo polinomio irreducible $f_i \in K[\mathtt{t}]$ existe, por el Lema II.1.1, un K-isomorfismo $\phi : K(\alpha_i) \to K(\beta_{ij})$ tal que $\phi(\alpha_i) = \beta_{ij}$. Como E_1 es un cuerpo de descomposición del polinomio f sobre K, entonces $E_1(\alpha_i) = E_1 = E_1(\beta_{ij})$ son cuerpos de descomposición de f sobre $K(\alpha_i)$ y $K(\beta_{ij})$, respectivamente. En virtud del Teorema II.1.2, existe un isomorfismo

$$\Phi : E_1 = E_1(\alpha_i) \to E_1 = E_1(\beta_{ij})$$

tal que $\Phi|K(\alpha_i) = \phi$. Nótese que para $1 \leq k \leq i-1$ la restricción

$$\Phi|_{K(\alpha_k)} : K(\alpha_k) \to K(\Phi(\alpha_k))$$

es un K-isomorfismo. Por tanto, aplicando de nuevo el Lema II.1.1, $\Phi(\alpha_k)$ es una de las raíces β_{kj_k} del polinomio $f_k \in K[\mathtt{t}]$. Por otro lado, aplicando Φ a los dos miembros de la igualdad $\alpha_i^{\ell_i} = a_i$ deducimos que $\beta_{ij}^{\ell_i} - \Phi(a_i) = 0$.

Ahora bien, Φ es un K-automorfismo, $a_i \in K(\alpha_1, \ldots, \alpha_{i-1})$, y $\Phi(\alpha_k) = \beta_{kj_k}$ para $1 \leq k \leq n$, de lo que se deduce que

$$\Phi(a_i) \in K(\beta_{1j_1}, \ldots, \beta_{i-1,j_{i-1}}) \subset K(\beta_{kj} : \ 1 \leq k \leq i-1, \ 1 \leq j \leq d_k).$$

De este modo, concluimos que cada β_{ij} es raíz de un polinomio del tipo

$$\mathtt{t}^{\ell_i} - a_{ij} \in K(\beta_{kj} : 1 \leq k \leq i-1, \ 1 \leq j \leq d_k)[\mathtt{t}].$$

□

Ya podemos demostrar *la mitad* del Teorema de Galois VII.1.1.

Proposición VII.1.5 (Galois) *Sea $f \in K[\mathtt{t}]$ un polinomio resoluble por radicales de grado ≥ 1. Entonces, el grupo $G_K(f)$ es resoluble.*

Demostración. Sea $L_f \subset \overline{K}$ un cuerpo de descomposición de f sobre K. Como f es resoluble por radicales sobre K, la extensión $L_f|K$ es quasiradical, luego es subextensión de una extensión radical $E_0|K$. Por el Lema VII.1.4 la clausura de Galois $E_1|K$ de $E_0|K$ es también una extensión radical. Nótese que $L_f|K$ es una subextensión de Galois de la extensión de Galois $E_1|K$, y se deduce de la segunda parte del Teorema fundamental de la teoría de Galois que el grupo de Galois $G(E_1 : L_f)$ es subgrupo normal de $G(E_1 : K)$ y

$$G_K(f) = G(L_f : K) \cong G(E_1 : K)/G(E_1 : L_f).$$

En virtud de la Proposición V.2.3, vol. I, para demostrar que $G_K(f)$ es resoluble es suficiente probar que el grupo $G(E_1 : K)$ es resoluble.

Como la extensión $E_1|K$ es radical, $E_1 := K(\alpha_1, \ldots, \alpha_n)$ para ciertos $\alpha_1, \ldots, \alpha_n \in \overline{K}$, y existen $a_1 \in K$ y $a_2, \ldots, a_n \in \overline{K}$, con $a_i \in K(\alpha_1, \ldots, \alpha_{i-1})$, de modo que α_i es raíz de un polinomio del tipo $\mathtt{t}^{p_i} - a_i$ para $1 \leq i \leq n$ donde, en virtud de la Observación VII.1.2, podemos suponer que p_i es un número primo. En particular, $\alpha_1^{p_1} = a_1 \in K$.

Vamos a probar por inducción sobre n que el grupo $G(E_1 : K)$ es resoluble, siendo obvio el caso $n = 0$, pues entonces $E_1 = K$, así que $G(E_1 : K) = \{\mathrm{id}\}$ es resoluble.

Supongamos que el resultado es cierto para $n-1$ y veamos que también lo es para n. Si $\alpha_1 \in K$, se tiene $E_1 = K(\alpha_2, \ldots, \alpha_n)$, luego el grupo $G(E_1 : K)$ es resoluble, por hipótesis de inducción. Por tanto, podemos suponer que $\alpha_1 \notin K$ y, por simplicidad, denotamos $p = p_1$.

Sea $f := P_{K,\alpha_1}$ el polinomio mínimo de α_1 sobre K, cuyo grado es mayor o igual que 2 porque $\alpha_1 \notin K$. Como la extensión $E_1|K$ es de Galois y contiene la raíz α_1 del polinomio f, que es irreducible en $K[\mathtt{t}]$, se deduce de la Proposición IV.1.6 que f factoriza en $E_1[\mathtt{t}]$ como producto de factores de grado 1. Como f divide al polinomio $\mathtt{t}^p - a_1$, cada raíz $\beta \in E_1$ de f distinta de α_1 satisface $\beta^p = a_1 = \alpha_1^p$, y por ello el cociente $\zeta := \alpha_1/\beta \in E_1$ cumple que $\zeta^p = 1$ y $\zeta \neq 1$, es decir, $\zeta \in \mathcal{U}_p(\overline{K})$ es una raíz primitiva p-ésima de la unidad, por lo que $\mathcal{U}_p(\overline{K}) = \langle\zeta\rangle$, esto es, las raíces en E_1 del polinomio $\mathtt{t}^p - 1$ son las potencias ζ^k donde $0 \leq k \leq p-1$. Lo anterior implica que $F := K(\zeta) \subset E_1$ es el cuerpo de descomposición sobre K del polinomio $\mathtt{t}^p - 1$, y consideramos la cadena de cuerpos $K \subset F \subset F(\alpha_1) \subset E_1$.

Para demostrar que $G(E_1 : K)$ es resoluble observamos primero que, por el Lema VI.1.4, el grupo $G(F : K)$ es abeliano, luego resoluble. Además las extensiones $E_1|K$ y $F|K$ son de Galois, esta última porque F es un cuerpo de descomposición de $\mathtt{t}^p - 1$ sobre K. Así, por la segunda parte del Teorema fundamental de la teoría de Galois se tiene

$$G(F : K) \cong G(E_1 : K)/G(E_1 : F), \tag{1.1}$$

luego empleando la Proposición V.2.3, vol. I, para probar la resolubilidad del grupo $G(E_1 : K)$ es suficiente probar que $G(E_1 : F)$ es resoluble.

Como la extensión $E_1|K$ es de Galois, también lo es $E_1|F$. Además,

$$g(\mathtt{t}) := \mathtt{t}^p - \alpha_1^p = (\mathtt{t} - \alpha_1) \cdot (\mathtt{t} - \alpha_1\zeta) \cdots (\mathtt{t} - \alpha_1\zeta^{p-1})$$

y cada factor $\mathtt{t} - \alpha_1\zeta^j \in F(\alpha_1)[\mathtt{t}]$ con $0 \leq j \leq p-1$, por lo que $F(\alpha_1)$ es un cuerpo de descomposición de $g \in F[\mathtt{t}]$ sobre F. Se deduce de la Proposición IV.1.6 que la extensión $F(\alpha_1)|F$ es de Galois y, por el Lema VI.1.4, el grupo $G_F(g) = G(F(\alpha_1) : F)$ es abeliano.

Puesto que $F(\alpha_1)|F$ es una subextensión de Galois de la extensión de Galois $E_1|F$, se deduce de la segunda parte del Teorema fundamental de la teoría de Galois IV.2.4 que $G(E_1 : F(\alpha_1))$ es un subgrupo normal del grupo $G(E_1 : F)$, y se tiene

$$G(F(\alpha_1) : F) \cong G(E_1 : F)/G(E_1 : F(\alpha_1)). \tag{1.2}$$

A la vista de (1.2) y la Proposición V.2.3, vol. I, para demostrar que $G(E_1 : F)$ es resoluble basta ver que lo son $G(F(\alpha_1) : F)$ y $G(E_1 : F(\alpha_1))$.

Por el Lema VI.1.4, el grupo $G(F(\alpha_1) : F)$ es abeliano, luego resoluble en virtud del Ejemplo V.2.4, vol. I. Sólo queda demostrar que $G(E_1 : F(\alpha_1))$. Ahora bien, como $F(\alpha_1) \subset E_1$ se tiene

$$E_1 = K(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F(\alpha_1)(\alpha_2, \ldots, \alpha_n)$$

y la extensión $F(\alpha_1)(\alpha_2, \ldots, \alpha_n)|F(\alpha_1)$ es de Galois y radical. Por hipótesis de inducción su grupo de Galois $G(E_1 : F(\alpha_1))$ es resoluble, y hemos acabado. □

Definición y Observación VII.1.6 (1) El Teorema de Galois sobre resolubilidad de ecuaciones polinómicas por radicales consiste en la Proposición VII.1.5 anterior y su recíproco. Para la demostración de dicho recíproco hemos de introducir nuevas nociones.

(2) Dada una extensión de Galois $L|K$ se define la *norma* de cada elemento $a \in L$ como

$$\mathsf{N}(a) := \prod_{\phi \in G(L:K)} \phi(a).$$

Nótese que $\mathsf{N}(a) \in K$. En efecto, para cada $\psi \in G(L:K) := G$ se tiene

$$\psi(\mathsf{N}(a)) = \psi\Big(\prod_{\phi \in G} \phi(a)\Big) = \prod_{\phi \in G} \psi(\phi(a)) = \prod_{\varphi \in G} \varphi(a) = \mathsf{N}(a),$$

luego $\mathsf{N}(a) \in \mathrm{Fix}(G) = K$.

Lema VII.1.7 (Artin–Dedekind) *Sean L un cuerpo y $\phi_1, \ldots, \phi_r$ automorfismos de L distintos dos a dos. Entonces $\phi_1, \ldots, \phi_r$ son* linealmente independientes sobre L, *es decir, si $a_1, \ldots, a_r \in L$ son tales que $a_1\phi_1 + \cdots + a_r\phi_r = 0$, entonces $a_1 = 0, \ldots, a_r = 0$.*

Demostración. Supongamos, por reducción al absurdo, que $\phi_1, \ldots, \phi_r$ son linealmente dependientes sobre L. Entonces, como los automorfismos son aplicaciones no nulas, existe $s \geq 2$ mínimo con la propiedad de que existe alguna relación del tipo

$$a_1\phi_{i_1} + \cdots + a_s\phi_{i_s} = 0 \tag{1.3}$$

de modo que $a_j \neq 0$ para $1 \leq j \leq s$ y $1 \leq i_1 < \cdots < i_s \leq r$. Tras reordenar los índices podemos suponer que $\phi_{i_j} = \phi_j$ para $1 \leq j \leq s$. Como $\phi_1 \neq \phi_2$ existe $z \in L$ tal que $\phi_1(z) \neq \phi_2(z)$, y si multiplicamos la igualdad (1.3) por $\phi_1(z)$ queda

$$a_1\phi_1(z)\phi_1 + a_2\phi_1(z)\phi_2 + \cdots + a_s\phi_1(z)\phi_s = 0. \tag{1.4}$$

Para cada $x \in L$ calculamos la imagen de zx por los dos miembros de (1.3) y resulta

$$a_1\phi_1(z)\phi_1(x) + a_2\phi_2(z)\phi_2(x) + \cdots + a_s\phi_s(z)\phi_s(x) = 0.$$

Como esto se cumple para cada $x \in L$ tenemos que

$$a_1\phi_1(z)\phi_1 + a_2\phi_2(z)\phi_2 + \cdots + a_s\phi_s(z)\phi_s = 0. \tag{1.5}$$

Restando (1.4) de (1.5) resulta

$$a_2(\phi_1(z) - \phi_2(z))\phi_2 + \cdots + a_s(\phi_1(z) - \phi_s(z))\phi_s = 0.$$

Los coeficientes $a_j(\phi_1(z) - \phi_2(z))$ son no nulos y el número de ellos es $s - 1$, contra la minimalidad de s, luego $\phi_1, \ldots, \phi_r$ son linealmente independientes sobre L. □

Teorema VII.1.8 (90 de Hilbert) *Sea $L|K$ una extensión de Galois cuyo grupo de Galois $G(L:K)=\langle\tau\rangle$ es cíclico, generado por un automorfismo τ. Entonces, un elemento $a\in L$ tiene norma 1 si y sólo si existe $b\in L$ no nulo tal que $a=b/\tau(b)$.*

Demostración. Si $n:=\operatorname{ord}\big(G(L:K)\big)$ se tiene $\tau^n=\mathrm{id}$ y en consecuencia $G(L:K)=\{\mathrm{id},\tau,\dots,\tau^{n-1}\}$. Si $a=b/\tau(b)$ para cierto $b\in L$ no nulo,

$$\mathsf{N}(a)=\frac{b}{\tau(b)}\cdot\frac{\tau(b)}{\tau^2(b)}\cdots\frac{\tau^{n-1}(b)}{\tau^n(b)}=\frac{b}{\tau^n(b)}=1.$$

Recíprocamente, suponemos que $\mathsf{N}(a)=1$. Para cada $x\in L$ sean $b_0(x):=ax$ y $b_i(x):=a\tau(b_{i-1}(x))$ para $1\le i\le n-1$. Veamos, por inducción, que para $0\le i\le n-1$ se cumple

$$b_i(x)=\tau^i(x)\prod_{j=0}^{i}\tau^j(a). \tag{1.6}$$

Esto es obvio para $i=0$, y si $i>0$ y lo suponemos probado para $i-1$,

$$\begin{aligned} b_i(x)=a\tau(b_{i-1}(x))&=a\tau\Big(\tau^{i-1}(x)\prod_{j=0}^{i-1}\tau^j(a)\Big)\\ &=a\tau^i(x)\prod_{j=0}^{i-1}\tau^{j+1}(a)=\tau^i(x)\prod_{j=0}^{i}\tau^j(a).\end{aligned}$$

Sumando las expresiones de los $b_i(x)$ que acabamos de obtener se tiene

$$\begin{aligned}\sum_{i=0}^{n-1}b_i(x)&=ax+\sum_{i=1}^{n-1}\tau^i(x)\prod_{j=0}^{i}\tau^j(a)\\ &=a_0\tau^0(x)+\sum_{i=1}^{n-1}\Big(\prod_{j=0}^{i}\tau^j(a)\Big)\tau^i(x)=\sum_{i=0}^{n-1}a_i\tau^i(x),\end{aligned}$$

donde

$$a_i:=\prod_{j=0}^{i}\tau^j(a)\in L,\quad\text{para }\ 0\le i\le n-1.$$

Por tanto $\sum_{i=0}^{n-1}a_i\tau^i(x)=\sum_{i=0}^{n-1}b_i(x)$, y $a_0=\tau^0(a)=a\neq 0$ pues $\mathsf{N}(a)=1$. Se deduce del Lema de Artin-Dedekind que existe $x\in L$ tal que $b:=\sum_{i=0}^{n-1}b_i(x)$

es no nulo, y comprobamos que $a = b/\tau(b)$. Como $\tau^n = \mathrm{id}$ y $\mathsf{N}(a) = 1$ resulta

$$b_n(x) = x\prod_{j=0}^{n}\tau^j(a) = ax\prod_{j=0}^{n-1}\tau^j(a) = ax\prod_{\phi\in G(L:K)}\phi(a) = ax\mathsf{N}(a) = ax = b_0(x),$$

y en consecuencia,

$$a\tau(b) = a\tau\Big(\sum_{i=0}^{n-1}b_i(x)\Big) = \sum_{i=1}^{n}a\tau(b_{i-1}(x)) = \sum_{i=1}^{n}b_i(x) = \sum_{i=0}^{n-1}b_i(x) = b,$$

es decir, $a = b/\tau(b)$. □

Teorema VII.1.9 *Sean n un entero positivo y supongamos que el cuerpo K contiene una raíz primitiva n-ésima de la unidad. Sea $L|K$ una extensión de Galois cuyo grupo de Galois $G(L:K)$ es cíclico de orden n.*

(1) *Existe un elemento primitivo α de la extensión $L|K$ cuyo polinomio mínimo sobre K es $P_{K,\alpha}(\mathtt{t}) := \mathtt{t}^n - a$ para cierto $a \in K$.*

(2) *Sea $u \in L$ tal que $u^n = b \in K \setminus \{0\}$. Entonces, la extensión $K(u)|K$ es de Galois, el grupo $G(K(u):K)$ es cíclico, su orden d divide a n y $u^d \in K$.*

Demostración. (1) Denotamos $\zeta \in K$ una raíz primitiva n-ésima de la unidad y σ un generador del grupo cíclico $G(L:K)$. Se tiene $\sigma^j(\zeta^{-1}) = \zeta^{-1}$ porque $\zeta^{-1} \in K$, y por tanto la norma de ζ^{-1} es 1, ya que

$$\mathsf{N}(\zeta^{-1}) = \prod_{j=0}^{n-1}\sigma^j(\zeta^{-1}) = \prod_{j=0}^{n-1}\zeta^{-1} = (\zeta^{-1})^n = \zeta^{-n} = 1/\zeta^n = 1.$$

Por el Teorema 90 de Hilbert existe $\alpha \in L$ tal que $\zeta^{-1} = \alpha/\sigma(\alpha)$, es decir, $\sigma(\alpha) = \zeta\alpha$. Esto implica que $\sigma^j(\alpha) = \zeta^j\alpha$ para $1 \le j \le n$. El caso $j = 1$ es obvio, y si lo suponemos probado para $j-1$, y puesto que $\sigma(\zeta) = \zeta$, se tiene

$$\sigma^j(\alpha) = \sigma(\sigma^{j-1}(\alpha)) = \sigma(\zeta^{j-1}\alpha) = \zeta^{j-1}\sigma(\alpha) = \zeta^{j-1}\cdot\zeta\alpha = \zeta^j\alpha.$$

Cada $\sigma^j(\alpha)$ es raíz del polinomio mínimo $P_{K,\alpha}$ de α sobre K y, como $\zeta^j \neq \zeta^k$ para $0 \le j < k \le n-1$ puesto que ζ es raíz primitiva n-ésima, se deduce que $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha$ son n raíces distintas de $P_{K,\alpha}$. En consecuencia,

$$n \le \deg(P_{K,\alpha}) = [K(\alpha):K] \le [L:K] = n,$$

luego $[K(\alpha) : K] = [L : K]$, esto es, $L = K(\alpha)$, es decir, α es un elemento primitivo de la extensión $L|K$ y $\deg(P_{K,\alpha}) = n$. Por otra parte, α es raíz del polinomio $f(\mathtt{t}) := \mathtt{t}^n - \alpha^n$, así que basta ver que $a := \alpha^n \in K$ para concluir que $P_{K,\alpha}(\mathtt{t}) = \mathtt{t}^n - a$. Como la extensión $L|K$ es de Galois, los elementos de K son aquellos elementos de L que quedan fijos por la acción de σ. Pero

$$\sigma(\alpha^n) = (\sigma(\alpha))^n = (\zeta\alpha)^n = \zeta^n\alpha^n = \alpha^n,$$

de donde concluimos que $a = \alpha^n \in K$, como queríamos.

(2) Cada $\zeta^j u$ es raíz de $g(\mathtt{t}) := \mathtt{t}^n - b$ pues

$$g(\zeta^j u) = (\zeta^n)^j u^n - b = u^n - b = 0,$$

y por tanto

$$g(\mathtt{t}) = \prod_{j=0}^{n-1} (\mathtt{t} - \zeta^j u),$$

es decir, g, que es múltiplo del polinomio mínimo $P_{K,u}$ de u sobre K, factoriza en $K(u)[\mathtt{t}]$ en producto de factores de grado 1. Por tanto, también $P_{K,u}$ factoriza en $K(u)[\mathtt{t}]$ en producto de factores de grado 1, luego $K(u)$ es un cuerpo de descomposición de $P_{K,u}$ sobre K. Esto implica, por la Proposición IV.1.6, que la extensión $K(u)|K$ es de Galois. Además, para todo $\tau \in G(K(u) : K)$,

$$(\tau(u))^n - b = \tau(u^n - b) = \tau(0) = 0,$$

por lo que $(\tau(u))^n = b = u^n$, así que, $(\tau(u)/u)^n = 1$. Existe por tanto una raíz n-ésima ξ_τ de la unidad, no necesariamente primitiva, tal que $\tau(u)/u = \xi_\tau$, esto es, $\tau(u) = \xi_\tau u$. Nótese que ξ_τ es potencia de ζ, luego pertenece a K. Se define de este modo un homomorfismo

$$\Psi : G(K(u) : K) \to \mathcal{U}_n(K),\ \tau \mapsto \xi_\tau,$$

ya que dados automorfismos $\tau_1, \tau_2 \in G(K(u) : K)$ se tiene

$$\xi_{\tau_1\cdot\tau_2} u = (\tau_1 \cdot \tau_2)(u) = \tau_2(\tau_1(u)) = \tau_2(\xi_{\tau_1} u) = \xi_{\tau_1}\tau_2(u) = \xi_{\tau_1}\xi_{\tau_2} u,$$

por lo que $\xi_{\tau_1\cdot\tau_2} = \xi_{\tau_1}\xi_{\tau_2}$, o sea, $\Psi(\tau_1 \cdot \tau_2) = \xi_{\tau_1\cdot\tau_2} = \xi_{\tau_1}\xi_{\tau_2} = \Psi(\tau_1)\Psi(\tau_2)$.

Además Ψ es inyectivo porque si $\tau \in \ker\Psi$ entonces $\xi_\tau = 1$, por lo que $\tau(u) = \xi_\tau u = u$, lo que significa que $\tau = \mathrm{id}$. En consecuencia, $G(K(u) : K)$ es isomorfo a un subgrupo del grupo cíclico $\mathcal{U}_n(K)$, luego también es cíclico y su orden d divide al orden n de $\mathcal{U}_n(K)$. Como el único subgrupo de orden

d de $\mathcal{U}_n(K)$ es el grupo $\mathcal{U}_d(K)$ formado por las raíces d-ésimas de la unidad, deducimos que $\operatorname{im}\Psi = \mathcal{U}_d(K)$.

Por último, como la extensión $K(u)|K$ es de Galois, para demostrar que u^d pertenece a K basta ver que queda fijo por la acción de cada K-automorfismo de $K(u)$. Pero para cada $\tau \in G(K(u) : K)$ se tiene

$$\tau(u^d) = \tau(u)^d = (\xi_\tau u)^d = \xi_\tau^d u^d = u^d.$$

□

Ya estamos en condiciones de demostrar el Teorema de Galois sobre resolubilidad de ecuaciones polinómicas por radicales.

Demostración de VII.1.1 En virtud de la Proposición VII.1.5 basta probar que si el grupo G es resoluble entonces f es resoluble por radicales.

Sea $L_f \subset \overline{K}$ un cuerpo de descomposición de f sobre K. Hay que demostrar que existe una extensión $E|L_f$ tal que $E|K$ es radical, y procedemos por inducción sobre el orden de G. Si $\operatorname{ord}(G) = 1$, entonces $[L_f : K] = \operatorname{ord}(G) = 1$, luego $L_f = K$ y basta elegir $E = L_f$. Supongamos el resultado cierto si el orden de G es menor que $n \geq 2$ y veamos que también es cierto si $\operatorname{ord}(G) = n$. Como G es finito posee algún subgrupo normal H maximal entre los subgrupos normales de G distintos de G.

Por el Teorema de la correspondencia, II.1.7, vol. I, la maximalidad de H implica que el cociente G/H es un grupo simple. En efecto, en caso contrario este grupo admitiría un subgrupo normal propio, que es de la forma N/H, donde $N \neq G$ es un subgrupo normal de G que contiene estrictamente a H, y esto contradice la maximalidad de H. Como G es resoluble se desprende de la Proposición V.2.3, vol. I, que G/H es resoluble luego, por el Ejemplo V.2.4 (7), vol. I, G/H es un grupo cíclico de orden primo p.

Sean $\zeta \in \overline{K}$ una raíz primitiva p-ésima de la unidad y $E_0 := L_f(\zeta)$ un cuerpo de descomposición sobre L_f del polinomio $\mathtt{t}^p - 1$. Así E_0 es un cuerpo de descomposición sobre K del producto $(\mathtt{t}^p - 1)f(\mathtt{t})$, luego la extensión $E_0|K$ es, por la Proposición IV.1.6, de Galois. Por el Lema VI.1.4 el grupo de Galois $G(E_0 : L_f)$ es abeliano y, por el Teorema IV.2.4, $G(E_0 : L_f) \lhd G(E_0 : K)$ y

$$G(L_f : K) \cong G(E_0 : K)/G(E_0 : L_f).$$

Por V.2.4 vol. I el grupo $G(E_0 : L_f)$ es resoluble, ya que es abeliano, mientras que $G(L_f : K)$ es resoluble por hipótesis. Se deduce de V.2.3, vol. I, que también es resoluble $G(E_0 : K)$. Sea $F := K(\zeta) \subset E_0$ el cuerpo de descomposición

sobre K del polinomio $\mathtt{t}^p - 1$. Como $E_0|K$ es una extensión de Galois y F es un subcuerpo de E_0 que contiene a K, la extensión $E_0|F$ es de Galois.

Se sigue de la definición que la extensión $F|K = K(\zeta)|K$ es radical. Además, observamos en VII.1.2 que la noción "ser extensión radical" es transitiva, luego basta encontrar un cuerpo E tal que $F \subset E_0 \subset E$ y la extensión $E|F$ sea radical, pues entonces $E|K$ es radical y se cumple que $L_f \subset E_0 \subset E$.

Veamos primero que el grupo $G(E_0 : F)$ es isomorfo a un subgrupo de $G(L_f : K)$. Para cada F-automorfismo $\phi : E_0 \to E_0$, y puesto que $L_f|K$ es una subextensión de Galois de $E_0|K$ y $K \subset F$, la restricción $\phi|_{L_f} : L_f \to L_f$ es un K-automorfismo. De este modo, la aplicación

$$\Psi : G(E_0 : F) \to G = G(L_f : K),\ \phi \mapsto \phi|_{L_f}$$

está bien definida y de hecho es un homomorfismo. Comprobemos que es inyectivo. Dado $\phi \in \ker \Psi$ la restricción $\phi|_{L_f}$ es el automorfismo identidad. Como $\phi(\zeta) = \zeta$ pues $\zeta \in F$, concluimos que $\phi|_{E_0} = \phi|_{L_f(\zeta)} = \mathrm{id}_{L_f(\zeta)} = \mathrm{id}_{E_0}$. Esto prueba la inyectividad de Ψ, por lo que $G(E_0 : F)$ es isomorfo al subgrupo $G_1 := \Psi(G(E_0 : F))$ de $G(L_f : K)$.

Ahora distinguimos dos casos. Si $G_1 \subsetneq G$, entonces $G(E_0 : F)$ es un grupo resoluble de orden estrictamente menor que el orden de G. Por hipótesis de inducción existe una extensión $E|E_0$ tal que $E|F$ es radical.

Por otro lado, si $G_1 = G$, sea $H_1 := \Psi^{-1}(H)$, que es un subgrupo normal de $G(E_0 : F)$ de índice p, porque H es subgrupo normal de G de índice p. El cuerpo $F_1 := \mathrm{Fix}(H_1)$ cumple, por el Teorema IV.2.1, que $H_1 = G(E_0 : F_1)$ y, como H_1 es un subgrupo normal de $G(E_0 : F)$, la extensión $F_1|F$ es, por el Teorema IV.2.4, de Galois y

$$G(F_1 : F) \cong G(E_0 : F)/G(E_0 : F_1) = G(E_0 : F)/H_1 \cong G/H \cong \mathbb{Z}_p.$$

Por el Teorema VII.1.9, y puesto que el polinomio $\mathtt{t}^p - 1$ factoriza en $F[\mathtt{t}]$ como producto de factores de grado 1, existe $\alpha \in F_1$ tal que $\alpha^p = a \in F$ y $F_1 = F(\alpha)$. Como $E_0|F_1$ es una extensión de Galois cuyo grupo de Galois $G(E_0 : F_1)$ es resoluble y su orden es menor que el de G existe, por hipótesis de inducción, una extensión $E|E_0$ tal que la extensión $E|F_1$ es radical.

Como también es radical la extensión $F_1|F$, ya que $F_1 = F(\alpha)$ y α es raíz del polinomio $\mathtt{t}^p - a$ para cierto $a \in F$, se deduce de VII.1.2 que $E|F$ es una extensión radical, como pretendíamos. □

1.a. Resultados acerca de la resolubilidad por radicales

Corolario VII.1.10 (Galois) *Sean $f \in K[\mathtt{t}]$ un polinomio irreducible de grado primo y $\overline{K}$ un cierre algebraico de K. Las siguientes afirmaciones son equivalentes:*

(1) *El polinomio f es resoluble por radicales sobre K.*

(2) *Para cada par de raíces distintas a, b de f en $\overline{K}$ se cumple que $K(a, b)$ es un cuerpo de descomposición de f sobre K.*

Demostración. Sea $G_K(f) := G(L_f : K)$, donde $L_f \subset \overline{K}$ es un cuerpo de descomposición de f sobre K. Por VI.1.2 (1), $G_K(f)$ es un subgrupo transitivo del grupo simétrico $\mathfrak{S}_p$, donde $p := \deg(f)$ e identificamos cada elemento de $G_K(f)$ con su restricción al conjunto $Z_{\overline{K}}(f)$ de raíces de f en $\overline{K}$. Se deduce entonces del Teorema A.5, vol. I., que G es resoluble si y sólo si la identidad es el único elemento de G que fija más de una raíz de f en $\overline{K}$. Esto último equivale a que $\{\mathrm{id}\} = G(L_f : K(a, b))$ para cada par de raíces distintas $a, b \in Z_{\overline{K}}(f)$. Puesto que $L_f|K$ es una extensión de Galois lo anterior equivale, por el Teorema fundamental de la Teoría de Galois, a que

$$L_f = \mathrm{Fix}(\mathrm{id}) = \mathrm{Fix}(G(L_f : K(a, b))) = K(a, b),$$

como queríamos demostrar. □

Corolario VII.1.11 *Sea $f \in \mathbb{Q}[\mathtt{t}]$ un polinomio de grado primo $p \geq 5$ resoluble por radicales. Entonces el número de raíces reales de f es 1 o p.*

Demostración. Como $\deg(f)$ es impar f posee alguna raíz real a, y supongamos que no es la única. Existe por tanto otra raíz $b \in \mathbb{R} \setminus \{a\}$ de f. Por el Corolario VII.1.10 el cuerpo $\mathbb{Q}(a, b) \subset \mathbb{R}$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$, luego todas las raíces de f son reales. □

Corolario VII.1.12 (Abel) (1) *El polinomio general de grado $n \geq 5$ sobre K no es resoluble por radicales.*

(2) *Todo polinomio $f \in K[\mathtt{t}]$ de grado ≤ 4 es resoluble por radicales sobre K.*

(3) *Para cada número primo $p \geq 5$ existe un polinomio irreducible $f \in \mathbb{Q}[\mathtt{t}]$ de grado p no resoluble por radicales sobre $\mathbb{Q}$.*

Demostración. (1) Por el Teorema VI.2.2 el grupo de Galois del polinomio general de grado n es el grupo simétrico $\mathcal{S}_n$ que, para $n \geq 5$, no es resoluble, según vimos en el Ejemplo V.2.4 (8), vol. I. Se deduce del Teorema de Galois VII.1.1 que el polinomio general de grado $n \geq 5$ sobre K no es resoluble por radicales.

(2) El grupo de Galois $G_K(f)$ de f sobre K es, por VI.3.1, VI.3.2, VI.3.3 y VI.3.4, subgrupo del grupo $\mathcal{S}_4$ de permutaciones de 4 elementos, y se deduce del Ejemplo V.2.4 (9) vol. I, y la Proposición V.2.3, vol. I, que $G_K(f)$ es un grupo resoluble. Esto implica, por el Teorema de Galois VII.1.1, que f es resoluble por radicales sobre K.

(3) Vimos en el Ejemplo VI.1.7 que existe un polinomio irreducible $f \in \mathbb{Q}[\mathtt{t}]$ de grado $p \geq 5$ cuyo grupo de Galois $G_{\mathbb{Q}}(f) = \mathcal{S}_p$ no es resoluble luego, por el Teorema de Galois, f no es resoluble por radicales sobre $\mathbb{Q}$. □

El tercer apartado del Corolario VII.1.12 anterior se puede extender a polinomios de grado $n \geq 5$, sin necesidad de que n sea primo. La demostración que conocemos de este resultado emplea el denominado *teorema de irreducibilidad de Hilbert* que enunciamos a continuación y cuya demostración debemos omitir pues requiere técnicas propias de Geometría Algebraica y Analítica.

Teorema VII.1.13 (De irreducibilidad de Hilbert) *Dado un polinomio irreducible*

$$f := f(\mathtt{x}_1, \ldots, \mathtt{x}_n, \mathtt{t}) \in \mathbb{Q}[\mathtt{x}_1, \ldots, \mathtt{x}_n, \mathtt{t}]$$

el conjunto formado por las n-uplas $\beta := (\beta_1, \ldots, \beta_n) \in \mathbb{Q}^n$ tales que el polinomio $f(\beta, \mathtt{t}) \in \mathbb{Q}[\mathtt{t}]$ es irreducible es infinito.

Corolario VII.1.14 *Para cada entero $n \geq 5$ existe un polinomio irreducible $f_n \in \mathbb{Q}[\mathtt{t}]$ cuyo grupo de Galois $G_{\mathbb{Q}}(f_n) = \mathcal{S}_n$. En particular, f_n no es resoluble por radicales.*

Demostración. La segunda parte se sigue directamente del Teorema de Galois VII.1.1 y de que para $n \geq 5$ el grupo simétrico $\mathcal{S}_n$ no es resoluble. Para la primera, sean $\mathtt{t}, \mathtt{x}_1, \ldots, \mathtt{x}_n$ indeterminadas sobre $\mathbb{Q}$. Denotamos por abreviar $\mathbb{Q}(\mathtt{x}) := \mathbb{Q}(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ y consideramos el polinomio general

$$g_n = g_n(\mathtt{x}, \mathtt{t}) := \prod_{i=1}^{n} (\mathtt{t} - \mathtt{x}_i) \in \mathbb{Q}[\mathtt{x}, \mathtt{t}].$$

Por la fórmulas de Cardano–Vieta VII.1.13, vol. II, se tiene

$$g_n(\mathtt{x},\mathtt{t}) = \mathtt{t}^n + \sum_{k=1}^{n}(-1)^k \mathtt{s}_k(\mathtt{x})\mathtt{t}^{n-k}$$

donde $\mathtt{s}_k$ es, para $1 \leq k \leq n$, la forma simétrica elemental de grado k. Denotamos por abreviar $\mathbb{Q}(\mathtt{s}) = \mathbb{Q}(\mathtt{s}_1,\ldots,\mathtt{s}_n)$, y así $g_n \in \mathbb{Q}(\mathtt{s})[\mathtt{t}]$. Por el Teorema VI.2.2, la extensión $\mathbb{Q}(\mathtt{x})|\mathbb{Q}(\mathtt{s})$ es de Galois y

$$G_{\mathbb{Q}(\mathtt{s})}(g_n) = G\big(\mathbb{Q}(\mathtt{x}) : \mathbb{Q}(\mathtt{s})\big) \cong \mathcal{S}_n.$$

En particular, $\deg(g_n) = n$ y $\operatorname{ord}\big(G_{\mathbb{Q}(\mathtt{s})}(g_n)\big) = n!$, lo que implica, por la Observación II.1.3 (4), que g_n es irreducible en $\mathbb{Q}(\mathtt{s})[\mathtt{t}]$.

Como la extensión $\mathbb{Q}(\mathtt{x})|\mathbb{Q}(\mathtt{s})$ es finita y $\mathbb{Q}$ es infinito se deduce de la prueba del Teorema del elemento primitivo II.2.2, que existen $m_1,\ldots,m_n \in \mathbb{Q}$ tales que $\alpha := m_1\mathtt{x}_1 + \cdots + m_n\mathtt{x}_n$ cumple que $\mathbb{Q}(\mathtt{x}) = \mathbb{Q}(\mathtt{s})(\alpha)$.

El grado del polinomio mínimo $p \in \mathbb{Q}(\mathtt{s})[\mathtt{t}]$ de α sobre $\mathbb{Q}(\mathtt{s})$ es el de la extensión $\mathbb{Q}(\mathtt{x})|\mathbb{Q}(\mathtt{s})$, es decir, $\deg(p) = n!$. Como el grupo de Galois de la extensión de Galois $\mathbb{Q}(\mathtt{x})|\mathbb{Q}(\mathtt{s})$ es $\mathcal{S}_n$, las raíces de p son las imágenes $\widetilde{\sigma}(\alpha)$ de α mediante el automorfismo $\widetilde{\sigma}$ de $\mathbb{Q}(\mathtt{x})$ asociado a cada permutación $\sigma \in \mathcal{S}_n$, y que cumple $\widetilde{\sigma}(\mathtt{x}_i) = \mathtt{x}_{\sigma(i)}$. Por tanto,

$$\widetilde{\sigma}(\alpha) = \widetilde{\sigma}(m_1\mathtt{x}_1 + \cdots + m_n\mathtt{x}_n) = m_1\mathtt{x}_{\sigma(1)} + \cdots + m_n\mathtt{x}_{\sigma(n)},$$

y en consecuencia,

$$p(\mathtt{t}) = \prod_{\sigma\in\mathcal{S}_n} (\mathtt{t} - (m_1\mathtt{x}_{\sigma(1)} + \cdots + m_n\mathtt{x}_{\sigma(n)})) \in \mathbb{Q}(\mathtt{s})[\mathtt{t}]. \tag{1.7}$$

Obsérvese que la extensión $\mathbb{Q}(\mathtt{x})|\mathbb{Q}(\mathtt{s})$ es finita, luego algebraica, y por la transitividad del grado de transcendencia, III.2.8,

$$\operatorname{tr\,deg}\mathbb{Q}(\mathtt{s})|\mathbb{Q} = \operatorname{tr\,deg}\mathbb{Q}(\mathtt{x})|\mathbb{Q} - \operatorname{tr\,deg}\mathbb{Q}(\mathtt{x})|\mathbb{Q}(\mathtt{s}) = n - 0 = n,$$

lo que implica que $\mathtt{s}_1,\ldots,\mathtt{s}_n$ son indeterminadas sobre $\mathbb{Q}$, es decir, elementos algebraicamente independientes. Para resaltar este hecho escribimos la fórmula (1.7) como

$$p(\mathtt{s}_1,\ldots,\mathtt{s}_n,\mathtt{t}) = \prod_{\sigma\in\mathcal{S}_n} (\mathtt{t} - (m_1\mathtt{x}_{\sigma(1)} + \cdots + m_n\mathtt{x}_{\sigma(n)})) \in \mathbb{Q}[\mathtt{s}_1,\ldots,\mathtt{s}_n,\mathtt{t}]. \tag{1.8}$$

Podemos aplicar el Teorema de irreducibilidad de Hilbert, VII.1.13, a los polinomios irreducibles del anillo $\mathbb{Q}[\mathtt{s}_1,\ldots,\mathtt{s}_n,\mathtt{t}]$, en particular a p, por lo que

existe $\beta := (\beta_1, \ldots, \beta_n) \in \mathbb{Q}^n$ tal que $\widehat{p}(\mathtt{t}) := p(\beta, \mathtt{t}) \in \mathbb{Q}[\mathtt{t}]$ es irreducible. Esto significa que $\widehat{p}(\mathtt{t})$ se obtiene a partir de p evaluando en $\mathtt{s}_k := \beta_k$ para $1 \leq k \leq n$.

Veamos que el polinomio $f_n(\mathtt{t}) := g_n(\beta, \mathtt{t}) \in \mathbb{Q}[\mathtt{t}]$ que se obtiene a partir de g_n evaluando en $\mathtt{s}_k = \beta_k$ para $1 \leq k \leq n$ es irreducible en $\mathbb{Q}[\mathtt{t}]$ y $G_{\mathbb{Q}}(f_n) = \mathcal{S}_n$. Por la Observación II.1.3 (4), para comprobar ambas cosas basta demostrar que $\mathrm{ord}(G_{\mathbb{Q}}(f_n)) = n!$.

Ahora bien, sean $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ las raíces de f_n y $L := \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ un cuerpo de descomposición de f_n sobre $\mathbb{Q}$. Como la extensión $L|\mathbb{Q}$ es de Galois,

$$\mathrm{ord}(G_{\mathbb{Q}}(f_n)) = \mathrm{ord}(G(L : \mathbb{Q})) = [L : \mathbb{Q}],$$

luego todo consiste en demostrar que $L|\mathbb{Q}$ es una extensión de grado $n!$. La clave consiste en observar que

$$\begin{aligned} \mathtt{t}^n + \sum_{k=1}^{n} (-1)^k \beta_k \mathtt{t}^{n-k} = g_n(\beta, \mathtt{t}) = f_n(\mathtt{t}) &= \prod_{k=1}^{n} (\mathtt{t} - \alpha_k) \\ &= \mathtt{t}^n + \sum_{k=1}^{n} (-1)^k \mathtt{s}_k(\alpha_1, \ldots, \alpha_n) \mathtt{t}^{n-k}, \end{aligned}$$

por lo que cada $\beta_k = \mathtt{s}_k(\alpha_1, \ldots, \alpha_n)$. De esto se deduce que

$$\widehat{p}(\mathtt{t}) = p(\beta, \mathtt{t}) = \prod_{\sigma \in \mathcal{S}_n} (\mathtt{t} - (m_1 \alpha_{\sigma(1)} + \cdots + m_n \alpha_{\sigma(n)})),$$

lo que en particular implica que $\widehat{\alpha} := m_1 \alpha_1 + \cdots + m_n \alpha_n \in L$ y

$$\begin{aligned} n! = \mathrm{ord}(\mathcal{S}_n) = \deg(\widehat{p}) = \deg(P_{\mathbb{Q},\widehat{\alpha}}) &= [\mathbb{Q}(\widehat{\alpha}) : \mathbb{Q}] \leq [L : \mathbb{Q}] \\ &= [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}] \leq n!, \end{aligned}$$

de donde se sigue la igualdad $[L : \mathbb{Q}] = n!$ buscada. □

Observación VII.1.15 Vimos en VI.4.1 que si f es un polinomio irreducible en $K[\mathtt{t}]$ de grado 5 su grupo de Galois $G_K(f)$ es uno de los cinco grupos siguientes

$$\mathbb{Z}_5,\ \mathcal{D}_5,\ \mathcal{A}f_5,\ \mathcal{A}_5 \quad \& \quad \mathcal{S}_5.$$

Se deduce del Teorema A.5, vol. I, que los tres primeros son resolubles y los dos últimos no lo son. Basta por tanto emplear la tabla en VI.4.5 y el Teorema

de Galois VII.1.1 para decidir si un polinomio de grado 5 irreducible en $K[\mathtt{t}]$ es resoluble por radicales sobre K.

Por otro lado, si f es reducible en $K[\mathtt{t}]$ existen $f_1, f_2 \in K[\mathtt{t}]$ de grado menor o igual que 4 tales que $f = f_1 f_2$. Ya hemos visto que tanto f_1 como f_2 son resolubles por radicales, luego también f lo es.

2. Construcciones con regla y compás. Problemas délicos.

En esta sección se prueba la irresolubilidad mediante regla y compás de los tres problemas délicos: la cuadratura del círculo, VII.2.10, la duplicación del cubo, VII.2.11 y la trisección del ángulo VII.2.12. Además, se determinan qué polígonos regulares son constructibles con regla y compás.

Comenzamos formalizando las ideas intuitivas de construcción con regla y compás. Sea $\mathcal{P}_0 \subset \mathbb{R}^2$ un conjunto finito y no vacío de puntos del plano euclídeo y consideramos las dos operaciones siguientes:

Operación 1 (*Regla*): Dibujar la línea que pasa por dos puntos de $\mathcal{P}_0$, o bien extendiéndola indefinidamente en ambas direcciones o bien considerando, exactamente, el segmento que une dichos puntos.

Operación 2 (*Compás*): Dibujar una circunferencia cuyo centro es un punto de $\mathcal{P}_0$ y cuyo radio es la distancia entre dos puntos de $\mathcal{P}_0$.

(1) Se dice que un punto de $\mathbb{R}^2$ es *constructible en un paso* a partir de $\mathcal{P}_0$ si es la intersección de dos rectas, o de dos circunferencias, o de una recta y una circunferencia, construidas mediante las operaciones 1 y 2.

(2) Un punto $P \in \mathbb{R}^2$ se dice *constructible* a partir de $\mathcal{P}_0$ si existe un conjunto finito de puntos $\{P_1, \ldots, P_r = P\} \subset \mathbb{R}^2$ tales que para $1 \leq i \leq r$ el punto P_i es constructible en un paso a partir del conjunto de puntos $\mathcal{P}_0 \cup \{P_1, \ldots, P_{i-1}\}$.

2.a. Construcciones básicas

Algunas construcciones sencillas, obtenidas aplicando sucesivamente operaciones con regla y compás, pero que serán fundamentales para nuestros propósitos, son las siguientes:

(VII.2.1) Mediatriz del segmento que une dos puntos dados. Sean $P, Q \in \mathbb{R}^2$ dos puntos distintos. Se denomina *mediatriz* del segmento S que une P y Q al conjunto de puntos que equidistan de P y Q. Dicha mediatriz es la

perpendicular a la recta que pasa por P y Q en el punto medio del segmento S. Para construirla con regla y compás procedemos como sigue:

(i) Se traza el segmento $\overline{PQ}$ que une P y Q.

(ii) Se traza la circunferencia Γ_1 de centro P y radio la distancia entre P y Q.

(iii) Se traza la circunferencia Γ_2 de centro Q y radio la distancia entre P y Q.

(iv) Sean A_1 y A_2 los puntos de intersección de Γ_1 y Γ_2.

(v) Se traza el segmento $\overline{A_1A_2}$ que los une.

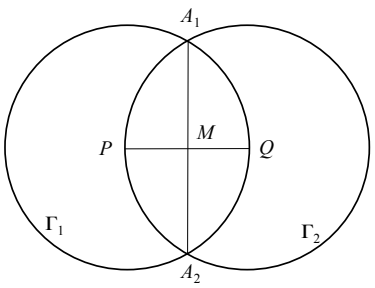


Figura 2.1: **Mediatriz**

(vi) El punto M de intersección de los segmentos $\overline{A_1A_2}$ y $\overline{PQ}$ es el punto medio del segmento $\overline{PQ}$.

Además, el segmento $\overline{A_1A_2}$ es perpendicular al segmento $\overline{PQ}$ y la recta que lo contiene es la mediatriz del segmento $\overline{PQ}$.

(VII.2.2) Perpendicular a una recta en uno de sus puntos. Sean $P, Q \in \mathbb{R}^2$ dos puntos distintos y r la recta que pasa por ellos. Para trazar la recta perpendicular a r que pasa por el punto P procedemos como sigue:

(i) Se traza la circunferencia Γ de centro P y radio la distancia entre P y Q.

(ii) Sean Q y A_2 los puntos de intersección de Γ con la recta r. Nótese que P es el punto medio del segmento que une A_1 y A_2.

(iii) La mediatriz del segmento $\overline{QA_2}$ es la perpendicular a la recta r que pasa por P.

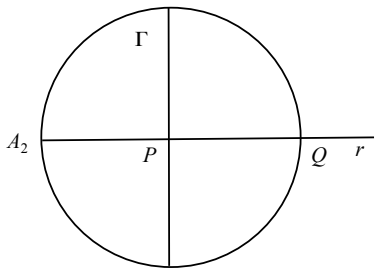


Figura 2.2: **Perpendicular**

(VII.2.3) Bisección del ángulo que forman dos rectas que se cortan. Sean r y s dos rectas que se cortan en un punto $P \in \mathcal{P}_0 \subset \mathbb{R}^2$ y pasan, respectivamente, por los puntos $Q, R \in \mathcal{P}_0 \setminus \{P\}$. Se llama *bisectriz* del par de rectas r, s o del ángulo que forman r y s, al conjunto de puntos que equidistan de r y s.

Dicha bisectriz es la unión de dos rectas perpendiculares que pasan por P, y se construye así:

(i) Sea Γ la circunferencia de centro P y radio la distancia entre P y Q. Nótese que $Q \in \Gamma$.

(ii) Sean A_1, A_2 los puntos de corte de s y Γ.

(iii) La bisectriz del par de rectas r, s es la unión de las mediatrices m_1 y m_2 de los segmentos $\overline{QA_1}$ y $\overline{QA_2}$.

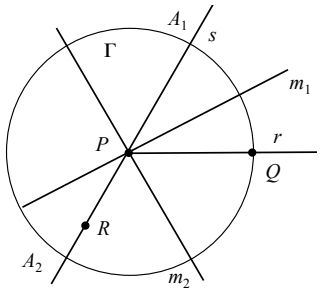


Figura 2.3: **Bisectriz**

(VII.2.4) Paralela a una recta r por un punto exterior a ella. Sean $P, Q, R \in \mathcal{P}_0$ tres puntos no alineados y r la recta que pasa por Q y R. Para trazar la recta paralela a r que pasa por P, procedemos como sigue:

(i) Se traza la circunferencia Γ de centro P y radio la distancia entre P y Q.

(ii) Si $\Gamma \cap r$ es un único punto éste es Q, y se traza la recta s que pasa por P y Q.

(iii) Si Γ corta a r en dos puntos $A_1 := Q$ y A_2, se traza la mediatriz s del segmento $\overline{A_1A_2}$. En ambos casos s es la recta perpendicular a r que pasa por el punto P.

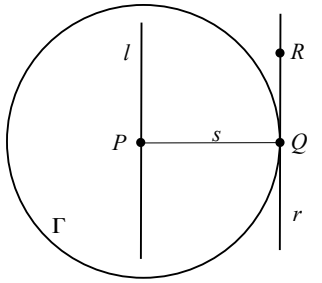


Figura 2.4: **Paralela**

(iv) La recta l perpendicular a s en el punto P es la recta paralela a r que pasa por P.

Definiciones y Observaciones VII.2.5 (1) Para *medir* hacen falta dos puntos de referencia, que en nuestro caso serán $(0,0), (1,0) \in \mathbb{R}^2$. De hecho, diremos que un punto $P \in \mathbb{R}^2$ es *constructible* si lo es a partir del conjunto $\mathcal{P}_0 := \{(0,0), (1,0)\}$. Además, diremos que un número $\alpha \in \mathbb{R}$ es *constructible* si existe un punto $(a,b) \in \mathbb{R}^2$ constructible tal que la longitud del segmento que une $(0,0)$ con (a,b) es igual a $|\alpha|$.

(2) La recta e_1 que pasa por los puntos $(0,0)$ y $(1,0)$ es, por definición, constructible, y por ello también lo es la recta e_2 que pasa por los puntos $(0,0)$ y $(0,1)$, por ser la perpendicular a e_1 que pasa por $(0,0)$.

(3) Relacionamos a continuación la constructibilidad de un punto de $\mathbb{R}^2$ con la constructibilidad de sus coordenadas.

Lema VII.2.6 *El punto $(a,b) \in \mathbb{R}^2$ es constructible si y sólo si $(a,0)$ y $(0,b)$ son puntos constructibles. Por tanto, $P := (a,b) \in \mathbb{R}^2$ es constructible si y sólo si los números reales $a, b \in \mathbb{R}$ son constructibles. En consecuencia, determinar qué números reales λ son constructibles, es decir, que segmentos de longitud $|\lambda|$ son constructibles, equivale a caracterizar qué puntos del plano son contructibles.*

Demostración. Supongamos que el punto P es constructible. Trazamos la recta r paralela a e_1 que pasa por P. Esta recta corta a e_2 en el punto $(0,b)$ que es, por tanto, constructible. A continuación, trazamos la recta s paralela a e_2 que pasa por P. Esta recta corta a e_1 en el punto $(a,0)$, que es, por tanto, constructible.

Recíprocamente, si los puntos $(a,0)$ y $(0,b)$ son constructibles, tanto la recta r paralela a e_1 que pasa por el punto $(0,b)$ como la recta s paralela a e_2 que pasa por el punto $(a,0)$ son constructibles, por lo que también lo es el punto (a,b) en que se cortan. □

Lema VII.2.7 *Dados segmentos constructibles de longitudes $1, a$ y b, donde $a > b > 0$, también son constructibles segmentos de longitudes $a+b, a-b, ab$ y a/b si $b \neq 0$. En particular todos los puntos de $\mathbb{Q}^2 \subset \mathbb{R}^2$ son constructibles.*

Demostración. El punto $(a,0)$ es constructible por ser a un número real constructible. La circunferencia de centro $(a,0)$ y radio b corta a la recta e_1 en los puntos $(a-b,0)$ y $(a+b,0)$ que son, por tanto, constructibles.

Probamos ahora que el punto $(ab,0)$ es constructible. Consideramos el triángulo Δ_1 de vértices $O := (0,0)$, $A := (a,0)$ y $E_2 := (0,1)$. Sean r la recta que pasa por los puntos A y E_2 y s la recta paralela a r que pasa por el punto $B := (0,b)$. Sea Δ_2 el triángulo de vértices O, B y C, donde C es el punto de intersección de la recta s con la recta e_1 que pasa por los puntos O y $E_1 := (1,0)$.

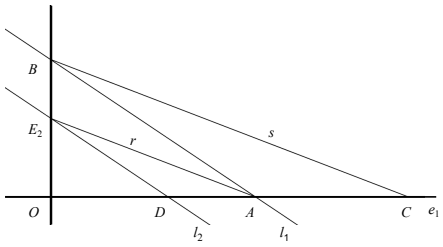


Figura 2.5: **Producto y cociente de dos longitudes constructibles**

Los triángulos Δ_1 y Δ_2 son semejantes porque comparten un ángulo y sus respectivos lados opuestos a este ángulo son paralelos. De este modo, si μ es la longitud del segmento $\overline{OC}$ se cumple, por el Teorema de Thales, que $\mu/b = a/1$, por lo que $\mu = ab$ es constructible.

Finalmente comprobemos que si $b \neq 0$ también el punto $(a/b, 0)$ es constructible. Sean Δ_3 el triángulo de vértices O, A y B, l_1 la recta que pasa por los puntos A y B y l_2 la recta paralela a r que pasa por el punto E_2. El triángulo Δ_3 es semejante al triángulo de vértices O, E_2 y $D := l_2 \cap e_1$ pues ambos triángulos comparten un ángulo y sus respectivos lados opuestos a este ángulo son paralelos. De este modo, si λ es la longitud del segmento $\overline{OD}$, se cumple que $\lambda/1 = a/b$, por lo que $\lambda = a/b$ es constructible.

Nótese que la constructibilidad de $a \pm b$ implica la de todos los enteros positivos y la de a/b la de los números racionales positivos. □

Lema VII.2.8 *Dados segmentos constructibles de longitudes* 1 *y* a*, el segmento de longitud* $\sqrt{a}$ *es constructible.*

Demostración. Se deduce del Lema VII.2.7 que los tres puntos $O := (0, 0)$, $E_1 := (1, 0)$ y $P := (a+1, 0)$ son constructibles, y también lo es el punto medio $M := ((a + 1)/2, 0)$ del segmento $\overline{OP}$.

Trazamos la circunferencia Γ de centro M y radio la distancia entre O y M, y la recta r perpendicular al segmento $\overline{OP}$ que pasa por el punto E_1. Si A_1 es uno de los puntos en que r corta a Γ, los triángulos rectángulos Δ_1 y Δ_2 de vértices O, E_1 y A_1 y A_1, E_1 y P, respectivamente, son semejantes, pues comparten los ángulos.

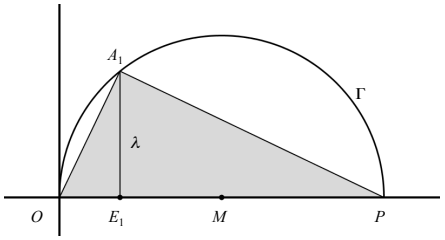


Figura 2.6: **Raíz cuadrada de una longitud constructible**

En consecuencia, la longitud λ del segmento $\overline{E_1A_1}$ cumple $\lambda/1 = a/\lambda$, esto es, $\lambda^2 = a$, con lo que $\lambda = \sqrt{a}$ es constructible. □

Teorema VII.2.9 (Números constructibles) *Un número real* α *es constructible si y sólo si existe una cadena finita de cuerpos*

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_n$$

tal que $\alpha \in K_n$ *y para* $1 \leq i \leq n$ *la extensión* $K_i|K_{i-1}$ *tiene grado* 2.

Demostración. Supongamos primero que $\alpha \in \mathbb{R}$ es constructible. Como los puntos $O := (0,0)$ y $E_1 := (1,0)$ son constructibles, también lo es el punto $Q := (\alpha, 0)$. Veamos que:

$(*)$ *Si un punto* $P := (a,b) \in \mathbb{R}^2$ *es constructible, entonces existe una cadena finita de cuerpos* $\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_n$ *tal que* $a, b \in K_n$ *y la extensión* $K_i|K_{i-1}$ *tiene grado* 2 *para* $1 \leq i \leq n$.

Recordamos que si un punto P es constructible, entonces existe una cantidad finita de puntos $P_1, \ldots, P_r := P$ tales que P_i es constructible en un paso a partir de los puntos $O := (0,0), E_1 := (1,0), P_1, \ldots, P_{i-1}$, donde $1 \leq i \leq r$ y tomaremos $r := 0$ si P es uno de los puntos O, E_1.

Vamos a demostrar la afirmación $(*)$ por inducción sobre r. Si $r = 0$ entonces, $P := E_1$ o $P := O$, y en ambos casos basta tomar $K_0 = \mathbb{Q}$. Supongamos que el resultado es cierto para $r-1$ y veamos que también es cierto para r.

Denotemos $P_{r-1} := (c,d)$ y, por hipótesis de inducción, existe una cadena finita de cuerpos $\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_{n-1}$ tal que $c, d \in K_{n-1}$ y la extensión $K_i|K_{i-1}$ tiene grado 2 para $1 \leq i \leq n-1$. Sea $S := \{O, E_1, P_1, \ldots, P_{r-1}\}$ y distinguimos tres casos:

(i) El punto P_r es la intersección de dos rectas que pasan por dos puntos del conjunto S cuyas coordenadas pertenecen al cuerpo K_{n-1}. Entonces, las coordenadas de P_r son la solución de un sistema compatible determinado formado por dos ecuaciones lineales con dos incógnitas con coeficientes en K_{n-1}. Por la regla de Cramer, las coordenadas de $P := P_r$ están en K_{n-1} y la cadena de cuerpos para el punto P_{r-1} también nos sirve para $P = P_r$, y se cumple $(*)$.

(ii) El punto P_r es la intersección de una recta que pasa por dos puntos del conjunto S cuyas coordenadas pertenecen a K_{n-1} y una circunferencia de centro un punto del conjunto S y radio r igual a la distancia entre dos puntos de S. Por tanto, las coordenadas de P_r son las soluciones de un sistema de ecuaciones del tipo

$$\begin{cases} a_1\mathtt{x} + b_1\mathtt{y} = c_1, \\ (\mathtt{x} - a_2)^2 + (\mathtt{y} - b_2)^2 = r^2, \end{cases}$$

cuyos coeficientes pertenecen a K_{n-1}. Un cálculo directo muestra que las soluciones del sistema anterior pertenecen a una extensión K_n de K_{n-1} de grado ≤ 2 de K_{n-1}, luego se cumple $(*)$.

(iii) El punto P_r es la intersección de dos circunferencias cuyos centros pertenecen al conjunto S y cuyos radios r_1 y r_2 son las distancias entre dos pares de puntos de S. Por tanto, las coordenadas de P_r son las soluciones de un sistema

de ecuaciones del tipo

$$\begin{cases} (\mathtt{x}-a_1)^2+(\mathtt{y}-b_1)^2=r_1^2, \\ (\mathtt{x}-a_2)^2+(\mathtt{y}-b_2)^2=r_2^2, \end{cases}$$

cuyos coeficientes pertenecen a K_{n-1}. Si restamos las dos ecuaciones anteriores obtenemos un sistema equivalente al anterior del tipo

$$\begin{cases} a_3\mathtt{x}+b_3\mathtt{y}=c_3, \\ (\mathtt{x}-a_2)^2+(\mathtt{y}-b_2)^2=r^2, \end{cases}$$

cuyos coeficientes pertenecen a K_{n-1}. En términos geométricos, hemos remplazado la intersección de dos circunferencias por la intersección de una de ellas con el eje radical de ambas. Estamos así en el caso anterior, y se cumple $(*)$.

Recíprocamente, supongamos que existe una torre de cuerpos en las condiciones del enunciado y vamos a demostrar, por inducción sobre n, que α es constructible. Esto es claro si $n=0$, pues entonces $\alpha\in\mathbb{Q}$, luego es constructible en virtud del Lema VII.2.7.

Supongamos el resultado cierto para $n-1$ y veamos que también es cierto para n. Por hipótesis de inducción todos los elementos de K_{n-1} son constructibles. Como $K_n|K_{n-1}$ es una extensión de grado 2 existe $\lambda\in K_{n-1}$ tal que $K_n:=K_{n-1}(\sqrt{\lambda})$. De este modo, existen $a,b\in K_{n-1}$ tales que $\alpha=a+b\sqrt{\lambda}$. Se deduce por tanto de VII.2.7 y VII.2.8 y la hipótesis de inducción, que el número α es constructible. □

2.b. Los tres problemas délicos Abordamos a continuación los problemas cuya solución anunciamos al principio de la sección.

Teorema VII.2.10 (Cuadratura del círculo.) No es constructible únicamente con regla y compás un cuadrado cuyo área coincida con la de un círculo dado.

Demostración. Si se pudiese construir un cuadrado cuyo área fuese igual a la del círculo de centro $(0,0)$ y radio 1, la longitud α del lado de dicho cuadrado sería, por el Teorema VII.2.9, un número algebraico sobre $\mathbb{Q}$ tal que $\alpha^2=\pi$. Pero entonces también π sería algebraico sobre $\mathbb{Q}$, lo que contradice el Teorema de Lindemann B.7. □

Teorema VII.2.11 (Duplicación del cubo.) Empleando únicamente regla y compás no es constructible un cubo cuyo volumen sea el doble del volumen de otro cubo dado.

Demostración. Como el cubo de volumen 1 es constructible, basta demostrar que el cubo de volumen 2 no es constructible. En caso contrario la longitud $\alpha := \sqrt[3]{2}$ del lado de dicho cubo sería un número constructible, y se deduce del Teorema VII.2.9 que existe una extensión $L|\mathbb{Q}$ cuyo grado es potencia de 2, digamos 2^r, tal que $\alpha \in L$. Como el polinomio mínimo de α sobre $\mathbb{Q}$ es, por el Criterio de Eisenstein, $\mathtt{t}^3 - 2$, se tiene $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ y, por tanto,

$$2^r = [L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 \cdot [L : \mathbb{Q}(\alpha)],$$

luego 3 divide a 2^r, y esto es una contradicción. □

Se dice que un ángulo α es *constructible* si lo es el punto $(\cos\alpha,\ \operatorname{sen}\alpha)$, es decir, si los números reales $\cos\alpha$ y $\operatorname{sen}\alpha$ son constructibles. De hecho, como $\operatorname{sen}\alpha = \pm\sqrt{1-\cos^2\alpha}$, la constructibilidad del ángulo α es equivalente a la constructibilidad del número real $\cos\alpha$.

Teorema VII.2.12 (Trisección del ángulo.) El ángulo $\pi/3$ no se puede trisecar empleando, únicamente, regla y compás.

Demostración. Si el ángulo $\beta := \pi/3$ fuese trisecable mediante regla y compás, el ángulo $\alpha := \pi/9$ sería constructible y, por tanto, también lo sería $u := \cos\alpha$. Vamos a calcular el polinomio mínimo de u. Utilizando las Fórmulas de De Moivre y denotando $i := \sqrt{-1}$ deducimos que

$$(\cos\alpha + i\operatorname{sen}\alpha)^3 = \cos 3\alpha + i\operatorname{sen} 3\alpha = \cos\beta + i\operatorname{sen}\beta = (1+\sqrt{3}i)/2,$$

e igualando las partes reales de ambos miembros resulta,

$$\begin{aligned} 1/2 = \cos^3\alpha - 3\cos\alpha\operatorname{sen}^2\alpha &= \cos^3\alpha - 3\cos\alpha(1-\cos^2\alpha) \\ &= 4\cos^3\alpha - 3\cos\alpha = 4u^3 - 3u. \end{aligned}$$

Por tanto u es raíz del polinomio $8\mathtt{t}^3 - 6\mathtt{t} - 1$, que es irreducible en $\mathbb{Z}[\mathtt{t}]$, luego el polinomio mínimo de u sobre $\mathbb{Q}$ es $P_{\mathbb{Q},u}(\mathtt{t}) = \mathtt{t}^3 - (3/4)\mathtt{t} - 1/8$ y, en particular, $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. Como estamos suponiendo que u es constructible existe, por el Teorema VII.2.9, una extensión $L|\mathbb{Q}$ de grado potencia de 2, digamos 2^r, tal que $u \in L$, por lo que

$$2^r = [L : \mathbb{Q}] = [L : \mathbb{Q}(u)] \cdot [\mathbb{Q}(u) : \mathbb{Q}] = 3 \cdot [L : \mathbb{Q}(u)],$$

luego $3|2^r$ y esto es una contradicción. □

2.c. Polígonos constructibles con regla y compás Para terminar éste capítulo presentamos un resultado debido a Gauss. En el mismo se determina para qué valores del entero $n \geq 3$ el polígono regular de n lados es *constructible,* es decir, para qué valores de n el ángulo central $2\pi/n$ de dicho polígono es constructible. Obtenemos el resultado en varias etapas.

Lema VII.2.13 *Para cada entero $r \geq 2$ el ángulo $2\pi/2^r$ es constructible.*

Demostración. Probamos el resultado por inducción sobre r. Para $r = 2$ es evidente, pues basta construir, empleando VII.2.2, dos rectas perpendiculares. Supongamos probado el resultado para $r-1$. Entonces el ángulo $\alpha := 2\pi/2^{r-1}$ sería constructible, y esto implica, por bisección, VII.2.3, la constructibilidad del ángulo $\alpha/2 = 2\pi/2^r$. □

Lema VII.2.14 *Sean m y n dos enteros positivos primos entre sí. Entonces, el ángulo $2\pi/mn$ es constructible si y sólo si los ángulos $2\pi/m$ y $2\pi/n$ son constructibles.*

Demostración. Recordemos que dados ángulos α y β se cumple la igualdad

$$\cos(\alpha + \beta) = \cos\alpha\cos\beta - \operatorname{sen}\alpha\operatorname{sen}\beta.$$

Esto implica, por el Lema VII.2.7, que si α y β son ángulos constructibles, entonces $\alpha + \beta$ también lo es. En particular, si el ángulo α es constructible y $r \in \mathbb{Z}$ también $r\alpha$ es constructible. Por ello, si el ángulo $2\pi/nm$ es constructible, también son constructibles los ángulos

$$2\pi/m = n(2\pi/nm) \quad \& \quad 2\pi/n = m(2\pi/nm).$$

Recíprocamente, si m y n son primos entre sí existen, por la Identidad de Bézout, III.1.7, vol. II, enteros $r, s \in \mathbb{Z}$ tales que $rn+sm = 1$. En consecuencia,

$$2\pi/nm = 2\pi(rn + sm)/mn = r(2\pi/m) + s(2\pi/n).$$

Así, si $2\pi/m$ y $2\pi/n$ son constructibles, entonces $2\pi/nm$ también lo es. □

El siguiente lema es mucho más general de lo que necesitamos, pero tiene interés por sí mismo.

Lema VII.2.15 *Sean $n > 2$ y $k > 0$ dos enteros primos entre sí. Los números $c := 2\cos 2k\pi/n$ y $s := 2\operatorname{sen} 2k\pi/n$ son algebraicos sobre $\mathbb{Q}$. Además, si φ denota la función de Euler se tiene*

$$[\mathbb{Q}(c):\mathbb{Q}] = \varphi(n)/2 \quad \& \quad [\mathbb{Q}(s):\mathbb{Q}] = \begin{cases} \varphi(n) & \text{si } n \notin 4\mathbb{Z} \\ \varphi(n)/4 & \text{si } n \equiv 4 \bmod 8 \\ \varphi(n)/2 & \text{si } n \equiv 0 \bmod 8 \end{cases}$$

Demostración. Sea $\zeta = e^{2\pi i k/n}$, que por ser raíz primitiva n-ésima de la unidad es raíz del n-ésimo polinomio ciclotómico Φ_n. Éste es un polinomio mónico e irreducible en $\mathbb{Z}[\mathtt{t}]$, según vimos en el Teorema VI.1.11, cuyo grado $d := \varphi(n)$ es par. Obsérvese que $\overline{\zeta} = \zeta^{-1}$ es también raíz primitiva n-ésima de la unidad, por lo que Φ_n es el polinomio mínimo de ζ^{-1} sobre $\mathbb{Q}$, y $c = \zeta + \zeta^{-1}$. Ahora bien, ζ^{-1} es raíz del polinomio $\mathtt{t}^d\Phi_n(1/\mathtt{t}) \in \mathbb{Z}[\mathtt{t}]$, que tiene grado d, y es mónico pues vimos en la Proposición VI.1.10 que $\Phi_n(0) = 1$. Por ello, $\Phi_n(\mathtt{t}) = \mathtt{t}^d\Phi_n(1/\mathtt{t})$, lo que significa que existen enteros $a_0 = 1, a_1, \ldots, a_{d/2}$ tales que

$$\Phi_n(\mathtt{t}) = a_{d/2}\mathtt{t}^{d/2} + \sum_{j=0}^{d/2-1} a_j(\mathtt{t}^{d-j} + \mathtt{t}^j),$$

y por tanto,

$$\mathtt{t}^{-d/2}\Phi_n(\mathtt{t}) = a_{d/2} + \sum_{j=0}^{d/2-1} a_j(\mathtt{t}^{d/2-j} + \mathtt{t}^{j-d/2}). \tag{2.9}$$

Comprobemos que para cada entero positivo k existe un polinomio $p_k(\mathtt{x}) \in \mathbb{Z}[\mathtt{x}]$ de grado k tal que $\mathtt{t}^k + \mathtt{t}^{-k} = p_k(\mathtt{t} + \mathtt{t}^{-1})$. Para $k = 1$ basta elegir $p_1(\mathtt{x}) = \mathtt{x}$, y se demuestra por inducción sobre k observando que

$$\begin{aligned} \mathtt{t}^k + \mathtt{t}^{-k} &= (\mathtt{t} + \mathtt{t}^{-1})(\mathtt{t}^{k-1} + \mathtt{t}^{-(k-1)}) - (\mathtt{t}^{k-2} + \mathtt{t}^{-(k-2)}) \\ &= (\mathtt{t} + \mathtt{t}^{-1})p_{k-1}(\mathtt{t} + \mathtt{t}^{-1}) - p_{k-2}(\mathtt{t} + \mathtt{t}^{-1}), \end{aligned}$$

y basta elegir $p_k(\mathtt{x}) = \mathtt{x}p_{k-1}(\mathtt{x}) - p_{k-2}(\mathtt{x})$. Sustituyendo en la igualdad (2.9),

$$\mathtt{t}^{-d/2}\Phi_n(\mathtt{t}) = a_{d/2} + \sum_{j=0}^{d/2-1} a_j p_{d/2-j}(\mathtt{t} + \mathtt{t}^{-1}).$$

Esto significa que el polinomio

$$\psi_n(\mathtt{x}) := a_{d/2} + \sum_{j=0}^{d/2-1} a_j p_{d/2-j}(\mathtt{x}) \in \mathbb{Z}[\mathtt{x}],$$

cuyo grado es $d/2$, cumple $\mathtt{t}^{-d/2}\Phi_n(\mathtt{t}) = \psi_n(\mathtt{t}+\mathtt{t}^{-1})$. En particular, al evaluar en $\mathtt{t} = \zeta$ resulta

$$0 = \zeta^{-d/2}\Phi_n(\zeta) = \psi_n(\zeta + \zeta^{-1}) = \psi_n(c),$$

por lo que basta demostrar que ψ_n es irreducible en $\mathbb{Q}[\mathtt{t}]$ para deducir que

$$[\mathbb{Q}(c) : \mathbb{Q}] = \deg(\psi_n) = d/2 = \varphi(n)/2.$$

Supongamos, por reducción al absurdo, que ψ_n es reducible en $\mathbb{Q}[\mathtt{t}]$. Existen por ello polinomios $g, h \in \mathbb{Q}[\mathtt{t}]$ de grados $d_1 \geq 1$ y $d/2 - d_1 \geq 1$, respectivamente, tales que $\psi_n = gh$, por lo que

$$\Phi_n(\mathtt{t}) = \mathtt{t}^{d/2}\psi_n(\mathtt{t} + \mathtt{t}^{-1}) = \mathtt{t}^{d_1}g(\mathtt{t} + \mathtt{t}^{-1})\mathtt{t}^{d/2-d_1}h(\mathtt{t} + \mathtt{t}^{-1})$$

de modo que

$$g_1(\mathtt{t}) = \mathtt{t}^{d_1}g(\mathtt{t} + \mathtt{t}^{-1}) \in \mathbb{Q}[\mathtt{t}] \quad \& \quad h_1(\mathtt{t}) = \mathtt{t}^{d/2-d_1}h(\mathtt{t} + \mathtt{t}^{-1}) \in \mathbb{Q}[\mathtt{t}]$$

son polinomios de grados $2d_1 \geq 2$ y $2d - 2d_1 \geq 2$ y $\Phi_n(\mathtt{t}) = g_1(\mathtt{t})h_1(\mathtt{t})$, lo que contradice la irreducibilidad de $\Phi_n(\mathtt{t})$.

Para calcular el grado de la extensión $\mathbb{Q}(s)|\mathbb{Q}$ observamos que

$$\operatorname{sen} 2k\pi/n = \cos(\pi/2 - 2k\pi/n) = \cos(2k\pi/n - \pi/2) = \cos 2\pi(4k-n)/4n,$$

y se trata de simplificar la fracción $(4k-n)/4n$ y aplicar lo probado anteriormente. Para ello distinguimos cuatro casos. Denotemos $d := \operatorname{mcd}(4n, 4k-n)$.

Caso 1. Supongamos que n es impar. Entonces $4n$ y $4k-n$ son primos entre sí, pues como $4k-n$ es impar también lo es d, que por tanto divide a n y a $4k-n$, luego divide a n y k, que son primos entre sí. En consecuencia la fracción $(4k-n)/4n$ es irreducible, y por lo ya visto,

$$[\mathbb{Q}(s) : \mathbb{Q}] = \varphi(4n)/2 = \varphi(4)\varphi(n)/2 = \varphi(n).$$

Caso 2. Supongamos que $n \equiv 2 \bmod 4$. Escribimos $n = 2m$ con m impar, y

$$d = \operatorname{mcd}(4n, 2(2k-m)) = 2\operatorname{mcd}(2n, 2k-m) = 2\operatorname{mcd}(4m, 2k-m) = 2,$$

pues $\operatorname{mcd}(4m, 2k-m) = 1$. En efecto, como $2k-m$ es impar, todo divisor común ℓ de $4m$ y $2k-m$ es impar, luego divide a m, así que divide a k y m, luego vale 1. Así, $(4k-n)/4n = (2k-m)/2n$ y $\operatorname{mcd}(2k-m, 2n) = 1$ y

$$[\mathbb{Q}(s) : \mathbb{Q}] = \varphi(2n)/2 = \varphi(4m)/2 = 2\varphi(m)/2 = \varphi(m) = \varphi(n).$$

Caso 3. Supongamos que $n \equiv 4 \bmod 8$. Entonces $n = 4m$ con m impar, y también k es impar ya que $\mathrm{mcd}(k, n) = 1$. Existen por ello enteros r y t tales que $m = 2r + 1$ y $k = 2t + 1$. Así,

$$(4k - n)/4n = (4k - 4m)/4n = (k - m)/n = 2(t - r)/4m = (t - r)/2m.$$

Observamos que $t - r$ y m son primos entre sí, pues si ℓ es un divisor común, también dividiría a $2(t - r) = k - m$ y a m, luego dividiría a k y a n, así que $\ell = 1$. Por tanto $\mathrm{mcd}(t - r, 2m) \in \{1, 2\}$, lo que implica, puesto que $\varphi(m) = \varphi(2m)$ y $\varphi(n) = \varphi(4m) = 2\varphi(m)$, que

$$[\mathbb{Q}(s) : \mathbb{Q}] = \varphi(m)/2 = \varphi(n)/4.$$

Caso 4. Supongamos que $n \equiv 0 \bmod 8$. En particular k es impar y existe un entero m tal que $n = 8m$. Entonces

$$(4k - n)/4n = (4k - 8m)/32m = (k - 2m)/8m.$$

Como k es impar también $k - 2m$ lo es, por lo que $\ell := \mathrm{mcd}(k - 2m, 8m)$ es impar, así que $\ell | m$ y a $\ell | (k - 2m)$, por lo que ℓ divide a $\mathrm{mcd}(k, m) = 1$. Así,

$$[\mathbb{Q}(s) : \mathbb{Q}] = \varphi(8m)/2 = \varphi(n)/2.$$

□

Observación VII.2.16 La prueba del Lema anterior proporciona un procedimiento recursivo para calcular los polinomios mínimos sobre $\mathbb{Q}$ de $\cos 2k\pi/n$ y $\operatorname{sen} 2k\pi/n$ cuando k y n son primos entre sí.

Lema VII.2.17 *Sean p un primo impar, k un entero positivo y $n := p^k$. Entonces, el ángulo $2\pi/n$ es constructible si y sólo si $k = 1$ y $p := 2^{2^r} + 1$ para cierto entero $r \geq 0$.*

Demostración. Suponemos en primer lugar que el ángulo $2\pi/n$ es constructible, es decir, el número real $c_n := \cos 2\pi/n$ es constructible, lo que por el Teorema VII.2.9 implica que existe un entero $\ell \geq 1$ tal que $[\mathbb{Q}(c_n) : \mathbb{Q}] = 2^{\ell-1}$. Entonces, en virtud del Lema VII.2.15 y denotando $\varphi : \mathbb{N} \to \mathbb{N}$ la función de Euler,

$$p^{k-1}(p - 1) = \varphi(n) = 2[\mathbb{Q}(c_n) : \mathbb{Q}] = 2^\ell,$$

En consecuencia, $k = 1$ y $p = 2^\ell + 1$. Para terminar la demostración de esta implicación es suficiente comprobar que también el exponente ℓ es una potencia

de 2. En caso contrario, existe un primo impar q que divide a ℓ y podemos escribir $\ell := qm$ para cierto entero m. Como q es impar se tiene

$$\mathtt{t}^q + 1 = (\mathtt{t}+1)\sum_{j=0}^{q-1}(-1)^j\mathtt{t}^j$$

y por tanto

$$p = 2^\ell + 1 = 2^{mq} + 1 = (2^m+1)\sum_{j=0}^{q-1}(-1)^j 2^{mj},$$

lo que es imposible porque p es un número primo y $1 < 2^m + 1 < p$. Existe por tanto un entero $r \geq 0$ tal que $\ell = 2^r$ y, en consecuencia, $p = 2^{2^r} + 1$.

Recíprocamente, suponemos que el número primo $p = 2^\ell + 1$ para cierto entero $\ell \geq 1$ y hemos de probar que $c := \cos(2\pi/p)$ es constructible. Denotamos $s := \operatorname{sen}(2\pi/p)$, $i := \sqrt{-1}$ y consideramos $\zeta := c + is \in \mathbb{C}$, que es una raíz primitiva p-ésima de la unidad. Por el Teorema VI.1.11, $\mathbb{Q}(\zeta)|\mathbb{Q}$ es una extensión de Galois, cuyo grupo de Galois es isomorfo al grupo cíclico $\mathbb{Z}_p^*$, cuyo orden es $p - 1 = 2^\ell$. Además $c = (\zeta + \zeta^{-1})/2 \in \mathbb{Q}(\zeta)$, así que tenemos una torre de cuerpos $\mathbb{Q} \subset \mathbb{Q}(c) \subset \mathbb{Q}(\zeta)$ y, como el grupo $G\big(\mathbb{Q}(\zeta) : \mathbb{Q}\big) = \mathbb{Z}_p^*$ es cíclico, su subgrupo $G(\mathbb{Q}(\zeta) : \mathbb{Q}(c))$ es normal. Esto implica, por la segunda parte del Teorema fundamental de la teoría de Galois, que la extensión $\mathbb{Q}(c)|\mathbb{Q}$ es de Galois y

$$G(\mathbb{Q}(c) : \mathbb{Q}) \cong G(\mathbb{Q}(\zeta) : \mathbb{Q})/G(\mathbb{Q}(\zeta) : \mathbb{Q}(c)).$$

En particular $G(\mathbb{Q}(c) : \mathbb{Q})$ es un grupo cíclico y su orden es, por el Lema VII.2.15, $[\mathbb{Q}(c) : \mathbb{Q}] = \varphi(p)/2 = 2^{\ell-1}$. Se deduce de la Proposición I.2.8, vol. I, que para $0 \leq j \leq \ell - 1$ el grupo $G(\mathbb{Q}(c) : \mathbb{Q})$ posee un único subgrupo H_j de orden $2^{\ell-1-j}$ y $H_{j+1} \subsetneq H_j$. Se tiene así una torre de cuerpos

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_{\ell-1} = \mathbb{Q}(c),$$

donde cada $K_j := \operatorname{Fix}(H_j)$ y cada extensión $K_{j+1}|K_j$ tiene grado 2. Esto implica, por el Teorema VII.2.9, que $c = \cos(2\pi/p)$ es constructible. □

Corolario VII.2.18 *Sea $n \geq 3$ un entero positivo. Entonces, el ángulo $2\pi/n$ es constructible si y sólo si n es potencia de 2 o $n := 2^r p_1 \cdots p_k$, donde r es un entero no negativo y $p_1, \ldots, p_k$ son números primos de la forma $p_j := 2^{2^{r_j}} + 1$ donde r_j es un entero no negativo para $1 \leq j \leq k$.*

Demostración. En virtud del Lema VII.2.13 el ángulo $2\pi/2^\ell$ es constructible para cada entero $\ell \geq 1$. Supongamos ahora que $n := 2^r p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, donde $r \geq 0$ y cada $\alpha_j \geq 1$ son números enteros. Si el ángulo $2\pi/n$ es constructible se deduce de VII.2.14 que cada ángulo $2\pi/p_j^{\alpha_j}$ es también constructible. Esto implica, en virtud del Lema VII.2.17, que cada $\alpha_j := 1$ y $p_j := 2^{2^{r_j}} + 1$ para algún entero no negativo r_j.

Recíprocamente, si $n := 2^r p_1 \cdots p_k$ y los números primos $p_1, \ldots, p_k$ cumplen la condición del enunciado, se desprende de VII.2.13 y VII.2.17 que los ángulos $2\pi/2^r$ y $2\pi/p_j$ son constructibles. Aplicando ahora el Lema VII.2.14 se concluye que el ángulo $2\pi/n$ es constructible. □

Ejemplos VII.2.19 (1) Se deduce de VII.2.17, con mucha paciencia, que los únicos números primos $p < 10^{40000}$ para los que se puede construir, únicamente con regla y compás, el polígono regular de p lados, son los siguientes:

$$3 = 2^{2^0} + 1, \;\; 5 = 2^{2^1} + 1, \;\; 17 = 2^{2^2} + 1, \;\; 257 = 2^{2^3} + 1 \quad \& \quad 65537 = 2^{2^4} + 1.$$

(2) **Construcción de un pentágono regular.** Comenzamos expresando *mediante radicales* $a := \cos(2\pi/5)$. Denotamos $b := \operatorname{sen}(2\pi/5)$ e $i := \sqrt{-1}$, y así $\zeta := a + bi$ es una raíz primitiva quinta de la unidad, luego $1 = \zeta^5 = (a + ib)^5$. Empleando la Fórmula del binomio de Newton e igualando las partes reales de ambos miembros se tiene $a^5 - 10a^3b^2 + 5ab^4 = 1$. Como $a^2 + b^2 = 1$ deducimos

$$a^5 - 10a^3(1 - a^2) + 5a(1 - a^2)^2 - 1 = 0.$$

Por tanto, $a \neq 1$ es una de las raíces del polinomio

$$f(\mathtt{t}) := 16\mathtt{t}^5 - 20\mathtt{t}^3 + 5\mathtt{t} - 1 = (\mathtt{t} - 1)(4\mathtt{t}^2 + 2\mathtt{t} - 1)^2,$$

y así, dado que $a > 0$, se tiene $a := (\sqrt{5} - 1)/4$.

Veamos ahora cómo se construye un pentágono regular inscrito en una circunferencia de radio 1. Consideramos los puntos $O := (0, 0)$, $E_1 := (1, 0)$ y la circunferencia Γ de centro O y radio 1. Sean e_1 la recta que pasa por O y E_1 y e_2 la recta perpendicular a e_1 que pasa por O. La circunferencia Γ corta a e_1 en los puntos E_1 y $E_3 := (-1, 0)$ y a e_2 en los puntos $E_2 := (0, 1)$ y $E_4 := (0, -1)$. Sea $M_1 := (-1/2, 0)$ el punto medio del segmento que une los puntos O y E_3. Consideramos la circunferencia Γ_1 de centro M_1 y cuyo radio es la distancia entre M_1 y E_2, que vale $\lambda := \sqrt{1 + 1/4} = \sqrt{5}/2$.

Esta circunferencia corta a e_1 en los puntos $A_1 := ((\sqrt{5}-1)/2, 0)$ y $A_2 := (-(\sqrt{5}+1)/2, 0)$. Denotamos $M_2 := ((\sqrt{5}-1)/4, 0)$ el punto medio del segmento que une O con A_1. Consideramos la recta r perpendicular a e_1 que pasa por M_2. Esta recta r corta a la circunferencia Γ en los puntos $V_2 := (a, b)$ y $V_5 := (a, -b)$. Sean Γ_2 la circunferencia de centro V_2 y radio la distancia de V_2 al punto E_1, y Γ_3 la circunferencia de centro V_5 y radio la distancia de V_5 al punto E_1. Estas circunferencias cortan a Γ en los pares de puntos E_1, V_3 y E_1, V_4, respectivamente. El polígono de vértices E_1, V_2, V_3, V_4, V_5 es el pentágono regular buscado.

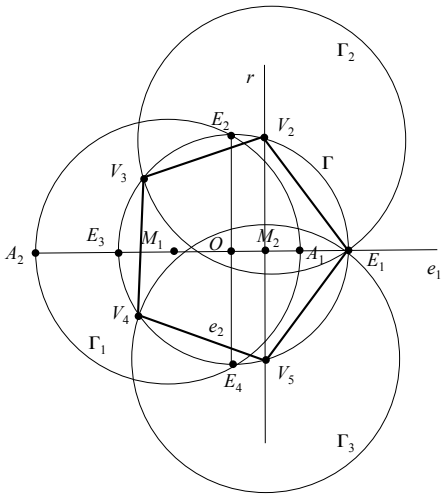


Figura 2.7: **Construcción de un pentágono regular**

Ejercicios y problemas propuestos

Número VII.1 Sean K un cuerpo y los polinomios de $K[\mathtt{t}]$ de grado n

$$f(\mathtt{t}) := \sum_{i=0}^{n} a_i \mathtt{t}^i \quad \& \quad g(\mathtt{t}) := \sum_{i=0}^{n} a_{n-i} \mathtt{t}^i.$$

Demostrar que f es resoluble por radicales sobre K si y sólo si g lo es.

Número VII.2 (1) Estudiar si el polinomio $f(\mathtt{t}) := \mathtt{t}^6 - 3\mathtt{t}^4 + 6\mathtt{t}^2 - 3$ es resoluble por radicales.

(2) Sea $\alpha \in \mathbb{C}$ una raíz de f. Calcular el polinomio mínimo de $\alpha^2 - 1$ sobre $\mathbb{Q}$.

Número VII.3 Sean $f, g \in \mathbb{Q}[\mathtt{t}]$ dos polinomios resolubles por radicales.

(1) ¿Se puede asegurar que también $f + g$ es resoluble por radicales?

(2) ¿Se puede asegurar que fg es resoluble por radicales?

Número VII.4 Sean $\xi := e^{2\pi i/7}$ y $L := \mathbb{Q}(\xi)$.

(1) ¿Cuántas subextensiones de grado dos posee la extensión $L|\mathbb{Q}$? Obtener elementos primitivos de dichas subextensiones y los polinomios mínimos sobre $\mathbb{Q}$ de dichos elementos.

(2) ¿Contiene L a $i := \sqrt{-1}$? Sea $\gamma := e^{\pi i/7}$. Demostrar que $\mathbb{Q}(\xi) = \mathbb{Q}(\gamma)$.

(3) ¿Es resoluble por radicales sobre $\mathbb{Q}$ el polinomio $h(\mathtt{t}) := \mathtt{t}^6 - \mathtt{t}^5 + \mathtt{t}^4 - \mathtt{t}^3 + \mathtt{t}^2 - \mathtt{t} + 1$?

Número VII.5 Sean K un cuerpo de característica 0 y $a, b, c, d \in K$. ¿Es resoluble por radicales sobre K el polinomio

$$f(\mathtt{t}) := \mathtt{t}^8 + a\mathtt{t}^7 + b\mathtt{t}^6 + c\mathtt{t}^5 + d\mathtt{t}^4 + c\mathtt{t}^3 + b\mathtt{t}^2 + a\mathtt{t} + 1?$$

Número VII.6 (1) Sea $f \in \mathbb{Q}[\mathtt{t}]$ un polinomio irreducible cuyo grado es un número primo. Supongamos que f posee al menos dos raíces reales y alguna raíz en $\mathbb{C} \setminus \mathbb{R}$. ¿Es f resoluble por radicales sobre $\mathbb{Q}$?

(2) Sean $p \equiv 1 \bmod 4$ un número primo y $f \in \mathbb{Q}[\mathtt{t}]$ un polinomio irreducible de grado p cuyo discriminante es negativo. Probar que f no es resoluble por radicales sobre $\mathbb{Q}$.

Número VII.7 (1) Sean K un cuerpo de característica 0 y $a, b \in K$ tales que $a \neq 0$ y $f(\mathtt{t}) := \mathtt{t}^5 + a\mathtt{t} + b$ es irreducible en $K[\mathtt{t}]$. Probar que f es resoluble por radicales sobre K si y sólo si existen $u, v \in K$ tales que

$$a = \frac{3125uv^4}{(u-1)^4(u^2-6u+25)} \quad \& \quad b = \frac{3125uv^5}{(u-1)^4(u^2-6u+25)}.$$

(2) Sean $p \equiv 3 \bmod 4$ un número primo y $f(\mathtt{t}) := \mathtt{t}^5 + 2p\mathtt{t} + 2p^2$. ¿Es f resoluble por radicales sobre $\mathbb{Q}$?

Número VII.8 Sean $\mathtt{x}, \mathtt{y}$ indeterminadas sobre $\mathbb{Q}$ y el polinomio

$$f(\mathtt{t}) := \mathtt{t}^5 + \frac{5\mathtt{y}^4(\mathtt{x}^2+1)^2(\mathtt{x}^2+\mathtt{x}-1)(\mathtt{x}^2-\mathtt{x}-1)}{4}\mathtt{t} + \frac{\mathtt{y}^5(\mathtt{x}^2+1)^3(\mathtt{x}^2+\mathtt{x}-1)(2\mathtt{x}-1)(\mathtt{x}+2)}{2}.$$

Demostrar que el grupo de Galois sobre $K := \mathbb{Q}(\mathtt{x}, \mathtt{y})$ del polinomio $f \in K[\mathtt{t}]$ es resoluble.

Número VII.9 Sean $K := \mathbb{Q}(\mathtt{x})$ y $f(\mathtt{t}) := \mathtt{t}^5 + 5(5\mathtt{x}^2 - 1)\mathtt{t} + 4(5\mathtt{x}^2 - 1)$. Calcular el grupo de Galois $G_K(f)$.

Número VII.10 Sean K un cuerpo de característica 0 y $\mathtt{t}, \mathtt{x}_1, \ldots, \mathtt{x}_n$ indeterminadas sobre K. Denotamos $\mathtt{s}_1, \ldots, \mathtt{s}_n$ las formas simétricas elementales en las indeterminadas $\mathtt{x}_1, \ldots, \mathtt{x}_n$ y consideramos el polinomio

$$f(\mathtt{t}) := \mathtt{t}^n + \sum_{j=0}^{n-1} (-1)^{n-j} \mathtt{s}_{n-j} \mathtt{t}^j = \prod_{k=1}^{n} (\mathtt{t} - \mathtt{x}_k)$$

y el cuerpo $L := K(\mathtt{s}_1, \ldots, \mathtt{s}_n)$. Demostrar que si $c_1, \ldots, c_n$ son elementos de K distintos dos a dos y $E := K(\mathtt{x}_1, \ldots, \mathtt{x}_n)$, entonces $u := \sum_{k=1}^{n} c_k \mathtt{x}_k$ es un elemento primitivo de la extensión $E|L$.

Número VII.11 (Lema de Artin) Sean G un grupo y K un cuerpo. Un *carácter* de G a valores en K es un homomorfismo de grupos $\chi : G \to K^* = K \setminus \{0\}$.

(1) Probar que cualesquiera caracteres $\chi_1, \ldots, \chi_n$ de G a valores en K distintos dos a dos son linealmente independientes sobre K, o sea, para cada n-upla $(a_1, \ldots, a_n) \in K^n$ donde algún $a_i \neq 0$ existe $g \in G$ tal que

$$\sum_{k=1}^{n} a_k \chi_k(g) \neq 0.$$

(2) Sean $\alpha_1, \ldots, \alpha_\ell \in K$ no nulos y distintos dos a dos y $a_1, \ldots, a_\ell \in K$ tales que

$$\sum_{k=1}^{\ell} a_k \alpha_k^n = 0 \quad \forall\, n \in \mathbb{Z}.$$

Demostrar que $a_k = 0$ para $1 \leq k \leq \ell$.

Número VII.12 Sean K un cuerpo con q elementos y $\mathtt{t}$ una indeterminada sobre K.

(1) Calcular el orden del grupo de Galois $G(K(\mathtt{t}) : K)$.

(2) Para cada $a \in K^* = K \setminus \{0\}$ consideramos los K-automorfismos

$$\phi_a : K(\mathtt{t}) \to K(\mathtt{t}),\ \mathtt{t} \mapsto a\mathtt{t} \quad \& \quad \psi_a : K(\mathtt{t}) \to K(\mathtt{t}),\ \mathtt{t} \mapsto \mathtt{t} + a.$$

Sea $\gamma \in G\big(K(\mathtt{t}) : K\big)$ definido por $\gamma(\mathtt{t}) := 1/\mathtt{t}$. Demostrar que el grupo $G(K(\mathtt{t}) : K)$ está generado por el conjunto $S := \{\gamma, \phi_a, \psi_a : a \in K^*\}$.

(3) Sean L el cuerpo fijo de $G\big(K(\mathtt{t}) : K\big)$ y

$$u := \frac{(\mathtt{t}^{q^2} - \mathtt{t})^{q+1}}{(\mathtt{t}^q - \mathtt{t})^{q^2+1}}.$$

Demostrar que u es un elemento primitivo de la extensión $L|K$.

Número VII.13 (Ternas pitagóricas) Emplear el Teorema 90 de Hilbert para demostrar que una terna (x, y, z) de números enteros no nulos primos dos a dos cumple $x^2 + y^2 = z^2$ si y sólo si existen $s, m, n \in \mathbb{Z}$ tales que $(sx, sy, sz) = (m^2 - n^2, 2mn, m^2 + n^2)$.

Número VII.14 (Forma aditiva del Teorema 90 de Hilbert) (1) Sean $L|K$ una extensión de Galois y $x \in L$. Se llama *traza* de x a

$$\mathsf{T}(x) := \sum_{\sigma \in G(L:K)} \sigma(x).$$

Demostrar que $\mathsf{T}(x) \in K$.

(2) Supongamos que $\mathrm{char}(K) = 0$ y que el grupo de Galois $G(L : K) := \langle \sigma \rangle$ es cíclico. Probar que la traza de un elemento $x \in L$ es nula si y sólo si existe $\alpha \in L$ tal que $x = \alpha - \sigma(\alpha)$.

Número VII.15 (Teorema de la base normal) Sean K un cuerpo de característica 0 y $L|K$ una extensión de Galois cuyo grupo de Galois es $G(L:K) := \{\sigma_1, \ldots, \sigma_n\}$.

(1) Probar que existe $u \in L$ tal que la matriz $A := (a_{ij}) \in \mathcal{M}_n(L)$ cuyos coeficientes son $a_{ij} := \sigma_i(\sigma_j^{-1}(u))$ tiene determinante no nulo.

(2) Demostrar que el conjunto $\mathcal{B} := \{\sigma_j(u) : 1 \leq j \leq n\}$ es una base de L como K-espacio vectorial.

Número VII.16 Sean m y n enteros positivos y $M := \operatorname{mcm}(m, n)$ su mínimo común múltiplo. Supongamos que los polígonos regulares de m y n lados son constructibles con regla y compás. Demostrar que también es constructible con regla y compás el polígono con M lados.

Número VII.17 Demostrar que si n es un divisor de $2^{32} - 1$, el polígono regular de n lados es constructible con regla y compás.

Número VII.18 ¿Para qué valores del entero positivo n es trisecable con regla y compás el ángulo $2\pi/n$?

APÉNDICE A

Otra demostración del Teorema Fundamental del Álgebra

En este apéndice empleamos el Teorema II.1.9, que asegura la existencia de cierre algebraico de cualquier cuerpo, y el Teorema Fundamental de los polinomios simétricos, VII.1.16, vol. II, para dar una prueba, distinta de la vista en V.2.13, vol. II, de que el cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado.

Veamos en primer lugar que basta probar que todo polinomio $f \in \mathbb{R}[\mathtt{t}]$ con $\deg(f) \geq 1$ tiene una raíz en $\mathbb{C}$. Supongamos cierta esta afirmación por un momento y sea $g \in \mathbb{C}[\mathtt{t}]$ un polinomio de grado ≥ 1. Denotemos por τ la conjugación de $\mathbb{C}$, es decir, la involución $\tau : \mathbb{C} \to \mathbb{C}$, $a + bi \mapsto a - bi$, donde $i = \sqrt{-1}$, que cumple $\mathbb{R} = \mathrm{Fix}(\tau) := \{z \in \mathbb{C} : \tau(z) = z\}$, y sea $\widehat{\tau}$ el homomorfismo inducido

$$\mathbb{C}[\mathtt{t}] \to \mathbb{C}[\mathtt{t}],\ \sum_{j=0}^{d} \alpha_j \mathtt{t}^j \mapsto \sum_{j=0}^{d} \tau(\alpha_j)\mathtt{t}^j.$$

Veamos que $g\widehat{g} \in \mathbb{R}[\mathtt{t}]$ para cada $g \in \mathbb{C}[\mathtt{t}]$. Si $g(\mathtt{t}) := \sum_{j=0}^{d} \alpha_j \mathtt{t}^j$, entonces $\widehat{g}(\mathtt{t}) = \sum_{j=0}^{d} \tau(\alpha_j)\mathtt{t}^j$, luego

$$g\widehat{g}(\mathtt{t}) = \sum_{j=0}^{e} b_j \mathtt{t}^j,\ \text{con}\ \ b_j = \sum_{\ell=0}^{j} \alpha_\ell \tau(\alpha_{j-\ell}).$$

Así $f = g\widehat{g} \in \mathbb{R}[\mathtt{t}]$, ya que

$$\tau(b_j) = \tau\Big(\sum_{\ell=0}^{j} \alpha_\ell \tau(\alpha_{j-\ell})\Big) = \sum_{\ell=0}^{j} \tau(\alpha_\ell)\alpha_{j-\ell} = \sum_{k=0}^{j} \alpha_k \tau(\alpha_{j-k}) = b_j.$$

Estamos suponiendo que los polinomios con coeficientes en $\mathbb{R}$ tienen alguna raíz compleja, luego existe $u \in \mathbb{C}$ tal que $0 = f(u) = g(u)\widehat{g}(u) = 0$. Si $g(u) = 0$

hemos terminado, mientras que si $g(u) \neq 0$ entonces $\widehat{g}(u) = 0$, así que $\tau(u) \in \mathbb{C}$ es una raíz de g, pues

$$0 = \tau(0) = \tau\big(\widehat{g}(u)\big) = \tau\Big(\sum_{j=0}^{d} \tau(\alpha_j) u^j\Big) = \sum_{j=0}^{d} \alpha_j \tau(u)^j = g(\tau(u)).$$

Por tanto, todo se reduce a probar que cada polinomio $f \in \mathbb{R}[\mathtt{t}]$ tiene alguna raíz en $\mathbb{C}$, y podemos asumir, además, que f es mónico e irreducible en $\mathbb{R}[\mathtt{t}]$, sin más que sustituirlo por cualquiera de sus factores irreducibles mónicos. Denotamos $d := 2^m n$, con n impar, el grado de f y veamos, por inducción sobre m, que f tiene una raíz en $\mathbb{C}$. Para $m = 0$ basta aplicar el Teorema de Bolzano, pues como el grado de f es impar,

$$\lim_{x \to -\infty} f(x) = -\infty \quad \& \quad \lim_{x \to +\infty} f(x) = +\infty.$$

Supongamos ahora el resultado cierto para polinomios mónicos e irreducibles en $\mathbb{R}[\mathtt{t}]$ cuyo grado es de la forma $d' := 2^{m-1} n'$ con n' impar. Como $\mathbb{R}$ tiene característica 0 y $f \in \mathbb{R}[\mathtt{t}]$ es irreducible, las raíces de f en un cierre algebraico $\overline{\mathbb{R}}$ de $\mathbb{R}$ son simples, luego f posee d raíces distintas $\zeta_1, \ldots, \zeta_d$ en $\overline{\mathbb{R}}$. Hemos de probar que alguna de ellas pertenece a $\mathbb{C}$. Para cada entero $s \in \mathbb{Z}$ consideramos el polinomio

$$g_s(\mathtt{t}) := \prod_{1 \leq i < j \leq d} (\mathtt{t} - \zeta_i - \zeta_j - s\zeta_i\zeta_j) \in \overline{\mathbb{R}}[\mathtt{t}],$$

que es simétrico en los símbolos $\zeta_1, \ldots, \zeta_d$. Por el Teorema de los polinomios simétricos elementales, VII.1.16, vol. II, y las Fórmulas de Cardano–Vieta aplicadas a los coeficientes de $f \in \mathbb{R}[\mathtt{t}]$, deducimos que $g_s \in \mathbb{R}[\mathtt{t}]$. Además,

$$\deg(g_s) = d(d-1)/2 = 2^{m-1} n(2^m n - 1) \quad \& \quad n' := n(2^m n - 1) \text{ es impar.}$$

Por hipótesis de inducción, para cada $s \in \mathbb{Z}$ alguna de las raíces de g_s pertenece a $\mathbb{C}$, esto es, para cada $s \in \mathbb{Z}$ existen índices $1 \leq i_s < j_s \leq d$ tales que $\mu_s := \zeta_{i_s} + \zeta_{j_s} - s\zeta_{i_s}\zeta_{j_s} \in \mathbb{C}$. Como $\mathbb{Z}$ no es finito y $M := \{(i,j) : 1 \leq i < j \leq d\}$ sí lo es, la aplicación $\mathbb{Z} \to M$, $s \mapsto (i_s, j_s)$ no es inyectiva, luego existen $r, s \in \mathbb{Z}$ tales que $i_s = i_r$, $j_s = j_r$ y $s \neq r$. Esto implica que,

$$\begin{cases} \zeta_{i_r} + \zeta_{j_r} - r\zeta_{i_r}\zeta_{j_r} = \mu_r \\ \zeta_{i_r} + \zeta_{j_r} - s\zeta_{i_r}\zeta_{j_r} = \mu_s \end{cases}$$

luego $(s-r)\zeta_{i_r}\zeta_{j_r} = \mu_r - \mu_s$. Despejando, $\omega_2 := \zeta_{i_r}\zeta_{j_r} = (\mu_r - \mu_s)/(s-r) \in \mathbb{C}$, por lo que $2\omega_1 = \xi_{i_r} + \xi_{j_r} = \mu_r + r\omega_2 \in \mathbb{C}$. Por tanto, ζ_{i_r} y ζ_{j_r} son las raíces del polinomio

$$h(\mathtt{t}) := (\mathtt{t} - \zeta_{i_r})(\mathtt{t} - \zeta_{j_r}) = \mathtt{t}^2 - (\zeta_{i_r} + \zeta_{j_r})\mathtt{t} + \zeta_{i_r}\zeta_{j_r} = \mathtt{t}^2 - 2\omega_1\mathtt{t} + \omega_2 \in \mathbb{C}[\mathtt{t}],$$

y todo se reduce a demostrar que alguna (y por tanto las dos) de las raíces del polinomio de segundo grado $h \in \mathbb{C}[\mathtt{t}]$ pertenece a $\mathbb{C}$. Dichas raíces son

$$\omega_1 + \sqrt{\omega_1^2 - \omega_2} \quad \& \quad \omega_1 + \sqrt{\omega_1^2 - \omega_2},$$

así que se trata de probar que $\sqrt{\omega_1^2 - \omega_2} \in \mathbb{C}$. Denotando $\omega_1^2 - \omega_2 := a + bi \in \mathbb{C}$, donde $a, b \in \mathbb{R}$, buscamos $x, y \in \mathbb{R}$ tales que $a + bi = (x + yi)^2$, o sea, $a = x^2 - y^2$ y $b = 2xy$.

Si $b = 0$ y $a \geq 0$ existe $x \in \mathbb{R}$ tal que $a = x^2$, y entonces elegimos $y = 0$, mientras que si $b = 0$ y $a < 0$ existe $y \in \mathbb{R}$ tal que $-a = y^2$, y entonces tomamos $x = 0$. Por otro lado, si $b \neq 0$, los elementos $x, y \in \mathbb{R}$ buscados deben cumplir las igualdades

$$\begin{cases} x^2 & - & y^2 & = & a \\ & 2xy & & = & b \end{cases}$$

y despejando $y = b/2x$ en la segunda ecuación y sustituyendo este valor en la primera, se trata de demostrar que existe $x \in \mathbb{R}$ tal que $x^2 - b^2/4x^2 = a$, esto es, debemos probar que el polinomio

$$h(\mathtt{t}) := 4\mathtt{t}^4 - 4a\mathtt{t}^2 - b^2 \in \mathbb{R}[\mathtt{t}]$$

tiene alguna raíz $x \in \mathbb{R}$. Podemos reescribir $h(\mathtt{t}) = (2\mathtt{t}^2 - a)^2 - (a^2 + b^2)$, por lo que si h tiene alguna raíz $x \in \mathbb{R}$ debe cumplir

$$(2x^2 - a)^2 = (a^2 + b^2) \quad \Longleftrightarrow \quad 2x^2 = a \pm \sqrt{a^2 + b^2}.$$

Como $a^2 + b^2 \geq 0$ existe $c \in \mathbb{R}$ tal que $a^2 + b^2 = c^2$. Cambiando c por $-c$ podemos suponer que $c > 0$ y, como

$$(c - a)(c + a) = c^2 - a^2 = b^2,$$

los signos en $\mathbb{R}$ de $c - a$ y $c + a$ coinciden. Si los dos fuesen negativos lo sería su suma $2c$, y esto es falso. Así $c + a$ es positivo, luego también lo es $(a + c)/2$, que por ello es un cuadrado en $\mathbb{R}$. Existe por tanto $x \in \mathbb{R}$ tal que $x^2 = (a + c)/2 = (a + \sqrt{a^2 + b^2})/2$, como queríamos.

APÉNDICE B

Algunos números transcendentes

Demostramos en este Apéndice la existencia de infinitos números reales *transcendentes,* esto es, transcendentes sobre $\mathbb{Q}$, y algunos ejemplos: e, π y el número de ℓ de Liouville son transcendentes. También exponemos, sin demostración, el teorema de Lindemann-Weierstrass, del que de hecho se desprende la trascendencia de e y π, y la solución de Gelfond y Schneider al séptimo de los problmas planteados por Hilbert en su célebre conferencia de 1900 en París: dados números algebraicos $\alpha \in \mathbb{C} \setminus \{0, 1\}$ y $\beta \in \mathbb{C} \setminus \mathbb{Q}$ el número α^β es transcendente.

La prueba de que hay infinitos números reales transcendentes se debe a Cantor y fue objeto de controversia en la época en que la presentó a la comunidad matemática porque no exhibe explícitamente ningún número transcendente; la demostración es de carácter existencial.

Teorema B.1 (Cantor) *Existen infinitos números reales transcendentes.*

Demostración. Con las notaciones del Corolario I.2.5, el cierre algebraico de $\mathbb{Q}$ en $\mathbb{R}$ es el cuerpo

$$\overline{\mathbb{Q}}_{\mathbb{R}} = \{a \in \mathbb{R} : \ a \text{ es algebraico sobre } \mathbb{Q}\}.$$

Como $\mathbb{R} = \overline{\mathbb{Q}}_{\mathbb{R}} \sqcup (\mathbb{R} \setminus \overline{\mathbb{Q}}_{\mathbb{R}})$ no es numerable, es suficiente probar que $\overline{\mathbb{Q}}_{\mathbb{R}}$ es numerable, lo que implica que $\mathbb{R} \setminus \overline{\mathbb{Q}}_{\mathbb{R}}$ es infinito no numerable. Hemos probado en I.1.10 (2) que el anillo de polinomios $\mathbb{Q}[\mathtt{t}]$ es numerable, y las fibras de la aplicación

$$\overline{\mathbb{Q}}_{\mathbb{R}} \to \mathbb{Q}[\mathtt{t}],\ a \mapsto P_{\mathbb{Q},a}$$

son finitas, pues cada polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$ tiene tantas raíces distintas como grado. Esto demuestra que también $\overline{\mathbb{Q}}_{\mathbb{R}}$ es numerable. □

Observación B.2 En el resto de esta sección presentamos ejemplos de algunos números transcendentes. Comenzamos con dos lemas auxiliares.

Lema B.3 *Sea $\phi : \mathbb{Z} \to \mathbb{Z}$ una función tal que $\lim_{n\to+\infty} \phi(n) = 0$. Entonces, existe un entero positivo n_0 tal que $\phi(n) = 0$ para cada $n > n_0$.*

Demostración. Dado $\varepsilon = 1/2$, existe $n_0 \in \mathbb{Z}^+$ tal que $|\phi(n)| < \varepsilon$ para cada $n > n_0$. Así, $|\phi(n)|$ es un entero no negativo y menor que $1/2$ para cada $n \geq n_0$, luego ha de ser nulo, esto es, $\phi(n) = 0$ para cada $n > n_0$. □

Lema B.4 *Sean m un entero positivo, p un número primo, $s := mp + p - 1$ y el polinomio*

$$f_p(\mathtt{t}) := \frac{\mathtt{t}^{p-1} \cdot (\mathtt{t}-1)^p \cdot (\mathtt{t}-2)^p \cdots (\mathtt{t}-m)^p}{(p-1)!} \in \mathbb{Q}[\mathtt{t}].$$

Entonces, dados índices i, j tales que $0 \leq i \leq s$ y $0 \leq j \leq m$, se cumple que $f_p^{(i)}(j) \in p\mathbb{Z}$ si $(i, j) \neq (p-1, 0)$, mientras que $f_p^{(p-1)}(0) = (-1)^{pm} \cdot m!^p$.

Demostración. Escribimos $(p-1)!f_p = q_1 \cdot q_2$ donde $q_1, q_2 \in \mathbb{Z}[\mathtt{t}]$ son

$$q_1(\mathtt{t}) := \mathtt{t}^{p-1} \quad \& \quad q_2(\mathtt{t}) := \prod_{j=1}^{m} (\mathtt{t}-j)^p.$$

Nótese que $q_1^{(k)}(0) = (p-1)!$ si $k = p-1$ mientras que $q_1^{(k)}(0) = 0$ si $k \neq p-1$. Por la Fórmula de Leibniz, V.2.7 vol. II, se tiene, para cada entero i no negativo,

$$(q_1 \cdot q_2)^{(i)} = \sum_{k=0}^{i} \binom{i}{k} q_1^{(k)} \cdot q_2^{(i-k)}. \tag{I.1}$$

Calculamos las derivadas en 0 de f_p. Para $0 \leq i < p-1$ se deduce de la igualdad (I.1) que $(q_1 \cdot q_2)^{(i)}(0) = 0$, luego $f_p^{(i)}(0) = 0$, mientras que si $i \geq p-1$

$$(q_1 \cdot q_2)^{(i)}(0) = \binom{i}{p-1} q_1^{(p-1)}(0) \cdot q_2^{(i-(p-1))}(0) = (p-1)!\binom{i}{p-1} \cdot q_2^{(i-(p-1))}(0). \tag{I.2}$$

En particular, para $i := p-1$ resulta

$$(p-1)!f_p^{(p-1)}(0) = (q_1 \cdot q_2)^{(p-1)}(0) = (p-1)! \cdot q_2(0) = (p-1)! \cdot (-1)^{pm} \cdot m!^p,$$

y simplificando, $f_p^{(p-1)}(0) = (-1)^{pm} \cdot m!^p$. Por otro lado, si $i > p-1$,

$$(p-1)!f^{(i)}(0) = (q_1 \cdot q_2)^{(i)}(0) = (p-1)!\binom{i}{p-1} \cdot q_2^{(i-(p-1))}(0),$$

esto es, $f^{(i)}(0) = \binom{i}{p-1} \cdot q_2^{(i-(p-1))}(0)$. Escribimos el polinomio $\mathtt{q}_2$ como

$$q_2(\mathtt{t}) = \cdots + c\mathtt{t}^{i-(p-1)} + \cdots,$$

donde $c \in \mathbb{Z}$ y sólo hemos resaltado el monomio que tiene interés al calcular la derivada $q_2^{(i-(p-1))}(0)$. De hecho $q_2^{(i-(p-1))}(0) = c(i-(p-1))!$, lo que muestra que si $i > p-1$,

$$f_p^{(i)}(0) = c\binom{i}{p-1}(i-(p-1))! = \frac{c \cdot i!}{(p-1)!} = c\prod_{\ell=p}^{i} \ell \in p\mathbb{Z}.$$

De este modo hemos terminado el cálculo en lo que respecta al valor en 0 de las derivadas de f_p, y pasamos a calcular $f_p^{(i)}(j)$ para $1 \leq j \leq m$. Escribimos $(p-1)!f_p = g_1 \cdot g_2$ donde $g_1, g_2 \in \mathbb{Z}[\mathtt{t}]$ están definidos mediante

$$g_1(\mathtt{t}) := (\mathtt{t}-j)^p \quad \& \quad g_2(\mathtt{t}) := \mathtt{t}^{p-1} \cdot \prod_{k=1,\ k\neq j}^{m} (\mathtt{t}-k)^p.$$

Como la única derivada no nula de g_1 en $t := j$ es $g_1^{(p)}(j) = p!$, aplicando de nuevo la Fórmula de Leibniz se tiene, para $0 \leq i \leq s$,

$$\begin{aligned}(p-1)!f_p^{(i)}(j) = (g_1g_2)^{(i)}(j) &= \sum_{k=0}^{i} \binom{i}{k} g_1^{(k)}(j) \cdot g_2^{(i-k)}(j) \\ &= \begin{cases} 0 & \text{si } i < p \\ p!\binom{i}{p} g_2^{(i-k)}(j) & \text{si } p \leq i \leq s. \end{cases}\end{aligned}$$

Dividiendo ambos miembros por $(p-1)!$ resulta finalmente,

$$f_p^{(i)}(j) = \begin{cases} 0 & \text{si } i < p \\ p \cdot \binom{i}{p} \cdot g_2^{(i-k)}(j) \in p\mathbb{Z} & \text{si } p \leq i \leq s, \end{cases}$$

y esto demuestra la afirmación del enunciado. □

Teorema B.5 (Hermite) *El número e es transcendente.*

Demostración. En caso contrario, quitando denominadores en el polinomio mínimo de e sobre $\mathbb{Q}$, se obtiene un polinomio

$$\mathtt{p}(\mathtt{t}) := a_m\mathtt{t}^m + a_{m-1}\mathtt{t}^{m-1} + \cdots + a_1\mathtt{t} + a_0 \in \mathbb{Z}[\mathtt{t}]$$

tal que $a_0 a_m \neq 0$ y $\mathtt{p}(e) = 0$. Sea $p > m^{m+1} + 1$ un número primo, y consideremos el polinomio de grado $s := mp + p - 1$

$$f_p(\mathtt{t}) := \frac{\mathtt{t}^{p-1} \cdot (\mathtt{t}-1)^p \cdot (\mathtt{t}-2)^p \cdots (\mathtt{t}-m)^p}{(p-1)!} \in \mathbb{Q}[\mathtt{t}].$$

Nótese que para cada número real t en el intervalo abierto $(0, m)$ y cada entero no negativo $j < m$ se cumple que $|t - j| < m$, luego

$$|f_p(t)| \leq m^{p-1} m^{pm}/(p-1)! = m^s/(p-1)! \quad \text{para } 0 < t < m. \tag{I.3}$$

También tiene grado s el polinomio $g_p := f_p + f_p' + \cdots + f_p^{(s)} \in \mathbb{Q}[\mathtt{t}]$, y como la derivada $f_p^{(s+1)} \equiv 0$ es el polinomio idénticamente nulo, $g_p' = g_p - f_p$. Definimos la función de clase infinito $h_p : \mathbb{R} \to \mathbb{R}$, $t \mapsto e^{-t} g_p(t)$, cuya derivada cumple

$$h_p'(t) = -e^{-t} g_p(t) + e^{-t} g_p'(t) = -e^{-t}\big(g_p(t) - g_p'(t)\big) = -e^{-t} f_p(t),$$

y por tanto, para $0 \leq j \leq m$ se cumple,

$$a_j \int_0^j e^{-t} f_p(t) dt = -a_j \int_0^j h_p'(t) dt = a_j\big(h_p(0) - h_p(j)\big) = a_j\big(g_p(0) - e^{-j} g_p(j)\big).$$

Multiplicamos ambos miembros por e^j y sumamos. Puesto que $\mathtt{p}(e) = 0$, por el Lema B.4 se tiene,

$$\begin{aligned}\sum_{j=0}^m a_j e^j \int_0^j e^{-t} f_p(t) dt &= g_p(0) \sum_{j=0}^m a_j e^j - \sum_{j=0}^m a_j g_p(j) = g_p(0)\mathtt{p}(e) - \sum_{j=0}^m a_j g_p(j) \\ &= -\sum_{j=0}^m a_j g_p(j) = -\sum_{j=0}^m \sum_{i=0}^s a_j f_p^{(i)}(j) = -\big(a_0(-1)^{pm} \cdot m! + pk(p)\big)\end{aligned}$$

para cierto entero $k(p)$. El miembro de la derecha de esta igualdad es un número entero que depende de p luego también es entero el miembro de la izquierda. Además, por (I.3),

$$\begin{aligned}0 &\leq \lim_{p\to+\infty} \Big|\sum_{j=0}^m a_j e^j \int_0^j e^{-t} f_p(t) dt\Big| \leq \sum_{j=0}^m |a_j e^j| \cdot \Big(\lim_{p\to+\infty} \int_0^j |f_p(t)| dt\Big) \\ &\leq \sum_{j=0}^m |a_j e^j| \cdot \Big(\lim_{p\to+\infty} \frac{j \cdot m^s}{(p-1)!}\Big) \leq \sum_{j=0}^m |a_j e^j| \cdot \Big(\lim_{p\to+\infty} \frac{m^{s+1}}{(p-1)!}\Big) \\ &= \sum_{j=0}^m |a_j e^j| \cdot \Big(\lim_{p\to+\infty} \frac{m^{p(m+1)}}{(p-1)!}\Big) = 0,\end{aligned}$$

pues $\lim_{p\to+\infty} \frac{m^{p(m+1)}}{(p-1)!} = 0$. Para probar esto último sea $n := m^{m+1} < p-1$, y

$$\lim_{p\to+\infty} \frac{m^{p(m+1)}}{(p-1)!} = \lim_{p\to+\infty} \frac{n^p}{(p-1)!} = \lim_{p\to+\infty} \Big(\frac{n^{n+1}}{n!} \cdot \frac{n}{n+1} \cdots \frac{n}{p-2} \cdot \frac{n}{p-1}\Big)$$
$$\leq \lim_{p\to+\infty} \frac{n^{n+2}}{n!} \cdot \frac{1}{p-1} = 0,$$

pues $n/k \leq 1$ para $n+1 \leq k \leq p-2$ y $n^{n+2}/n!$ no depende de p. Así,

$$\lim_{p\to+\infty} \big(a_0(-1)^{pm} \cdot m! + pk(p)\big) = \lim_{p\to+\infty} \Big(\sum_{j=0}^{m} a_j e^j \int_0^j e^{-t} f_p(t)dt\Big) = 0,$$

y se deduce del Lema B.3 que $a_0(-1)^{qm} \cdot m! + qk(q) = 0$ para cada primo $q > m^{m+1} + 1$. Sin embargo, eligiendo $q > a_0$ esto es falso, pues $qk(q) \in q\mathbb{Z}$ pero $a_0(-1)^{qm} \cdot m!$ no lo es. □

Nuestro siguiente objetivo es demostrar la transcendencia de π. Antes necesitamos un lema auxiliar.

Lema B.6 *Para cada $\omega \in \mathbb{C} \setminus \{0\}$ y cada $f(\mathtt{t}) := \sum_{k=0}^{n} a_k \mathtt{t}^k \in \mathbb{C}[\mathtt{t}]$, denotamos*

$$\mathcal{J}_f(\omega) := \int_{S_\omega} e^{\omega - z} f(z)dz,$$

donde S_ω es el segmento del plano complejo de extremos 0 y ω. Entonces,

(1) *Para cada entero $k \geq 1$ se cumple*

$$\int e^{-z} z^k dz = -e^{-z}\Big(k! + \sum_{j=0}^{k-1} \frac{k!}{(k-j)!} z^{k-j}\Big).$$

(2)

$$\mathcal{J}_f(\omega) = e^{\omega} \sum_{k=0}^{n} f^{(k)}(0) - \sum_{k=0}^{n} f^{(k)}(\omega).$$

(3) Si denotamos $\widehat{f}(\mathtt{t}) := \sum_{k=0}^{n} |a_j| \mathtt{t}^k \in \mathbb{R}[\mathtt{t}]$, se tiene $|\mathcal{J}_f(\omega)| \leq |\omega| \cdot e^{|\omega|} \cdot \widehat{f}(|\omega|)$.

Demostración. (1) Demostramos la igualdad por inducción sobre k. Para $k = 1$ se tiene

$$\int e^{-z} z dz = -\int z d(e^{-z}) = -\Big(ze^{-z} - \int e^{-z} dz\Big) = e^{-z}(1+z).$$

Supongamos probado el resultado para $k-1$. Integrando por partes,

$$\int e^{-z}z^k dx = \int z^k d(-e^{-z}) = -e^{-z}z^k + k\int e^{-z}z^{k-1}dz$$
$$= -e^{-z}\Big(z^k + k\Big((k-1)! + \sum_{j=0}^{k-2}\frac{(k-1)!}{(k-1-j)!}z^{k-1-j}\Big)\Big).$$

Si en la última igualdad denotamos $\ell := 1+j$ resulta

$$\int e^{-z}z^k dz = -e^{-z}\Big(z^k + k! + \sum_{\ell=1}^{k-1}\frac{k!}{(k-\ell)!}z^{k-\ell}\Big) = e^{-z}\Big(k! + \sum_{\ell=0}^{k-1}\frac{k!}{(k-\ell)!}z^{k-\ell}\Big).$$

(2) La fórmula obtenida en el apartado anterior es también válida para $k=0$ si interpretamos $0!z^0/0! = 1$, pues $\int e^{-z}dz = -e^{-z}$. Así,

$$\mathcal{J}_f(\omega) = e^\omega \int_{S_\omega} e^{-z}f(z)dz = e^\omega \sum_{k=0}^n a_k \int_{S_\omega} e^{-z}z^k dz$$
$$= e^\omega \sum_{k=0}^n a_k\Big(-e^{-z}\Big(k! + \sum_{j=0}^{k-1}\frac{k!}{(k-j)!}z^{k-j}\Big)\Big)_{z=0}^{z=\omega} = e^\omega \sum_{k=0}^n a_k\cdot k!$$
$$-\sum_{k=0}^n a_k\Big(k! + \sum_{j=0}^{k-1}\frac{a_k\cdot k!}{(k-j)!}\omega^{k-j}\Big) = e^\omega\sum_{k=0}^n f^{(k)}(0) - \sum_{k=0}^n f^{(k)}(\omega).$$

(3) Por la desigualdad triangular, y puesto que el módulo de la integral es menor o igual que integral del módulo, de la definición se desprende que

$$|\mathcal{J}_f(\omega)| \le \int_{S_\omega}|e^{\omega-z}|\cdot|f(z)|dz \le \int_{S_\omega}|e^{\omega-z}|\cdot\sum_{k=0}^n|a_k|\cdot|z|^k dz. \qquad \text{(I.4)}$$

En la última integral z pertenece a S_ω, y entre los puntos de dicho segmento el de mayor módulo es ω. Además, si $\omega - z = r(\cos\theta + i\,\mathrm{sen}\,\theta)$ con $r\ge 0$ se tiene, por ser la exponencial real una función creciente y $|\omega - z| \le |\omega|$ para cada $z\in S_\omega$,

$$|e^{\omega-z}| = |e^{r(\cos\theta + i\,\mathrm{sen}\,\theta)}| = |e^{r\cos\theta}\cdot e^{ir\,\mathrm{sen}\,\theta}| = e^{r\cos\theta} \le e^r = e^{|\omega-z|} \le e^{|\omega|}.$$

Sustituyendo en (I.4) las desigualdades $|z|\le|\omega|$ y $|e^{\omega-z}|\le e^{|\omega|}$, y puesto que la longitud del segmento S_ω es $|\omega|$, resulta finalmente

$$|\mathcal{J}_f(\omega)| \le \int_{S_\omega} e^{|\omega|}\cdot\sum_{k=0}^n|a_k|\cdot|\omega|^k dz = \int_{S_\omega} e^{|\omega|}\cdot\widehat{f}(|\omega|)dz = |\omega|\cdot e^{|\omega|}\cdot\widehat{f}(|\omega|).$$

□

Teorema B.7 (Lindemann) *El número π es transcendente.*

Demostración. Denotemos $i := \sqrt{-1}$, que es algebraico por ser raíz del polinomio $\mathtt{t}^2 + 1$. Razonaremos por reducción al absurdo. Si π fuese algebraico también lo sería $i\pi$, por el Corolario I.2.3 (4). Sean m el grado del polinomio mínimo $g := P_{\mathbb{Q},\pi i}$ de πi sobre $\mathbb{Q}$ y $\pi i := \theta_1, \theta_2, \ldots, \theta_m \in \mathbb{C}$ las raíces complejas de g. Llamando b al mínimo común múltiplo de los denominadores de los coeficientes de g, el producto bg es un polinomio con coeficientes enteros, de grado mínimo entre los que tienen a θ_1 por raíz y no son nulos. Si

$$bg(\mathtt{t}) := b\mathtt{t}^m + \sum_{j=0}^{m-1} b_j \mathtt{t}^j \in \mathbb{Z}[\mathtt{t}] \quad \Longrightarrow \quad 0 = b^m g(\theta_k) = (b\theta_k)^m + \sum_{j=0}^{m-1} a_j (b\theta_k)^j$$

para ciertos $a_j \in \mathbb{Z}$.

Existe por tanto un polinomio mónico $h(\mathtt{t}) := \mathtt{t}^m + \sum_{j=0}^{m-1} a_j \mathtt{t}^j \in \mathbb{Z}[\mathtt{t}]$ tal que $h(b\theta_k) = 0$ para $1 \leq k \leq m$. Como $e^{\pi i} + 1 = 0$, resulta que

$$(1 + e^{\theta_1}) \cdots (1 + e^{\theta_m}) = 0.$$

Desarrollamos mediante la propiedad distributiva el miembro de la izquierda y, como $1 = e^0$ y

$$e^{\varepsilon_1\theta_1 + \cdots + \varepsilon_n\theta_m} = e^{\varepsilon_1\theta_1} \cdots e^{\varepsilon_m\theta_m} \quad \forall\ \varepsilon = (\varepsilon_1, \ldots, \varepsilon_m) \in \Lambda := \{0,1\}^m,$$

se obtiene una suma de 2^m sumandos

$$\sum_{\varepsilon \in \Lambda} e^{\phi_\varepsilon} = (1 + e^{\theta_1}) \cdots (1 + e^{\theta_m}) = 0,$$

donde $\phi_\varepsilon := \varepsilon_1\theta_1 + \cdots + \varepsilon_m\theta_m$. Sea q el número de m-uplas $\varepsilon \in \Lambda$ tales que $\phi_\varepsilon = 0$. Nótese que tanto q como $n := 2^m - q$ son positivos, pues $\phi_\varepsilon = 0$ si $\varepsilon = (0, \ldots, 0)$, mientras que $\phi_\varepsilon = \theta_1 \neq 0$ si $\varepsilon = (1, 0, \ldots, 0)$. Renombramos $\omega_1, \ldots, \omega_n \in \mathbb{C}$ aquellos $\phi_\varepsilon \neq 0$, por lo que

$$q + e^{\omega_1} + \cdots + e^{\omega_n} = \sum_{\phi_\varepsilon = 0} e^{\phi_\varepsilon} + e^{\omega_1} + \cdots + e^{\omega_n} = 0. \tag{I.5}$$

Vamos a demostrar que si $p \in \mathbb{Z}$ es un número primo suficientemente grande los coeficientes del polinomio

$$f_p(\mathtt{t}) = b^{np}\mathtt{t}^{p-1}(\mathtt{t} - \omega_1)^p \cdots (\mathtt{t} - \omega_n)^p$$

son números enteros. Denotando $\omega_{n+1} = \cdots = \omega_{2^m} = 0$ a aquellas sumas ϕ_ε que son nulas, basta probar que el polinomio

$$\Phi(\mathtt{t}) := \prod_{j=1}^{2^m}(\mathtt{t}-\omega_j) = \mathtt{t}^q \prod_{j=1}^{n}(\mathtt{t}-\omega_j)^p$$

tiene coeficientes racionales, y que el denominador de cada uno de sus coeficientes es b^n. Pero el miembro de la izquierda es un polinomio simétrico, con coeficientes en $\mathbb{Z}$, respecto de $\omega_1, \ldots, \omega_{2^n}$, luego también es simétrico respecto de $\theta_1, \ldots, \theta_m$. Se deduce del Teorema Fundamental de los polinomios simétricos, VII.1.16, vol. II, que los coeficientes de Φ son el resultado de evaluar las formas simétricas elementales en los coeficientes del polinomio $g(\mathtt{t}) := (\mathtt{t}-\theta_1)\cdots(\mathtt{t}-\theta_m)$. Como los coeficientes de este último polinomio son números racionales cuyo denominador es b, queda probado que $f_p \in \mathbb{Z}[\mathtt{t}]$ para p suficientemente grande. Además, dividiendo por $\mathtt{t}^p$, se deduce que también

$$g_p(\mathtt{t}) = b^{np}(\mathtt{t}-\omega_1)^p \cdots (\mathtt{t}-\omega_n)^p \in \mathbb{Z}[\mathtt{t}].$$

Como $\deg(f_p) := np + p - 1 = r$, con las notaciones del Lema anterior B.6, y utilizando su apartado (2) y la igualdad (I.5) se tiene

$$\begin{aligned}\mathcal{J}_p &= \sum_{j=1}^{n} \mathcal{J}_{f_p}(\omega_j) = \sum_{j=1}^{n} \int_{S_\omega} e^{\omega_j - z} f_p(z)dz \\ &= \sum_{j=1}^{n}\Big(e^{\omega_j}\sum_{k=0}^{r} f_p^{(k)}(0) - \sum_{k=0}^{r} f_p^{(k)}(\omega_j)\Big) = -q\sum_{k=0}^{r} f_p^{(k)}(0) - \sum_{k=0}^{r}\sum_{j=1}^{n} f_p^{(k)}(\omega_j).\end{aligned} \tag{I.6}$$

Nuestro siguiente objetivo es comprobar que si elegimos p suficientemente grande, entonces $(p-1)! \leq |\mathcal{J}_p|$. Para ello probaremos que $\mathcal{J}_p$ es un múltiplo entero y no nulo de $(p-1)!$.

Comenzamos viendo que el sumatorio $\sum_{k=0}^{r}\sum_{j=1}^{n} f_p^{(k)}(\omega_j)$ en (I.6) es múltiplo de $p!$, para lo que basta comprobar que lo es cada sumando $\sum_{j=1}^{n} f_p^{(k)}(\omega_j)$. Ahora bien, $f_p(\mathtt{t}) = \mathtt{t}^{p-1}\prod_{j=1}^{n}(b\mathtt{t} - b\omega_j)^p$, luego $\sum_{j=1}^{n} f_p^{(k)}(\omega_j)$ es un polinomio con coeficientes enteros simétrico respecto de $b\omega_1, \ldots, b\omega_n$, y por tanto es un polinomio con coeficientes enteros simétrico respecto de los 2^m números $b\omega_1, \ldots, b\omega_{2^m}$. El Teorema Fundamental de los polinomios simétricos implica, puesto que $f_p \in \mathbb{Z}[\mathtt{t}]$, que $\sum_{j=1}^{n} f_p^{(k)}(\omega_j)$ es un número entero. Veamos que es múltiplo de $p!$.

Nótese que $f_p^{(k)}(\omega_j) = 0$ si $k < p$ puesto que ω_j es raíz de multiplicidad p de f_p. Por otro lado, sea $k \geq p$ y escribimos $f_p(\mathtt{t}) := (\mathtt{t} - \omega_j)^p \psi_j(\mathtt{t})$. Al aplicar la Fórmula de Leibniz, V.2.7 vol. II, y como la única derivada no nula de $(\mathtt{t}-\omega_j)^p$ en ω_j es la de orden p y vale $p!$, la suma $\sum_{j=1}^n f_p^{(k)}(\omega_j)$ es un múltiplo entero de $p!$. En cuanto al primer sumando en el miembro de la derecha de (I.6), como 0 es raíz de multiplicidad $p-1$ de f_p, resulta que $f_p^{(k)}(0) = 0$ si $k < p-1$. Además, si escribimos $f_p(\mathtt{t}) = b^{np}\mathtt{t}^{p-1}h_p(\mathtt{t})^p$, donde

$$h_p(\mathtt{t}) := (\mathtt{t} - \omega_1)\cdots(\mathtt{t} - \omega_n)$$

se deduce de la Fórmula de Leibniz que $f_p^{(k)}(0)$ es un múltiplo entero de $p!$ si $k \geq p$, mientras que la derivada de orden $p-1$ es

$$\begin{aligned} f_p^{(p-1)}(0) = b^{np}(p-1)!h_p^p(0) &= b^{np}(p-1)!(-1)^{np}(\omega_1\cdots\omega_n)^p \\ &= (p-1)!g_p(0) \in (p-1)!\mathbb{Z}. \end{aligned}$$

Por tanto $\mathcal{J}_p \in (p-1)!\mathbb{Z}$, pues hemos comprobado que todos los sumandos que aparecen en la expresión (I.6) son múltiplos de $(p-1)!$. Para demostrar que $\mathcal{J}_p$ no es nulo demostraremos que eligiendo p adecuadamente, $\mathcal{J}_p$ no es múltiplo de p. Como hemos probado que la suma $\sum_{k=0}^r f_p^{(k)}(\omega_j) \in p\mathbb{Z}$, se trata de elegir p de modo que el sumando $q\sum_{k=0}^r f_p^{(k)}(0)$ no sea múltiplo de p.

Nótese que $q \in \mathbb{Z}$ no depende de p, y eligiendo $p > q$ aseguramos que $q \notin p\mathbb{Z}$, luego basta elegir p suficientemente grande para que $\sum_{k=0}^r f_p^{(k)}(0) \notin p\mathbb{Z}$. Pero $\sum_{k\neq p-1} f_p^{(k)}(0) \in p\mathbb{Z}$, así que hay que lograr que $(p-1)!g_p(0) = f_p^{(p-1)}(0) \notin p\mathbb{Z}$, y para ello es suficiente que $g_p(0) = (-1)^{np}(b\omega_1\cdots b\omega_n)^p \notin p\mathbb{Z}$. Basta pues tomar p suficientemente grande, ya que $b\omega_1\cdots b\omega_n$ es un número que se conoce antes de elegir p.

Por último, con las notaciones de B.6 (3), $\mathcal{J}_{f_p}(\omega_j) \leq |\omega_j|\cdot e^{|\omega_j|}\cdot \widehat{f}(|\omega_j|)$ para $1 \leq j \leq n$, y sumando,

$$(p-1)! \leq |\mathcal{J}_p| \leq \sum_{j=1}^n \mathcal{J}_{f_p}(\omega_j)| \leq \sum_{j=1}^n |\omega_j|\cdot e^{|\omega_j|}\cdot \widehat{f}_p(|\omega_j|) \leq K^{p+1} = K^2\cdot K^{p-1},$$

para cierto entero $K \geq 2$ y todo primo p suficientemente grande. Pero esto es falso, ya que $\lim_{n\to\infty}\{K^{2n}/(2n)!\} = 0$. En efecto, para cada $n \in \mathbb{N}$ con $K^3 < n$,

$$0 \leq \frac{K^{2n}}{(2n)!} = \frac{(K \overset{n)}{\cdots} K)\cdot(K \overset{n)}{\cdots} K)}{(1\cdots n)\cdot(n+1)\cdots 2n} \leq K^n\cdot\Big(\frac{K}{n}\Big)^n = \Big(\frac{K^2}{n}\Big)^n < \frac{1}{K^n},$$

y $\lim_{n\to\infty}\{1/K^n\} = 0$. □

Corolario B.8 *De entre los dos números $e+\pi$ y $e\pi$ al menos uno es transcendente.*

Demostración. En efecto, si $e+\pi$ y $e\pi$ fuesen algebraicos, tanto e como π también lo serían, en virtud de la Proposición I.2.3 (4), y hemos demostrado en los Teoremas B.5 y B.7 que esto es falso. □

Observaciones B.9 (1) Se sospecha que tanto $e+\pi$ y $e\pi$ son transcendentes pero hoy en día esto es una conjetura. Tampoco se conoce si π^e es o no transcendente.

(2) Nuestro siguiente objetivo es exponer un procedimiento debido a Liouville para construir números transcendentes.

Lema B.10 *Sean $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ un número algebraico y $n := [\mathbb{Q}(\alpha):\mathbb{Q}]$. Entonces, existe un número real positivo c tal que $|\alpha - a/b| > c/b^n$ para todo par de enteros positivos a y b.*

Demostración. Para aquellas fracciones $r := a/b \in \mathbb{Q}$ tales que $|\alpha - r| \geq 1$ basta elegir cualquier $c < 1$. Es por tanto suficiente encontrar un número real c que satisfaga la desigualdad del enunciado para todas las fracciones r tales que $|\alpha - r| < 1$.

Como $[\mathbb{Q}(\alpha):\mathbb{Q}] = n$, multiplicando los coeficientes del polinomio mínimo de α sobre $\mathbb{Q}$ por el mínimo común múltiplo de los denominadores de dichos coeficientes se obtiene un polinomio $f \in \mathbb{Z}[\mathtt{t}]$ de grado n e irreducible en $\mathbb{Q}[\mathtt{t}]$ tal que $f(\alpha) = 0$. En particular, como $n > 1$ y f es irreducible, no tiene raíces racionales, luego $f(r) \neq 0$. Por el Teorema del valor medio, existe un número real ζ_r en el intervalo de extremos α y r tal que

$$-f(r) = f(\alpha) - f(r) = f'(\zeta_r)(\alpha - r),$$

y como $f(r) \neq 0$ también $f'(\zeta_r) \neq 0$. Despejando, $|\alpha - r| = |f(r)|/|f'(\zeta_r)|$. Además,

$$|\alpha - \zeta_r| \leq |\alpha - r| < 1 \quad \Longrightarrow \quad \zeta_r \in [\alpha - 1, \alpha + 1] := I_\alpha.$$

Como f' es una función continua, el intervalo I_α es compacto y $f'(\zeta_r) \neq 0$, existe

$$C := 1 + \text{máx}\{|f'(u)| : u \in I_\alpha\} > 1,$$

y por tanto $c := 1/C < 1$. Éste es el número real que buscamos. En efecto, por un lado

$$|\alpha - r| = |f(r)|/|f'(\zeta_r)| > |f(r)|/C = c|f(r)|,$$

y por otro, como $f \in \mathbb{Z}[\mathtt{t}]$ tiene grado n, el número $|b^n f(r)| = |b^n f(a/b)|$ es entero positivo, luego $|f(r)| \geq 1/b^n$. Finalmente, $|\alpha - r| > c|f(r)| \geq c/b^n$. □

Teorema B.11 (Liouville) *El número* $\ell := \sum_{m=1}^{\infty} 10^{-m!}$, *denominado* de Liouville, *es transcendente.*

Demostración. Supongamos por reducción al absurdo que ℓ es algebraico y distinguimos dos casos, según que ℓ sea o no un número racional.

Caso 1. Suponemos que $\ell \in \mathbb{R} \setminus \mathbb{Q}$. Entonces $n := [\mathbb{Q}(\ell) : \mathbb{Q}] > 1$ y existe, por el Lema B.10, un número real $c > 0$ tal que $|\ell - a/b| > c/b^n$ para cualesquiera números enteros positivos a y b. Como $\mathbb{R}$ es un cuerpo arquimediano existe un entero $j > 0$ tal que $cb^{j-n} > 1$, donde $b = 10^{j!}$. El número $a = b\sum_{m=1}^{j} 10^{-m!}$ es entero, y por tanto

$$|\ell - a/b| > c/b^n > b^{n-j}/b^n = b^{-j}. \tag{I.7}$$

Sin embargo, al operar resulta

$$\begin{aligned} |\ell - a/b| &= \Big| \sum_{m=1}^{\infty} 10^{-m!} - \sum_{m=1}^{j} 10^{-m!} \Big| = \sum_{m=j+1}^{\infty} 10^{-m!} < 10^{-(j+1)!} \sum_{k=0}^{\infty} 10^{-k} \\ &= \frac{10^{-(j+1)!}}{1 - 1/10} = \frac{10 \cdot 10^{-(j+1)!}}{9} < 10 \cdot 10^{-(j+1)!} \\ &= 10 \cdot \left(10^{j!}\right)^{-(j+1)} = 10 \cdot b^{-(j+1)} < b^{-j}, \end{aligned}$$

lo que contradice (I.7).

Obsérvese que el cálculo anterior es válido no sólo para el exponente j elegido, sino también para todos los enteros mayores que él.

Caso 2. Suponemos que $\ell \in \mathbb{Q}$. En consecuencia, existen números enteros u, v tales que $\ell := u/v$. Con las notaciones del caso anterior, para todo entero j suficientemente grande,

$$\frac{a}{b} = \sum_{m=1}^{j} 10^{-m!} < \sum_{m=1}^{\infty} 10^{-m!} = \ell = \frac{u}{v}.$$

Por tanto, $bu - av$ es un entero positivo, luego $bu - av \geq 1$, y según acabamos de ver,

$$b^{-j} > |\ell - a/b| = \ell - a/b = u/v - a/b = (bu - av)/bv \geq 1/bv,$$

esto es, $v > b^{j-1}$ para todo entero j suficientemente grande, y esto es imposible. □

(B.12) Otros números transcendentes. (1) No demostraremos en este texto el teorema de Lindemann-Weierstrass, que afirma que si $n \geq 2$ y $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ son números algebraicos distintos dos a dos y $c_1, \ldots, c_n \in \mathbb{C}$ son números algebraicos no todos nulos, entonces

$$c_1 e^{\alpha_1} + \cdots + c_n e^{\alpha_n} \neq 0.$$

(2) En consecuencia, si $n \geq 1$ y $\alpha_1, \ldots, \alpha_n, c_1, \ldots, c_n$ son números algebraicos no nulos tales que $\alpha_i \neq \alpha_j$ si $i \neq j$, el número $\gamma := c_1 e^{\alpha_1} + \cdots + c_n e^{\alpha_n}$ es transcendente. En efecto, en caso contrario $c_0 := -\gamma$ es algebraico y se tiene

$$c_0 e^0 + c_1 e^{\alpha_1} + \cdots + c_n e^{\alpha_n} = 0,$$

los números $0 = \alpha_0$, $\alpha_1, \ldots, \alpha_n$ son distintos dos a dos y $c_0, \ldots, c_n$ son números algebraicos no todos nulos. Esto contradice el Teorema de Lindemann-Weierstrass.

(3) En particular, si $\alpha \in \mathbb{C} \setminus \{0\}$ es un número algebraico, entonces e^α es transcendente.

(4) De esto se deducen los Teoremas B.5 y B.7 de Hermite y Lindemann, respectivamente. En efecto, como $\alpha := 1 \in \mathbb{C} \setminus \{0\}$ es algebraico, $e = e^\alpha$ es transcendente. Además, si π fuese algebraico también lo sería $\pi i \neq 0$, por lo que $-1 = e^{\pi i}$ sería transcendente, y esto es falso.

(5) Si $\beta \in \mathbb{R} \setminus \{1\}$ es un número real positivo y algebraico, entonces su logaritmo neperiano $\alpha := \log \beta$ es transcendente. En efecto, en caso contrario, y puesto que $\alpha \neq 0$, se deduce de (3) que $\beta = e^\alpha$ es transcendente, contra la hipótesis.

(6) Si $\alpha \in \mathbb{R} \setminus \{0\}$ es un número algebraico, entonces $\operatorname{sen} \alpha$, $\cos \alpha$ y $\operatorname{tg} \alpha$ son números transcendentes. En efecto, para el seno y el coseno basta emplear el apartado (2), ya que

$$\operatorname{sen} \alpha = (1/2i)e^{i\alpha} - (1/2i)e^{-i\alpha} \quad \& \quad \cos \alpha = (1/2)e^{i\alpha} + (1/2)e^{-i\alpha}.$$

En cuanto a la tangente, supongamos que

$$\operatorname{tg} \alpha = \operatorname{sen} \alpha / \cos \alpha = (e^{-i\alpha} - e^{i\alpha})i/(e^{i\alpha} + e^{-i\alpha})$$

es algebraico. Nótese que

$$e^{i\alpha}\operatorname{tg}\alpha + e^{-i\alpha}\operatorname{tg}\alpha = ie^{-i\alpha} - ie^{i\alpha} \quad \Longrightarrow \quad (\operatorname{tg}\alpha + i)e^{i\alpha} + (\operatorname{tg}\alpha - i)e^{-i\alpha} = 0,$$

luego los números $c_1 := \operatorname{tg}\alpha + i$ y $c_2 := \operatorname{tg}\alpha - i$ son algebraicos y distintos, también son algebraicos $\alpha_1 := i\alpha$ y $\alpha_2 := -i\alpha$ y, sin embargo, $c_1 e^{\alpha_1} + c_2 e^{\alpha_2} = 0$, en contradicción con el Teorema de Lindemann-Weierstrass.

(7) El séptimo de los problemas planteados por Hilbert en la conferencia que impartió en París en el año 1900 proponía decidir si dados números algebraicos $\beta \in \mathbb{C}\setminus\mathbb{Q}$ y $\alpha \in \mathbb{C}\setminus\{0,1\}$ se puede asegurar que α^β es transcendente. En 1934, Gelfond y Schneider respondieron afirmativamente la pregunta de Hilbert. Nótese que, por ejemplo, esto implica que $2^{\sqrt{2}}$ es un número transcendente.

(8) Existen varios números de los que se ignora si son transcendentes, aunque se sospecha que lo son. Señalamos dos de ellos:

(8.1) La constante γ de Euler-Mascheroni, definida como

$$\gamma := \lim_{n\to\infty} \Big(\sum_{k=1}^{n} \frac{1}{k} - \log n \Big).$$

(8.2) La constante de Catalan, que aparece en el contexto de las integrales elípticas, y está definida como

$$G := \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^2}.$$

APÉNDICE C

Resolución por radicales

Hemos señalado en el Corolario VII.1.12 que los polinomios de grado menor o igual que 4 son resolubles por radicales. Nuestro objetivo ahora es encontrar fórmulas explícitas, que sólo involucran radicales, para calcular las raíces de estos polinomios. Ya hemos visto que para polinomios generales de grado ≥ 5 no existe una fórmula de esta naturaleza. Aunque las fórmulas que obtendremos son poco útiles salvo en algunos casos particulares, hemos decidido dedicarles unas páginas en este texto porque su obtención supuso uno de los más notables retos matemáticos en el Renacimiento. Supondremos por simplicidad que el cuerpo de coeficientes K tiene característica distinta de 2 y 3, para poder emplear la transformación de Tschirnhaus.

(C.1) Cálculo de las raíces de los polinomios de grado 2. Las raíces del polinomio $f(\mathtt{t}) := \mathtt{t}^2 - 2a\mathtt{t} + b \in K[\mathtt{t}]$ en su cuerpo de descomposición son

$$t_1 := a + \sqrt{a^2 - b} \quad \& \quad t_2 := a - \sqrt{a^2 - b}.$$

En efecto, escribimos

$$f(\mathtt{t}) = \mathtt{t}^2 - 2a\mathtt{t} + b = (\mathtt{t} - a)^2 - (a^2 - b),$$

y por tanto, si t es una raíz de f debe cumplir que $t - a = \pm\sqrt{a^2 - b}$, o sea, $t = a \pm \sqrt{a^2 - b}$. Recíprocamente, tanto t_1 como t_2 son raíces de f, ya que

$$f(t_i) = t_i^2 - 2at_i + b = (t_i - a)^2 - (a^2 - b) = 0.$$

El siguiente lema es muy elemental pero útil; permite suponer que la suma de las raíces del polinomio cuyas raíces queremos calcular es nula.

Lema C.2 (Transformación de Tschirnhaus) *Para cada polinomio*

$$f(\mathtt{t}) := \mathtt{t}^n + \sum_{k=0}^{n-1} a_k \mathtt{t}^k$$

de grado $n \geq 1$ con coeficientes en K, el coeficiente b_{n-1} que multiplica a $\mathtt{t}^{n-1}$ en el polinomio $h(\mathtt{t}) := f(\mathtt{t} - a_{n-1}/n)$ es 0.

Demostración. Al evaluar f en $\mathtt{t} - a_{n-1}/n$ se tiene

$$\mathtt{t}^n + \sum_{j=0}^{n-1} b_j \mathtt{t}^j := h(\mathtt{t}) = f(\mathtt{t} - a_{n-1}/n) = \left(\mathtt{t} - \frac{a_{n-1}}{n}\right)^n + \sum_{k=0}^{n-1} a_k \left(\mathtt{t} - \frac{a_{n-1}}{n}\right)^k.$$

Deducimos que $b_{n-1} = a_{n-1} - na_{n-1}/n = 0$, sin más que comparar los coeficientes correspondientes al monomio de grado $n-1$. □

Emplearemos en este Apéndice un mismo modo de proceder para resolver las ecuaciones polinómicas de grados 3 y 4, pero queremos antes explicar el procedimiento *ad hoc* descubierto por Tartaglia en el año 1535 para calcular las raíces de los polinomios de grado 3. Empleando la transformación de Tschirnhaus es suficiente calcular las raíces del polinomio $f(\mathtt{t}) = \mathtt{t}^3 + p\mathtt{t} - q$. Si x es una de ellas Tartaglia buscó dos números u y v tales que $x = u - v$ y al sustituir esta expresión en el polinomio f resulta

$$0 = f(u-v) = (u-v)^3 + p(u-v) - q \quad \Longrightarrow \quad u^3 - v^3 + (u-v)(p - 3uv) = q.$$

Tartaglia eligió, entre las diversas formas de escribir x como resta $x = u - v$, la que cumple $p = 3uv$, por lo que la ecuación anterior se reescribe $u^3 - v^3 = q$. Se trata por tanto de resolver el sistema de ecuaciones

$$\begin{cases} u^3 - v^3 = q \\ uv = p/3 \end{cases}$$

Entonces $y = u^3$ cumple la igualdad

$$y^2 - qy - (p/3)^3 = u^6 - (u^3 - v^3)u^3 - u^3v^3 = 0,$$

así que y es una de las raíces del polinomio $g(\mathtt{t}) = \mathtt{t}^2 - q\mathtt{t} - (p/3)^3$.

Este argumento está presente en todos los procedimientos de resolución de ecuaciones polinómicas: reducir el problema a obtener las soluciones de una ecuación de grado menor. En nuestro caso podemos suponer que

$$u^3 = y = (q + \sqrt{q^2 + 4p^3/27})/2 \quad \& \quad v^3 = u^3 - q = (-q + \sqrt{q^2 + 4p^3/27})/2$$

y, sin precisar que significa *raíz cúbica,* Tartaglia obtiene

$$x = u - v = \sqrt[3]{(q + \sqrt{q^2 + 4p^3/27})/2} - \sqrt[3]{(-q + \sqrt{q^2 + 4p^3/27})/2}.$$

No vamos a entrar en más detalles, pero hay que señalar que la expresión anterior es ambigua pues aunque cada número real tiene una única raíz cúbica real tiene, salvo que sea nulo, tres raíces cúbicas complejas distintas, y hay que explicar qué significa el símbolo $\sqrt[3]{\cdot}$ en la fórmula anterior. Veremos a continuación como calcular de modo más sistemático todas las raíces de los polinomios de grado 3 o 4.

(C.3) Cálculo de las raíces de los polinomios de grado 3. Las raíces del polinomio irreducible $f(\mathtt{t}) := \mathtt{t}^3 + b\mathtt{t}^2 + c\mathtt{t} + d \in K[\mathtt{t}]$ en $\overline{K}$ son

$$t_1 := (-b+s_1+s_2)/3, \quad t_2 := (-b+s_1\xi^2+s_2\xi)/3 \quad \& \quad t_3 := (-b+s_1\xi+s_2\xi^2)/3,$$

donde $\xi \in \mathbb{C}$ es una raíz del polinomio ciclotómico $\Phi_2(\mathtt{t}) := \mathtt{t}^2 + \mathtt{t} + 1$ y s_1^3, s_2^3 son las raíces del polinomio de grado 2

$$g(\mathtt{t}) := \mathtt{t}^2 + (2b^3 - 9bc + 27d)\mathtt{t} + (b^6 - 9cb^4 + 27c^2b^2 - 27c^3),$$

que recibe el nombre de *resolvente cuadrática de* f, de modo que $s_1 s_2 = b^2 - 3c$.

Demostración. Sea ξ una raíz de Φ_2. Entonces $\xi^3 - 1 = (\xi - 1)\Phi_2(\xi) = 0$, por lo que $\xi^3 = 1$, luego la otra raíz de Φ_2 es $\xi^2 = 1/\xi$. Sea $L \subset \overline{K}$ un cuerpo de descomposición de $f \cdot \Phi_2$ sobre K. La imagen de ξ por un K-automorfismo σ de L es, por el Lema II.1.1, una raíz de Φ_2, es decir, ξ o ξ^2. Denotemos t_1, t_2 y t_3 las raíces de f en $\overline{K}$ (que todavía no sabemos que toman los valores del enunciado), y que son distintas porque f es irreducible. De nuevo por el Lema II.1.1, la imagen de cada t_i por σ es otra de las raíces t_j de f. Definimos

$$s_1 := t_1 + \xi t_2 + \xi^2 t_3 \quad \& \quad s_2 := t_1 + \xi^2 t_2 + \xi t_3,$$

y observamos que

$$\begin{aligned} \sigma(s_1) &= \sigma(t_1) + \sigma(\xi)\sigma(t_2) + \sigma(\xi^2)\sigma(t_3) \quad \& \\ \sigma(s_2) &= \sigma(t_1) + \sigma(\xi^2)\sigma(t_2) + \sigma(\xi)\sigma(t_3). \end{aligned}$$

Como t_1, t_2 y t_3 son distintos también lo son sus imágenes $\sigma(t_1)$, $\sigma(t_2)$ y $\sigma(t_3)$, que son elementos del conjunto $\{t_1, t_2, t_3\}$. Por tanto $\sigma(s_i)$ es una combinación $\sigma(s_i) = u_i t_1 + v_i t_2 + w_i t_3$ donde, de nuevo por la inyectividad de σ, los números u_i, v_i, w_i son distintos dos a dos y pertenecen al conjunto $\{1, \xi, \xi^2\}$. Como $1 = \xi^0$ lo anterior dice que para $i = 1, 2$, existen $\alpha_i, \beta_i, \gamma_i$ distintos dos a dos y pertenecientes al conjunto $\{0, 1, 2\}$ tales que

$$\sigma(s_i) := \xi^{\alpha_i} t_1 + \xi^{\beta_i} t_2 + \xi^{\gamma_i} t_3.$$

Además, si $\sigma(\xi) = \xi$ entonces $\sigma(\xi^2) = \xi^2$, mientras que si $\sigma(\xi) = \xi^2$ entonces $\sigma(\xi^2) = \xi^4 = \xi$. Esto implica que la imagen de s_1 determina la de s_2, por lo que las posibles imágenes de s_1 y s_2 por un K-automorfismo σ de L son las seis siguientes:

$$\left\{\begin{array}{rclcrcl}
\sigma(s_1) & = & t_1+\xi t_2+\xi^2 t_3 = s_1 & \& & \sigma(s_2) & = & t_1+\xi^2 t_2+\xi t_3 = s_2,\\
\sigma(s_1) & = & t_1+\xi^2 t_2+\xi t_3 = s_2 & \& & \sigma(s_2) & = & t_1+\xi t_2+\xi^2 t_3 = s_1,\\
\sigma(s_1) & = & \xi t_1+\xi^2 t_2+t_3 = \xi s_1 & \& & \sigma(s_2) & = & \xi t_1+\xi^2 t_2+t_3 = \xi^2 s_2,\\
\sigma(s_1) & = & \xi t_1+t_2+\xi^2 t_3 = \xi s_2 & \& & \sigma(s_2) & = & \xi^2 t_1+t_2+\xi t_3 = \xi^2 s_1,\\
\sigma(s_1) & = & \xi^2 t_1+t_2+\xi t_3 = \xi^2 s_1 & \& & \sigma(s_2) & = & \xi^2 t_3+\xi t_1+t_2 = \xi s_2\\
\sigma(s_1) & = & \xi^2 t_1+\xi t_2+t_3 = \xi^2 s_2 & \& & \sigma(s_2) & = & t_3+\xi^2 t_2+\xi t_1 = \xi^2 s_2
\end{array}\right.$$

De este modo, como $\xi^3 = 1$, bien $\sigma(s_1^3) = s_1^3$ y $\sigma(s_2^3) = s_2^3$, o $\sigma(s_1^3) = s_2^3$ y $\sigma(s_2^3) = s_1^3$. En consecuencia cada automorfismo $\sigma \in G(L : K)$ deja fijos $s_1^3 + s_2^3$ y $s_1^3 s_2^3$ y, como la extensión $L|K$ es de Galois, tanto $s_1^3 + s_2^3$ como $s_1^3 s_2^3$ pertenecen a K, esto es, el polinomio

$$g(\mathtt{t}) := (\mathtt{t} - s_1^3)(\mathtt{t} - s_2^3) = \mathtt{t}^2 - (s_1^3 + s_2^3)\mathtt{t} + s_1^3 s_2^3 \in K[\mathtt{t}].$$

Vamos a demostrar que ésta es la resolvente cuadrática del enunciado. Por las Fórmulas de Cardano–Vieta VII.1.13, vol. II, se tiene

$$\begin{aligned}\mathtt{t}^3 + b\mathtt{t}^2 + c\mathtt{t} + d = f(\mathtt{t}) &= (\mathtt{t} - t_1)(\mathtt{t} - t_2)(\mathtt{t} - t_3)\\ &= \mathtt{t}^3 - (t_1 + t_2 + t_3)\mathtt{t}^2 + (t_1t_2 + t_1t_3 + t_2t_3)\mathtt{t} - t_1t_2t_3,\end{aligned}$$

y como $\xi^2 + \xi + 1 = 0$, resulta que

$$s_1 + s_2 = 2t_1 + (\xi + \xi^2)(t_2 + t_3) = 2t_1 - (t_2 + t_3) = 3t_1 - (t_1 + t_2 + t_3) = 3t_1 + b,$$

mientras que, al multiplicar,

$$\begin{aligned}s_1 s_2 = t_1^2 + t_2^2 + t_3^2 + (\xi + \xi^2)(t_1t_2 + t_1t_3 + t_2t_3) &= (t_1 + t_2 + t_3)^2\\ + (\xi + \xi^2 - 2)(t_1t_2 + t_1t_3 + t_2t_3) &= (t_1 + t_2 + t_3)^2\\ - 3(t_1t_2 + t_1t_3 + t_2t_3) &= b^2 - 3c.\end{aligned}$$

En consecuencia, el término independiente del polinomio g es

$$s_1^3 s_2^3 = (s_1 s_2)^3 = (b^2 - 3c)^3 = b^6 - 9cb^4 + 27c^2b^2 - 27c^3.$$

Por otro lado, como $f(t_1) = 0$, el opuesto del coeficiente de $\mathtt{t}$ en $g(\mathtt{t})$ es

$$\begin{aligned} s_1^3 + s_2^3 &= (s_1+s_2)^3 - 3s_1s_2(s_1+s_2) = (3t_1+b)^3 - 3(b^2-3c)(3t_1+b) \\ &= 27t_1^3 + 27bt_1^2 + 9b^2t_1 + b^3 - 9b^2t_1 - 3b^3 + 27ct_1 + 9bc \\ &= 27(t_1^3 + bt_1^2 + ct_1) - 2b^3 + 9bc = 27(f(t_1) - d) - 2b^3 + 9bc \\ &= -2b^3 + 9bc - 27d. \end{aligned}$$

Sustituyendo los valores de $s_1^3 + s_2^3$ y $s_1^3 s_2^3$ que acabamos de obtener llegamos finalmente a

$$g(\mathtt{t}) = \mathtt{t}^2 + (2b^3 - 9bc + 27d)\mathtt{t} + (b^6 - 9cb^4 + 27c^2b^2 - 27c^3).$$

Sean $r_1 := s_1^3$ y $r_2 := s_2^3$ las raíces del polinomio de segundo grado g. Entonces, las raíces t_1, t_2 y t_3 de f son las soluciones del sistema de ecuaciones lineales

$$\left\{ \begin{array}{rcrcrcl} t_1 & + & t_2 & + & t_3 & = & -b \\ t_1 & + & \xi t_2 & + & \xi^2 t_3 & = & s_1 \\ t_1 & + & \xi^2 t_2 & + & \xi t_3 & = & s_2 \end{array} \right. \tag{I.1}$$

Este sistema es compatible y determinado pues el determinante de la matriz de coeficientes es $3(\xi^2 - \xi) \neq 0$, y su solución es

$$t_1 := (-b + s_1 + s_2)/3, \;\; t_2 := (-b + s_1\xi^2 + s_2\xi)/3 \;\; \& \;\; t_3 := (-b + s_1\xi + s_2\xi^2)/3.$$

En el párrafo anterior hemos cometido una imprecisión deliberada. Al calcular las raíces de g no obtenemos s_1 ni s_2 sino sus cubos $r_1 = s_1^3$ y $r_2 = s_2^3$. Pero t_1, t_2 y t_3 se expresan en función de s_1 y s_2, no de sus cubos. Como "elevar al cubo" es una función no inyectiva de $\mathbb{C}$ en $\mathbb{C}$, hemos de precisar qué raíces cúbicas s_1 y s_2 de r_1 y r_2 elegimos. La respuesta está dada por los cálculos precedentes, en los que vimos que $s_1 s_2 = b^2 - 3c$. □

Observación y Ejemplo C.4 (1) Si $b = 0$ en C.3, entonces

$$f(\mathtt{t}) := \mathtt{t}^3 + c\mathtt{t} + d \quad \& \quad g(\mathtt{t}) := \mathtt{t}^2 + 27d\mathtt{t} - 27c^3,$$

y si $\xi \in \mathbb{C}$ es una raíz del polinomio $\mathtt{t}^2 + \mathtt{t} + 1$, las raíces de f son

$$t_1 := (s_1 + s_2)/3, \quad t_2 := (s_1\xi^2 + s_2\xi)/3 \quad \& \quad t_3 := (s_1\xi + s_2\xi^2)/3,$$

donde s_1^3 y s_2^3 son las raíces de la resolvente cuadrática g de f. En consecuencia,

$$s_1^3 = \frac{-27d + \sqrt{27^2d^2 + 108c^3}}{2} \quad \& \quad s_2^3 = \frac{-27d - \sqrt{27^2d^2 + 108c^3}}{2}.$$

Como, además, $s_1 s_2 = -3c$, las raíces de f son

$$t_1 := \sqrt[3]{-\tfrac{d}{2} + \sqrt{\tfrac{d^2}{4} + \tfrac{c^3}{27}}} \; + \; \sqrt[3]{-\tfrac{d}{2} - \sqrt{\tfrac{d^2}{4} + \tfrac{c^3}{27}}},$$
$$t_2 := \xi^2 \sqrt[3]{-\tfrac{d}{2} + \sqrt{\tfrac{d^2}{4} + \tfrac{c^3}{27}}} \; + \; \xi \sqrt[3]{-\tfrac{d}{2} - \sqrt{\tfrac{d^2}{4} + \tfrac{c^3}{27}}},$$
$$t_3 := \xi \sqrt[3]{-\tfrac{d}{2} + \sqrt{\tfrac{d^2}{4} + \tfrac{c^3}{27}}} \; + \; \xi^2 \sqrt[3]{-\tfrac{d}{2} - \sqrt{\tfrac{d^2}{4} + \tfrac{c^3}{27}}}.$$

(2) Para calcular las raíces del polinomio de grado tres $f(\mathtt{t}) := \mathtt{t}^3 + 3\mathtt{t}^2 + \mathtt{t} + 1$ es útil emplear la transformación de Tschirnhaus y considerar el polinomio auxiliar

$$h(\mathtt{t}) := f(\mathtt{t} - 1) = (\mathtt{t} - 1)^3 + 3(\mathtt{t} - 1)^2 + (\mathtt{t} - 1) + 1 = \mathtt{t}^3 - 2\mathtt{t} + 2,$$

que carece de término en $\mathtt{t}^2$. Denotando $\xi := e^{2\pi i/3}$, que es una raíz cúbica primitiva de la unidad, y aplicando el apartado anterior con $c := -2$ y $d := 2$ se obtienen las raíces t_1, t_2 y t_3 de h, que son

$$t_1 := \sqrt[3]{-1 + \sqrt{1 - \tfrac{8}{27}}} \; + \; \sqrt[3]{-1 - \sqrt{1 - \tfrac{8}{27}}},$$
$$t_2 := \xi^2 \sqrt[3]{-1 + \sqrt{1 - \tfrac{8}{27}}} \; + \; \xi \sqrt[3]{-1 - \sqrt{1 - \tfrac{8}{27}}},$$
$$t_3 := \xi \sqrt[3]{-1 + \sqrt{1 - \tfrac{8}{27}}} \; + \; \xi^2 \sqrt[3]{-1 - \sqrt{1 - \tfrac{8}{27}}}$$

y así las raíces de f son $u_1 := t_1 - 1$, $u_2 := t_2 - 1$ y $u_3 := t_3 - 1$.

(C.5) Cálculo de las raíces de los polinomios de grado 4. Empleando la transformación de Tschirnhaus, C.2, es suficiente calcular las raíces de los polinomios de grado 4 de la forma

$$f(\mathtt{t}) := \mathtt{t}^4 + c\mathtt{t}^2 + d\mathtt{t} + e \in K[\mathtt{t}],$$

que son

$$t_1 := (\sqrt{-s_1} + \sqrt{-s_2} + \sqrt{-s_3})/2, \qquad t_2 := (\sqrt{-s_1} - \sqrt{-s_2} - \sqrt{-s_3})/2$$
$$t_3 := (-\sqrt{-s_1} + \sqrt{-s_2} - \sqrt{-s_3})/2 \quad \& \quad t_4 := (-\sqrt{-s_1} - \sqrt{-s_2} + \sqrt{-s_3})/2,$$

donde s_1, s_2 y s_3 son las raíces de la resolvente cúbica de f, véase VI.3.3, que es el polinomio

$$g(\mathtt{t}) := \mathtt{t}^3 - 2c\mathtt{t}^2 + (c^2 - 4e)\mathtt{t} + d^2.$$

Además, $\sqrt{-s_1}$, $\sqrt{-s_2}$ y $\sqrt{-s_3}$ deben elegirse de modo que

$$\sqrt{-s_1}\cdot\sqrt{-s_2}\cdot\sqrt{-s_3}=-d.$$

Demostración. Sean t_1,t_2,t_3,t_4 las raíces de f en $\overline{K}$. Hemos probado en la Proposición VI.3.3 que las raíces de g son

$$s_1:=(t_1+t_2)(t_3+t_4),\quad s_2:=(t_1+t_3)(t_2+t_4)\quad\&\quad s_3:=(t_1+t_4)(t_2+t_3).$$

Nótese que $t_1+t_2+t_3+t_4=0$, ya que el coeficiente del monomio de f de grado 3 es 0. Así, $t_3+t_4=-(t_1+t_2)$, $t_2+t_4=-(t_1+t_3)$ y $t_2+t_3=-(t_1+t_4)$, por lo que

$$\left\{\begin{array}{rcrcrcrcc} t_1 & + & t_2 & + & t_3 & + & t_4 & = & 0\\ t_1 & + & t_2 & & & & & = & \sqrt{-s_1}\\ t_1 & & & + & t_3 & & & = & \sqrt{-s_2}\\ t_1 & & & & & + & t_4 & = & \sqrt{-s_3}\end{array}\right. \tag{I.2}$$

Este sistema de ecuaciones lineales en las incógnitas t_1,t_2,t_3 y t_4 es compatible determinado pues el determinante de la matriz de coeficientes es $-2\neq 0$, y su solución es la propuesta en el enunciado.

Nótese que cada número complejo no nulo tiene dos raíces cuadradas, por lo que hemos de especificar cuáles son las seleccionadas al emplear los símbolos $\sqrt{-s_1}$, $\sqrt{-s_2}$ y $\sqrt{-s_3}$. De las Fórmulas de Cardano-Vieta, VII.1.13 vol. II aplicadas al polinomio f, se tiene

$$d=-(t_1t_2t_3+t_1t_2t_4+t_1t_3t_4+t_2t_3t_4).$$

En consecuencia, empleando las igualdades del sistema (I.2),

$$\begin{aligned}\sqrt{-s_1}\cdot\sqrt{-s_2}\cdot\sqrt{-s_3}&=(t_1+t_2)(t_1+t_3)(t_1+t_4)\\ &=\big(t_1^2+(t_2+t_3)t_1+t_2t_3\big)(t_1+t_4)\\ &=t_1^3+(t_2+t_3+t_4)t_1^2+(t_1t_2t_3+t_1t_2t_4+t_1t_3t_4+t_2t_3t_4)\\ &=t_1^3-t_1^3+(t_1t_2t_3+t_1t_2t_4+t_1t_3t_4+t_2t_3t_4)=-d.\end{aligned}$$

□

Ejemplo C.6 Vamos a calcular las raíces del polinomio

$$f(\mathtt{t}):=\mathtt{t}^4-(5/2)\mathtt{t}^2+4\mathtt{t}+(113/16).$$

Con las notaciones de C.5, $c:=-5/2$, $d:=4$ y $e:=113/16$. Por tanto,

$$-2c=5,\quad c^2-4e=-22\quad\&\quad d^2=16,$$

luego la resolvente cúbica de f es

$$g(\mathtt{t}) := \mathtt{t}^3 - 2c\mathtt{t}^2 + (c^2 - 4e)\mathtt{t} + d^2 = \mathtt{t}^3 + 5\mathtt{t}^2 - 22\mathtt{t} + 16.$$

Es fácil darse cuenta de que $s_1 := 1$ es raíz de g, y al dividir g entre $\mathtt{t} - 1$ resulta

$$g(\mathtt{t}) = (\mathtt{t} - 1)(\mathtt{t}^2 + 6\mathtt{t} - 16) = (\mathtt{t} - 1)(\mathtt{t} - 2)(\mathtt{t} + 8),$$

por lo que $s_2 := 2$ y $s_3 := -8$ son las restantes raíces de g. Elegimos sus raíces cuadradas de modo que

$$-4 = -d = \sqrt{-s_1} \cdot \sqrt{-s_2} \cdot \sqrt{-s_3} = \sqrt{-1} \cdot \sqrt{-2} \cdot \sqrt{8},$$

así que tomamos $\sqrt{-s_1} = i$, $\sqrt{-s_2} = \sqrt{2}i$ y $\sqrt{-s_3} = 2\sqrt{2}$, donde denotamos $\sqrt{2}$ el único número real positivo cuyo cuadrado vale 2 e $i := \sqrt{-1}$.

Aplicando la Proposición C.5 concluimos finalmente que las raíces de f son

$$\begin{cases} t_1 &=& (\sqrt{-s_1} + \sqrt{-s_2} + \sqrt{-s_3})/2 &=& \big((1+\sqrt{2})i + 2\sqrt{2}\big)/2 \\ t_2 &=& (\sqrt{-s_1} - \sqrt{-s_2} - \sqrt{-s_3})/2 &=& \big((1-\sqrt{2})i - 2\sqrt{2}\big)/2 \\ t_3 &=& (-\sqrt{-s_1} + \sqrt{-s_2} - \sqrt{-s_3})/2 &=& \big((\sqrt{2}-1)i - 2\sqrt{2}\big)/2 \\ t_4 &=& (-\sqrt{-s_1} - \sqrt{-s_2} + \sqrt{-s_3})/2 &=& \big((-1-\sqrt{2})i + 2\sqrt{2}\big)/2 \end{cases}$$

APÉNDICE D

Teorema de Chevalley-Warning

Dedicamos este apéndice a probar el Teorema de Chevalley-Warning, que permite analizar la isotropía de las formas homogéneas sobre cuerpos finitos. Antes necesitamos el siguiente lema auxiliar.

Lema D.1 *Sean K un cuerpo finito con q elementos y n un entero no negativo. Entonces*

$$\sum_{x\in K} x^n = \begin{cases} -1 & si\ n \neq 0 \quad \& \quad n \in (q-1)\mathbb{Z}. \\ 0 & si\ n = 0 \quad o \quad n \notin (q-1)\mathbb{Z}. \end{cases}$$

Demostración. Para $n = 0$ se tiene $\sum_{x\in K} x^n = \mathrm{Card}(K) = q = 0$, ya que la característica de un cuerpo finito divide a su cardinal. Suponemos ahora que $n \neq 0$ y distinguimos los dos casos del enunciado.

Caso 1. Si $(q-1)\,|n$ existe $r \in \mathbb{Z}$ tal que $n = (q-1)r$, y como $\mathrm{ord}(K^*) = q-1$ tenemos que $x^n = x^{(q-1)r} = 1$ para cada $x \in K^*$. Así,

$$\sum_{x\in K} x^n = \sum_{x\in K^*} x^n = \mathrm{ord}(K^*) = q - 1 = -1.$$

Caso 2. Si $(q-1)\not| n$ existen $r, s \in \mathbb{Z}$ tales que $n = (q-1)s + r$, donde $s \geq 0$ y $0 < r < q-1$. Por tanto, para cada $x \in K^*$, y puesto que $x^{q-1} = 1$, se tiene

$$x^n = x^{(q-1)s+r} = x^{(q-1)s}x^r = x^r.$$

En consecuencia

$$y := \sum_{x\in K} x^n = \sum_{x\in K^*} x^n = \sum_{x\in K^*} x^r.$$

Por V.1.7 K^* es cíclico, y elegimos un generador suyo ζ. Como $\zeta K^* = K^*$ se tiene

$$y = \sum_{x\in K^*} x^r = \sum_{x\in K^*} (\zeta x)^r = \zeta^r\big(\sum_{x\in K^*} x^r\big) = \zeta^r y \quad \Longrightarrow \quad y(\zeta^r - 1) = 0,$$

y $\zeta^r \neq 1$, porque $0 < r < q-1 = o(\zeta)$, así que $y = 0$. □

Teorema D.2 (Teorema de Chevalley–Warning) *Sean K un cuerpo finito de característica p, m un entero positivo, $\mathtt{x} := (\mathtt{x}_1, \ldots, \mathtt{x}_m)$ indeterminadas sobre K y $f_1, \ldots, f_r \in K[\mathtt{x}]$ no nulos tales que* $\deg(f_1) + \cdots + \deg(f_r) < m$. *Entonces, el número de elementos del conjunto*

$$\mathcal{Z} = \{x \in K^m : \, f_1(x) = 0, \ldots, f_r(x) = 0\}$$

es múltiplo de p. En particular, si $\mathcal{Z}$ no es vacío, entonces $\mathrm{Card}(\mathcal{Z}) \geq p$.

Demostración. Sea q el cardinal de K y consideramos el polinomio

$$f(\mathtt{x}) := (1 - f_1(\mathtt{x})^{q-1}) \cdots (1 - f_r(\mathtt{x})^{q-1}) \in K[\mathtt{x}].$$

Para cada $x \in K^m$ se cumple que

$$f(x) = \begin{cases} 1 & \text{si } x \in \mathcal{Z} \\ 0 & \text{si } x \in K^m \setminus \mathcal{Z}. \end{cases}$$

En efecto, si $x \in \mathcal{Z}$ cada $f_i^{q-1}(x) = 0$, luego $f(x) = 1$. Por otra parte, si $x \in K^m \setminus \mathcal{Z}$, entonces existe $i = 1, \ldots, r$ tal que $f_i(x) \neq 0$, es decir, $f_i(x) \in K^*$. Como K^* es un grupo de orden $q - 1$, tenemos que $f_i^{q-1}(x) = 1$ y por tanto $f(x) = 0$.

Esto implica que $\mathrm{Card}(\mathcal{Z}) \bmod p = \sum_{x \in K^m} f(x) \bmod p$, y todo se reduce a probar que la suma $\sum_{x \in K^m} f(x)$ es nula, como elemento de K. Denotando $\nu := (\nu_1, \ldots, \nu_m)$ y $\mathtt{x}^\nu = \mathtt{x}_1^{\nu_1} \cdots \mathtt{x}_m^{\nu_m}$ escribimos abreviadamente

$$f(\mathtt{x}) = \sum_{\nu} a_\nu \mathtt{x}^\nu.$$

Como la suma $\deg(f_1) + \cdots + \deg(f_r)$ es menor que m resulta

$$\begin{aligned} \deg(f) = \deg\Big(\prod_{i=1}^{r}(1 - f_i^{q-1})\Big) &= \sum_{i=1}^{r} \deg\left(1 - f_i^{q-1}\right) \\ &= (q-1)\sum_{i=1}^{r} \deg(f_i) < m(q-1). \end{aligned}$$

En consecuencia, para cada multiíndice $\nu = (\nu_1, \ldots, \nu_m)$ tal que el coeficiente a_ν de f es no nulo, se tiene $|\nu| = \nu_1 + \cdots + \nu_m < m(q-1)$. Además,

$$\sum_{x \in K^m} f(x) = \sum_{x \in K^m} \sum_{\nu} a_\nu x^\nu = \sum_{\nu} a_\nu \Big(\sum_{x \in K^m} x^\nu \Big),$$

por lo que es suficiente comprobar que $\sum_{x\in K^m} x^\nu = 0$ para cada multiíndice ν tal que $|\nu| = \nu_1 + \cdots + \nu_m < m(q-1)$. Pero si se da esta última desigualdad entonces alguno de los ν_i, digamos ν_1, es menor que $q-1$, así que, $\nu_1 = 0$ o $1 \le \nu_1 \notin (q-1)\mathbb{Z}$. Se deduce del Lema D.1 que $\sum_{x_1\in K} x_1^{\nu_1} = 0$, y concluimos que

$$\sum_{x\in K^m} x^\nu = \sum_{z\in K^{m-1}} z^\mu \sum_{x_1\in K} x_1^{\nu_1} = 0,$$

donde $z := (x_2, \ldots, x_m)$ y $\mu := (\nu_2, \ldots, \nu_m)$. □

Corolario D.3 *Sean K un cuerpo finito y $f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_m]$ una forma cuadrática, donde $m \ge 3$. Entonces, existe $a \in K^m$ con alguna coordenada no nula tal que $f(a) = 0$.*

Demostración. Sea $p = \mathrm{char}(K)$. Aplicando el Teorema D.2 con $r := 1$ y $\deg(f) := 2 < 3 \le m$, la ecuación $f(\mathtt{x}) = 0$ tiene al menos $p > 1$ soluciones, pues $f(0) = 0$. Por tanto, f tiene una solución no nula en K^m. □

Observaciones D.4 El Corolario anterior no se aplica a las formas cuadráticas en dos variables, que se estudian directamente. Se tiene lo siguiente.

(1) Para decidir si una forma cuadrática en dos variables,

$$f(\mathtt{x}_1, \mathtt{x}_2) = a\mathtt{x}_1^2 + b\mathtt{x}_1\mathtt{x}_2 + c\mathtt{x}_2^2 \in K[\mathtt{x}_1, \mathtt{x}_2],$$

se anula en algún punto $\zeta := (a_1, a_2) \in K^2$, una de cuyas coordenadas es no nula, basta estudiar si alguno de los polinomios de grado 2 en una variable $a\mathtt{x}_1^2 + b\mathtt{x}_1 + c$ y $a + b\mathtt{x}_2 + c\mathtt{x}_2^2$ tiene alguna raíz en K.

(2) Si $K := \mathbb{F}_p$ donde p es un primo impar, la Ley de reciprocidad cuadrática permite decidir si un polinomio del tipo $\mathtt{t}^2 - a$ tiene alguna raíz en $\mathbb{F}_p$. Obsérvese. además, que si $g(\mathtt{t}) := \mathtt{t}^2 + b\mathtt{t} + c \in \mathbb{F}_p[\mathtt{t}]$ y $p \ne 2$, y denotamos $\mathtt{x} := \mathtt{t} + b/2$ y $a := b^2/4 - c$, se tiene

$$\mathtt{t}^2 + b\mathtt{t} + c = (\mathtt{t} + b/2)^2 + c - b^2/4 = \mathtt{x}^2 - a,$$

lo que reduce el problema de decidir si g tiene alguna raíz en $\mathbb{F}_p$ a decidir si la tiene un polinomio de la forma $\mathtt{x}^2 - a$. Por otro lado, los polinomios de grado 2 en una variable con coeficientes en $K := \mathbb{F}_2$ son las siguientes:

$$\mathtt{t}^2,\ \mathtt{t}^2 + \mathtt{t} = \mathtt{t}(\mathtt{t}+1),\ \mathtt{t}^2 + 1 = (\mathtt{t}+1)^2 \quad \& \quad \mathtt{t}^2 + \mathtt{t} + 1.$$

Los tres primeros tienen alguna raíz en $\mathbb{F}_2$, pero no el último, que por tanto es irreducible en $\mathbb{F}_2[\mathtt{t}]$.

APÉNDICE E

Soluciones a los ejercicios propuestos

Soluciones a los ejercicios del Capítulo I

Número I.1 Caracterizar los números complejos α tales que $E := \{a+b\alpha : a, b \in \mathbb{Q}\}$ es un subcuerpo de $\mathbb{C}$. Dar un ejemplo de un α que satisface esta condición y otro que no la cumple.

Solución. Supongamos que E es un cuerpo. Como $\alpha \in E$ también $\alpha^2 \in E$, luego existen $a, b \in \mathbb{Q}$ tales que $\alpha^2 = a + b\alpha$. Así, existe $f(\mathtt{t}) := \mathtt{t}^2 - b\mathtt{t} - a \in \mathbb{Q}[\mathtt{t}]$ tal que $f(\alpha) = 0$. Recíprocamente, si existe un polinomio de grado 2 con coeficientes en $\mathbb{Q}$ que tiene a α por raíz éste es algebraico sobre $\mathbb{Q}$ y su polinomio mínimo tiene grado menor o igual que 2. Si el grado es 1 entonces $\alpha \in \mathbb{Q}$, luego $E = \mathbb{Q}$ es un cuerpo. Si vale 2, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ y una base de $\mathbb{Q}(\alpha)$ como $\mathbb{Q}$-espacio vectorial es $\{1, \alpha\}$, es decir, $\mathbb{Q}(\alpha) = \{a + b\alpha : a, b \in \mathbb{Q}\} = E$. En particular, E es un subcuerpo de $\mathbb{C}$. Así, E es subcuerpo de $\mathbb{C}$ si y sólo si α es raíz de algún polinomio en $\mathbb{Q}[\mathtt{t}]$ de grado 2.

Como $\alpha := \sqrt{-1}$ es raíz del polinomio $\mathtt{t}^2 + 1$, cumple esta condición. Sin embargo $\alpha := \sqrt[3]{2}$ no la cumple, pues al ser $f(\mathtt{t}) := \mathtt{t}^3 - 2$ un polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$ que tiene a α por raíz, es su polinomio mínimo, luego los polinomios no nulos con coeficientes racionales de los que $\sqrt[3]{2}$ es raíz son múltiplos de f y su grado es mayor o igual que 3. □

Número I.2 Encontrar una extensión de cuerpos $L|K$ tal que existan $\alpha, \beta \in L \setminus K$, de modo que $\alpha \neq \pm\beta$ y $K(\alpha) = K(\beta)$. ¿Qué relación hay entre los polinomios mínimos de α y de β sobre K?

Solución. Elegimos $K := \mathbb{Q}$ y $\alpha := \sqrt{2}$, $\beta := 1 + \alpha$, que cumplen $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, ya que $\alpha \in \mathbb{Q}(\beta)$ y $\beta \in \mathbb{Q}(\alpha)$, pero $\alpha \neq \pm\beta$. Ahora bien, si se da la igualdad $K(\alpha) = K(\beta)$ los polinomios mínimos sobre K de α y β tienen igual grado:

$$\deg(P_{K,\alpha}) = [K(\alpha) : K] = [K(\beta) : K] = \deg(P_{K,\beta}).$$

□

Número I.3 ¿Cuáles son las raíces en un cuerpo K de característica p del polinomio $\mathtt{t}^p - 1$?

Solución. Sea $u \in K$ una raíz del polinomio $f(\mathtt{t}) := \mathtt{t}^p - 1$. Por la Fórmula de Newton,

$$(u-1)^p = \sum_{j=0}^{p} (-1)^{p-j} \binom{p}{j} u^j. \tag{I.1}$$

Vimos en el Ejemplo VI.2.7, vol. II, que para $0 < j < p$ el número combinatorio $\binom{p}{j}$ es un número entero múltiplo de p. Como $\mathrm{char}(K) = p$, esto implica que de la suma en (I.1) sólo son no nulos los sumandos para $j = 0$ y $j = p$, es decir,

$$(u-1)^p = u^p + (-1)^p = u^p - 1 = f(u) = 0.$$

Como K es cuerpo, $u - 1 = 0$, así que $u = 1$ es la única raíz de f en K. □

Número I.4 Para los siguientes valores de $\alpha \in \mathbb{C}$ encontrar el polinomio mínimo de α sobre $\mathbb{Q}$ y el grado de la extensión $\mathbb{Q}(\alpha)|\mathbb{Q}$:

$$\alpha := (\sqrt{3}-1)/2, \quad \alpha := (i+1)\sqrt{5}/3 \quad \& \quad \alpha := \sqrt{1-\sqrt{11}}.$$

Solución. (1) Si elevamos al cuadrado los dos miembros de la igualdad $2\alpha + 1 = \sqrt{3}$ se tiene $4\alpha^2 + 4\alpha - 2 = 0$. Además $\alpha \notin \mathbb{Q}$ pues $\sqrt{3} \notin \mathbb{Q}$, así que $P_{\mathbb{Q},\alpha}(\mathtt{t}) = \mathtt{t}^2 + \mathtt{t} - 1/2$.

(2) Elevamos al cuadrado la igualdad $3\alpha = (1+i)\sqrt{5}$ para obtener $9\alpha^2 = 10i$. Elevando al cuadrado de nuevo, $81\alpha^4 = -100$, luego α es raíz del polinomio $f(\mathtt{t}) := \mathtt{t}^4 + 100/81$. Vamos a demostrar que éste es el polinomio mínimo de α sobre $\mathbb{Q}$.

El polinomio mínimo de $\sqrt{5}$ sobre $\mathbb{Q}$ es $\mathtt{t}^2 - 5$ porque tiene a $\sqrt{5} \in \mathbb{R} \setminus \mathbb{Q}$ por raíz, así que $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$. Además $i = 9\alpha^2/10 \in \mathbb{Q}(\alpha)$, luego $\sqrt{5} = 3\alpha/(1+i) \in \mathbb{Q}(\alpha)$. En consecuencia, $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{5}) \subsetneq \mathbb{Q}(\alpha)$, y el contenido $\mathbb{Q}(\sqrt{5}) \subsetneq \mathbb{Q}(\alpha)$ es estricto pues $\alpha \in \mathbb{C} \setminus \mathbb{R}$. Así, $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{5})] \geq 2$ y, por la transitividad del grado,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{5})] \cdot [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] \geq 2 \cdot 2 = 4 = \deg(f) \geq [\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Esto implica, por un lado, que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, y por otro que $f = P_{\mathbb{Q},\alpha}$.

(3) También en este caso elevamos al cuadrado, para obtener $\sqrt{11} = 1 - \alpha^2$, y elevando al cuadrado de nuevo resulta $\alpha^4 - 2\alpha^2 - 10 = 0$. Por tanto $P_{\mathbb{Q},\alpha}(\mathtt{t}) = \mathtt{t}^4 - 2\mathtt{t}^2 - 10$, pues este polinomio es, por el Criterio de Eisenstein, irreducible en $\mathbb{Q}[\mathtt{t}]$. □

Número I.5 (1) Sean $L|K$ una extensión finita y $f \in K[\mathtt{t}]$ un polinomio irreducible. Probar que si f tiene alguna raíz en L entonces el grado de f divide al grado $[L : K]$ de la extensión.

(2) Supongamos que $[L : K]$ es un número primo. Demostrar que cada elemento $\alpha \in L \setminus K$ cumple que $L = K(\alpha)$.

Solución. (1) Sea $u \in L$ una raíz de f. Entonces $K \subset K(u) \subset L$ y $f := P_{K,u}$, luego

$$[L : K] = [K(u) : K] \cdot [L : K(u)] = \deg(f) \cdot [L : K(u)],$$

por lo que $\deg(f)$ divide a $[L : K]$.

(2) Aplicando la transitividad del grado a los cuerpos $K \subsetneq K(\alpha) \subset L$ resulta

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

Como $[L : K]$ es primo y $[K(\alpha) : K] \neq 1$, se tiene $[L : K(\alpha)] = 1$, o sea, $L = K(\alpha)$. □

Número I.6 Sean $a := \sqrt{5} + \sqrt{-5}$ y $b := \sqrt[4]{5}$. Calcular el grado de la extensión $\mathbb{Q}(a, b)|\mathbb{Q}(b)$.

Solución. Como $\sqrt{5} = b^2$ y $\sqrt{-5} = ib^2$, donde $i := \sqrt{-1} \in \mathbb{C}$, se tiene

$$E := \mathbb{Q}(a, b) = \mathbb{Q}(b^2 + \sqrt{-5}, b) = \mathbb{Q}(\sqrt{-5}, b) = \mathbb{Q}(ib^2, b) = \mathbb{Q}(i, b) = \mathbb{Q}(b)(i).$$

Puesto que $\mathbb{Q}(b) \subset \mathbb{R}$ mientras que $i \in \mathbb{C} \setminus \mathbb{R}$, el polinomio mínimo de i sobre $\mathbb{Q}(b)$ es $\mathtt{t}^2 + 1$, y por tanto $[E : \mathbb{Q}(b)] = [\mathbb{Q}(b)(i) : \mathbb{Q}(b)] = \deg(\mathtt{t}^2 + 1) = 2$. □

Número I.7 Sean $E|K$ una extensión y $\alpha \in E$ un elemento algebraico sobre K. Demostrar que si el grado de la extensión $K(\alpha)|K$ es impar entonces $K(\alpha^2) = K(\alpha)$.

Solución. Denotamos $L := K(\alpha^2)$ y $f(\mathtt{t}) := \mathtt{t}^2 - \alpha^2 \in L[\mathtt{t}]$, que cumple $f(\alpha) = 0$. El polinomio mínimo g de α sobre L divide a f en $L[\mathtt{t}]$, y por tanto $\deg(g) \leq 2$. Ahora bien,

$$[K(\alpha) : K] = [K(\alpha) : L] \cdot [L : K] = \deg(g) \cdot [L : K],$$

luego $\deg(g)$ es impar, así que $[K(\alpha) : L] = \deg(g) = 1$, es decir, $K(\alpha) = L = K(\alpha^2)$. □

Número I.8 Sean $L|K$ una extensión de cuerpos, $f \in K[\mathtt{t}] \setminus K$ y $\alpha \in L$ transcendente sobre K.

(1) Demostrar que $f(\alpha)$ es transcendente sobre K.

(2) Demostrar que si $\beta \in L$ satisface $f(\beta) = \alpha$ entonces β es transcendente sobre K.

Solución. (1) El polinomio $g(\mathtt{t}) := f(\mathtt{t}) - f(\alpha) \in K(f(\alpha))[\mathtt{t}]$ no es nulo porque $\deg(f) > 0$, y cumple que $g(\alpha) = 0$. Por tanto la extensión $K(\alpha)|K(f(\alpha))$ es algebraica. Si $f(\alpha)$ fuese algebraico sobre K la extensión $K(f(\alpha))|K$ sería algebraica también, por lo que $K(\alpha)|K$ sería una extensión algebraica. Esto es falso ya que α es transcendente sobre K, luego también $f(\alpha)$ es transcendente sobre K.

(2) Nótese que $K \subsetneq K(\alpha) \subset K(\beta)$ pues $\alpha = f(\beta) \in K(\beta)$. Si β fuese algebraico sobre K la extensión $K(\beta)|K$ sería finita, luego también lo sería $K(\alpha)|K$, y esto es falso porque α es transcendente sobre K. □

Número I.9 Sea $K(\alpha,\beta)|K$ una extensión de cuerpos de modo que $\alpha \notin K$ es algebraico sobre K y β es transcendente sobre K. Demostrar que la extensión $K(\alpha,\beta)|K$ no es simple.

Solución. Suponemos, por reducción al absurdo, que existe $x \in K$ de modo que $K(\alpha,\beta) = K(x)$. Por ser β transcendente sobre K la extensión $K(\beta)|K$ no es finita, luego tampoco lo es la extensión $K(x)|K = K(\alpha,\beta)|K$. Por tanto x es transcendente sobre K y, como $\alpha \in K(x)$, se escribe $\alpha = p(x)/q(x)$ para ciertos polinomios no nulos $p, q \in K[\mathtt{t}]$. Además, sustituyendo α por $1/\alpha$ si es preciso podemos suponer que $d := \deg(q) \geq \deg(p) := e$. Más aún, podemos suponer que $d > e$ pues si $e = d$ el cociente se escribe como

$$\alpha = p(x)/q(x) = a + r(x)/p(x)$$

donde $a \in K$ y $r \in K[\mathtt{t}]$ es un polinomio no nulo, ya que $\alpha \notin K$, y $\deg(r) < \deg(q)$. De este modo basta sustituir α por $\alpha - a$ y p por r para que se cumpla lo supuesto.

Al ser α algebraico sobre K, existe $f(\mathtt{t}) := \sum_{i=0}^{n} a_i \mathtt{t}^i \in K[\mathtt{t}]$ irreducible tal que $f(\alpha) = 0$. La irreducibilidad de f asegura que $a_0 = f(0) \neq 0$. Si escribimos

$$p(\mathtt{t}) = \sum_{j=0}^{e} b_j \mathtt{t}^j \quad \& \quad q(\mathtt{t}) = \sum_{k=0}^{d} c_k \mathtt{t}^k,$$

al sustituir resulta

$$0 = f(\alpha)q(x)^n = \sum_{i=0}^{n} a_i p(x)^i q(x)^{-i} q(x)^n = \sum_{i=0}^{n} a_i p(x)^i q(x)^{n-i}$$

luego, puesto que x es transcendente sobre K, ha de ser nulo el polinomio

$$g(\mathtt{t}) := \sum_{i=0}^{n} a_i p(\mathtt{t})^i q(\mathtt{t})^{n-i}.$$

Vamos a llegar a contradicción probando que g no es nulo. Ya vimos que $a_0 \neq 0$ y si denotamos

$$h_i(\mathtt{t}) := p(\mathtt{t})^i q(\mathtt{t})^{n-i} = \Big(\sum_{j=0}^{e} b_j \mathtt{t}^j\Big)^i \Big(\sum_{k=0}^{d} c_k \mathtt{t}^k\Big)^{n-i},$$

su grado es

$$\deg(h_i) = ei + d(n-i) = dn + i(e-d).$$

Como $e < d$, para todo $i > 0$ se tiene $\deg(h_0) > \deg(h_i)$, luego $\deg(g) = \deg(h_0) = dn$. Por tanto $g \neq 0$, lo que nos proporciona la contradicción buscada. □

Número I.10 Sean K un cuerpo y $f(\mathtt{t}) := \mathtt{t}^n - a \in K[\mathtt{t}]$. Supongamos que f es irreducible en $K[\mathtt{t}]$. Dados un divisor m de n y una raíz α de f, calcular el polinomio mínimo de α^m sobre K.

Solución. Existe $d \in \mathbb{Z}$ tal que $n = md$ y observamos que α^m es raíz de $g(\mathtt{t}) := \mathtt{t}^d - a$, ya que

$$g(\alpha^m) = \alpha^{md} - a = \alpha^n - a = f(\alpha) = 0.$$

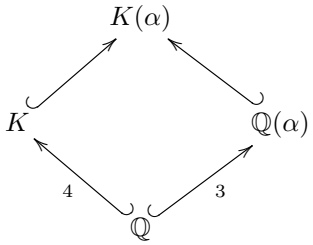
De hecho g es irreducible en $K[\mathtt{t}]$ y por ello es el polinomio mínimo de α^m sobre K. Si no lo fuese existirían polinomios $h, \ell \in K[\mathtt{t}]$ de grado positivo tales que $g = h\ell$, y por tanto,

$$f(\mathtt{t}) = \mathtt{t}^n - a = (\mathtt{t}^m)^d - a = g(\mathtt{t}^m) = h(\mathtt{t}^m) \cdot \ell(\mathtt{t}^m) = p(\mathtt{t}) \cdot q(\mathtt{t}),$$

y los polinomios $p(\mathtt{t}) := h(\mathtt{t}^m)$ y $q(\mathtt{t}) := \ell(\mathtt{t}^m)$ tienen grado positivo, lo que contradice la irreducibilidad de f. □

Número I.11 Hallar los polinomios mínimos de $\alpha := \sqrt[3]{5}$ sobre los cuerpos $\mathbb{Q}$ y $K := \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Solución. El polinomio $f(\mathtt{t}) := \mathtt{t}^3 - 5 \in \mathbb{Q}[\mathtt{t}]$ es irreducible, por el Criterio de Eisenstein, así que es el polinomio mínimo de α sobre $\mathbb{Q}$. Esto implica que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, mientras que por el Ejemplo I.2.4, $[K : \mathbb{Q}] = 4$. Se tiene por tanto un diagrama,



Como $\mathrm{mcd}(3, 4) = 1$ se tiene $[K(\alpha) : K] = 3$, por el Ejemplo I.2.4, y así $P_{K,\alpha} = f$. □

Número I.12 Dados $k \in \mathbb{Z} \setminus 7\mathbb{Z}$ y $\alpha_k := 2k\pi/7$ calcular el polinomio mínimo de $u := 2\cos\alpha_k$ sobre $\mathbb{Q}$.

Solución. El número complejo $\zeta := e^{2k\pi i/7}$ tiene módulo 1, luego $\zeta \cdot \overline{\zeta} = 1$, así que

$$u = \zeta + \overline{\zeta} = \zeta + (\zeta \cdot \overline{\zeta}/\zeta) = \zeta + \zeta^{-1}.$$

En VI.2.7, vol. II introdujimos el polinomio ciclotómico

$$\Phi_7(\mathtt{t}) = \mathtt{t}^6 + \mathtt{t}^5 + \mathtt{t}^4 + \mathtt{t}^4 + \mathtt{t}^3 + \mathtt{t}^2 + \mathtt{t} + 1 = \frac{\mathtt{t}^7 - 1}{\mathtt{t} - 1},$$

que tiene a ζ por raíz porque $\zeta^7 = 1$. Dividiendo entre $\mathtt{t}^3$ obtenemos

$$\mathtt{t}^{-3}\Phi_7(\mathtt{t}) = (\mathtt{t}^3 + \mathtt{t}^{-3}) + (\mathtt{t}^2 + \mathtt{t}^{-2}) + (\mathtt{t} + \mathtt{t}^{-1}) + 1, \tag{I.2}$$

y los dos primeros sumandos se reescriben como

$$\mathtt{t}^3+\mathtt{t}^{-3}=(\mathtt{t}+\mathtt{t}^{-1})^3-3(\mathtt{t}+\mathtt{t}^{-1}) \quad \& \quad \mathtt{t}^2+\mathtt{t}^{-2}=(\mathtt{t}+\mathtt{t}^{-1})^2-2.$$

Sustituyendo en la igualdad (I.2) resulta

$$\mathtt{t}^{-3}\Phi_7(\mathtt{t})=(\mathtt{t}+\mathtt{t}^{-1})^3-3(\mathtt{t}+\mathtt{t}^{-1})+(\mathtt{t}+\mathtt{t}^{-1})^2-2+(\mathtt{t}+\mathtt{t}^{-1})+1,$$

y al evaluar ambos miembros en $\mathtt{t}=\zeta$ se tiene

$$\begin{aligned}0=\zeta^{-3}\Phi_7(\zeta)&=(\zeta+\zeta^{-1})^3-3(\zeta+\zeta^{-1})+(\zeta+\zeta^{-1})^2-2+(\zeta+\zeta^{-1})+1\\&=u^3+u^2-2u-1,\end{aligned}$$

es decir, u es raíz del polinomio $g(\mathtt{t}):=\mathtt{t}^3+\mathtt{t}^2-2\mathtt{t}-1$. Éste es el polinomio mínimo de u sobre $\mathbb{Q}$. Para comprobarlo basta ver que es irreducible en $\mathbb{Z}[\mathtt{t}]$, para lo que basta demostrar, puesto que $\deg(g)=3$, que carece de raíces enteras. Esto es evidente, ya que $g(1)=-1$ y $g(-1)=1$. □

Número I.13 Sea $\mathfrak{a}$ el ideal de $\mathbb{Q}[\mathtt{t}]$ generado por los polinomios

$$f(\mathtt{t}):=\mathtt{t}^4+\mathtt{t}^3+2\mathtt{t}^2+\mathtt{t}+1 \quad \& \quad g(\mathtt{t}):=\mathtt{t}^3+4\mathtt{t}^2+4\mathtt{t}+3.$$

Probar que el cociente $K:=\mathbb{Q}[\mathtt{t}]/\mathfrak{a}$ es un cuerpo extensión de $\mathbb{Q}$. Hallar el grado y un elemento primitivo de la extensión $K|\mathbb{Q}$.

Solución. Como $\mathbb{Q}[\mathtt{t}]$ es un dominio euclídeo, el ideal $\mathfrak{a}$ es principal, generado por $\mathrm{mcd}_{\mathbb{Q}[\mathtt{t}]}(f,g)$. Para calcular éste empleamos el Algoritmo de Euclides. Se tiene

$$f(\mathtt{t})=(\mathtt{t}-3)g(\mathtt{t})+10(\mathtt{t}^2+\mathtt{t}+1) \quad \& \quad g(\mathtt{t})=(\mathtt{t}+3)(\mathtt{t}^2+\mathtt{t}+1),$$

luego $\mathfrak{a}$ es el ideal generado por el polinomio irreducible $h(\mathtt{t}):=\mathtt{t}^2+\mathtt{t}+1$. La irreducibilidad de h implica que el cociente $K=\mathbb{Q}[\mathtt{t}]/\mathfrak{a}$ es un cuerpo extensión de $\mathbb{Q}$ y de hecho $K=\mathbb{Q}(\alpha)$, donde $\alpha:=\mathtt{t}+\mathfrak{a}$. Finalmente,

$$[K:\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}]=\deg(P_{\mathbb{Q},\alpha})=\deg(h)=2.$$

□

Número I.14 (1) Probar que el polinomio $f(\mathtt{t}):=\mathtt{t}^5-\mathtt{t}-1$ es irreducible en $\mathbb{Q}[\mathtt{t}]$.

(2) Sean $a,b\in\mathbb{Q}$. ¿Tienen los polinomios $\mathtt{t}^5-\mathtt{t}-1$ y $\mathtt{t}^3+a\mathtt{t}+b$ alguna raíz compleja común?

(3) Sea $\alpha:=[\mathtt{t}]$ la clase de $\mathtt{t}$ en $\mathbb{Q}[\mathtt{t}]/(\mathtt{t}^5-\mathtt{t}-1)$. Escribir el elemento $1/(1+\alpha+\alpha^3)$ como expresión polinómica en α con coeficientes en $\mathbb{Q}$.

Solución. (1) Es suficiente demostrar que f es irreducible en $\mathbb{Z}[\mathtt{t}]$ y, como ningún divisor del término independiente $f(0) = -1$ es raíz de f, éste carece, en virtud del Teorema V.2.11, vol. II, de factores de grado 1 en $\mathbb{Z}[\mathtt{t}]$. Por tanto, si f fuese reducible en $\mathbb{Q}[\mathtt{t}]$, y puesto que carece de término en $\mathtt{t}^4$, se escribiría como producto

$$f(\mathtt{t}) := (\mathtt{t}^3 + a\mathtt{t}^2 + b\mathtt{t} + c)(\mathtt{t}^2 - a\mathtt{t} - c)$$

para ciertos $a, b, c \in \mathbb{Z}$ tales que $c^2 = 1$. Igualando coeficientes resulta que

$$\begin{cases} a^2 + c &= b \\ a(b+c) &= c \\ c(a+b) &= 1 \end{cases}$$

Al multiplicar la tercera ecuación por c resulta $c = a + b$, lo que sustituido en la primera se lee $a^2 + a = 0$, luego $a = 0$ o $a = -1$. En el primer caso se deduce de la segunda ecuación que $c = 0$, y esto es falso. Por tanto $a = -1$, y así $c = b - 1$ y

$$b - 1 = c = ab + ac = -b - c = -b + 1 - b = 1 - 2b,$$

esto es, $b = 2/3 \notin \mathbb{Z}$.

(2) Sea $g(\mathtt{t}) := \mathtt{t}^3 + a\mathtt{t} + b$ y supongamos que existe $u \in \mathbb{C}$ tal que $f(u) = g(u) = 0$. Como f es irreducible es el polinomio mínimo de u sobre $\mathbb{Q}$, luego g es múltiplo de f. Esto es falso ya que $\deg(g) < \deg(f)$. Por tanto f y g no comparten ninguna raíz.

(3) Denotemos $h(\mathtt{t}) := \mathtt{t}^3 + \mathtt{t} + 1$. Se trata de hallar un polinomio $q \in \mathbb{Q}[\mathtt{t}]$ tal que $q \cdot h - 1 \in f\mathbb{Q}[\mathtt{t}]$. Hecho esto se tiene, al evaluar en α y puesto que $f(\alpha) = 0$, la igualdad $q(\alpha)h(\alpha) = 1$, es decir,

$$1/(1 + \alpha + \alpha^3) = 1/h(\alpha) = q(\alpha).$$

Para calcular $q(\mathtt{t})$ observamos que $\mathrm{mcd}_{\mathbb{Z}[\mathtt{t}]}(f, h) = 1$, y aplicamos el Algoritmo de Euclides:

$$f(\mathtt{t}) = (\mathtt{t}^2 - 1) \cdot h(\mathtt{t}) - \mathtt{t}^2, \quad h(\mathtt{t}) = \mathtt{t} \cdot \mathtt{t}^2 + (\mathtt{t} + 1) \quad \& \quad \mathtt{t}^2 = (\mathtt{t} + 1) \cdot (\mathtt{t} - 1) + 1.$$

Leyendo estas igualdades de atrás hacia adelante obtenemos una Identidad de Bézout:

$$\begin{aligned} 1 &= \mathtt{t}^2 - (\mathtt{t} - 1) \cdot (\mathtt{t} + 1) = \mathtt{t}^2 - (\mathtt{t} - 1) \cdot (h(\mathtt{t}) - \mathtt{t} \cdot \mathtt{t}^2) \\ &= (\mathtt{t}^2 - \mathtt{t} + 1) \cdot \mathtt{t}^2 - (\mathtt{t} - 1) \cdot h(\mathtt{t}) = (\mathtt{t}^2 - \mathtt{t} + 1) \cdot \big((\mathtt{t}^2 - 1)h(\mathtt{t}) - f(\mathtt{t})\big) \\ &\quad - (\mathtt{t} - 1) \cdot h(\mathtt{t}) = (\mathtt{t}^4 - \mathtt{t}^3) \cdot h(\mathtt{t}) - (\mathtt{t}^2 - \mathtt{t} + 1) \cdot f(\mathtt{t}), \end{aligned}$$

luego $q(\mathtt{t}) := \mathtt{t}^4 - \mathtt{t}^3$, así que $1/(1 + \alpha + \alpha^3) = \alpha^4 - \alpha^3$. □

Número I.15 Sean K un cuerpo, $E := K(\mathtt{t})$ y $L := K\big(\mathtt{t}^3(1+\mathtt{t})^{-1}\big)$, donde $\mathtt{t}$ es una indeterminada. Probar que $E|L$ es una extensión algebraica simple y calcular $[E : L]$.

Solución. Desde luego $E = L(\mathtt{t})$, lo que muestra que la extensión $E|L$ es simple. Para ver que es algebraica, sea $\alpha := \mathtt{t}^3(1+\mathtt{t})^{-1} \in L$. Así $\mathtt{t}^3 - \alpha(1+\mathtt{t}) = 0$, y por tanto $\mathtt{t}$ es raíz del polinomio $f(\mathtt{x}) := \mathtt{x}^3 - \alpha\mathtt{x} - \alpha \in L[\mathtt{x}]$. Ahora es suficiente demostrar que este polinomio es irreducible en $L[\mathtt{x}]$ para concluir que $[E : L] = \deg(f) = 3$.

En primer lugar se debe observar que α es transcendente sobre K, pues en caso contrario serían algebraicas las extensiones $E|L$ y $L|K$, luego también lo sería $E|K$ y esto es falso, por I.2.2. Sea $\mathtt{y}$ otra indeterminada y consideremos el isomorfismo de anillos $\varphi : K(\mathtt{y})[\mathtt{t}] \to K(\alpha)[\mathtt{t}] = L[\mathtt{t}]$ que cumple $\varphi(\mathtt{y}) = \alpha$, $\varphi(\mathtt{t}) = \mathtt{t}$ y $\varphi(a) = a$ para cada $a \in K$.

Como la irreducibilidad se preserva por isomorfía es suficiente comprobar que el polinomio $g(\mathtt{x}) := \mathtt{x}^3 - \mathtt{y}\mathtt{x} - \mathtt{y}$ es irreducible en $K(\mathtt{y})[\mathtt{x}]$. Por el Lema de Gauss, VI.1.5, vol. II, esto equivale a que g sea irreducible en el anillo $K[\mathtt{y}][\mathtt{x}] = K[\mathtt{x}][\mathtt{y}]$. Ahora bien, $g = -(\mathtt{x}+1)\mathtt{y} + \mathtt{x}^3$ es irreducible en $K[\mathtt{x}][\mathtt{y}]$ porque tiene grado 1, como polinomio en la variable $\mathtt{y}$, y $\mathrm{mcd}_{K[\mathtt{x}]}(\mathtt{x}+1,\ \mathtt{x}^3) = 1$. □

Soluciones a los ejercicios del Capítulo II

Número II.1 Sean $f(\mathtt{t}) := \mathtt{t}^6 - 1$, $i := \sqrt{-1}$ y $\omega \neq 1$ tal que $\omega^3 = 1$. Hallar el grado de la extensión $L_f|L$, donde L_f denota un cuerpo de descomposición de f sobre cada uno de los siguientes cuerpos L: $\mathbb{Q}$, $\mathbb{Q}(i)$ y $\mathbb{Q}(\omega)$.

Solución. Vimos en el Ejercicio VI.7, vol. II que f factoriza en $\mathbb{Z}[\mathtt{t}]$ como

$$f(\mathtt{t}) = (\mathtt{t}+1)\cdot(\mathtt{t}-1)\cdot(\mathtt{t}^2+\mathtt{t}+1)\cdot(\mathtt{t}^2-\mathtt{t}+1),$$

y vamos a calcular sus raíces en $\mathbb{C}$. Una de ellas es ω, pues $\omega^6 = (\omega^3)^2 = 1$. De hecho ω es raíz del factor $g(\mathtt{t}) := \mathtt{t}^2+\mathtt{t}+1 = (\mathtt{t}^3-1)/(\mathtt{t}-1)$. También

$$g(\omega^2) = \omega^4 + \omega^2 + 1 = \omega + \omega^2 + 1 = g(\omega) = 0.$$

Por tanto, las raíces del factor $h(\mathtt{t}) := \mathtt{t}^2 - \mathtt{t} + 1 = g(-\mathtt{t})$ son $-\omega$ y $-\omega^2$, luego

$$f(\mathtt{t}) = (\mathtt{t}+1)\cdot(\mathtt{t}-1)\cdot(\mathtt{t}-\omega)\cdot(\mathtt{t}-\omega^2)\cdot(\mathtt{t}+\omega)\cdot(\mathtt{t}+\omega^2),$$

así que $L_f := \mathbb{Q}(\omega)$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$ y $P_{\mathbb{Q},\omega}(\mathtt{t}) = \mathtt{t}^2+\mathtt{t}+1$, luego

$$[L_f : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(P_{\mathbb{Q},\omega}) = \deg(g) = 2.$$

Más aún, como $L_f = \mathbb{Q}(\omega)$ es un cuerpo de descomposición de f sobre $\mathbb{Q}(\omega)$, resulta $[L_f : \mathbb{Q}(\omega)] = 1$. Por último, $E := \mathbb{Q}(i)(\omega)$ es un cuerpo de descomposición de f sobre $\mathbb{Q}(i)$ y $[E : \mathbb{Q}(i)] = 2$. Para demostrar esto último, y puesto que $g(\omega) = 0$ y $g \in \mathbb{Q}(i)[\mathtt{t}]$ tiene grado 2, es suficiente comprobar que $\omega \notin \mathbb{Q}(i)$. Supongamos, por reducción al absurdo, que $\omega \in \mathbb{Q}(i)$. Entonces $\mathbb{Q} \subsetneq \mathbb{Q}(\omega) \subset \mathbb{Q}(i)$, y además,

$$[\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}] = 2 \quad \Longrightarrow \quad [\mathbb{Q}(i) : \mathbb{Q}(\omega)] = \frac{[\mathbb{Q}(i) : \mathbb{Q}]}{[\mathbb{Q}(\omega) : \mathbb{Q}]} = 1,$$

es decir, $\mathbb{Q}(i) = \mathbb{Q}(\omega)$. Así $i \in \mathbb{Q}(\omega)$, lo que significa que existen $a, b \in \mathbb{Q}$ tales que $i = a + b\omega$. Al elevar al cuadrado,

$$-1 = (a+b\omega)^2 = a^2 + b^2\omega^2 + 2ab\omega = a^2 - b^2(1+\omega) + 2ab\omega = a^2 - b^2 + b(2a-b)\omega,$$

y por ser $\{1, \omega\}$ linealmente independientes sobre $\mathbb{Q}$, se tiene $a^2 - b^2 + 1 = 0$ y $b(2a-b) = 0$. De la primera igualdad $b^2 = 1 + a^2 > 0$ se desprende que $b \neq 0$, luego $b = 2a$, así que $1 = 3a^2$, que es falso pues $\sqrt{3} \notin \mathbb{Q}$. □

Número II.2 Probar que si L_f es un cuerpo de descomposición sobre K de un polinomio irreducible $f(\mathtt{t}) := \mathtt{t}^4 + a\mathtt{t}^2 + b \in K[\mathtt{t}]$, entonces existe una subextensión $E|K$ de $L_f|K$ tal que $[E : K] = 2$.

Solución. Si $\alpha \in L_f$ es una raíz de f, entonces, $\alpha^2 \in L_f$ es raíz del polinomio $g(\mathtt{t}) := \mathtt{t}^2 + a\mathtt{t} + b \in K[\mathtt{t}]$. También este polinomio es irreducible en $K[\mathtt{t}]$, pues en caso contrario sería producto $g = g_1 g_2$ de dos polinomios $g_1, g_2 \in K[\mathtt{t}]$ de grado 1, y así $f(\mathtt{t}) = g(\mathtt{t}^2) = g_1(\mathtt{t}^2)g_2(\mathtt{t}^2)$ sería reducible en $K[\mathtt{t}]$, contra la hipótesis. Por tanto, $g = P_{K,\alpha^2}$ es el polinomio mínimo de α^2 sobre K, luego $E := K(\alpha^2)$ cumple $[E : K] = \deg(g) = 2$ y $E|K$ es subextensión de $L_f|K$. □

Número II.3 Sean K un cuerpo, $a \in K$ y m y n enteros positivos primos entre sí. Demostrar que el polinomio $f(\mathtt{t}) := \mathtt{t}^{mn} - a$ es irreducible en $K[\mathtt{t}]$ si y sólo si los polinomios $g(\mathtt{t}) := \mathtt{t}^m - a$ y $h(\mathtt{t}) := \mathtt{t}^n - a$ son irreducibles en $K[\mathtt{t}]$.

Solución. Supongamos que alguno de los polinomios g o h, digamos g, es reducible en $K[\mathtt{t}]$. Entonces existen $g_1, g_2 \in K[\mathtt{t}]$ de grado al menos 1 y $g(\mathtt{t}) = g_1(\mathtt{t})g_2(\mathtt{t})$. Así, los polinomios $f_i(\mathtt{t}) := g_i(\mathtt{t}^n) \in K[\mathtt{t}]$ tienen grado mayor o igual que 1 y

$$f(\mathtt{t}) = \mathtt{t}^{mn} - a = (\mathtt{t}^n)^m - a = g(\mathtt{t}^n) = g_1(\mathtt{t}^n)g_2(\mathtt{t}^n) = f_1(\mathtt{t})f_2(\mathtt{t}),$$

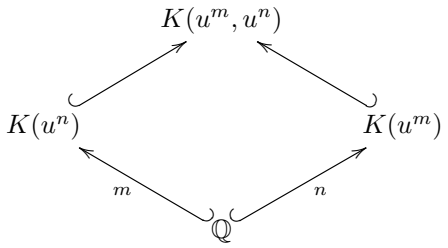
por lo que $f(\mathtt{t})$ es reducible en $K[\mathtt{t}]$. Supongamos, recíprocamente, que tanto $g(\mathtt{t})$ como $h(\mathtt{t})$ son irreducibles en $K[\mathtt{t}]$. Denotemos L un cuerpo de descomposición de f sobre K y sea $u \in L$ una raíz de f. Vamos a demostrar que f es el polinomio mínimo de u sobre K, lo que probará la irreducibilidad de f en $K[\mathtt{t}]$. Basta pues comprobar que $[K(u) : K] = \deg(f) = mn$. Ahora bien,

$$g(u^n) = u^{mn} - a = f(u) = 0 \quad \& \quad h(u^m) = u^{mn} - a = f(u) = 0,$$

y como g y h son irreducibles deducimos que $g = P_{K,u^n}$ y $h = P_{K,u^m}$ son los polinomios mínimos de u^n y u^m sobre K. En particular,

$$[K(u^n) : K] = \deg(P_{K,u^n}) = \deg(g) = m \quad \&$$
$$[K(u^m) : K] = \deg(P_{K,u^m}) = \deg(h) = n.$$

Como $\mathrm{mcd}(m,n)=1$ lo anterior implica que $[K(u^m,u^n):K]=mn$:



y todo se reduce a comprobar que $K(u^m,u^n)=K(u)$. La inclusión $K(u^m,u^n)\subset K(u)$ es evidente. Para la otra empleamos la Identidad de Bézout. Como $\mathrm{mcd}(m,n)=1$ existen enteros k,ℓ tales que $1=mk+n\ell$, luego

$$u=u^{mk+n\ell}=(u^m)^k\cdot(u^n)^\ell\in K(u^m,u^n),$$

por lo que $K(u)\subset K(u^m,u^n)$. □

Número II.4 Sean K un cuerpo con $\mathrm{char}(K)\neq 2$ y $u,v\in K$ que no son un cuadrado en K. Sean $\sqrt{u}$ y $\sqrt{v}$ raíces del polinomio $f(\mathtt{t}):=(\mathtt{t}^2-u)(\mathtt{t}^2-v)$ en un cuerpo de descomposición L_f de f sobre K tales que $K(\sqrt{u})\neq K(\sqrt{v})$. Probar que

$$K(\sqrt{u},\sqrt{v})=K(\sqrt{u}+\sqrt{v})\quad\&\quad[K(\sqrt{u},\sqrt{v}):K]=4.$$

Solución. Como u y v no son cuadrados en K los polinomios mínimos de $\sqrt{u}$ y $\sqrt{v}$ sobre K son $\mathtt{t}^2-u$ y $\mathtt{t}^2-v$, respectivamente, luego $[K(\sqrt{u}):K]=[K(\sqrt{v}):K]=2$. Es evidente que

$$K\subset L:=K(\sqrt{u}+\sqrt{v})\subset E=K(\sqrt{u},\sqrt{v})\quad\&\quad\sqrt{v}\notin K(\sqrt{u})$$

porque en caso contrario $K\subsetneq K(\sqrt{v})\subset K(\sqrt{u})$ y, por la transitividad del grado,

$$2=[K(\sqrt{u}):K]=[K(\sqrt{u}):K(\sqrt{v})]\cdot[K(\sqrt{v}):K]=2[K(\sqrt{u}):K(\sqrt{v})],$$

de donde $[K(\sqrt{u}):K(\sqrt{v})]=1$, es decir, $K(\sqrt{u})=K(\sqrt{v})$, contra la hipótesis. En consecuencia, $K\subsetneq K(\sqrt{u})\subsetneq K(\sqrt{u})(\sqrt{v})=E$, por lo que

$$[E:K]=[E:K(\sqrt{u})]\cdot[K(\sqrt{u}):K]=2\cdot[K(\sqrt{u})(\sqrt{v}):K(\sqrt{u})]=4,$$

lo que prueba la segunda afirmación del enunciado.

Para demostrar la primera observamos que $\sqrt{uv}\in L$ ya que

$$u+v+2\sqrt{uv}=(\sqrt{u}+\sqrt{v})^2\in L.$$

Además $\sqrt{v}\notin K(\sqrt{u})$, luego $\sqrt{uv}\notin K$, esto es, $K\subsetneq K(\sqrt{uv})\subset L\subset E$, así que

$$4=[E:K]=[E:L]\cdot[L:K(\sqrt{uv})]\cdot[K(\sqrt{uv}):K]=2\cdot[E:L]\cdot[L:K(\sqrt{uv})].$$

Para probar que $E = L$ basta ver $[E : L] = 1$, lo que por la igualdad anterior equivale a que $L \neq K(\sqrt{uv})$. En caso contrario $\sqrt{u} + \sqrt{v} \in K(\sqrt{uv})$, luego existen $x, y \in K$ tales que $\sqrt{u} + \sqrt{v} = x + y\sqrt{uv}$, y elevando al cuadrado,

$$u + v + 2\sqrt{uv} = (\sqrt{u} + \sqrt{v})^2 = (x + y\sqrt{uv})^2 = x^2 + y^2uv + 2xy\sqrt{uv}.$$

Esta igualdad equivale a las dos siguientes:

$$\begin{cases} x^2 + y^2uv = u + v \\ xy = 1 \end{cases}$$

Por tanto $u + v = x^2 + uv/x^2$, esto es, $x^4 - (u + v)x^2 + uv = 0$, es decir, x^2 es raíz del polinomio

$$\mathtt{t}^2 - (u + v)\mathtt{t} + uv = (\mathtt{t} - u)(\mathtt{t} - v),$$

luego $u = x^2$ o $v = x^2$, que es falso pues ni u ni v son cuadrados en K. □

Número II.5 Sean $p \in \mathbb{Z}$ un número primo y L_f un cuerpo de descomposición del polinomio $f(\mathtt{t}) := \mathtt{t}^p - 3$ sobre $\mathbb{Q}$. Calcular el grado $[L_f : \mathbb{Q}]$.

Solución. Una raíz de f es el número real $r := \sqrt[p]{3}$. Si u es otra de ellas se cumple que $u^p = 3 = r^p$, luego $(u/r)^p = 1$, y por tanto $u/r = \xi^k$ donde $0 \leq k \leq p-1$ y $\xi := e^{2\pi i/p}$. Así, las raíces de f son los números $\{r\xi^k : 0 \leq k \leq p - 1\}$. De aquí se deduce que un cuerpo de descomposición de f sobre $\mathbb{Q}$ es $L_f = \mathbb{Q}(r, \xi)$. Por el Criterio de Eisenstein y el Lema de Gauss, f es irreducible en $\mathbb{Q}[\mathtt{t}]$, luego es el polinomio mínimo de r sobre $\mathbb{Q}$, así que $[\mathbb{Q}(r) : \mathbb{Q}] = \deg(f) = p$.

En virtud de VI.2.7, vol. II, el polinomio mínimo de ξ sobre $\mathbb{Q}$ es el ciclotómico $\Phi_p(\mathtt{t}) = \sum_{i=0}^{p-1} \mathtt{t}^i$, luego $[\mathbb{Q}(\xi) : \mathbb{Q}] = \deg(\Phi_p) = p - 1$. Como $\mathrm{mcd}(p - 1, p) = 1$, por el Ejemplo I.2.4 se tiene,

$$[L_f : \mathbb{Q}] = [\mathbb{Q}(r, \xi) : \mathbb{Q}] = [\mathbb{Q}(r) : \mathbb{Q}] \cdot [\mathbb{Q}(\xi) : \mathbb{Q}] = p(p - 1).$$

□

Número II.6 Probar que $u := \mathrm{tg}(2\pi/5)$ es un número algebraico sobre $\mathbb{Q}$ y encontrar su polinomio mínimo. ¿Es $\mathbb{Q}(u)$ un cuerpo de descomposición sobre $\mathbb{Q}$ de algún polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$?

Solución. Sean $k = 1, 2$ y $\alpha_k := 2k\pi/5$. Aplicando la Fórmula de De Moivre se tiene

$$\begin{aligned} 1 = e^{2k\pi i} = e^{5\alpha_k i} = (e^{\alpha_k i})^5 = (\cos\alpha_k + i\,\mathrm{sen}\,\alpha_k)^5 = \cos^5\alpha_k + 5i\cos^4\alpha_k\,\mathrm{sen}\,\alpha_k \\ - 10\cos^3\alpha_k\,\mathrm{sen}^2\alpha_k - 10i\cos^2\alpha_k\,\mathrm{sen}^3\alpha_k + 5\cos\alpha_k\,\mathrm{sen}^4\alpha_k + i\,\mathrm{sen}^5\alpha_k, \end{aligned}$$

e igualando las partes imaginarias de ambos miembros obtenemos

$$5\cos^4\alpha_k\,\mathrm{sen}\,\alpha_k - 10\cos^2\alpha_k\,\mathrm{sen}^3\alpha_k + \mathrm{sen}^5\alpha_k = 0.$$

Dividiendo por $\cos^5 \alpha_k$, y denotando $u_k := \operatorname{sen} \alpha_k / \cos \alpha_k \neq 0$, se tiene

$$u_k(u_k^4 - 10u_k^2 + 5) = u_k^5 - 10u_k^3 + 5u_k = 0,$$

luego u_k es raíz del polinomio $f(\mathtt{t}) := \mathtt{t}^4 - 10\mathtt{t}^2 + 5 \in \mathbb{Z}[\mathtt{t}]$, que es un polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$, por el Lema de Gauss y el Criterio de Eisenstein. En consecuencia u_k es algebraico sobre $\mathbb{Q}$ y su polinomio mínimo sobre $\mathbb{Q}$ es $P_{\mathbb{Q},u_k} = f$. Como $u = u_1$ deducimos que u es algebraico sobre $\mathbb{Q}$ y su polinomio mínimo sobre $\mathbb{Q}$ es f.

Para terminar vamos a demostrar que $\mathbb{Q}(u)$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$. Las raíces de f en $\mathbb{C}$ son $u_1, -u_1, u_2, -u_2$, y denotando $\alpha = \alpha_1$,

$$u_2 = \operatorname{tg}(\alpha_2) = \operatorname{tg}(2\alpha) = 2\operatorname{tg}(\alpha)/(1 - \operatorname{tg}^2(\alpha)) = 2u/(1 - u^2) \in \mathbb{Q}(u).$$

En consecuencia,

$$f(\mathtt{t}) = (\mathtt{t} - u) \cdot (\mathtt{t} + u) \cdot (\mathtt{t} - 2u/(1 - u^2)) \cdot (\mathtt{t} + 2u/(1 - u^2)),$$

así que f factoriza en $\mathbb{Q}(u)[\mathtt{t}]$ en producto de polinomios de grado uno, por lo que $\mathbb{Q}(u)$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$. □

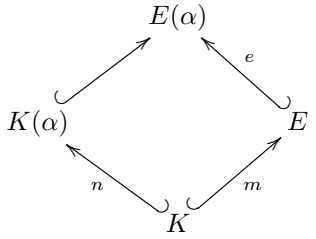
Número II.7 (1) Sean $E|K$ una extensión de cuerpos de grado m y $f \in K[\mathtt{t}]$ un polinomio irreducible de grado n. Sean $d := \operatorname{mcd}(m, n)$ y $D := n/d$. Probar que el grado de cada factor irreducible de f en $E[\mathtt{t}]$ es múltiplo de D.

(2) Demostrar que para cada $k \in \mathbb{Z}$ el polinomio

$$f_k(\mathtt{t}) := \mathtt{t}^4 - 2\mathtt{t}^3 + 4\mathtt{t}^2 - 2\mathtt{t} + (4k + 2)$$

es irreducible en el anillo de polinomios $\mathbb{Q}(\sqrt{2})[\mathtt{t}]$.

Solución. (1) Sea e el grado de un factor irreducible h de f en $E[\mathtt{t}]$. Elegimos una raíz α de h en un cuerpo de descomposición de h sobre E. Por la irreducibilidad, $h = P_{E,\alpha}$ es el polinomio mínimo de α sobre E, luego $[E(\alpha) : E] = \deg(h) = e$. Además $f(\alpha) = 0$, pues h divide a f. Así $f = P_{K,\alpha}$, luego $[K(\alpha) : K] = n$. Empleando la transitividad del grado en el diagrama



resulta $n \cdot [E(\alpha) : K(\alpha)] = em$, y dividiendo ambos miembros por d se tiene

$$D \cdot [E(\alpha) : K(\alpha)] = (n/d) \cdot [E(\alpha) : K(\alpha)] = e \cdot (m/d).$$

Esto implica que D divide al producto $e \cdot (m/d)$, y como los enteros D y m/d son primos entre sí deducimos que D divide a e, como queríamos probar.

(2) Denotemos $K := \mathbb{Q}$ y $E := \mathbb{Q}(\sqrt{2})$, que es el cuerpo de fracciones de $A := \mathbb{Z}[\sqrt{2}]$, que según vimos en el Ejemplo IV.1.9 (4), vol. II, es un dominio euclídeo. Con las notaciones del apartado anterior, $m = 2$ y $f := f_k$, que es irreducible en $K[\mathtt{t}]$ por el Criterio de Eisenstein, tiene grado $n = 4$, luego $d = D = 2$. Se deduce del apartado anterior que el grado de los factores irreducibles de f en $E[\mathtt{t}]$ es par. Queremos ver que, de hecho, el propio f es irreducible en $E[\mathtt{t}]$ y suponemos, por reducción al absurdo, que no lo es. Entonces sus factores irreducibles y mónicos en $E[\mathtt{t}]$ tienen grado 2 y, por el Lema de Gauss, pertenecen a $A[\mathtt{t}]$, pues f es un polinomio primitivo. Existen, en consecuencia, polinomios mónicos $h_1, h_2 \in A[\mathtt{t}]$ de grado 2 tales que $f = h_1 h_2$. Haciendo actuar sobre los dos miembros de esta igualdad el automorfismo

$$\overline{\tau} : A[\mathtt{t}] \to A[\mathtt{t}],\ \sum_{i=0}^{k} a_i \mathtt{t}^i \mapsto \sum_{i=0}^{k} \tau(a_i)\mathtt{t}^i$$

inducido por $\tau : A \to A$, $a+b\sqrt{2} \mapsto a-b\sqrt{2}$, y puesto que $f \in \mathbb{Z}[\mathtt{t}]$ y $\tau|_{\mathbb{Z}}$ es la identidad, resulta que $\overline{\tau}(f) = f$. Como los automorfismos preservan la irreducibilidad, se tienen dos factorizaciones de f en $A[\mathtt{t}]$ como producto de polinomios irreducibles:

$$h_1 \cdot h_2 = f = \overline{\tau}(f) = \overline{\tau}(h_1 \cdot h_2) = \overline{\tau}(h_1) \cdot \overline{\tau}(h_2).$$

Puesto que $A[\mathtt{t}]$ es un dominio de factorización única y cada h_i y cada $\overline{\tau}(h_i)$ es mónico, se tiene

$$\text{bien } \ h_i = \overline{\tau}(h_i) \ \text{ para } \ i = 1, 2, \ \text{ o } \ h_1 = \overline{\tau}(h_2) \ \text{ y } \ h_2 = \overline{\tau}(h_1).$$

En el primer caso los coeficientes de cada h_i quedan fijos por τ, luego son números enteros. Esto significa que cada $h_i \in \mathbb{Z}[\mathtt{t}]$, lo que es imposible porque f es irreducible en $\mathbb{Z}[\mathtt{t}]$. Así, necesariamente, se da el segundo caso, esto es, $h_1 = \overline{\tau}(h_2)$ y $h_2 = \overline{\tau}(h_1)$. Por tanto existen números enteros x_1, x_2, x_3 y x_4 tales que

$$h_1(\mathtt{t}) := \mathtt{t}^2+(x_1+x_2\sqrt{2})\mathtt{t}+(x_3+x_4\sqrt{2}) \quad \& \quad h_2(\mathtt{t}) := \mathtt{t}^2+(x_1-x_2\sqrt{2})\mathtt{t}+(x_3-x_4\sqrt{2}).$$

Comparando los coeficientes de $\mathtt{t}^3$ y $\mathtt{t}^2$ en la igualdad $f = h_1 h_2$ resulta

$$\begin{cases} -2 &= (x_1 + x_2\sqrt{2}) &+ &(x_1 - x_2\sqrt{2}) &= &2x_1 \\ 4 &= (x_3 + x_4\sqrt{2}) &+ &(x_3 - x_4\sqrt{2}) &+ &x_1^2 \ - \ 2x_2^2. \end{cases}$$

En consecuencia $x_1 = -1$ y $2(x_3 - x_2^2) = 3$, que es una contradicción. □

Número II.8 Sean K un cuerpo en el que el polinomio $f(\mathtt{t}) := \mathtt{t}^2 + 1$ no tiene ninguna raíz, y denotemos i una raíz de f en un cierre algebraico de K. Supongamos que todo elemento de $K(i)$ es el cuadrado de un elemento de $K(i)$. Probar que toda suma de cuadrados en K es un cuadrado en K y calcular la característica de K.

Solución. Como no tiene raíces en K, el polinomio f es irreducible en $K[\mathtt{t}]$, luego es el polinomio mínimo de i sobre K. Así, cada elemento de $K(i)$ se escribe, de modo único, como $a+bi$ con $a,b\in K$. Demostramos primero que a^2+b^2 es un cuadrado en K para cada $a,b\in K$. Por hipótesis, existen $c,d\in K$ tales que

$$a+bi=(c+di)^2=(a^2-c^2)+2cdi \quad\Longrightarrow\quad a=c^2-d^2 \quad \& \quad b=2cd.$$

En consecuencia, $a^2+b^2=(c^2-d^2)^2+4c^2d^2=(c^2+d^2)^2$. Supongamos demostrado, por inducción, que toda suma de $n-1$ cuadrados de elementos de K es un cuadrado en K. Entonces, dados $a_1,\ldots,a_n\in K$ existe, por lo que acabamos de probar, $b\in K$ tal que $a_{n-1}^2+a_n^2=b^2$, luego

$$\sum_{k=1}^{n} a_k^2=\sum_{k=1}^{n-2} a_k^2+(a_{n-1}^2+a_n^2)=\sum_{k=1}^{n-2} a_k^2+b^2=c^2,$$

para cierto $c\in K$. Esto implica, en particular, que $\mathrm{char}(K)=0$. En efecto, si $\mathrm{char}(K)=p$ para cierto primo p existiría, por lo que acabamos de demostrar, $a\in K$ tal que

$$-1=1+\overset{p-1)}{\cdots}+1=1^2+\overset{p-1)}{\cdots}+1^2=a^2,$$

esto es, $f(a)=0$, contra la hipótesis. □

Número II.9 Encontrar elementos primitivos de las subextensiones $L_f|\mathbb{Q}$ de $\mathbb{C}|\mathbb{Q}$, donde L_f es un cuerpo de descomposición de f sobre $\mathbb{Q}$, en los siguientes casos:

$$f(\mathtt{t}):=\mathtt{t}^9-1, \quad f(\mathtt{t}):=\mathtt{t}^4+5\mathtt{t}^2+6 \quad \& \quad f(\mathtt{t}):=\mathtt{t}^6-8.$$

Encontrar los grados de las extensiones $L_f|\mathbb{Q}$.

Solución. Las potencias de $\xi:=e^{2\pi i/9}$ son raíces de $f(\mathtt{t}):=\mathtt{t}^9-1$, ya que

$$f(\xi^k)=\xi^{9k}-1=(e^{2\pi i})^k-1=0.$$

Además $\xi^k\neq\xi^j$ si $j\neq k$ y $0\leq j,k\leq 8$. En efecto, en caso contrario existirían j,k tales que $0\leq j<k\leq 8$ y $\xi^k=\xi^j$, luego $0<\ell=k-j\leq 8$ y $\xi^\ell=1$. Así, el ángulo $\alpha:=2\pi\ell/9$ cumple, denotando $i:=\sqrt{-1}$, que

$$\cos\alpha+i\,\mathrm{sen}\,\alpha=e^{i\alpha}=\xi^\ell=1,$$

de donde se deduce que $\cos\alpha=1$, y esto es falso, pues $0<\alpha<2\pi$. Así, las potencias $\{\xi^k:0\leq k\leq 8\}$ son nueve raíces distintas del polinomio f, luego $L_f:=\mathbb{Q}(\xi)$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$, ya que $f(\mathtt{t})=\prod_{k=0}^{8}(\mathtt{t}-\xi^k)$. Vimos en el Ejercicio VI.7, vol. II, que $f(\mathtt{t})=(\mathtt{t}^3-1)\cdot(\mathtt{t}^6+\mathtt{t}^3+1)$ y que el factor $f_1(\mathtt{t}):=\mathtt{t}^6+\mathtt{t}^3+1$ es irreducible en $\mathbb{Q}[\mathtt{t}]$.

Como $\xi^3=\cos(2\pi/3)+i\,\mathrm{sen}(2\pi/3)\neq 1$, deducimos que $f_1(\xi)=0$ y por ello f_1 es el polinomio mínimo de ξ sobre $\mathbb{Q}$. En consecuencia, $[\mathbb{Q}(\xi):\mathbb{Q}]=6$.

Por otro lado, al factorizar en $\mathbb{C}[\mathtt{t}]$ el polinomio $\mathtt{t}^4+5\mathtt{t}^2+6$ resulta,

$$f(\mathtt{t}) := \mathtt{t}^4+5\mathtt{t}^2+6 = (\mathtt{t}^2+2)(\mathtt{t}^2+3) = (\mathtt{t}-\sqrt{2}i)\cdot(\mathtt{t}+\sqrt{2}i)\cdot(\mathtt{t}-\sqrt{3}i)\cdot(\mathtt{t}+\sqrt{3}i),$$

luego $L_f := \mathbb{Q}(\sqrt{2}i, \sqrt{3}i)$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$. Así,

$$\sqrt{3}i/\sqrt{2}i = \sqrt{3}/\sqrt{2} = \sqrt{6}/2 \in L_f,$$

por lo que $\sqrt{6} \in L_f$ y $2\sqrt{3}i = \sqrt{6}\cdot\sqrt{2}i \in \mathbb{Q}(\sqrt{2}i, \sqrt{6})$, así que $L_f = \mathbb{Q}(\sqrt{6}, \sqrt{2}i)$.

Además $\mathtt{t}^2-6 = P_{\mathbb{Q},\sqrt{6}}$, el polinomio $\mathtt{t}^2+2$ tiene a $\sqrt{2}i$ por raíz y $\sqrt{2}i \notin \mathbb{Q}(\sqrt{6})$, lo que implica que

$$[L_f:\mathbb{Q}] = [\mathbb{Q}(\sqrt{6})(\sqrt{2}i):\mathbb{Q}(\sqrt{6})]\cdot[\mathbb{Q}(\sqrt{6}):\mathbb{Q}] = 2\cdot[\mathbb{Q}(\sqrt{6})(\sqrt{2}i):\mathbb{Q}(\sqrt{6})] = 4.$$

Se desprende de la prueba del Teorema del elemento primitivo que $L_f := \mathbb{Q}(\sqrt{2}i+\sqrt{6})$.

Por último estudiamos $f(\mathtt{t}) := \mathtt{t}^6-8 = (\mathtt{t}^2)^3-2^3$, una de cuyas raíces es $\sqrt{2}$. Denotamos $\mu := e^{2\pi i/6} = e^{\pi i/3}$, que es una raíz primitiva sexta de la unidad, es decir, las potencias $\{\mu^j : 0 \le j \le 5\}$ son las seis raíces complejas de $\mathtt{t}^6-1$. En consecuencia

$$\mathtt{t}^6-8 = \prod_{j=0}^{5}(\mathtt{t}-\sqrt{2}\mu^j)$$

por lo que un cuerpo de descomposición de f sobre $\mathbb{Q}$ es $L_f = \mathbb{Q}(\sqrt{2}, \mu)$. Para calcular el grado de la extensión $L_f|\mathbb{Q}$ observamos que $\mu^3 = -1$, esto es,

$$0 = \mu^3+1 = (\mu+1)(1-\mu+\mu^2),$$

y puesto que $\mu \in \mathbb{C}\setminus\mathbb{Q}(\sqrt{2})$, se deduce que $P_{\mathbb{Q}(\sqrt{2}),\mu}(\mathtt{t}) = \mathtt{t}^2-\mathtt{t}+1$. En particular

$$[L_f:\mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2})(\mu):\mathbb{Q}(\sqrt{2})] = \deg(P_{\mathbb{Q}(\sqrt{2}),\mu}) = 2.$$

Además $P_{\mathbb{Q},\sqrt{2}}(\mathtt{t}) = \mathtt{t}^2-2$, así que $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$. Por la transitividad del grado,

$$[L_f:\mathbb{Q}] = [L_f:\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 4,$$

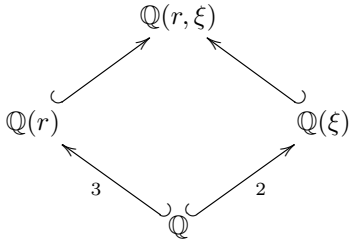
y por la prueba del Teorema del elemento primitivo $L_f = \mathbb{Q}(\sqrt{2}+\mu)$. □

Número II.10 Hallar un elemento primitivo u de la extensión $L_f|\mathbb{Q}$, donde L_f es un cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^3-7$. Hallar el polinomio mínimo de u sobre $\mathbb{Q}$.

Solución. Sea $r := \sqrt[3]{7}$ el único número real cuyo cubo es 7. El polinomio mínimo de r sobre $\mathbb{Q}$ es f, pues éste es irreducible, por el Criterio de Eisenstein. Cualquier otra raíz α de f cumple que $\alpha^3 = 7 = r^3$, luego $(\alpha/r)^3 = 1$, así que $\alpha/r = \xi^k$ para algún

exponente $k \in \{0,1,2\}$, donde $\xi := e^{2\pi i/3}$. Por tanto, las raíces de f en $\mathbb{C}$ son r, $r\xi$ y $r\xi^2$, así que un cuerpo de descomposición de f sobre $\mathbb{Q}$ es $L_f := \mathbb{Q}(r,\xi)$. De la prueba del Teorema del elemento primitivo se deduce que $L_f = \mathbb{Q}(u)$ donde $u := r + \xi$.

Para calcular su polinomio mínimo determinamos antes su grado. Nótese que $P_{\mathbb{Q},r} = f$ tiene grado 3 y $P_{\mathbb{Q},\xi}(\mathtt{t}) = \mathtt{t}^2 + \mathtt{t} + 1$ es de grado 2. Aplicando el Ejemplo I.2.4 en el diagrama



resulta que $[L_f : \mathbb{Q}] = [Q(r,\xi) : \mathbb{Q}] = 2 \cdot 3 = 6$. Por tanto, $P_{\mathbb{Q},u} \in \mathbb{Q}[\mathtt{t}]$ es el único polinomio mónico de grado 6 que tiene a u por raíz. Para calcularlo operamos, teniendo en cuenta que $\xi^3 = 1$ y $\xi^2 = -(1+\xi)$. Se tiene entonces

$$7 = r^3 = (u-\xi)^3 = u^3 - 3u^2\xi + 3u\xi^2 - \xi^3 = u^3 - 3u^2\xi - 3u(1+\xi) - 1.$$

Despejando, expresamos ξ y ξ^2 como función racional de u:

$$\xi = \frac{u^3 - 3u - 8}{3u(u+1)} \quad \& \quad \xi^2 = \frac{(u^3 - 3u - 8)^2}{9u^2(u+1)^2}.$$

Sustituyendo estos valores en la igualdad $1 + \xi + \xi^2 = 0$ se obtiene

$$1 + \frac{u^3 - 3u - 8}{3u(u+1)} + \frac{(u^3 - 3u - 8)^2}{9u^2(u+1)^2} = 0,$$

y multiplicando esta expresión por $9u^2(u+1)^2$ resulta que u es raíz del polinomio de grado 6

$$g(\mathtt{t}) := 9\mathtt{t}^2(\mathtt{t}+1)^2 + 3\mathtt{t}(\mathtt{t}+1)(\mathtt{t}^3 - 3\mathtt{t} - 8) + (\mathtt{t}^3 - 3\mathtt{t} - 8)^2,$$

luego $g = P_{\mathbb{Q},u}$ es el polinomio mínimo de u sobre $\mathbb{Q}$. □

Número II.11 Sea $\alpha := 1/(\sqrt{2} + \sqrt[3]{3})$. Encontrar el polinomio mínimo de α sobre $\mathbb{Q}$. Escribir α como expresión polinómica en $\sqrt{2}$ y $\sqrt[3]{3}$ con coeficientes racionales.

Solución. Al elevar al cubo los dos miembros de la igualdad $\alpha^{-1} - \sqrt{2} = \sqrt[3]{3}$ resulta

$$\alpha^{-3} - 3\sqrt{2}\alpha^{-2} + 6\alpha^{-1} - 2\sqrt{2} = 3.$$

Al multiplicar por α^3 se tiene $1 - 3\sqrt{2}\alpha + 6\alpha^2 - 2\sqrt{2}\alpha^3 = 3\alpha^3$, y agrupando términos adecuadamente, $1 + 6\alpha^2 - 3\alpha^3 = \sqrt{2}\alpha(3 + 2\alpha^2)$. Al elevar al cuadrado ambos miembros resulta

$$1 + 36\alpha^4 + 9\alpha^6 + 12\alpha^2 - 6\alpha^3 - 36\alpha^5 = 2\alpha^2(9 + 4\alpha^4 + 12\alpha^2).$$

Tras simplificar y expresar el resultado según las potencias decrecientes de α queda

$$\alpha^6 - 36\alpha^5 + 12\alpha^4 - 6\alpha^3 - 6\alpha^2 + 1 = 0. \tag{II.3}$$

Por tanto α es raíz del polinomio $f(\mathtt{t}) := \mathtt{t}^6 - 36\mathtt{t}^5 + 12\mathtt{t}^4 - 6\mathtt{t}^3 - 6\mathtt{t}^2 + 1$, y veremos ahora que éste es el polinomio minimo de α sobre $\mathbb{Q}$. Para ello basta comprobar que el grado de la extensión $\mathbb{Q}(\alpha)|\mathbb{Q}$ es 6. Por la prueba del Teorema del elemento primitivo,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha^{-1}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2} + \sqrt[3]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) : \mathbb{Q}] = 2 \cdot 3 = 6,$$

pues $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ y los enteros 2 y 3 son primos entre sí.

En la segunda parte se trata de expresar α como polinomio en $u := \sqrt{2}$ y $v := \sqrt[3]{3}$. Para ello dividimos la igualdad (II.3) entre $\alpha^5 \neq 0$ y tenemos

$$\begin{aligned}\alpha &= 36 - 12\alpha^{-1} + 6\alpha^{-2} + 6\alpha^{-3} - \alpha^{-5} \\ &= 36 - 12(\sqrt{2} + \sqrt[3]{3}) + 6(\sqrt{2} + \sqrt[3]{3})^2 + 6(\sqrt{2} + \sqrt[3]{3})^3 - (\sqrt{2} + \sqrt[3]{3})^5.\end{aligned}$$

□

Número II.12 Sea $L|K$ una extensión algebraica de cuerpos de característica 0. Supongamos que existe un entero positivo n tal que $[K(u) : K] \leq n$ para cada $u \in L$. Demostrar que la extensión $L|K$ es finita, de grado menor o igual que n.

Solución. Sea $\alpha \in L$ tal que $[K(u) : K] \leq [K(\alpha) : K] = m \leq n$ para todo $u \in K$. Es evidente que basta demostrar que $L = K(\alpha)$. Suponemos, por reducción al absurdo, que $K(\alpha) \subsetneq L$ y elegimos $\beta \in L \setminus K(\alpha)$. Así, $[K(\alpha)(\beta) : K(\alpha)] > 1$ y, por el Teorema del elemento primitivo, existe $\gamma \in L$ tal que $K(\alpha, \beta) = K(\gamma)$. Así resulta

$$[K(\alpha) : K] < [K(\alpha)(\beta) : K(\alpha)] \cdot [K(\alpha) : K] = [K(\alpha, \beta) : K] = [K(\gamma) : K].$$

lo que contradice la elección de α. □

Número II.13 Sean K un cuerpo y $f(\mathtt{t}) := \mathtt{t}^5 - a \in K[\mathtt{t}]$, donde $a \in K$ es un elemento no nulo.

(1) Demostrar que f posee cinco raíces distintas en un cierre algebraico $\overline{K}$ de K si y sólo si la característica de K es distinta de 5.

(2) Suponemos que $\mathrm{char}(K) \neq 5$. Demostrar que f es irreducible en $K[\mathtt{t}]$ si y sólo si a no es potencia quinta de un elemento de K.

Solución. (1) Si $\mathrm{char}(K) \neq 5$ la derivada $f'(\mathtt{t}) = 5\mathtt{t}^4$ tiene a 0 por única raíz, que no es raíz de f, así que en este caso f tiene 5 raíces simples en $\overline{K}$. Recíprocamente, supongamos que $\mathrm{char}(K) = 5$, y sea $u \in \overline{K}$ una raíz de f. Entonces $f(\mathtt{t}) = (\mathtt{t} - u)g(\mathtt{t})$ para cierto polinomio $g(\mathtt{t}) \in K[\mathtt{t}]$. Derivando,

$$0 \equiv 5\mathtt{t}^4 = f'(\mathtt{t}) = g(\mathtt{t}) + (\mathtt{t} - u)g'(\mathtt{t}),$$

luego $g(u) = 0$, así que existe $h \in K[\mathtt{t}]$ tal que $g(\mathtt{t}) = (\mathtt{t} - u)h(\mathtt{t})$. En consecuencia, $f(\mathtt{t}) = (\mathtt{t} - u)^2 g(\mathtt{t})$ y u es raíz doble de f. Por ello f tiene, a lo sumo, cuatro raíces distintas en $\overline{K}$.

(2) Si existe $b \in K$ tal que $a = b^5$, entonces la factorización

$$\mathtt{t}^5 - a = \mathtt{t}^5 - b^5 = (\mathtt{t} - b)(\mathtt{t}^4 + b\mathtt{t}^3 + b^2\mathtt{t}^2 + b^3\mathtt{t} + b^4)$$

muestra que f es reducible en $K[\mathtt{t}]$. Recíprocamente, si a no es potencia quinta de un elemento de K el polinomio f carece de factores de grado 1 en $K[\mathtt{t}]$, luego si fuese reducible en $K[\mathtt{t}]$ sería producto de dos factores en $K[\mathtt{t}]$ de grados 2 y 3.

Sean $\overline{K}$ un cierre algebraico de K y $u \in \overline{K}$ una raíz de f. Hemos probado en el apartado anterior que el polinomio $\mathtt{t}^5 - 1$ tiene 5 raíces distintas $\zeta_i \in \overline{K}$, donde $1 \leq i \leq 5$. Los productos $u\zeta_i$ son raíces, distintas dos a dos, de f porque

$$f(u\zeta_i) = (u\zeta_i)^5 - a = u^5\zeta_i^5 - a = u^5 - a = a - a = 0.$$

Por tanto, la factorización de f en $\overline{K}[\mathtt{t}]$ es $f(\mathtt{t}) = \prod_{i=1}^{5}(\mathtt{t} - u\zeta_i)$, así que, reordenando las raíces de f si es preciso, podemos suponer, puesto que $K[\mathtt{t}]$ y $\overline{K}[\mathtt{t}]$ son dominios de factorización única, que la factorización de f en $K[\mathtt{t}]$ en producto de factores irreducibles es $f(\mathtt{t}) = g(\mathtt{t})h(\mathtt{t})$, donde

$$g(\mathtt{t}) := \prod_{i=1}^{2}(\mathtt{t} - u\zeta_i) \quad \& \quad h(\mathtt{t}) := \prod_{i=3}^{5}(\mathtt{t} - u\zeta_i).$$

En particular, $\zeta_1\zeta_2 u^2 = g(0) \in K$ y, además, $b := (\zeta_1\zeta_2)^3 u$ cumple que

$$b^5 = ((\zeta_1\zeta_2)^3 u)^5 = (\zeta_1^5)^3 \cdot (\zeta_2^5)^3 \cdot u^5 = 1 \cdot 1 \cdot a = a.$$

En consecuencia, a es potencia quinta de b y $b \in K$, contra la hipótesis, porque

$$b = (\zeta_1\zeta_2)^3 u = (\zeta_1\zeta_2)^3 u^6 \cdot u^{-5} = ((\zeta_1\zeta_2 u^2))^3 a^{-1} = g(0)^3 a^{-1} \in K.$$

□

Número II.14 Un cuerpo K se llama *real* si -1 no es suma de cuadrados de elementos de K.

(1) Demostrar que todo cuerpo real tiene característica cero.

(2) Sean K un cuerpo real y $L|K$ una extensión finita de grado impar. Probar que L es real.

Solución. (1) Si $\mathrm{char}(K) = p \neq 0$ se tiene $1 + \overset{p)}{\cdots} + 1 = 0$, luego $-1 = 1^2 + \overset{p-1)}{\cdots} + 1^2$ es suma de cuadrados de elementos de K, por lo que K no es real.

(2) Probaremos que L es real por inducción sobre el grado $n := [L : K]$, siendo obvio el caso $n = 1$, pues entonces $L = K$. Suponemos $n > 1$ y, por el Teorema del elemento

primitivo II.2.2, existe $\theta \in L$ tal que $L = K(\theta) = K[\theta]$. Supongamos, por reducción al absurdo, que L no es real. Existen por tanto un entero positivo r y elementos $\zeta_1, \ldots, \zeta_r \in L$ tales que

$$-1 = \zeta_1^2 + \cdots + \zeta_r^2.$$

Como $L = K[\theta]$, para $1 \leq j \leq r$ existe un polinomio $f_j \in K[\mathtt{t}]$ de grado $m_j < n$ tal que $\zeta_j = f_j(\theta)$. El polinomio $1 + \sum_{j=1}^r f_j^2(\mathtt{t})$ se anula en θ ya que

$$1 + \sum_{j=1}^r f_j^2(\theta) = 1 + \sum_{j=1}^r \zeta_j^2 = 0,$$

luego es múltiplo en $K[\mathtt{t}]$ del polinomio mínimo $f = P_{K,\theta}$ de θ sobre K. Así, existe $g \in K[\mathtt{t}]$ tal que $1 + \sum_{j=1}^r f_j^2 = fg$, y vamos a demostrar que el grado de g es impar y menor que n. Contando grados, y ya que $\deg(f) = [K(\theta) : K] = [L : K] = n$,

$$\deg\Big(\sum_{j=1}^r f_j^2\Big) = \deg\Big(1 + \sum_{j=1}^r f_j^2\Big) = \deg(fg) = \deg(f) + \deg(g) = n + \deg(g). \quad \text{(II.4)}$$

Escribimos $f_j := a_j \mathtt{t}^{m_j} +$ términos de grado menor que m_j y definimos

$$m := \max\{m_j : \ 1 \leq j \leq r\} \leq n - 1.$$

Denotamos $J := \{1 \leq j \leq r : \ m_j = m\}$, que es un conjunto no vacío, y así

$$\sum_{j=1}^r f_j^2 = \Big(\sum_{j \in J} a_j^2\Big)\mathtt{t}^{2m} + \text{ términos de grado menor que } 2m,$$

y $\sum_{j \in J} a_j^2 \neq 0$. En caso contrario escogemos un índice $j \in J$ y denotamos $b_k := a_k/a_j$ para cada $k \in J$ con $k \neq j$. Así, $-1 = \sum_{k \neq j} b_k^2$, que es imposible pues el cuerpo K es real. Por tanto,

$$\deg\Big(\sum_{j=1}^r f_j^2\Big) = 2m \quad \Longrightarrow \quad \deg(g) = 2m - n \leq 2(n-1) - n \leq n - 2 < n.$$

El anillo $K[\mathtt{t}]$ es un DFU, luego g es producto de polinomios irreducibles en $K[\mathtt{t}]$, y alguno de ellos tiene grado impar, pues la suma de sus grados, que es el grado de g, lo es. Existe por tanto un polinomio mónico e irreducible $h \in K[\mathtt{t}]$ que divide a g en $K[\mathtt{t}]$, cuyo grado $\deg(h) := d$ es impar y $d \leq \deg(g) < n$.

Sean E un cuerpo de descomposición de h sobre K y $\alpha \in E$ una raíz de h. Nótese que $[K(\alpha) : K] = \deg(P_{K,\alpha}) = \deg(h) = d$, luego la extensión $K(\alpha)|K$ tiene grado impar $d < n$, lo que implica, por la hipótesis de inducción, que el cuerpo $K(\alpha)$ es real. Sin embargo, como $h(\alpha) = 0$ y $h|g$, también $g(\alpha) = 0$, y por ello

$$1 + \sum_{j=1}^r f_j(\alpha)^2 = f(\alpha)g(\alpha) = 0 \quad \Longrightarrow \quad -1 = \sum_{j=1}^r f_j(\alpha)^2.$$

Así -1 es suma de cuadrados de elementos del cuerpo $K(\alpha)$, y esto es una contradicción, ya que hemos demostrado que $K(\alpha)$ es un cuerpo real. □

Número II.15 Sean K un cuerpo, $a \in K \setminus \{0\}$, p un número primo y $f(\mathtt{t}) := \mathtt{t}^p - a$.

(1) Demostrar que si u es una raíz de f en un cierre algebraico $\overline{K}$ de K, toda raíz de f en $\overline{K}$ es de la forma ζu para cierto $\zeta \in \overline{K}$ tal que $\zeta^p = 1$.

(2) Demostrar que si f es reducible en $K[\mathtt{t}]$, entonces f tiene alguna raíz en K.

Solución. (1) Cualquier raíz $v \in \overline{K}$ de f cumple que $v^p = a = u^p$, luego el cociente $\zeta := v/u$ cumple $\zeta^p = v^p/u^p = 1$ y $v = \zeta u$.

(2) Como f es reducible en $K[\mathtt{t}]$ existen polinomios mónicos $g, h \in K[\mathtt{t}]$ de grado mayor o igual que 1 tales que $f := gh$. Como las raíces de g lo son de f, si denotamos $d := \deg(g)$ existen $\zeta_1, \ldots, \zeta_d \in \overline{K}$ tales que cada $\zeta_j^p = 1$ y las raíces de g en $\overline{K}$ son $\zeta_1 u, \ldots, \zeta_d u$, por lo que

$$g(\mathtt{t}) = (\mathtt{t} - \zeta_1 u) \cdots (\mathtt{t} - \zeta_d u).$$

Igualando los términos independientes, se tiene $(-1)^d \zeta_1 \cdots \zeta_d u^d = g(0) \in K$, y el producto $\zeta := \zeta_1 \cdots \zeta_d \in \overline{K}$ cumple que $\zeta^p = \zeta_1^p \cdots \zeta_d^p = 1$ y $\zeta u^d = (-1)^d g(0) \in K$. Por otro lado, como $1 \leq d \leq p-1$ se tiene $\mathrm{mcd}(d, p) = 1$ y, por la identidad de Bézout, existen enteros k, ℓ tales que $1 = dk + \ell p$. De este modo, $w := \zeta^k u \in \overline{K}$ cumple que

$$w^p = \zeta^{kp} u^p = (\zeta^p)^k u^p = 1 \cdot a = a,$$

es decir, $f(w) = 0$, y $w \in K$, lo que muestra que f posee una raíz en K, puesto que

$$w = \zeta^k u = \zeta^k u^{dk+\ell p} = (\zeta u^d)^k \cdot (u^p)^\ell = (-1)^d g(0) a^\ell \in K.$$

□

Número II.16 Calcular el polinomio mínimo de $a + b$ sobre $\mathbb{Q}$, donde

$$a := \sqrt[5]{2} \quad \& \quad b := \sqrt[3]{-7/2 - \sqrt{3981}/18} + \sqrt[3]{-7/2 + \sqrt{3981}/18}.$$

Solución. El polinomio $f(\mathtt{t}) := \mathtt{t}^5 - 2$ es irreducible en $\mathbb{Z}[\mathtt{t}]$ por el Criterio de Eisenstein, luego lo es en $\mathbb{Q}[\mathtt{t}]$, y $f(a) = 0$. Por tanto, $P_{\mathbb{Q},a} = f$ es el polinomio mínimo de a sobre $\mathbb{Q}$. Vamos a calcular el polinomio mínimo de b sobre $\mathbb{Q}$. Denotamos

$$c := -7/2 + \sqrt{3981}/18 \quad \& \quad d := -7/2 - \sqrt{3981}/18,$$

de modo que $b := \sqrt[3]{c} + \sqrt[3]{d}$. Elevando al cubo resulta

$$b^3 = c + d + 3(\sqrt[3]{c^2 d} + \sqrt[3]{c d^2}) = -7 + 3\sqrt[3]{cd}(\sqrt[3]{c} + \sqrt[3]{d}) = -7 + 3b\sqrt[3]{cd}. \tag{II.5}$$

Observamos que

$$-cd = \Big(\frac{\sqrt{3981}}{18} + \frac{7}{2}\Big)\Big(\frac{\sqrt{3981}}{18} - \frac{7}{2}\Big) = \frac{1}{4}\Big(\frac{3981}{81} - 49\Big) = \frac{1}{4} \cdot \frac{12}{81} = \frac{1}{27},$$

luego $\sqrt[3]{cd} = -1/3$. Sustituyendo en la igualdad (II.5) obtenemos $b^3 + b + 7 = 0$. Esto implica que el polinomio mínimo de b sobre $\mathbb{Q}$ es $g(\mathtt{t}) := P_{\mathbb{Q},b}(\mathtt{t}) = \mathtt{t}^3 + \mathtt{t} + 7$, pues g es irreducible en $\mathbb{Q}[\mathtt{t}]$ ya que $\deg(g) = 3$ y g carece de raíces enteras, porque

$$g(1) = 9, \quad g(-1) = 5, \quad g(7) = 357 \quad \& \quad g(-7) = -343.$$

Por la Observación I.2.6 (4), $a + b$ es raíz del polinomio $p(\mathtt{x}) \in \mathbb{Z}[\mathtt{x}]$ definido por

$$p(\mathtt{x}) = \mathrm{Res}_{\mathtt{t}}(f(\mathtt{t}), g(\mathtt{x} - \mathtt{t})).$$

Para calcularlo explícitamente escribimos

$$\begin{aligned} f(\mathtt{t}) &= \mathtt{t}^5 - 2 \quad \& \\ g(\mathtt{x} - \mathtt{t}) &= (\mathtt{x} - \mathtt{t})^3 + \mathtt{x} - \mathtt{t} + 7 = -\mathtt{t}^3 + 3\mathtt{x}\mathtt{t}^2 - (1 + 3\mathtt{x}^2)\mathtt{t} + (\mathtt{x}^3 + \mathtt{x} + 7). \end{aligned}$$

Denotando, para abreviar, $a(\mathtt{x}) := 3\mathtt{x}$, $b(\mathtt{x}) := -(1 + 3\mathtt{x}^2)$ y $c(\mathtt{x}) := \mathtt{x}^3 + \mathtt{x} + 7$, la resultante de estos dos polinomios en la indeterminada $\mathtt{t}$ es

$$p(\mathtt{x}) = \mathrm{Res}_{\mathtt{t}}(f(\mathtt{t}), g(\mathtt{x} - \mathtt{t})) = \det \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -2 \\ -1 & a(\mathtt{x}) & b(\mathtt{x}) & c(\mathtt{x}) & 0 & 0 & 0 & 0 \\ 0 & -1 & a(\mathtt{x}) & b(\mathtt{x}) & c(\mathtt{x}) & 0 & 0 & 0 \\ 0 & 0 & -1 & a(\mathtt{x}) & b(\mathtt{x}) & c(\mathtt{x}) & 0 & 0 \\ 0 & 0 & 0 & -1 & a(\mathtt{x}) & b(\mathtt{x}) & c(\mathtt{x}) & 0 \\ 0 & 0 & 0 & 0 & -1 & a(\mathtt{x}) & b(\mathtt{x}) & c(\mathtt{x}) \end{bmatrix}$$

$$\begin{aligned} &= \mathtt{x}^{15} + 5\mathtt{x}^{13} + 35\mathtt{x}^{12} + 10\mathtt{x}^{11} + 134\mathtt{x}^{10} + 500\mathtt{x}^9 + 240\mathtt{x}^8 + 2735\mathtt{x}^7 + 3530\mathtt{x}^6 \\ &+ 1273\mathtt{x}^5 - 6355\mathtt{x}^4 + 12695\mathtt{x}^3 + 1320\mathtt{x}^2 + 22405\mathtt{x} + 16167, \end{aligned}$$

y para demostrar que p es el polinomio mínimo de $a+b$ sobre $\mathbb{Q}$ es suficiente comprobar que el grado de la extensión $\mathbb{Q}(a + b)|\mathbb{Q}$ es 15.

Ahora bien, de la prueba del Teorema del elemento primitivo se desprende que $\mathbb{Q}(a, b) = \mathbb{Q}(a + b)$, luego todo se reduce a ver que $[\mathbb{Q}(a, b) : \mathbb{Q}] = 15$. Esto se deduce inmediatamente del Ejemplo I.2.4, pues como $\mathrm{mcd}(\deg(f), \deg(g) = 1$ se tiene

$$[\mathbb{Q}(a, b) : \mathbb{Q}] = \deg(f) \cdot \deg(g) = 3 \cdot 5 = 15.$$

□

Número II.17 (1) Dado un primo $p \in \mathbb{Z}$, ¿cuál es el polinomio mínimo de $\sqrt[3]{p}$ sobre el cuerpo $\mathbb{Q}$?

(2) Demostrar que $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$.

(3) Calcular el grado de la extensión $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})|\mathbb{Q}$.

(4) Calcular el polinomio mínimo de $\sqrt[3]{2} + \sqrt[3]{3}$ sobre $\mathbb{Q}$.

Solución. (1) El polinomio $\mathtt{t}^3 - p \in \mathbb{Z}[\mathtt{t}]$ es irreducible, por el Criterio de Eisenstein, luego también lo es en $\mathbb{Q}[\mathtt{t}]$, y tiene a $\sqrt[3]{p}$ por raíz. En consecuencia, el polinomio mínimo de $\sqrt[3]{p}$ sobre $\mathbb{Q}$ es $\mathtt{t}^3 - p$.

(2) Se deduce del apartado anterior que $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ es una base de $\mathbb{Q}(\sqrt[3]{2})$ como $\mathbb{Q}$-espacio vectorial. Supongamos, por reducción al absurdo, que $\sqrt[3]{3} \in \mathbb{Q}(\sqrt[3]{2})$. Esto significa que existen números racionales q_1, q_2 y q_3 tales que

$$\sqrt[3]{3} = q_1 + q_2\sqrt[3]{2} + q_3\sqrt[3]{4}.$$

Elevando al cubo ambos miembros se tiene

$$\begin{aligned}
3 &= (q_1 + q_2\sqrt[3]{2} + q_3\sqrt[3]{4})^3 = (q_1 + q_2\sqrt[3]{2})^3 + 3q_3(q_1 + q_2\sqrt[3]{2})^2\sqrt[3]{4} \\
&+ 3q_3^2(q_1 + q_2\sqrt[3]{2})\sqrt[3]{16} + 4q_3^3 = q_1^3 + 3q_1^2q_2\sqrt[3]{2} + 3q_1q_2^2\sqrt[3]{4} + 2q_2^3 \\
&+ 3q_3(q_1^2 + 2q_1q_2\sqrt[3]{2} + q_2^2\sqrt[3]{4})\sqrt[3]{4} + 6q_3^2(q_1 + q_2\sqrt[3]{2})\sqrt[3]{2} + 4q_3^3 = q_1^3 + 3q_1^2q_2\sqrt[3]{2} \\
&+ 3q_1q_2^2\sqrt[3]{4} + 2q_2^3 + 3q_1^2q_3\sqrt[3]{4} + 12q_1q_2q_3 + 6q_2^2q_3\sqrt[3]{2} + 6q_1q_3^2\sqrt[3]{2} + 6q_2q_3^2\sqrt[3]{4} + 4q_3^3 \\
&= (q_1^3 + 2q_2^3 + 4q_3^3 + 12q_1q_2q_3) + (3q_1^2q_2 + 6q_2^2q_3 + 6q_1q_3^2)\sqrt[3]{2} \\
&+ (3q_1q_2^2 + 3q_1^2q_3 + 6q_2q_3^2)\sqrt[3]{4},
\end{aligned}$$

y pasando de miembro esto equivale a que

$$(q_1^3+2q_2^3+4q_3^3+12q_1q_2q_3-3)+3(q_1^2q_2+2q_2^2q_3+2q_1q_3^2)\sqrt[3]{2}+3(q_1q_2^2+q_1^2q_3+2q_2q_3^2)\sqrt[3]{4} = 0.$$

Como 1, $\sqrt[3]{2}$ y $\sqrt[3]{4}$ son $\mathbb{Q}$-linealmente independientes lo anterior implica que

$$\left\{\begin{array}{rcrcrcrcl}
q_1^3 & + & 2q_2^3 & + & 4q_3^3 & + & 12q_1q_2q_3 & = & 3 \\
q_1^2q_2 & + & 2q_2^2q_3 & + & 2q_1q_3^2 & & & = & 0 \\
q_1q_2^2 & + & q_1^2q_3 & + & 2q_2q_3^2 & & & = & 0
\end{array}\right.$$

Escribimos cada $q_i \in \mathbb{Q}$ como un cociente de números enteros con el mismo denominador:

$$q_1 := a/d, \quad q_2 := b/d \quad \& \quad q_3 := c/d,$$

lo que reemplazado en el sistema anterior nos dice que

$$\left\{\begin{array}{rcrcrcrcl}
a^3 & + & 2b^3 & + & 4c^3 & + & 12abc & = & 3d^3 \\
a^2b & + & 2b^2c & + & 2ac^2 & & & = & 0 \\
ab^2 & + & a^2c & + & 2bc^2 & & & = & 0
\end{array}\right. \tag{II.6}$$

Como estas tres igualdades son homogéneas del mismo grado podemos suponer que $\mathrm{mcd}(a, b, c) = 1$, sin más que dividir las tres ecuaciones por su máximo común divisor. Vamos a demostrar que a es impar. En caso contrario existe $a_1 \in \mathbb{Z}$ tal que $a = 2a_1$, por lo que sustituyendo este valor en la primera igualdad,

$$3d^3 = 8a_1^3 + 2b^3 + 4c^3 + 12abc \in 2\mathbb{Z},$$

luego existe $d_1 \in \mathbb{Z}$ tal que $d = 2d_1$. Entonces,

$$2b^3 = 3d^3 - 8a_1^3 - 4c^3 - 12abc = 24d_1^3 - 8a_1^3 - 4c^3 - 12abc \in 4\mathbb{Z},$$

lo que implica que b es par. Sea $b_1 \in \mathbb{Z}$ tal que $b = 2b_1$ y despejando,

$$4c^3 = 3d^3 - a^3 - 2b^3 - 12abc = 24d_1^3 - 8a_1^3 - 16b_1^3 - 48a_1b_1c = 8(3d_1^2 - a_1^3 - 2b_1^3 - 6a_1b_1c),$$

es decir,

$$c^3 = 2(3d_1^2 - a_1^3 - 2b_1^3 - 6a_1b_1c).$$

Por tanto c^3 es par, así que también c es par. Hemos probado que a, b y c son pares, y esto contradice que $\mathrm{mcd}(a, b, c) = 1$.

Hemos probado así que a es impar, y empleando la segunda igualdad en el sistema (II.6) se tiene

$$a^2b = -2c(b^2 + ac) \in 2\mathbb{Z},$$

así que b es par. Por la tercera igualdad en (II.6) se tiene $a^2c = -b(ab + 2c^2) \in 2\mathbb{Z}$, luego también c es par. Existen por tanto los enteros positivos

$$m := \mathrm{máx}\{k \in \mathbb{Z}^+ : 2^k | b\} \quad \& \quad n := \mathrm{máx}\{k \in \mathbb{Z}^+ : 2^k | c\}.$$

Sean $B, C \in \mathbb{Z}$ números impares tales que $b = 2^m B$ y $c = 2^n C$. La segunda igualdad en (II.6) se reescribe

$$\begin{aligned} 2^m Ba^2 = a^2b = -2c(b^2 + ca) &= -2^{n+1}C(2^{2m}B^2 + 2^nCa) \\ &= -2^{n+2}C(2^{2m-1}B^2 + 2^{n-1}Ca), \end{aligned}$$

lo que implica, puesto que B y a^2 son impares, que $m \geq n + 2$. Utilizando ahora la tercera igualdad en (II.6) obtenemos

$$\begin{aligned} 2^n Ca^2 = a^2c = -b(2c^2 + ab) &= -2^m B(2^{2n+1}C^2 + 2^m aB) \\ &= -2^{m+1}B(2^{2n}C^2 + 2^{m-1}aB), \end{aligned}$$

y esto implica, al ser Ca^2 impar, que $n \geq m + 1$. Es evidente que las desigualdades $m \geq n + 2$ y $n \geq m + 1$ son incompatibles, lo que nos proporciona la contradicción buscada.

(3) Consideremos la torre de cuerpos $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{3})$, de donde

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

Hemos probado en el primer apartado que

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(P_{\mathbb{Q}, \sqrt[3]{2}}) = \deg(\mathtt{t}^3 - 2) = 3,$$

lo que sustituído en la igualdad anterior nos proporciona

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) : \mathbb{Q}] = 3 \cdot [\mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{2})],$$

y vamos a demostrar que $[\mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{2})] = 3$. Si denotamos $K := \mathbb{Q}(\sqrt[3]{2})$ se tiene

$$[\mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{2})] = [K(\sqrt[3]{3}) : K] = \deg(P_{K,\sqrt[3]{3}}),$$

y basta probar que $P_{K,\sqrt[3]{3}} = \mathtt{t}^3 - 3$, o lo que es igual, hay que demostrar que $\mathtt{t}^3 - 3$ es irreducible en $K[\mathtt{t}]$. En caso contrario, y puesto que tiene grado 3, alguna de sus raíces en $\mathbb{C}$ pertenecería a K. Esto es falso, pues dichas raíces son $\sqrt[3]{3}$, $\sqrt[3]{3}\zeta$ y $\sqrt[3]{3}\zeta^2$, donde $\zeta := e^{2\pi/3}$, y en el apartado anterior hemos demostrado que $\sqrt[3]{3} \notin K$, mientras que $\sqrt[3]{3}\zeta$, $\sqrt[3]{3}\zeta^2$ son números complejos no reales, así que no pertenecen a $K \subset \mathbb{R}$. Esto demuestra que $P_{K,\sqrt[3]{3}}(\mathtt{t}) = \mathtt{t}^3 - 3$, y en consecuencia

$$\begin{aligned}[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) : \mathbb{Q}] &= 3 \cdot [\mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{2})] \\ &= 3 \cdot [K(\sqrt[3]{3}) : K] = 3 \cdot \deg(P_{K,\sqrt[3]{3}}) = 3 \cdot \deg(\mathtt{t}^3 - 3) = 9.\end{aligned}$$

(4) Denotemos $u := \sqrt[3]{2}$ y $v := \sqrt[3]{3}$. Se desprende de la prueba del Teorema del elemento primitivo que $\mathbb{Q}(u+v) = \mathbb{Q}(u,v)$ luego, por el apartado anterior, el grado del polinomio mínimo de $u+v$ sobre $\mathbb{Q}$ es 9. Así, todo se reduce a encontrar un polinomio de grado 9 que tenga a $u+v$ por raíz.

Vimos en la Observación I.2.6 que, puesto que $f(\mathtt{t}) := \mathtt{t}^3 - 2$ y $g(\mathtt{t}) := \mathtt{t}^3 - 3$ son los polinomios mínimos de u y v sobre $\mathbb{Q}$, y denotando $h(\mathtt{x}, \mathtt{t}) = g(\mathtt{x} - \mathtt{t})$, el polinomio

$$p(\mathtt{x}) = \mathrm{Res}_{\mathtt{t}}(f(\mathtt{t}), g(\mathtt{x} - \mathtt{t})) \in \mathbb{Q}[\mathtt{t}]$$

es no nulo y $p(u+v) = 0$. Basta pues calcular p y comprobar que tiene grado 9. Comenzamos por calcular

$$g(\mathtt{x} - \mathtt{t}) = (\mathtt{x} - \mathtt{t})^3 - 3 = -\mathtt{t}^3 + 3\mathtt{x}\mathtt{t}^2 - 3\mathtt{x}^2\mathtt{t} + (\mathtt{x}^3 - 3),$$

y a continuación,

$$\begin{aligned}p(\mathtt{x}) = \mathrm{Res}_{\mathtt{t}}(f(\mathtt{t}), g(\mathtt{x} - \mathtt{t})) &= \det \begin{bmatrix} 1 & 0 & 0 & -2 & 0 & 0 \\ 0 & 1 & 0 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & 0 & -2 \\ -1 & 3\mathtt{x} & -3\mathtt{x}^2 & \mathtt{x}^3 - 3 & 0 & 0 \\ 0 & -1 & 3\mathtt{x} & -3\mathtt{x}^2 & \mathtt{x}^3 - 3 & 0 \\ 0 & 0 & -1 & 3\mathtt{x} & -3\mathtt{x}^2 & \mathtt{x}^3 - 3 \end{bmatrix} \\ &= \det \begin{pmatrix} \mathtt{x}^3 - 5 & 6\mathtt{x} & -6\mathtt{x}^2 \\ -3\mathtt{x}^2 & \mathtt{x}^3 - 5 & 6\mathtt{x} \\ 3\mathtt{x} & -3\mathtt{x}^2 & \mathtt{x}^3 - 5 \end{pmatrix} = \mathtt{x}^9 - 15\mathtt{x}^6 - 87\mathtt{x}^3 - 125.\end{aligned}$$

Éste es, por tanto, el polinomio mínimo de $\sqrt[3]{2} + \sqrt[3]{3}$ sobre $\mathbb{Q}$. □

Soluciones a los ejercicios del Capítulo III

Número III.1 Sean $F := K(\mathtt{t})$ y $L := K\big(\mathtt{t}^2/(1+\mathtt{t}^3)\big)$, donde K es un cuerpo y $\mathtt{t}$ es una indeterminada. Demostrar que la extensión $F|L$ es algebraica y simple y calcular su grado.

Solución. Desde luego $F := L(\mathtt{t})$, lo que muestra que F es extensión simple de L. Además, como $\mathrm{mcd}(\mathtt{t}^2, 1+\mathtt{t}^3) = 1$, se deduce del Teorema de Lüroth que la extensión $F|L$ es algebraica y

$$[F : L] = \text{máx}\,\{\deg(1+\mathtt{t}^3),\ \deg(\mathtt{t}^2)\} = 3.$$

□

Número III.2 Sean $E|K$ una extensión de cuerpos y $u \in E \setminus K$.

(1) Demostrar que existe una subextensión $L|K$ de $E|K$ que es maximal entre las que no contienen a u.

(2) Demostrar que u es algebraico sobre L y que la extensión $E|L$ es algebraica.

Solución. (1) Podemos suponer que $K \subset E$ y definimos en el conjunto

$$\mathcal{F} := \{F|K : F|K \text{ es subextensión de } E|K \text{ y } u \notin F\}$$

la relación de orden: $F_1|K \preceq F_2|K$ si $F_1 \subset F_2$. Toda cadena $\mathcal{C} := \{F_i|K\}_{i\in I}$ en $\mathcal{F}$ tiene cota superior en $\mathcal{F}$; basta tomar $F := \bigcup_{i\in I} F_i$. Por el Lema de Zorn $\mathcal{F}$ tiene algún elemento maximal $L|K$, que por definición es maximal entre las subextensiones de $E|K$ que no contienen a u.

(2) Si $u^2 \in L$ entonces u es raíz del polinomio $\mathtt{t}^2 - u^2 \in L[\mathtt{t}]$, luego u es algebraico sobre K. Por otro lado, si $u^2 \notin L$ entonces $L \subsetneq L(u^2)$ y, por ser $L|K$ maximal en $\mathcal{F}$, se deduce que $L(u^2)|K \notin \mathcal{F}$, es decir, $u \in L(u^2)$. Esto implica que u es algebraico sobre L, pues si fuese transcendente, se deduce de la Observación III.1.2 al Teorema de Lüroth que $[L(u) : L(u^2)] = 2$.

Para terminar, supongamos que la extensión $E|L$ no es algebraica, por lo que existe $t \in E$ transcendente sobre L. En particular $L \subsetneq L(t)$ y, por ser $L|K$ una subextensión de $E|K$ maximal entre las que no contienen a u, se cumple que $u \in L(t)$. De este modo $L(u)|L$ es una subextensión propia de $L(t)|L$ lo que implica, por el Teorema de Lüroth, que la extensión $L(t)|L(u)$ es algebraica.

Pero acabamos de demostrar que también es algebraica la extensión $L(u)|L$, y se deduce de la Proposición I.2.7 que $L(t)|L$ es una extensión algebraica. Esto es una contradicción, y por tanto, la extensión $E|L$ es algebraica. □

Número III.3 Sea $K(u)|K$ una extensión transcendente de cuerpos. Demostrar que también $K(u^4, u^6)|K$ es una extensión transcendente y calcular su grado de transcendencia.

Solución. Como $u^2 = u^6/u^4$ se tiene $K(u^2) \subset K(u^4, u^6)$, y esta inclusión es de hecho una igualdad porque $u^4 = (u^2)^2$ y $u^6 = (u^2)^3$ pertenecen a $K(u^2)$. Además la extensión $K(u)|K(u^2)$ es finita, y por tanto algebraica, ya que u es raíz del polinomio $\mathtt{t}^2 - u^2 \in K(u^2)[\mathtt{t}]$. En consecuencia $\operatorname{tr\,deg}\, K(u)|K(u^2) = 0$, y por la transitividad del grado de transcendencia aplicada a la torre de cuerpos $K \subset K(u^2) \subset K(u)$ resulta

$$\begin{aligned}\operatorname{tr\,deg}\, K(u^4, u^6)|K &= \operatorname{tr\,deg}\, K(u^2)|K = \operatorname{tr\,deg}\, K(u)|K \\ &\quad - \operatorname{tr\,deg}\, K(u)|K(u^2) = \operatorname{tr\,deg}\, K(u)|K = 1,\end{aligned}$$

lo que prueba, en particular, que la extensión $K(u^4, u^6)|K$ es transcendente. □

Número III.4 Sea $\{u, v\}$ una base de transcendencia de la extensión de cuerpos $L|K$. Calcular el grado de transcendencia de la extensión $K(u^2, uv)|K$.

Solución. Tanto u como v son algebraicos sobre $E := K(u^2, uv)$, porque son raíces, respectivamente, de los polinomios $\mathtt{t}^2 - u^2 \in E[\mathtt{t}]$ y $u^2\mathtt{t}^2 - (uv)^2 \in E[\mathtt{t}]$. Por tanto la extensión $K(u, v)|E$ es algebraica, y como $L|K(u, v)$ es algebraica, deducimos que $L|E$ también lo es. Así, $\operatorname{tr\,deg}\, L|E = 0$ y por la transitividad del grado de transcendencia se tiene

$$\operatorname{tr\,deg}\, E|K = \operatorname{tr\,deg}\, L|E + \operatorname{tr\,deg}\, E|K = \operatorname{tr\,deg}\, L|K = \operatorname{tr\,deg}\, K(u, v)|K = 2.$$

□

Número III.5 Sean $E|K$ una extensión de cuerpos y $x, y \in E$. Determinar razonadamente la veracidad o falsedad de las siguientes afirmaciones.

(1) Si x o y es transcendente sobre K entonces $x + y$ o xy es transcendente sobre K.

(2) Si x es transcendente sobre K pero y es algebraico sobre K, entonces $x + y$ es transcendente sobre K.

(3) Si x es transcendente sobre K mientras que y es algebraico sobre K, entonces xy es transcendente sobre el cuerpo K.

(4) Si tanto x como y son elementos transcendentes sobre K entonces, x, y son algebraicamente independientes sobre K.

(5) Si x es transcendente sobre K e y es transcendente sobre $K(x)$, entonces x, y son algebraicamente independientes sobre K.

Solución. (1) Supongamos que tanto $a := x + y$ como $b := xy$ son algebraicos sobre K. Como

$$f(\mathtt{t}) := (\mathtt{t} - x)(\mathtt{t} - y) = \mathtt{t}^2 - a\mathtt{t} + b \in K(a, b)[\mathtt{t}],$$

y $f(x) = f(y) = 0$, los elementos x e y son algebraicos sobre $K(a, b)$, y la extensión $K(a, b)|K$ es, por el Corolario I.2.3, algebraica. Por transitividad, tanto x como y serían algebraicos sobre K, lo cual es falso. Por tanto, alguno de los dos elementos, $x + y$ o xy es transcendente sobre K.

(2) Si $x + y$ fuese algebraico sobre K, y puesto que la resta de elementos algebraicos también lo es, se deduce que $x = (x+y)-y$ es algebraico sobre K, contra la hipótesis.

(3) Esta afirmación es falsa; basta elegir $y = 0$, que es algebraico sobre K y, sea quien sea x, el producto $xy = 0$ es también algebraico sobre K.

(4) También este aserto es falso; basta tomar un elemento transcendente cualquiera x e $y := x^2$, que también es transcendente sobre K. Sin embargo x, y son algebraicamente dependientes sobre K pues el polinomio $f(\mathtt{x}, \mathtt{y}) := \mathtt{x}^2 - \mathtt{y} \in K[\mathtt{x}, \mathtt{y}]$ es no nulo y $f(x, y) = x^2 - y = 0$.

(5) Vamos a demostrar que, efectivamente, x, y son algebraicamente independientes sobre K. En caso contrario existe un polinomio no nulo $f \in K[\mathtt{x}, \mathtt{y}] = K[\mathtt{x}][\mathtt{y}]$ tal que $f(x, y) = 0$. Escribimos

$$f := \sum_{j=0}^{n} a_j(\mathtt{x})\mathtt{y}^j \text{ donde cada } a_j \in K[\mathtt{x}].$$

El polinomio

$$g(\mathtt{y}) := \sum_{j=0}^{n} a_j(x)\mathtt{y}^j \in K(x)[\mathtt{y}]$$

es nulo pues $g(y) = f(x, y) = 0$ e y es transcendente sobre $K(x)$. Así, cada $a_j(x) = 0$ y, por ser x transcendente sobre K, se tiene $a_j(\mathtt{x}) = 0$ para $0 \leq j \leq n$, luego $f = 0$. □

Número III.6 Dada una extensión de cuerpos $L|K$, y elementos $t_1, \ldots, t_n \in L$ algebraicamente independientes sobre K se denota

$$E := K(t_1, \ldots, t_n) \quad \& \quad F := K(t_1^{m_1}, \ldots, t_n^{m_n}),$$

donde $m_1, \ldots, m_n$ son enteros positivos. Demostrar que la extensión $E|F$ es finita y calcular su grado.

Solución. Vamos a demostrar, por inducción sobre n, que $E|F$ es una extensión de grado $\prod_{j=1}^{n} m_j$. El caso $n = 1$ se desprende directamente del Teorema de Lüroth, pues $E|F = K(t_1)|K(t_1^{m_1})$ es una extensión finita de grado m_1. Para el paso inductivo introducimos los cuerpos auxiliares $K_1 := K(t_1)$ y

$$E_1 := K(t_1, t_2^{m_2}, \ldots, t_n^{m_n}) = K_1(t_2^{m_2}, \ldots, t_n^{m_n}).$$

Como $t_1, \ldots, t_n$ son algebraicamente independientes sobre K, los elementos $t_2, \ldots, t_n$ lo son sobre K_1 y, por la hipótesis de inducción, la extensión

$$K_1(t_2, \ldots, t_n)|K_1(t_2^{m_2}, \ldots, t_n^{m_n})$$

es finita, de grado $\prod_{j=2}^{n} m_j$.

Por otro lado, t_1 es transcendente sobre $K_2 := K(t_2^{m_2}, \ldots, t_n^{m_n})$ y, por el Teorema de Lüroth, la extensión $K_2(t_1)|K_2(t_1^{m_1})$ es finita, de grado $[K_2(t_1) : K_2(t_1^{m_1})] = m_1$. Aplicando la transitividad del grado a los cuerpos

$$F = K_2(t_1^{m_1}) \subset K_2(t_1) = K_1(t_2^{m_2}, \ldots, t_n^{m_n}) = E_1 \subset K_1(t_2, \ldots, t_n) = E,$$

resulta finalmente

$$\begin{aligned}[E : F] &= [E : E_1] \cdot [E_1 : F] \\ &= [K_1(t_2, \ldots, t_n) : K_1(t_2^{m_2}, \ldots, t_n^{m_n})] \cdot [K_2(t_1) : K_2(t_1^{m_1})] = \prod_{j=1}^{n} m_j.\end{aligned}$$

□

Número III.7 Sean p un número primo, $\mathtt{x}$ e $\mathtt{y}$ indeterminadas sobre $\mathbb{Z}_p$ y consideremos los cuerpos $E := \mathbb{Z}_p(\mathtt{x}, \mathtt{y})$ y $K := \mathbb{Z}_p(\mathtt{x}^p, \mathtt{y}^p)$. Demostrar que la extensión $E|K$ es finita y calcular su grado. ¿Cuál es el grado de transcendencia de la extensión $K|\mathbb{Z}_p$? Demostrar que $E|K$ no es una extensión simple.

Solución. Por el Ejercicio anterior III.6, $[E : K] = p^2$. Para la segunda parte utilizamos la transitividad del grado de transcendencia y que, por III.2.7, $\operatorname{tr\,deg} E|\mathbb{Z}_p = 2$. Por ello, como $\operatorname{tr\,deg} E|K = 0$ por ser $E|K$ algebraica,

$$2 = \operatorname{tr\,deg} E|\mathbb{Z}_p = \operatorname{tr\,deg} E|K + \operatorname{tr\,deg} K|\mathbb{Z}_p = \operatorname{tr\,deg} K|\mathbb{Z}_p.$$

Por último, supongamos que existe $u \in E$ tal que $E = K(u)$. Como $u \in \mathbb{Z}_p(\mathtt{x}, \mathtt{y})$ existen polinomios no nulos $f, g \in \mathbb{Z}_p[\mathtt{x}, \mathtt{y}]$ tales que $u = f(\mathtt{x}, \mathtt{y})/g(\mathtt{x}, \mathtt{y})$. Escribiendo $f(\mathtt{x}, \mathtt{y}) := \sum_{i,j} a_{ij} \mathtt{x}^i \mathtt{y}^j$, donde cada $a_{ij} \in \mathbb{Z}_p$ se tiene, por el Pequeño Teorema de Fermat y la Fórmula del binomio de Newton,

$$(f(\mathtt{x}, \mathtt{y}))^p = \Big(\sum_{i,j} a_{ij} \mathtt{x}^i \mathtt{y}^j \Big)^p = \sum_{i,j} a_{ij}^p \mathtt{x}^{pi} \mathtt{y}^{pj} = \sum_{i,j} a_{ij} (\mathtt{x}^p)^i (\mathtt{y}^p)^j = f(\mathtt{x}^p, \mathtt{y}^p).$$

Por la misma razón $(g(\mathtt{x}, \mathtt{y}))^p = g(\mathtt{x}^p, \mathtt{y}^p)$, y por tanto

$$u^p = (f(\mathtt{x}, \mathtt{y}))^p / (g(\mathtt{x}, \mathtt{y}))^p = f(\mathtt{x}^p, \mathtt{y}^p)/g(\mathtt{x}^p, \mathtt{y}^p) \in K.$$

Así, $h(\mathtt{t}) := \mathtt{t}^p - u^p \in K[\mathtt{t}]$ y $h(u) = 0$, luego $[K(u) : K] \leq p < p^2 = [E : K]$, por lo que $E \neq K(u)$, que es una contradicción. □

Número III.8 (1) Sean $L|E$ y $E|F$ extensiones de cuerpos y $A \subset L$. Probar que si $E|F$ es algebraica también lo es $E(A)|F(A)$. Probar que si $t_1, \ldots, t_n \in L$ son algebraicamente independientes sobre F también son algebraicamente independientes sobre E.

(2) Dadas extensiones de cuerpos $L|E$ y $E|K$ demostrar que $L|K$ es finitamente generada si y sólo si tanto $L|E$ como $E|K$ lo son.

Solución. (1) Hemos de probar que cada $x \in E(A)$ es algebraico sobre $F(A)$. Existen $a_1, \ldots, a_n \in A$ y dos polinomios $f, g \in E[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ tales que $g(a_1, \ldots, a_n) \neq 0$ y $x = f(a_1, \ldots, a_n)/g(a_1, \ldots, a_n)$. Cada $a_j \in F(A)$, luego es algebraico sobre $F(A)$. Además, cada elemento de E es algebraico sobre $F(A)$. Por el Corolario I.2.3 la suma y producto de elementos algebraicos es también algebraico, así que $f(a_1, \ldots, a_n)$ y $g(a_1, \ldots, a_n)$ son algebraicos sobre $F(A)$, luego lo es su cociente x.

Para la segunda parte de este apartado supongamos, por reducción al absurdo, que $t_1, \ldots, t_n \in L$ son elementos algebraicamente dependientes sobre E. Podemos suponer, sin pérdida de generalidad, que t_n es un elemento algebraico sobre el cuerpo $K := E(t_1, \ldots, t_{n-1})$, es decir, $K(t_n)|K$ es una extensión algebraica, y denotamos $A := \{t_1, \ldots, t_{n-1}\}$.

Como la extensión $E|F$ es algebraica se deduce de lo que acabamos de probar que también lo es la extensión $E(A)|F(A) = K|F(A)$. Se sigue de la Proposición I.2.7 que $K(t_n)|F(A)$ es una extensión algebraica, luego t_n es algebraico sobre $F(A)$, y esto implica que $t_1, \ldots, t_n$ son algebraicamente dependientes sobre F, lo que es falso.

(2) Si $L|E$ y $E|K$ son extensiones finitamente generadas existen subconjuntos finitos $A \subset L$ y $B \subset E$ tales que $L = E(A)$ y $E = K(B)$. En consecuencia,

$$L = K(B)(A) = K(A \cup B),$$

así que la extensión $L|K$ es finitamente generada. Supongamos, recíprocamente, que $L|K$ es finitamente generada. Es obvio que $L|E$ también lo es, ya que si el conjunto finito $C \subset L$ cumple que $L = K(C)$, entonces $L = E(C)$. Sólo queda demostrar que $E|K$ es finitamente generada.

Sea $B := \{v_1, \ldots, v_m\} \subset E$ un conjunto de cardinal máximo entre los subconjuntos de E algebraicamente independientes sobre K. Su existencia está garantizada porque en L, y por tanto en E, no hay más de $\operatorname{tr.deg} L|K$ elementos algebraicamente independientes. Nótese que, por la maximalidad de B, la extensión $E|K(B)$ es algebraica.

Como la extensión $L|K$ es finitamente generada también $L|K(B)$ lo es, luego admite, por el Teorema de Steinitz, una base de transcendencia finita, es decir, existen $t_1, \ldots, t_n \in L$ algebraicamente independientes sobre $F := K(B)$ tales que $L|F(T)$ es una extensión finita, donde $T := \{t_1, \ldots, t_n\}$.

Nótese que $K \subset F \subset E \subset L$, y vamos a demostrar que $E|F$ es una extensión finita. En tal caso será finitamente generada, luego existe un subconjunto finito $D \subset E$

tal que $E = F(D) = K(B)(D) = K(B \cup D)$, lo que prueba que la extensión $E|K$ es finitamente generada.

Para demostrar que $E|F$ es finita basta comprobar que $[E : F] \leq [L : F(T)]$, pues la extensión $L|F(T)$ es finita. Para probar esta desigualdad es suficiente probar que cualquier subconjunto finito $\{\alpha_1, \ldots, \alpha_r\}$ de elementos de E que son F-linealmente independientes, también son $F(T)$-linealmente independientes como elementos de L.

Sean $\xi_1, \ldots, \xi_r \in F(T)$ tales que $\sum_{i=1}^r \xi_i \alpha_i = 0$. Sean $h, h_i \in F[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ con $1 \leq i \leq r$, tales que $h \neq 0$ y

$$\xi_i = h_i(t_1, \ldots, t_n)/h(t_1, \ldots, t_n).$$

Por tanto, $\sum_{i=1}^r h_i(t_1, \ldots, t_n)\alpha_i = 0$. Escribimos $h_i := \sum_\nu a_{\nu i} t^\nu$, donde la suma es finita, $\nu = (\nu_1, \ldots, \nu_n)$, $t^\nu = t_1^{\nu_1} \cdots t_n^{\nu_n}$ y cada $a_{\nu i} \in F$. En consecuencia,

$$0 = \sum_{i=1}^r h_i(t_1, \ldots, t_n)\alpha_i = \sum_{i=1}^r \Big(\sum_\nu a_{\nu i} t^\nu \Big) \alpha_i = \sum_\nu \Big(\sum_{i=1}^r a_{\nu i} \alpha_i \Big) t^\nu. \tag{III.7}$$

Como la extensión $E|F$ es algebraica y $t_1, \ldots, t_n$ son algebraicamente independientes sobre F, también lo son, por el apartado (1), sobre E. Se sigue de la igualdad (III.7) que $\sum_{i=1}^r a_{\nu i}\alpha_i = 0$ para cada multiíndice ν. Como $\alpha_1, \ldots, \alpha_r$ son F-linealmente independientes, cada $a_{\nu i} = 0$, esto es, $h_i = 0$ y por ello $\xi_1 = 0, \ldots, \xi_r = 0$. □

Número III.9 Utilizar el Teorema de Lindemann-Weierstrass para demostrar que dados números algebraicos $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ linealmente independientes sobre $\mathbb{Q}$, los números $e^{\alpha_1}, \ldots, e^{\alpha_n}$ son algebraicamente independientes sobre $\mathbb{Q}$.

Solución. Denotemos $\omega_k := e^{\alpha_k}$ para $1 \leq k \leq n$ y supongamos, por reducción al absurdo, que $\omega_1, \ldots, \omega_n$ son algebraicamente dependientes sobre $\mathbb{Q}$. Sin pérdida de generalidad podemos suponer, por el Lema III.2.3, que ω_n es algebraico sobre $\mathbb{Q}(\omega_1, \ldots, \omega_{n-1})$ luego, quitando denominadores, existen polinomios $g_0, \ldots, g_m \in \mathbb{Q}[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$, no todos nulos, tales que

$$g_m(\omega_1, \ldots, \omega_{n-1})\omega_n^m + g_{m-1}(\omega_1, \ldots, \omega_{n-1})\omega_n^{m-1} + \cdots + g_0(\omega_1, \ldots, \omega_{n-1}) = 0. \tag{III.8}$$

Escribimos $g_k := \sum_{0 \leq j_\ell \leq d_{k,\ell}} a_{j_1,\ldots,j_{n-1},k} \mathtt{x}_1^{j_1} \cdots \mathtt{x}_{n-1}^{j_{n-1}}$, donde cada $a_{j_1,\ldots,j_{n-1},k} \in \mathbb{Q}$, y evaluamos dichos polinomios en $\mathtt{x}_\ell := \omega_\ell = e^{\alpha_\ell}$. Así la igualdad (III.8) se reescribe

$$\sum_{0 \leq j_\ell \leq d_{m,\ell}} a_{j_1,\ldots,j_{n-1},m} (e^{\alpha_1})^{j_1} \cdots (e^{\alpha_{n-1}})^{j_{n-1}} e^{m\alpha_n} + \cdots$$
$$+ \sum_{0 \leq j_\ell \leq d_{0,\ell}} a_{j_1,\ldots,j_{n-1},0} (e^{\alpha_1})^{j_1} \cdots (e^{\alpha_{n-1}})^{j_{n-1}} = 0.$$

En consecuencia,

$$\sum_{0\le j_k\le d_{m,\ell}} a_{j_1,\ldots,j_{n-1},\ell} e^{j_1\alpha_1+\cdots+j_{n-1}\alpha_{n-1}+m\alpha_n}+\cdots \\ +\sum_{0\le j_k\le d_{0,\ell}} a_{j_1,\ldots,j_{n-1},0} e^{j_1\alpha_1+\cdots+j_{n-1}\alpha_{n-1}}=0.$$

Por ser $\alpha_1,\ldots,\alpha_n$ linealmente independientes sobre $\mathbb{Q}$ los exponentes

$$\{j_1\alpha_1+\cdots+j_{n-1}\alpha_{n-1}+k\alpha_n:\ 0\le k\le m,\ 0\le j_\ell\le d_{k,\ell}\}$$

son distintos dos a dos. Entonces, por el Teorema de Lindemann-Weierstrass, cada coeficiente $a_{j_1,\ldots,j_{n-1},k}=0$, luego $g_0=0,\ldots,g_m=0$, y esto es falso. □

Número III.10 Utilizar el Teorema de Lindemann-Weierstrass para demostrar que para cada número algebraico $\alpha\in\mathbb{R}\setminus\{0\}$ los números $\operatorname{senh}\alpha$, $\cosh\alpha$ y $\operatorname{tgh}\alpha$ son transcendentes.

Solución. Para el seno y el coseno hiperbólico basta aplicar directamente B.12 (2), ya que

$$\operatorname{senh}\alpha=(1/2)e^{\alpha}-(1/2)e^{-\alpha}\quad\&\quad\cosh\alpha=(1/2)e^{\alpha}+(1/2)e^{-\alpha}.$$

Supongamos que $\operatorname{tgh}\alpha=(e^{\alpha}-e^{-\alpha})/(e^{\alpha}+e^{-\alpha})$ es algebraico. Quitando denominadores,

$$(\operatorname{tgh}\alpha-1)e^{\alpha}+(\operatorname{tgh}\alpha+1)e^{-\alpha}=0,$$

luego $\alpha_1=\alpha$ y $\alpha_2=-\alpha$ son números algebraicos distintos, tanto $c_1:=\operatorname{tgh}\alpha-1$ como $c_2:=\operatorname{tgh}\alpha+1$ son algebraicos, no ambos nulos, pero $c_1e^{\alpha_1}+c_2e^{\alpha_2}=0$, lo que contradice el Teorema de Lindemann-Weierstrass. □

Número III.11 Emplear el Teorema de Gelfond-Schneider para probar que $e^{-\pi/2}$ es un número transcendente. ¿Es transcendente e^{π}?

Solución. Como $\alpha:=i\in\mathbb{C}\setminus\{0,1\}$ y $\beta:=i\in\mathbb{C}\setminus\mathbb{Q}$ son algebraicos, el Teorema de Gelfand-Schneider asegura que i^i es un número transcendente, y vamos a comprobar que $e^{-\pi/2}=i^i$. Para ello basta observar que

$$(i^i)^i=i^{i^2}=i^{-1}=-i=\cos(-\pi/2)+i\operatorname{sen}(-\pi/2)=e^{-\pi i/2}=(e^{-\pi/2})^i,$$

y que si dos números $z_1,z_2\in\mathbb{C}\setminus\{0\}$ cumplen que $z_1^i=z_2^i$, entonces $(z_1^i)^i=(z_2^i)^i$, es decir, $z_1^{-1}=z_2^{-1}$, por lo que $z_1=z_2$.

Para la segunda parte basta observar que, de nuevo por el Teorema de Gelfand-Schneider, $(-1)^i$ es transcendente, y que $e^{\pi}=(-1)^i$. Esta última igualdad se deduce de que $e^{-i\pi}=-1$, y por ello $(-1)^i=(e^{-i\pi})^i=e^{\pi}$. □

Soluciones a los ejercicios del Capítulo IV

Número IV.1 Sea α la raíz séptima real de 5. ¿Cuáles de las siguientes extensiones son de Galois?

$$\mathbb{Q}(\alpha)|\mathbb{Q}, \quad \mathbb{Q}(\sqrt{5},\alpha)|\mathbb{Q}(\alpha), \quad \mathbb{Q}(\sqrt{-5})|\mathbb{Q} \quad \& \quad \mathbb{R}(\sqrt{-7})|\mathbb{R}.$$

Solución. La extensión $\mathbb{Q}(\alpha)|\mathbb{Q}$ no es de Galois porque el polinomio $\mathtt{t}^7-5$ es irreducible en $\mathbb{Q}[\mathtt{t}]$, tiene a $\alpha \in \mathbb{Q}(\alpha)$ por raíz, pero $\beta := \alpha e^{2\pi i/7}$ es raíz de f y no pertenece a $\mathbb{Q}(\alpha) \subset \mathbb{R}$, ya que β no es un número real.

Comprobemos que las restantes extensiones tienen grado 2, lo que por IV.1.5 (3) implica que son de Galois. Como $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$, pues el polinomio mínimo de $\sqrt{5}$ sobre $\mathbb{Q}$ es $\mathtt{t}^2 - 5$, y $\mathrm{mcd}(2,7) = 1$, se deduce de I.2.4 que

$$[\mathbb{Q}(\sqrt{5},\alpha) : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha)(\sqrt{5}) : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2.$$

Por otra parte, los polinomios $\mathtt{t}^2+5$ y $\mathtt{t}^2+7$ son irreducibles en $\mathbb{R}[\mathtt{t}]$, luego en $\mathbb{Q}[\mathtt{t}]$, pues carecen de raíces reales y tienen a $\sqrt{-5}$ y $\sqrt{-7}$ por raíces, respectivamente. Así,

$$[\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}] = \deg(\mathtt{t}^2+5) = 2 \quad \& \quad [\mathbb{R}(\sqrt{-7}) : \mathbb{R}] = \deg(\mathtt{t}^2+7) = 2.$$

□

Número IV.2 Sea $E := \mathbb{Q}(r)$, donde $r := \sqrt[4]{2}$ es el único número real positivo cuya potencia cuarta vale 2. ¿Existen números reales α y β tales que

$$\mathbb{Q}(\alpha) \neq E \neq \mathbb{Q}(\beta) \quad \& \quad E = \mathbb{Q}(\alpha,\beta)?$$

Solución. Por el Criterio de Eisenstein el polinomio mínimo de r sobre $\mathbb{Q}$ es $\mathtt{t}^4-2$, que tiene grado 4, luego $[E : \mathbb{Q}] = 4$. Si existieran α y β en las condiciones del enunciado se tendría

$$\mathbb{Q} \subsetneq \mathbb{Q}(\alpha) \subsetneq E \quad \& \quad \mathbb{Q} \subsetneq \mathbb{Q}(\beta) \subsetneq E,$$

luego los grados de las extensiones $\mathbb{Q}(\alpha)|\mathbb{Q}$ y $\mathbb{Q}(\beta)|\mathbb{Q}$ son divisores propios de 4 distintos de 1, o sea, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = 2$.

Sean $f := P_{\mathbb{Q},\alpha}$ y $g := P_{\mathbb{Q},\beta}$ los polinomios mínimos de α y β sobre $\mathbb{Q}$, respectivamente. Las raíces de f son α y $\alpha_1 = f(0)/\alpha \in \mathbb{Q}(\alpha) \subset E$ y las de g son β y $\beta_1 = g(0)/\beta \in \mathbb{Q}(\beta) \subset E$. Por tanto, $E = \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha,\alpha_1,\beta,\beta_1)$ es el cuerpo de descomposición del producto fg sobre $\mathbb{Q}$, luego la extensión $E|\mathbb{Q}$ es de Galois. Sin embargo esto es falso, pues el polinomio $h(\mathtt{t}) := \mathtt{t}^4 - 2$ es irreducible en $\mathbb{Q}[\mathtt{t}]$, tiene a $r \in E$ por raíz, pero también $ri \in \mathbb{C} \setminus E$ es raíz de h. □

Número IV.3 Sean $E \subset \mathbb{R}$ un cuerpo que contiene a $\mathbb{Q}$ de modo que la extensión $E|\mathbb{Q}$ es de Galois, y $F := E(\sqrt{-1})$. ¿Se puede asegurar que la extensión $F|\mathbb{Q}$ es también de Galois?

Solución. Puesto que la extensión $E|\mathbb{Q}$ es de Galois existe, por la Proposición IV.1.6, un polinomio $f \in \mathbb{Q}[\mathtt{t}]$ tal que E es el cuerpo de descomposición de f sobre $\mathbb{Q}$. Como $E \subset \mathbb{R}$ todas las raíces de f en $\mathbb{C}$, digamos $a_1, \ldots, a_k$, son números reales, y el menor subcuerpo de $\mathbb{R}$ que las contiene es $E := \mathbb{Q}(a_1, \ldots, a_k)$. Sea $g(\mathtt{t}) := (\mathtt{t}^2+1)f(\mathtt{t})$ cuyas raíces son las de f y, además, $\pm\sqrt{-1}$. Así,

$$F = E(\sqrt{-1}) = \mathbb{Q}(a_1, \ldots, a_k, \sqrt{-1})$$

es un cuerpo de descomposición de g sobre $\mathbb{Q}$, así que la extensión $F|\mathbb{Q}$ es de Galois. □

Número IV.4 Sean $L|K$ una extensión algebraica y $\phi : L \to L$ un homomorfismo de cuerpos tal que $\phi|_K = \mathrm{id}_K$. Demostrar que $\phi \in G(L : K)$, esto es, que ϕ es un automorfismo.

Solución. Como L es un cuerpo, ϕ es inyectiva, por lo que se trata de probar que es sobreyectiva. Sea $\alpha \in L$ y denotemos $f := P_{K,\alpha}$ el polinomio mínimo de α sobre K. Sean $\alpha_1 := \alpha, \ldots, \alpha_r$ las raíces de f en L y $E := K(\alpha_1, \ldots, \alpha_r)$. La extensión $E|K$ es finita, en virtud del Corolario I.2.3, pues es algebraica y finitamente generada. Además, por el Lema II.1.1, $\phi(\alpha_i)$ es raíz de f para $1 \leq i \leq r$, por lo que $\phi(E) \subset E$. Por tanto $\phi|_E : E \to E$ es una aplicación lineal e inyectiva del K-espacio vectorial de dimensión finita E en sí mismo, luego es sobreyectiva. Como $\alpha \in E$ existe $\beta \in E \subset L$ tal que $\phi(\beta) = \alpha$, y hemos concluido. □

Número IV.5 Sean K un cuerpo de característica 0 y $E|K$ y $F|K$ dos subextensiones de Galois de la extensión $L|K$. Demostrar que $(E \cap F)|K$ es extensión de Galois.

Solución. La extensión $(E \cap F)|K$ es finita por serlo $E|K$, y para probar que es de Galois emplearemos, puesto que $\mathrm{char}(K) = 0$, la caracterización obtenida en la Proposición IV.1.6. Fijamos un cierre algebraico $\overline{L}$ de L y sea $f \in K[\mathtt{t}]$ un polinomio irreducible que tiene una raíz $\alpha \in E \cap F$. Por ser de Galois la extensión $E|K$ existen $a \in K$ y $\alpha := \alpha_1, \ldots, \alpha_r \in E$ tales que

$$f(t) := a(\mathtt{t} - \alpha_1) \cdots (\mathtt{t} - \alpha_r).$$

Pero $F \subset \overline{L}$ y f factoriza en $F[\mathtt{t}]$ en producto de factores de grado 1, pues la extensión $F|K$ es de Galois y la raíz α de f pertenece al cuerpo F, luego $\alpha_1, \ldots, \alpha_r \in F$. Por tanto, f factoriza en $(E \cap F)[\mathtt{t}]$ en producto de factores de grado 1. □

Número IV.6 Sean $L|K$ una extensión de Galois y $\alpha \in L$ tal que el único automorfismo de L que deja fijo α es la identidad. Demostrar que $L = K(\alpha)$.

Solución. El enunciado afirma que $G(L : K(\alpha)) = \{\mathrm{id}_L\}$ y, por el Teorema fundamental de la teoría de Galois, $K(\alpha) = \mathrm{Fix}(G(L : K(\alpha))) = \mathrm{Fix}(\mathrm{id}_L) = L$. □

Número IV.7 Sean K un cuerpo y $\mathtt{t}$ una indeterminada sobre K.

(1) Demostrar que las siguientes afirmaciones son equivalentes, en cuyo caso se dice que K posee la *propiedad de la extensión:*

(1.1) Cada automorfismo de $K(\mathtt{t})$ es extensión de un automorfismo de K.

(1.2) Para cada automorfismo $\varphi : K(\mathtt{t}) \to K(\mathtt{t})$ se cumple que $\varphi(K) = K$.

(1.3) Para cada automorfismo $\varphi : K(\mathtt{t}) \to K(\mathtt{t})$ se cumple que $\varphi(K) \subset K$.

(2) Sea K un cuerpo en el que cada uno de sus elementos es, bien un cuadrado bien el opuesto de un cuadrado. Demostrar que K posee la propiedad de la extensión. Deducir que los cuerpos algebraicamente cerrados tienen la propiedad de la extensión.

(3) Sea K un cuerpo en el que el polinomio $f(\mathtt{t}) := \mathtt{t}^2 + 1$ no tiene raíces. Sea $i := \sqrt{-1}$ una raíz de f en un cierre algebraico de K, y supongamos que $K(i)$ es un cuerpo algebraicamente cerrado. Probar que cada elemento de K es, un cuadrado o el opuesto de un cuadrado y, por tanto, posee la propiedad de la extensión. Deducir que $G(\mathbb{R}(\mathtt{t}) : \mathbb{R}) = \mathrm{Aut}(\mathbb{R}(\mathtt{t}))$.

(4) Demostrar que toda extensión algebraica de $\mathbb{Q}$ posee la propiedad de la extensión.

(5) Encontrar un cuerpo que no posee la propiedad de la extensión.

Solución. (1) Veamos que (1.1) $\Longrightarrow$ (1.2) Por la hipótesis existe un automorfismo $\psi : K \to K$ tal que $\varphi|_K = \psi$, luego $\varphi(K) = \psi(K) = K$. Es obvio que (1.2) $\Longrightarrow$ (1.3) y, finalmente, demostramos que (1.3) $\Longrightarrow$ (1.1) Sea $\varphi \in \mathrm{Aut}(K(\mathtt{t}))$. Por hipótesis $\varphi(K) \subset K$, y aplicando la hipótesis al automorfismo inverso $\varphi^{-1} \in \mathrm{Aut}(K(\mathtt{t}))$, se deduce que $\varphi^{-1}(K) \subset K$, por lo que

$$\varphi(K) \subset K = \varphi\big(\varphi^{-1}(K)\big) \subset \varphi(K),$$

luego $\varphi(K) = K$. Así, φ es extensión del automorfismo $\psi := \varphi|_K : K \to K$.

(2) Supongamos que K no posee la propiedad de la extensión. Esto significa, por el apartado anterior, que existe un automorfismo $\varphi : K(\mathtt{t}) \to K(\mathtt{t})$ tal que

$$M := \{x \in K : \varphi(x) \in K(\mathtt{t}) \setminus K\} \neq \varnothing.$$

Para cada $x \in M$ existen polinomios no nulos $f_x, g_x \in K[\mathtt{t}]$ primos entre sí tales que g_x es mónico y $\varphi(x) = f_x/g_x \in K(\mathtt{t}) \setminus K$. Estos polinomios son únicos, luego está bien definida la aplicación

$$\delta : M \to \mathbb{Z}^+,\ x \mapsto \delta(x) := \deg(f_x) + \deg(g_x).$$

Sea $x \in M$ tal que $\delta(x) \leq \delta(y)$ para todo $y \in M$. Cambiando x por $-x$ si es preciso podemos suponer que existe $y \in K$ tal que $x := y^2$. De hecho $y \in M$ pues en caso contrario $\varphi(y) \in K$, y esto implica que $\varphi(x) = \varphi(y^2) = (\varphi(y))^2 \in K$, lo que es falso. Además,

$$f_y^2/g_y^2 = (f_y/g_y)^2 = (\varphi(y))^2 = \varphi(y^2) = \varphi(x) = f_x/g_x,$$

y g_y^2 es mónico, pues g_y lo es, y f_y^2 y g_y^2 son primos entre sí ya que f_y y g_y lo son. En consecuencia, $f_y^2 = f_x$ y $g_y^2 = g_x$, lo que implica que

$$\delta(x) = \deg(f_x) + \deg(g_x) = \deg(f_y^2) + \deg(g_y^2) = 2(\deg(f_y) + \deg(g_y)) = 2\delta(y).$$

En particular $\delta(y) < \delta(x)$ contra la elección de x. La segunda parte de este apartado es evidente, porque si K es algebraicamente cerrado y $x \in K$ el polinomio $\mathtt{t}^2 - x \in K[\mathtt{t}]$ tiene alguna raíz $y \in K$, esto es, $x = y^2$.

(3) Como f tiene grado 2 y no tiene raíces en K es irreducible en $K[\mathtt{t}]$, luego es el polinomio mínimo de i sobre K, lo que implica que $[K(i) : K] = 2$. Así, dado $x \in K \subset K(i)$ existen, por ser $K(i)$ algebraicamente cerrado, $a, b \in K$ tales que $x = (a + bi)^2 = (a^2 - b^2) + 2abi$, lo que implica que $x = a^2 - b^2$ y $ab = 0$. Si $a = 0$ entonces $x = -b^2$, mientras que si $b = 0$ resulta que $x = a^2$, lo que prueba lo requerido. Así, por el apartado (2), K posee la propiedad de la extensión.

El cuerpo $\mathbb{R}$ de los números reales cumple estas hipótesis, así que todo automorfismo de $\mathbb{R}(\mathtt{t})$ es extensión de un automorfismo de $\mathbb{R}$ que, por IV.1.2, es la identidad. Esto demuestra la igualdad $G(\mathbb{R}(\mathtt{t}) : \mathbb{R}) = \mathrm{Aut}(\mathbb{R}(\mathtt{t}))$.

(4) Dadas una extensión algebraica $K|\mathbb{Q}$ y un automorfismo $\varphi : K(\mathtt{t}) \to K(\mathtt{t})$ hemos de probar que $\varphi(K) \subset K$. Si $x \in K$ existe, por ser algebraico sobre $\mathbb{Q}$, un polinomio no nulo $f(\mathtt{t}) := \sum_{j=0}^{n} a_j \mathtt{t}^j \in \mathbb{Q}[\mathtt{t}]$ tal que $f(x) = 0$. En virtud de IV.1.2 la restricción $\varphi|_{\mathbb{Q}} : \mathbb{Q} \to K(\mathtt{t})$ es la inclusión, y se tiene

$$0 = \varphi(0) = \varphi\Big(\sum_{j=0}^{n} a_j x^j\Big) = \sum_{j=0}^{n} \varphi(a_j)\varphi(x^j) = \sum_{j=0}^{n} a_j \varphi(x)^j = f(\varphi(x)),$$

luego $\varphi(x) \in K(\mathtt{t})$ es algebraico sobre $\mathbb{Q}$, luego sobre K. Así, por III.1.2 (2), $\varphi(x) \in K$.

(5) Sean L un cuerpo arbitrario, $\mathtt{x}$ una indeterminada sobre L y $K := L(\mathtt{x})$. El automorfismo

$$\varphi : K(\mathtt{t}) = L(\mathtt{x}, \mathtt{t}) \to K(\mathtt{t}) = L(\mathtt{x}, \mathtt{t}),\ f(\mathtt{x}, \mathtt{t})/g(\mathtt{x}, \mathtt{t}) \mapsto f(\mathtt{t}, \mathtt{x})/g(\mathtt{t}, \mathtt{x})$$

no cumple la condición $\varphi(K) \subset K$, pues $\mathtt{x} \in K$ y $\varphi(\mathtt{x}) = \mathtt{t} \notin K$. □

Número IV.8 Sea $L|K$ una extensión de Galois y consideremos, para cada automorfismo $\sigma \in G(L : K)$, el homomorfismo de anillos

$$\widehat{\sigma} : L[\mathtt{t}] \to L[\mathtt{t}],\ \sum_{i=0}^{d} a_i \mathtt{t}^i \mapsto \sum_{i=0}^{d} \sigma(a_i)\mathtt{t}^i.$$

(1) Probar que un polinomio $h \in L[\mathtt{t}]$ pertenece a $K[\mathtt{t}]$ si y sólo si $\widehat{\tau}(h) = h$ para cada $\tau \in G(L : K)$.

(2) Demostrar que para cada $g \in L[\mathtt{t}]$ se cumple que $\widehat{g} := \prod_{\sigma \in G(L:K)} \widehat{\sigma}(g) \in K[\mathtt{t}]$.

(3) Sean $f(\mathtt{t}) = \mathtt{t}^n + \sum_{j=0}^{n-1} b_j \mathtt{t}^j \in L[\mathtt{t}]$ un polinomio mónico y $L = K(b_0, \ldots, b_{n-1})$. Demostrar que si $\sigma, \tau \in G(L:K)$ son distintos, entonces $\widehat{\sigma}(f) \neq \widehat{\tau}(f)$, y probar que si $\widehat{f}$ es irreducible en $K[\mathtt{t}]$, entonces f es irreducible en $L[\mathtt{t}]$.

(4) Probar que para cada $n \in \mathbb{Z}^+$ el polinomio $f_n(\mathtt{t}) = \mathtt{t}^n - \sqrt{2}$ es irreducible en $\mathbb{Q}(\sqrt{2})[\mathtt{t}]$.

Solución. (1) Un polinomio $h(\mathtt{t}) := \sum_{i=0}^{d} a_i \mathtt{t}^i \in L[\mathtt{t}] \setminus K[\mathtt{t}]$ si y sólo si para algún índice $0 \leq i \leq d$ se tiene $a_i \notin K = \mathrm{Fix}(G(L:K))$, esto es, $\tau(a_i) \neq a_i$ para algún automorfismo $\tau \in G(L:K)$, o lo que es igual, $\widehat{\tau}(h) \neq h$.

(2) Aplicamos el criterio del apartado anterior. Para cada $\tau \in G(L:K)$ se tiene

$$\widehat{\tau}(\widehat{g}) = \widehat{\tau}\Big(\prod_{\sigma \in G(L:K)} \widehat{\sigma}(g)\Big) = \prod_{\sigma \in G(L:K)} \widehat{\tau}(\widehat{\sigma}(g)) \prod_{\sigma \in G(L:K)} (\widehat{\sigma}\widehat{\tau})(g) = \prod_{\alpha \in G(L:K)} \widehat{\alpha}(g) = \widehat{g},$$

por lo que $\widehat{g} \in K[\mathtt{t}]$.

(3) Como $\sigma \neq \tau$ pero $\sigma|_K = \mathrm{id} = \tau|_K$ y $L = K(b_0, \ldots, b_{n-1})$, existe un índice $0 \leq j \leq n-1$ tal que $\sigma(b_j) \neq \tau(b_j)$, por lo que $\widehat{\sigma}(f) \neq \widehat{\tau}(f)$. Supongamos ahora, por reducción al absurdo, que $\widehat{f}$ es irreducible en $K[\mathtt{t}]$ pero f es reducible en $L[\mathtt{t}]$. Existen por tanto polinomios de grado positivo $g, h \in L[\mathtt{t}]$ tales que $f := gh$. Entonces,

$$\begin{aligned}\widehat{f} := \prod_{\sigma \in G(L:K)} \widehat{\sigma}(f) &= \prod_{\sigma \in G(L:K)} \widehat{\sigma}(gh) = \prod_{\sigma \in G(L:K)} \widehat{\sigma}(g)\widehat{\sigma}(h) \\ &= \Big(\prod_{\sigma \in G(L:K)} \widehat{\sigma}(g)\Big) \cdot \Big(\prod_{\sigma \in G(L:K)} \widehat{\sigma}(h)\Big) = \widehat{g} \cdot \widehat{h},\end{aligned}$$

y $\widehat{g}, \widehat{h} \in K[\mathtt{t}]$, por el apartado (2), y su grado es positivo, luego $\widehat{f}$ es reducible en $K[\mathtt{t}]$, que es una contradicción.

(4) La extensión $L|\mathbb{Q}$, donde $L := \mathbb{Q}(\sqrt{2})$, es de Galois pues $[L:\mathbb{Q}] = 2$. Por ello el grupo de Galois $G(L:\mathbb{Q}) = \{\sigma_1 = \mathrm{id}, \sigma_2\}$, donde $\sigma_2(\sqrt{2}) = -\sqrt{2}$. Con las notaciones del apartado (2) se tiene

$$\widehat{f}_n = \widehat{\sigma}_1(f_n) \cdot \widehat{\sigma}_2(f_n) = (\mathtt{t}^n - \sqrt{2})(\mathtt{t}^n + \sqrt{2}) = \mathtt{t}^{2n} - 2$$

que es irreducible en $\mathbb{Q}[\mathtt{t}]$. Por el apartado (3), f_n es irreducible en $\mathbb{Q}(\sqrt{2})[\mathtt{t}]$. □

Número IV.9 Dada una extensión de Galois $L|K$ de cuerpos de característica 0 denotamos $G := G(L:K)$ su grupo de Galois y fijamos $u \in L$. Definimos el polinomio

$$f(\mathtt{t}) := \prod_{\phi \in G} (\mathtt{t} - \phi(u)).$$

(1) Probar que f pertenece a $K[\mathtt{t}]$ y es potencia del polinomio mínimo de u sobre K.

(2) Probar que f es irreducible en $K[\mathtt{t}]$ si y sólo si u es elemento primitivo de $L|K$.

Solución. (1) Escribimos $G := \{\phi_1, \ldots, \phi_n\}$, de modo que

$$f(\mathtt{t}) := (\mathtt{t} - \phi_1(u)) \cdots (\mathtt{t} - \phi_n(u)) = \mathtt{t}^n + \sum_{k=1}^{n} (-1)^k \mathtt{s}_k(\phi_1(u), \ldots, \phi_n(u)) \mathtt{t}^{n-k},$$

donde $\mathtt{s}_1, \ldots, \mathtt{s}_n$ son las formas simétricas elementales en n indeterminadas. Por ser de Galois la extensión $L|K$ se cumple que $K := \mathrm{Fix}(G)$, luego para demostrar que $f \in K[\mathtt{t}]$ basta ver que los coeficientes de f quedan fijos por la acción de cada elemento de G. Sean pues $a_k := (-1)^k \mathtt{s}_k(\phi_1(u), \ldots, \phi_n(u))$ el coeficiente de f que acompaña a $\mathtt{t}^{n-k}$ y $\phi_j \in G$. Por la Proposición I.1.3, vol. I.,

$$G = \{\phi_1 \cdot \phi_j, \ldots, \phi_n \cdot \phi_j\},$$

y puesto que los polinomios $\mathtt{s}_k$ son simétricos, resulta

$$\begin{aligned} \phi_j(a_k) &= (-1)^k \phi_j(\mathtt{s}_k(\phi_1(u), \ldots, \phi_n(u))) = (-1)^k \mathtt{s}_k(\phi_j(\phi_1(u)), \ldots, \phi_j(\phi_n(u))) \\ &= (-1)^k \mathtt{s}_k((\phi_1 \cdot \phi_j)(u), \ldots, (\phi_n \cdot \phi_j)(u)) = (-1)^k \mathtt{s}_k(\phi_1(u), \ldots, \phi_n(u)) = a_k. \end{aligned}$$

Para la segunda parte, denotemos $g := P_{K,u}$ el polinomio mínimo de u sobre K y consideremos el subgrupo $H := G(L : K(u))$ de G. El polinomio f es múltiplo en $K[\mathtt{t}]$ de g porque $f \in K[\mathtt{t}]$ y $f(u) = 0$. En consecuencia, g factoriza en $L[\mathtt{t}]$ como producto de factores de grado 1 ya que f lo hace. Denotamos $u := u_1, u_2, \ldots, u_m$ las raíces de $g(\mathtt{t}) := (\mathtt{t} - u_1) \cdots (\mathtt{t} - u_m)$ en L. Obsérvese que $m = [K(u) : K]$ porque $\mathrm{char}(K) = 0$, lo que implica que las raíces de g son simples. Además, toda raíz de f lo es de g. Para comprobarlo fijamos una raíz $\phi_i(u)$ de f y escribimos

$$g(\mathtt{t}) := \sum_{k=0}^{d} c_k \mathtt{t}^k \in K[\mathtt{t}].$$

Entonces,

$$g(\phi_i(u)) = \sum_{k=0}^{d} c_k \phi_i(u)^k = \phi_i\Big(\sum_{k=0}^{d} c_k u^k\Big) = \phi_i(g(u)) = \phi_i(0) = 0.$$

Obsérvese que dados $\sigma, \tau \in G$ se cumple que $\sigma(u) = \tau(u)$ si y sólo si $(\tau^{-1} \circ \sigma)(u) = u$, esto es, si y sólo si $\sigma \cdot \tau^{-1} \in H$. En consecuencia, las clases de congruencia por la derecha del grupo G respecto de su subgrupo H son los conjuntos $\{C_i : \ 1 \le i \le m\}$, donde

$$C_i = \{\phi \in G : \phi(u) = u_i\}.$$

Nótese, además, que $\mathrm{Card}(C_i) = \mathrm{ord}(H) = r$ para $1 \le i \le r$, pues todas las clases laterales tienen el mismo orden que H. Puesto que hemos probado que $u_1, \ldots, u_m$ son las raíces distintas de f podemos reescribirlo del siguiente modo:

$$f(\mathtt{t}) = \prod_{i=1}^{m} \prod_{\phi \in C_i} (\mathtt{t} - \phi(u)) = \prod_{i=1}^{m} (\mathtt{t} - u_i)^r = \Big(\prod_{i=1}^{m} (\mathtt{t} - u_i)\Big)^r = g(\mathtt{t})^r,$$

lo que demuestra que f es potencia de g.

(2) El polinomio $f \in K[\mathtt{t}]$, que tiene a u por raíz, es irreducible en $K[\mathtt{t}]$ si y sólo si coincide con el polinomio mínimo g de u sobre K, y esto equivale a que $\deg(f) = \deg(g)$. Por un lado, $\deg(g) = \deg(P_{K,u}) = [K(u) : K]$, mientras que, como la extensión $L|K$ es de Galois,

$$\deg(f) = \operatorname{ord}(G(L : K)) = [L : K] = [L : K(u)] \cdot [K(u) : K] = [L : K(u)] \cdot \deg(g).$$

Por tanto, f es irreducible si y sólo si $[L : K(u)] = 1$, esto es, $L = K(u)$. □

Número IV.10 Sean K un cuerpo, $f \in K[\mathtt{t}]$ un polinomio de grado n y E un cuerpo de descomposición de f sobre K en el que f posee n raíces distintas $\xi_1, \ldots, \xi_n$. Demostrar que para cada polinomio $p \in K[\mathtt{t}]$ existe otro $g \in K[\mathtt{t}]$ de grado n del que son raíces $\{p(\xi_i) : 1 \leq i \leq n\}$.

Solución. Hay que probar que los coeficientes del polinomio $g(\mathtt{t}) := \prod_{j=1}^{n}(\mathtt{t} - p(\xi_j))$ pertenecen al cuerpo K. Denotemos u_k el coeficiente de $\mathtt{t}^k$ en el polinomio g y $\mathtt{s}_1, \ldots, \mathtt{s}_n \in \mathbb{Z}[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ las formas simétricas elementales en n variables. Por las Fórmulas de Cardano-Vieta,

$$u_k = (-1)^k \mathtt{s}_k(p(\xi_1), \ldots, p(\xi_n)),$$

y puesto que $K = \operatorname{Fix}(G(L : K))$ ya que la extensión $E|K$ es de Galois, es suficiente comprobar que $\phi(u_k) = u_k$ para cada $\phi \in G(L : K)$. Para ello observamos dos cosas. En primer lugar, para $1 \leq i \leq n$ se cumple que $\phi(\xi_i) \in M := \{\xi_1, \ldots, \xi_n\}$, en virtud del Lema II.1.1. Por tanto, la restricción $\phi|_M : M \to M$ es una aplicación inyectiva, luego biyectiva. En segundo, escribiendo $p(\mathtt{t}) := \sum_{i=0}^{d} a_i \mathtt{t}^i \in K[\mathtt{t}]$ resulta

$$\phi(p(\xi_j)) = \phi\Big(\sum_{i=0}^{d} a_i \xi_j^i\Big) = \sum_{i=0}^{d} a_i \phi(\xi_j)^i = p(\phi(\xi_j)),$$

y obtenemos finalmente, por la simetría del polinomio $\mathtt{s}_k$,

$$\begin{aligned}\phi(u_k) &= (-1)^k \phi(\mathtt{s}_k(p(\xi_1), \ldots, p(\xi_n))) = (-1)^k \mathtt{s}_k(\phi(p(\xi_1)), \ldots, \phi(p(\xi_n))) \\ &= (-1)^k \mathtt{s}_k(p(\phi(\xi_1)), \ldots, p(\phi(\xi_n))) = (-1)^k \mathtt{s}_k(p(\xi_1), \ldots, p(\xi_n)) = u_k,\end{aligned}$$

como queríamos demostrar. □

Número IV.11 Sean $\alpha := e^{\pi i/3}$ y β una raíz del polinomio $f(\mathtt{t}) := \mathtt{t}^4 - 6\mathtt{t}^2 + 6$. Encontrar generadores de la clausura de Galois $L|\mathbb{Q}$ de las siguientes extensiones y calcular en cada caso el grado de $L|\mathbb{Q}$:

$$\mathbb{Q}(\sqrt[4]{3})|\mathbb{Q}, \quad \mathbb{Q}(\alpha)|\mathbb{Q}, \quad \mathbb{Q}(\beta)|\mathbb{Q} \quad \& \quad \mathbb{Q}(\sqrt[5]{2})|\mathbb{Q}.$$

Solución. (1) Sea $\gamma := \sqrt[4]{3}$. La clausura de Galois $L|\mathbb{Q}$ de $\mathbb{Q}(\gamma)|\mathbb{Q}$ es el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio mínimo $P_{\mathbb{Q},\gamma}(\mathtt{t}) := \mathtt{t}^4 - 3$. Sus raíces son $\{\gamma, -\gamma, i\gamma, -i\gamma\}$, donde $i := \sqrt{-1}$, así que $L = \mathbb{Q}(\gamma, i)$. Además, por la transitividad del grado, y puesto que $\mathbb{Q}(\gamma) \subset \mathbb{R}$,

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\gamma)] \cdot [\mathbb{Q}(\gamma) : \mathbb{Q}] = [\mathbb{Q}(\gamma)(i) : \mathbb{Q}(\gamma)] \cdot 4 = 2 \cdot 4 = 8.$$

(2) El número α es raíz de $\mathtt{t}^3 + 1 = (\mathtt{t} + 1) \cdot (\mathtt{t}^2 - \mathtt{t} + 1)$ porque $\alpha^3 = e^{\pi i} = -1$. Como $\alpha \notin \mathbb{Q}$ esto implica que su polinomio mínimo es $\mathtt{t}^2 - \mathtt{t} + 1$. Por ello la extensión $\mathbb{Q}(\alpha)|\mathbb{Q}$ tiene grado 2, luego es de Galois, y por eso coincide con su clausura de Galois.

(3) Al resolver la ecuación $\mathtt{t}^4 - 6\mathtt{t}^2 + 6 = 0$ se obtiene $\mathtt{t}^2 = 3 \pm \sqrt{3}$, luego las raíces de f en $\mathbb{C}$ son

$$\eta := \sqrt{3 + \sqrt{3}}, \;\; -\eta, \;\; \beta := \sqrt{3 - \sqrt{3}} \quad \& \quad -\beta,$$

donde la elección de β en lugar de η es irrelevante. La clausura de Galois de $\mathbb{Q}(\beta)|\mathbb{Q}$ es, por tanto, $L|\mathbb{Q}$, donde $L := \mathbb{Q}(\beta, \eta)$. De hecho,

$$\beta \cdot \eta = \sqrt{6} \quad \& \quad \sqrt{2} = \sqrt{6}/\sqrt{3} = \beta \cdot \eta/(3 - \beta^2),$$

por lo que $L = \mathbb{Q}(\beta, \sqrt{2})$. Para calcular el grado de la extensión $L|\mathbb{Q}$ vamos a demostrar que $\sqrt{2} \notin \mathbb{Q}(\beta) := E$. Supongamos lo contrario, o lo que es igual, $L = E := \mathbb{Q}(\beta)$. Aplicando la transitividad del grado a la cadena de cuerpos $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\beta)(\sqrt{2}) = L$ resulta, puesto que $f = P_{\mathbb{Q},\beta}$ es el polinomio mínimo de β sobre $\mathbb{Q}$,

$$[\mathbb{Q}(\sqrt{2})(\beta) : \mathbb{Q}(\sqrt{2})] = [E : \mathbb{Q}(\sqrt{2})] = \frac{[E : \mathbb{Q}]}{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]} = \frac{[\mathbb{Q}(\beta) : \mathbb{Q}]}{2} = \frac{\deg(f)}{2} = 2,$$

luego el polinomio mínimo $f_1 \in \mathbb{Q}(\sqrt{2})[\mathtt{t}]$ de β sobre $\mathbb{Q}(\sqrt{2})$ tiene grado 2 y divide en $\mathbb{Q}(\sqrt{2})[\mathtt{t}]$ a f. Por ello las raíces de f_1 son β y otra de las raíces de f, es decir, bien $-\beta$, bien $\pm\eta$. En consecuencia, el producto de las raíces de f_1, que es $f_1(0) \in \mathbb{Q}(\sqrt{2})$ es $-\beta^2 = \sqrt{3} - 3$ o $\pm\beta\eta = \pm\sqrt{6}$. Esto es una contradicción pues como $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, ni $-\beta^2$ ni $\beta\eta$ pertenecen a $\mathbb{Q}(\sqrt{2})$.

Lo anterior demuestra que $[\mathbb{Q}(\beta)(\sqrt{2}) : \mathbb{Q}(\beta)] = 2$, y finalmente,

$$[L : \mathbb{Q}] = [\mathbb{Q}(\beta)(\sqrt{2}) : \mathbb{Q}(\beta)] = 2 \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

(4) Sea $r := \sqrt[5]{2} \in \mathbb{R}$. La clausura de Galois de $\mathbb{Q}(r)|\mathbb{Q}$ es el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio mínimo $P_{\mathbb{Q},r}(\mathtt{t}) := \mathtt{t}^5 - 2$. Sea v otra raíz de $P_{\mathbb{Q},r}$. Entonces $v^5 = r^5$, luego $(v/r)^5 = 1$, así que $v/r = \xi^k$, donde $\xi := e^{2\pi i/5}$, y $0 \le k \le 4$. Por tanto, la clausura de Galois de $\mathbb{Q}(r)|\mathbb{Q}$ es $L|\mathbb{Q}$, con $L = \mathbb{Q}(r, \xi)$. El polinomio mínimo de ξ sobre $\mathbb{Q}$ es $\Phi_5(\mathtt{t}) := \mathtt{t}^4 + \mathtt{t}^3 + \mathtt{t}^2 + \mathtt{t} + 1$, por lo que

$$[\mathbb{Q}(r) : \mathbb{Q}] = \deg(P_{\mathbb{Q},r}) = 5 \quad \& \quad [\mathbb{Q}(\xi) : \mathbb{Q}] = \deg(P_{\mathbb{Q},\xi}) = \deg(\Phi_5) = 4.$$

Como $\mathrm{mcd}(4, 5) = 1$ se deduce del Ejemplo I.2.4 que $[L : \mathbb{Q}] = 4 \cdot 5 = 20$. □

Número IV.12 Sean $A := \mathbb{Z}[\sqrt{2}]$, $\xi := e^{\pi i/5}$, donde $i := \sqrt{-1} \in \mathbb{C}$, y $L \subset \mathbb{C}$ un cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $\mathtt{t}^{10} - 2$. Se pide:

(1) Hallar el polinomio mínimo de ξ sobre $\mathbb{Q}$ y estudiar si es irreducible en $A[\mathtt{t}]$.

(2) Encontrar el polinomio mínimo de $\sqrt[10]{2}$ sobre $\mathbb{Q}$ y factorizarlo en producto de polinomios irreducibles en el anillo $A[\mathtt{t}]$.

(3) Calcular el grado $n := [L : \mathbb{Q}]$ de la extensión $L|\mathbb{Q}$.

(4) Demostrar que para cada divisor positivo d de n la extensión $L|\mathbb{Q}$ admite alguna subextensión de grado d.

(5) ¿Cuántas subextensiones $E|\mathbb{Q}$ de $L|\mathbb{Q}$ tienen grado 8? ¿Cuántas tienen grado 5?

(6) ¿Es abeliano el grupo de Galois $G(L : \mathbb{Q})$?

Solución. (1) Como $\xi^5 = \cos\pi + i \operatorname{sen}\pi = -1$, resulta

$$0 = \xi^5 + 1 = (\xi + 1)(\xi^4 - \xi^3 + \xi^2 - \xi + 1),$$

luego ξ es raíz del segundo factor, ya que $\xi \neq -1$. Como el polinomio ciclotómico

$$\Phi_5(\mathtt{t}) := \mathtt{t}^4 + \mathtt{t}^3 + \mathtt{t}^2 + \mathtt{t} + 1$$

es irreducible en $\mathbb{Q}[\mathtt{t}]$, en virtud de VI.2.7, vol. II, también lo es su imagen por el isomorfismo

$$\mathbb{Q}[\mathtt{t}] \to \mathbb{Q}[\mathtt{t}],\ p(\mathtt{t}) \mapsto p(-\mathtt{t}).$$

En consecuencia, $f(\mathtt{t}) := P_{\mathbb{Q},\xi}(\mathtt{t}) = \Phi_5(-\mathtt{t}) = \mathtt{t}^4 - \mathtt{t}^3 + \mathtt{t}^2 - \mathtt{t} + 1$.

Veamos que f es también irreducible en $A[\mathtt{t}]$, y para ello comenzamos calculando sus raíces $x \in \mathbb{C}$. Como $f(x) = 0$, entonces $x^5 + 1 = 0$ y $x \neq -1$, luego $x^{10} = (-1)^2 = 1$ y $x^2 \neq 1$. Por tanto x es un generador del grupo cíclico $\mathcal{U}_{10} := \langle\xi\rangle$ de orden 10 formado por las raíces décimas de la unidad. Los generadores de este grupo son las potencias $x := \xi^j$ donde $\operatorname{mcd}(j, 10) = 1$, esto es, el conjunto de raíces de f en $\mathbb{C}$ es

$$Z_{\mathbb{C}}(f) = \{\xi, \xi^3, \xi^7, \xi^9\}.$$

Ninguna de estas raíces es un número real, luego $Z_{\mathbb{C}}(f) \cap A = \varnothing$. Como $A \subset \mathbb{R}$, si f es reducible en $A[\mathtt{t}]$ será producto de dos polinomio mónicos de $A[\mathtt{t}]$ de grado dos.

Por otro lado, también en $\mathbb{R}[\mathtt{t}]$ el polinomio f es producto de dos polinomios de grado dos, pues f carece de raíces reales. Como ξ tiene módulo 1,

$$\xi \cdot \xi^9 = \xi^{10} = 1 = \xi \cdot \overline{\xi} \quad \Longrightarrow \quad \xi^9 = \overline{\xi} \quad \Longrightarrow \quad \xi^7 = \overline{\xi^3}.$$

En consecuencia, la factorización de f como producto de polinomios irreducibles de $\mathbb{C}[\mathtt{t}]$ es

$$f = (\mathtt{t} - \xi) \cdot (\mathtt{t} - \overline{\xi}) \cdot (\mathtt{t} - \xi^3) \cdot (\mathtt{t} - \overline{\xi^3}). \tag{IV.9}$$

Denotamos

$$a := \xi + \overline{\xi} \in \mathbb{R} \quad \& \quad b := \xi^3 + \overline{\xi^3} \in \mathbb{R}.$$

Como $\xi \cdot \overline{\xi} = \xi^3 \cdot \overline{\xi^3} = 1$, a partir de (IV.9) se obtiene esta factorización de f en $\mathbb{R}[\mathtt{t}]$:

$$\mathtt{t}^4 - \mathtt{t}^3 + \mathtt{t}^2 - \mathtt{t} + 1 = f(\mathtt{t}) = (\mathtt{t}^2 - a\mathtt{t} + 1) \cdot (\mathtt{t}^2 - b\mathtt{t} + 1), \tag{IV.10}$$

luego $a + b = 1$ y $ab + 2 = 1$. Entonces, $a(1 - a) + 1 = 0$, o sea, $a^2 - a - 1 = 0$, es decir,

$$a = (1 + \sqrt{5})/2 \quad \& \quad b = (1 - \sqrt{5})/2.$$

Vimos en el Ejemplo IV.1.9 (4), vol. II que A es un dominio euclídeo, luego el anillo de polinomios $A[\mathtt{t}]$ es un DFU, así que (IV.10) sería la factorización de f en producto de polinomios irreducibles en $A[\mathtt{t}]$ si f no fuese irreducible en este último anillo. Por ello $a \in A$, luego $\sqrt{5} \in K := \mathbb{Q}(\sqrt{2})$, y esto contradice lo probado en el Ejemplo I.2.4. En consecuencia $f = P_{\mathbb{Q},\xi}$ es irreducible en $A[\mathtt{t}]$.

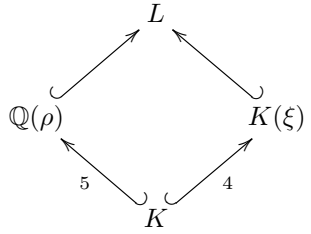
(2) Sea $\rho := \sqrt[10]{2}$ la única raíz décima real y positiva de 2. El polinomio $g(\mathtt{t}) := \mathtt{t}^{10} - 2$ tiene a ρ por raíz y es irreducible en $\mathbb{Z}[\mathtt{t}]$ por el Criterio de Eisenstein, luego lo es en $\mathbb{Q}[\mathtt{t}]$. Por tanto $P_{\mathbb{Q},\rho} = g$. Además, $g(\mathtt{t}) = g_1(\mathtt{t}) \cdot g_2(\mathtt{t})$, donde

$$g_1(\mathtt{t}) = \mathtt{t}^5 - \sqrt{2} \quad \& \quad g_2(\mathtt{t}) = \mathtt{t}^5 + \sqrt{2}$$

son polinomios irreducibles en $A[\mathtt{t}]$. En efecto, como $g_2(\mathtt{t}) = -g_1(-\mathtt{t})$ es suficiente probar que g_1 es irreducible en $A[\mathtt{t}]$ y, puesto que K es el cuerpo de fracciones de A basta probar, en virtud del Lema VI.1.5, vol. II, que g_1 es irreducible en $K[\mathtt{t}]$. Pero $g_1(\rho) = 0$, luego basta ver que $[\mathbb{Q}(\rho) : K] = 5 = \deg(g_1)$, y esto es obvio ya que

$$[\mathbb{Q}(\rho) : K] = \frac{[\mathbb{Q}(\rho) : \mathbb{Q}]}{[K : \mathbb{Q}]} = \frac{10}{2} = 5.$$

(3) Sea η una raíz de g. Entonces $\rho^{10} = \eta^{10} = 2$, luego $(\eta/\rho)^{10} = 1$. Por tanto existe un entero $0 \le k \le 9$ tal que $\eta = \rho\xi^k$. En particular $L = \mathbb{Q}(\rho, \xi)$. Acabamos de probar que $[\mathbb{Q}(\rho) : K] = 5$, y en el apartado (1) vimos que f es irreducible en $A[\mathtt{t}]$, luego en $K[\mathtt{t}]$. Así $f = P_{K,\xi}$, por lo que $[K(\xi) : K] = \deg(f) = 4$. Tenemos por tanto un diagrama de extensiones de cuerpos



Al ser 4 y 5 primos entre sí, $[L : K] = 4 \cdot 5 = 20$, en virtud del Ejemplo I.2.4 y, finalmente,

$$[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] = 20 \cdot 2 = 40.$$

(4) Por el Teorema fundamental de la teoría de Galois basta ver que el grupo de Galois $G := G(L : \mathbb{Q})$, que es un grupo de orden $40 = 2^3 \cdot 5$, tiene subgrupos de órdenes 2, 4, 5, 8, 10 y 20. Sólo la existencia de subgrupos de órdenes 10 y 20 requiere algún comentario; los otros casos se deducen inmediatamente de los Teoremas de Sylow.

Para tratar estos dos casos observamos que existe un subgrupo normal H de G de orden 5, ya que el número n_5 de subgrupos de G de orden 5 divide a 8 y $n_5 - 1 \in 5\mathbb{Z}$, es decir, $n_5 = 1$. De este modo, si H_2 y H_4 son subgrupos de G de órdenes 2 y 4, los subgrupos $K_1 := HH_2$ y $K_2 := HH_4$ de G tienen órdenes 10 y 20, ya que

$$\mathrm{ord}(K_1) = \frac{\mathrm{ord}\, H) \cdot \mathrm{ord}(H_2)}{\mathrm{ord}(H \cap H_2)} = \frac{5 \cdot 2}{1} = 10 \quad \& \qquad \mathrm{ord}(K_2) = \frac{\mathrm{ord}(H) \cdot \mathrm{ord}(H_4)}{\mathrm{ord}(H \cap H_4)} = \frac{5 \cdot 4}{1} = 20.$$

(5) Por el Teorema fundamental de la Teoría de Galois el número de subextensiones $E|\mathbb{Q}$ de $L|\mathbb{Q}$ de grado 8 es 1, pues coincide con el número de subgrupos de orden 5 de G. En cuanto al número de subextensiones $E|\mathbb{Q}$ de grado 5, coincide con el número n_2 de subgrupos de G de orden 8, que divide a 5 y cumple que $n_2 - 1 \in 2\mathbb{Z}$. Por tanto, $n_2 = 1$ o $n_2 = 5$.

Pero los elementos $\alpha := \rho^2$ y $\beta := \rho^2\xi$ de L cumplen que $\alpha^5 = \rho^{10} = 2$ y $\beta^5 = \rho^{10}\xi^5 = -2$, por lo que

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(P_{\mathbb{Q},\alpha}) = \deg(\mathtt{t}^5 - 2) = 5 \quad \& \qquad [\mathbb{Q}(\beta) : \mathbb{Q}] = \deg(P_{\mathbb{Q},\beta}) = \deg(\mathtt{t}^5 + 2) = 5,$$

y $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$, ya que $\alpha \in \mathbb{R}$ y $\beta \in \mathbb{C} \setminus \mathbb{R}$. Esto muestra que $L|\mathbb{Q}$ tiene al menos dos subextensiones de grado 5, luego tiene exactamente 5.

(6) Si $G(L : \mathbb{Q})$ fuese abeliano todos sus subgrupos serían normales. En particular, como sus subgrupos de orden 8 son, por el Teorema de Sylow, conjugados dos a dos, tendría un único subgrupo de orden 8, contra lo ya probado. □

Número IV.13 (1) Sea G un grupo abeliano de orden ocho tal que el orden máximo de los elementos de G es cuatro. Demostrar que G es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_4$ y calcular cuántos subgrupos tiene de cada orden.

(2) Sean $\xi := e^{\pi i/10}$, $\eta := \xi^4$, $i := \sqrt{-1}$ y $u := \eta + \eta^{-1}$. Calcular el polinomio mínimo de u sobre $\mathbb{Q}$ y decidir si el cuerpo $\mathbb{Q}(u)$ contiene a i.

(3) Demostrar que $\mathbb{Q}(\xi) = \mathbb{Q}(i, \eta)$, que $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{5})$ y que $[\mathbb{Q}(\xi) : \mathbb{Q}] = 8$. Calcular el polinomio mínimo de ξ sobre $\mathbb{Q}$.

(4) Probar que el grupo de Galois $G(\mathbb{Q}(\xi) : \mathbb{Q})$ es abeliano y encontrar generadores sobre $\mathbb{Q}$ de las subextensiones de $\mathbb{Q}(\xi)|\mathbb{Q}$.

(5) Sea E el cuerpo de descomposición sobre $\mathbb{Q}(\xi)$ del polinomio $f(\mathtt{t}) := \mathtt{t}^4 - 5$. Probar que la extensión $E|\mathbb{Q}$ es de Galois, calcular su grado y decidir si $G(E : \mathbb{Q})$ es o no abeliano.

Solución. (1) Los grupos abelianos de orden 8 son isomorfos, por el Teorema de Estructura de los grupos abelianos finitos, a uno de los tres siguientes: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_8$ y $\mathbb{Z}_2 \times \mathbb{Z}_4$. El primero carece de elementos de orden 4 y el segundo posee un elemento de orden 8. Por tanto G es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_4$. Los elementos de este grupo se clasifican, según su orden, del modo siguiente:

$$\text{Elementos de orden 1: } \{(0,0)\}; \quad \text{Elementos de orden 2: } \{(0,2),(1,0),(1,2)\}$$
$$\text{Elementos de orden 4: } \{(0,1),(0,3),(1,1),(1,3)\},$$

donde cada entero se ha identificado con su clase $\mathsf{mod}\,2$ para las primeras coordenadas y con su clase $\mathsf{mod}\,4$ para las segundas. De aquí se desprende que G posee, exactamente, tres subgrupos de orden 2. En cuanto a los de orden cuatro, son cíclicos o son isomorfos al grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$. De los primeros sólo hay dos, ya que $\langle(0,1)\rangle = \langle(0,3)\rangle$ y $\langle(1,1)\rangle = \langle(1,3)\rangle$. De los segundos sólo hay uno, pues ha de estar formado por el neutro $(0,0)$ y los tres elementos de orden dos que tiene G. En conclusión, G posee, exactamente, tres subgrupos de orden 4.

(2) Según vimos en el Ejemplo I.2.4, el polinomio mínimo sobre $\mathbb{Q}$ de $\eta := e^{2\pi i/5}$ es el polinomio ciclotómico

$$\Phi_5(\mathtt{t}) := P_{\eta,\mathbb{Q}}(\mathtt{t}) = \mathtt{t}^4 + \mathtt{t}^3 + \mathtt{t}^2 + \mathtt{t} + 1.$$

Por tanto,

$$\eta^4 + \eta^3 + \eta^2 + \eta + 1 = 0,$$

y dividiendo por η^2 deducimos que $\eta^2 + \eta + 1 + \eta^{-1} + \eta^{-2} = 0$. Ahora bien,

$$u^2 = (\eta + \eta^{-1})^2 = \eta^2 + \eta^{-2} + 2 \quad \Longrightarrow \quad u^2 + u = \eta^2 + \eta^{-2} + 2 + \eta + \eta^{-1} = 1.$$

Así, el polinomio $g(\mathtt{t}) := \mathtt{t}^2 + \mathtt{t} - 1$ tiene a u por raíz y es irreducible en $\mathbb{Q}[\mathtt{t}]$, pues ninguna de sus raíces es un número racional. Por tanto, $P_{\mathbb{Q},u}(\mathtt{t}) = g(\mathtt{t}) := \mathtt{t}^2 + \mathtt{t} - 1$. Para acabar este apartado observamos que $\eta \cdot \overline{\eta} = |\eta|^2 = 1$, es decir, $\overline{\eta} = \eta^{-1}$, así que

$$u = \eta + \eta^{-1} = \eta + \overline{\eta} = 2\cos 2\pi/5 \in \mathbb{R},$$

por lo que $\mathbb{Q}(u) \subset \mathbb{R}$ y en particular $i \notin \mathbb{Q}(u)$.

(3) Observamos que $\xi^5 = e^{\pi i/2} = i$, lo que junto con la igualdad obvia $\xi = \xi^5/\xi^4$ muestra que

$$\mathbb{Q}(\xi) = \mathbb{Q}(\xi^5, \xi^4) = \mathbb{Q}(i, \eta).$$

Por otro lado, u es la raíz positiva del polinomio g, esto es, $u := (\sqrt{5} - 1)/2$, y por ello,

$$\mathbb{Q}(u) = \mathbb{Q}(2u + 1) = \mathbb{Q}(\sqrt{5}).$$

Para demostrar que $[\mathbb{Q}(\xi) : \mathbb{Q}] = 8$ basta probar que $i \notin \mathbb{Q}(\eta)$. Una vez visto esto, y puesto que

$$\mathbb{Q} \subset \mathbb{Q}(\eta) \subset \mathbb{Q}(\eta)(i) = \mathbb{Q}(\xi),$$

tendremos

$$[\mathbb{Q}(\xi):\mathbb{Q}] = [\mathbb{Q}(\eta)(i):\mathbb{Q}(\eta)]\cdot[\mathbb{Q}(\eta):\mathbb{Q}] = 2\cdot\deg(P_{\mathbb{Q},\eta}) = 2\cdot 4 = 8.$$

Comprobemos pues que $i\notin\mathbb{Q}(\eta)$. En caso contrario, $\mathbb{Q}(i)|\mathbb{Q}$ y $\mathbb{Q}(u)|\mathbb{Q}$ serían, en virtud del apartado (2), dos subextensiones distintas, de grado 2, de $\mathbb{Q}(\eta)|\mathbb{Q}$. Por ser $\mathbb{Q}(\eta)|\mathbb{Q}$ una extensión de Galois de grado 4 lo anterior implica, por el Teorema fundamental, que el grupo de Galois $G(\mathbb{Q}(\eta):\mathbb{Q})$ posee al menos dos elementos de orden 2. Esto es falso, pues se prueba en el Ejemplo IV.1.9 que $G(\mathbb{Q}(\eta):\mathbb{Q})\cong\mathbb{Z}_5^*\cong\mathbb{Z}_4$.

Para terminar este apartado calculemos el polinomio mínimo $h := P_{\mathbb{Q},\xi}$ de ξ sobre $\mathbb{Q}$. Desde luego $\xi^{10} = e^{\pi i} = -1$, luego h divide a $h_1(\mathtt{t}) := \mathtt{t}^{10}+1$. Sabemos además que h tiene grado 8.

Por otro lado, $i^{10}+1 = i^2+1 = 0$, luego i es raíz de h_1, por lo que el polinomio mínimo $h_2(\mathtt{t}) := \mathtt{t}^2+1$ de i sobre $\mathbb{Q}$ divide a h_1. Como $h_2(\xi)\neq 0$, el cociente $h_1/h_2\in\mathbb{Q}[\mathtt{t}]$ es mónico de grado 8 y tiene a ξ por raíz luego, a fortiori, coincide con h. Para efectuar el cociente denotamos $\mathtt{x} := \mathtt{t}^2$ y resulta

$$h(\mathtt{t}) = \frac{h_1(\mathtt{t})}{h_2(\mathtt{t})} = \frac{\mathtt{t}^{10}+1}{\mathtt{t}^2+1} = \frac{\mathtt{x}^5+1}{\mathtt{x}+1} = \mathtt{x}^4-\mathtt{x}^3+\mathtt{x}^2-\mathtt{x}+1 = \mathtt{t}^8-\mathtt{t}^6+\mathtt{t}^4-\mathtt{t}^2+1.$$

(4) La extensión $\mathbb{Q}(\xi)|\mathbb{Q} = \mathbb{Q}(i,\eta)|\mathbb{Q}$ es de Galois, por ser el cuerpo de descomposición del polinomio

$$P_{\mathbb{Q},i}(\mathtt{t})\cdot P_{\mathbb{Q},\eta}(\mathtt{t}) = (\mathtt{t}^2+1)\cdot(\mathtt{t}^4+\mathtt{t}^3+\mathtt{t}^2+\mathtt{t}+1) = (\mathtt{t}-i)\cdot(\mathtt{t}+i)\prod_{k=1}^{4}(\mathtt{t}-\eta^k).$$

En particular el grupo de Galois $G(\mathbb{Q}(\xi):\mathbb{Q})$ tiene orden 8 y sus elementos quedan determinados por su acción sobre los generadores i y η que, por el Lema II.1.1, se transforman en raíces de los polinomios mínimos $P_{\mathbb{Q},i}$ y $P_{\mathbb{Q},\eta}$, respectivamente. Así, los automorfismos de $\mathbb{Q}(\xi) = \mathbb{Q}(i,\eta)$ transforman i en $\pm i$ y η en η^k con $1\leq k\leq 4$. Pero ya sabemos que existen exactamente 8 automorfismos luego

$$G(\mathbb{Q}(\xi):\mathbb{Q}) = \{\varphi_{j,k}:\ j=0,1,\ 1\leq k\leq 4\},$$

donde el automorfismo φ_{jk} queda determinado por las imágenes $\varphi_{j,k}(i) = (-1)^j i$ y $\varphi_{j,k}(\eta) = \eta^k$. Para comprobar que $G(\mathbb{Q}(\xi):\mathbb{Q})$ es abeliano basta observar que

$$(\varphi_{m,n}\cdot\varphi_{j,k})(i) = (-1)^{j+m}i \quad \& \quad (\varphi_{m,n}\cdot\varphi_{j,k})(\eta) = \eta^{kn},$$

por lo que $\varphi_{m,n}\cdot\varphi_{j,k} = \varphi_{j,k}\cdot\varphi_{m,n}$.

Para conocer las subextensiones de $\mathbb{Q}(\xi)|\mathbb{Q}$ es útil saber cuántas hay, y para ello demostraremos primero que los grupos $G(\mathbb{Q}(\xi):\mathbb{Q})$ y $\mathbb{Z}_2\times\mathbb{Z}_4$ son isomorfos. Para comprobarlo es suficiente, en virtud del apartado (1), probar que cada $\varphi_{j,k}^4 = \mathrm{id}_{\mathbb{Q}(\xi)}$ y que $\varphi_{0,2}^2\neq\mathrm{id}_{\mathbb{Q}(\xi)}$. Lo segundo es obvio, pues $\varphi_{0,2}^2(\eta) = \eta^4\neq\eta$, y para lo primero basta calcular:

$$\varphi_{j,k}^4(i) = (-1)^{4j}i = i \quad \& \quad \varphi_{j,k}^4(\eta) = \eta^{k^4}.$$

Por el Pequeño Teorema de Fermat, $k^4 = 1 + 5\ell$ para cierto entero ℓ, y por ello, como $\eta^5 = 1$,

$$\varphi_{j,k}^4(\eta) = \eta^{k^4} = \eta^{1+5\ell} = \eta \cdot \eta^{5\ell} = \eta \cdot (\eta^5)^\ell = \eta.$$

También hemos demostrado en el primer apartado que el grupo de Galois $G(\mathbb{Q}(\xi) : \mathbb{Q})$ posee, exactamente, tres subgrupos de orden 4 y tres subgrupos de orden 2. Esto implica, por el Teorema fundamental, que existen, exactamente, tres subextensiones $K_\ell|\mathbb{Q}$, $1 \leq \ell \leq 3$, de grado 2 y tres subextensiones $K_\ell|\mathbb{Q}$, $4 \leq \ell \leq 6$ de grado 4, y que éstas son todas las subextensiones propias de $\mathbb{Q}(\xi)|\mathbb{Q}$.

Se trata ahora de encontrar generadores de cada una de ellas. Hemos observado que $K_1 := \mathbb{Q}(i)$ y $K_2 := \mathbb{Q}(\sqrt{5})$ son cuerpos intermedios entre $\mathbb{Q}$ y $\mathbb{Q}(\xi)$ y cada uno de ellos tiene grado 2 sobre $\mathbb{Q}$. Pero esto implica que $K_3 := \mathbb{Q}(\sqrt{5}i)$ es otro cuerpo intermedio entre $\mathbb{Q}$ y $\mathbb{Q}(\xi)$, distinto de los anteriores y de grado 2, ya que $v := \sqrt{5}i$ es raíz del polinomio $\mathtt{t}^2 + 5$, que es irreducible en $\mathbb{Q}[\mathtt{t}]$.

Para justificar que K_3 no coincide ni con K_1 ni con K_2 es suficiente darse cuenta de que si, por ejemplo, $K_3 = K_1$, entonces $\sqrt{5}i \in \mathbb{Q}(i)$, luego $\sqrt{5} \in \mathbb{Q}(i)$, por lo que $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(i)$, lo que junto con la igualdad $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ implica que $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(i)$, y esto es falso, ya que $\mathbb{Q}(\sqrt{5}) \subset \mathbb{R}$. Así pues ya hemos encontrado generadores de las extensiones $K_1|\mathbb{Q}$, $K_2|\mathbb{Q}$ y $K_3|\mathbb{Q}$.

En cuanto a los cuerpos intermedios que proporcionan subextensiones de grado 4, una de ellas es $K_4 := \mathbb{Q}(i, \sqrt{5})$ y otra es $K_5 := \mathbb{Q}(\eta)$. Son distintas, porque, según vimos en el apartado (3), $i \notin \mathbb{Q}(\eta)$. Presentamos dos soluciones para buscar generadores de la extensión $K_6|\mathbb{Q}$.

Primera solución. Necesariamente, K_6 es el cuerpo fijo de uno de los automorfismos de orden 2 de la extensión $\mathbb{Q}(\xi)|\mathbb{Q}$ y para averiguar de cuál observamos que $\varphi_{1,4}$ tiene orden 2 y no fija ni i ni η, ya que $\varphi_{1,4}(i) = -i$ y $\varphi_{1,4}(\eta) = \eta^{-1}$. En consecuencia $K_6 = \mathrm{Fix}(\varphi_{1,4})$. Calculemos $\varphi_{1,4}(\xi)$:

$$\varphi_{1,4}(\xi^5) = \varphi_{1,4}(i) = -i = -\xi^5 \quad \& \quad \varphi_{1,4}(\xi^4) = \varphi_{1,4}(\eta) = \eta^{-1} = \xi^{-4}.$$

Al dividir obtenemos

$$\varphi_{1,4}(\xi) = \varphi_{1,4}(\xi^5/\xi^4) = -\xi^5/\xi^{-4} = -\xi^9.$$

Como $\xi^{10} = -1$, se tiene $\xi^9 = -\xi^{-1} = -\overline{\xi}$, esto es $\varphi_{14}(\xi) = \overline{\xi} = \xi^{-1}$. Pero entonces,

$$\varphi_{14}(\xi^{-1}) = (\varphi_{14}(\xi))^{-1} = (\xi^{-1})^{-1} = \xi.$$

En consecuencia, $\omega := \xi + \xi^{-1} \in \mathrm{Fix}(\varphi_{14}) = K_6$, y vamos a demostrar la igualdad $K_6 = \mathbb{Q}(\omega)$. Para ello basta probar que el polinomio mínimo de ω sobre $\mathbb{Q}$ tiene grado cuatro. Denotemos $v := \xi^2 + \xi^{-2}$. Entonces,

$$v^2 = (\xi^2 + \xi^{-2})^2 = \xi^4 + \xi^{-4} + 2,$$

y teniendo en cuenta que $h(\xi) = 0$ según hemos visto en el apartado (3),

$$\begin{aligned} v^2 - v &= \xi^4 + \xi^{-4} + 2 - \xi^2 - \xi^{-2} = \xi^{-4}(\xi^8 - \xi^6 + 2\xi^4 - \xi^2 + 1) \\ &= \xi^{-4}(\xi^8 - \xi^6 + \xi^4 - \xi^2 + 1) + 1 = \xi^{-4}h(\xi) + 1 = 1, \end{aligned}$$

esto es, $v^2 - v - 1 = 0$. Ahora, $\omega^2 = \xi^2 + \xi^{-2} + 2 = v + 2$, luego $v = \omega^2 - 2$, y sustituyendo,

$$0 = v^2 - v - 1 = (\omega^2 - 2)^2 - (\omega^2 - 2) - 1 = \omega^4 - 5\omega^2 + 5.$$

Como el polinomio $\mathtt{t}^4 - 5\mathtt{t}^2 + 5$ es irreducible en $\mathbb{Q}[\mathtt{t}]$, por el Criterio de Eisenstein, y tiene a ω por raíz, es su polinomio mínimo, por lo que $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$ lo que confirma que $\mathbb{Q}(\omega) = K_6$.

Segunda solución. Si no se sabe encontrar un elemento primitivo de la extensión $K_6|\mathbb{Q}$ podemos emplear una estrategia de carácter general. Como $\varphi_{1,4}(\xi) = -\xi^9$ y puesto que $\xi^{10} = -1$ se tiene

$$\begin{aligned} \varphi_{1,4}(\xi^j) = (-\xi^9)^j &= (-1)^j\xi^{9j} \\ &= (-1)^j\xi^{(10-1)j} = (-1)^j\xi^{10j}\xi^{-j} = (-1)^j(-1)^j\xi^{-j} = \xi^{-j}. \end{aligned}$$

Ahora bien, $\xi^{-j} = -\xi^{10}\xi^{-j} = -\xi^{10-j}$, por lo que $\varphi_{1,4}(\xi^j) = -\xi^{10-j}$. Puesto que cada elemento $x \in \mathbb{Q}(\xi)$ se escribe como $x := \sum_{j=0}^{7} x_j\xi^j$ para ciertos $x_j \in \mathbb{Q}$, resulta

$$\varphi_{1,4}(x) = \sum_{j=0}^{7} x_j\varphi_{1,4}(\xi^j) = -\sum_{j=0}^{7} x_j\xi^{10-j} = -(x_0\xi^{10} + x_1\xi^9 + x_2\xi^8) - \sum_{j=3}^{7} x_j\xi^{10-j}.$$

Ahora bien, sabemos que $\xi^8 = \xi^6 - \xi^4 + \xi^2 - 1$, lo que implica que $\xi^9 = \xi^7 - \xi^5 + \xi^3 - \xi$, luego sustituyendo estos valores,

$$\varphi_{1,4}(x) = x_0 + x_1(-\xi^7 + \xi^5 - \xi^3 + \xi) + x_2(-\xi^6 + \xi^4 - \xi^2 + 1) - \sum_{j=3}^{7} x_{10-j}\xi^j.$$

Por tanto, x pertenece al cuerpo fijo $K_6 := \mathrm{Fix}(\varphi_{1,4})$ de $\varphi_{1,4}$ si y sólo si

$$\begin{aligned} \sum_{j=0}^{7} x_j\xi^j &= x_0 + x_1(-\xi^7 + \xi^5 - \xi^3 + \xi) + x_2(-\xi^6 + \xi^4 - \xi^2 + 1) - \sum_{j=3}^{7} x_{10-j}\xi^j \\ &= (x_0 + x_2) + x_1\xi - x_2\xi^2 - (x_1 + x_7)\xi^3 + (x_2 - x_6)\xi^4 + (x_1 - x_5)\xi^5 \\ &\quad - (x_2 + x_4)\xi^6 - (x_1 + x_3)\xi^7. \end{aligned}$$

Como los vectores $\{\xi^j : 0 \le j \le 7\}$ son $\mathbb{Q}$-linealmente independientes,

$$\left\{\begin{array}{rcl} x_0 &=& x_0 + x_2 \\ x_2 &=& -x_2 \\ x_3 &=& -(x_1 + x_7) \\ x_4 &=& x_2 - x_6 \\ x_5 &=& x_1 - x_5 \\ x_6 &=& -(x_2 + x_4) \\ x_7 &=& -(x_1 + x_3) \end{array}\right. \iff \left\{\begin{array}{rcl} x_2 &=& 0 \\ x_3 &=& -(x_1 + x_7) \\ x_4 &=& -x_6 \\ x_1 &=& 2x_5 \end{array}\right.$$

Este sistema de ecuaciones lineales es equivalente a

$$\left\{\begin{array}{rcl} x_1 &=& 2x_5 \\ x_2 &=& 0 \\ x_6 &=& -x_4 \\ x_7 &=& -(2x_5 + x_3) \end{array}\right.$$

luego los elementos del subcuerpo $K_6 = \mathrm{Fix}(\varphi_{1,4})$ de $\mathbb{Q}(\xi)$ son los de la forma

$$\begin{aligned} x &= x_0 + 2x_5\xi + x_3\xi^3 + x_4\xi^4 + x_5\xi^5 - x_4\xi^6 - (2x_5 + x_3)\xi^7 \\ &= x_0 + x_3(\xi^3 - \xi^7) + x_4(\xi^4 - \xi^6) + x_5(2\xi + \xi^5 - 2\xi^7), \end{aligned}$$

y finalmente resulta

$$K_6 = \mathbb{Q}(\xi^3 - \xi^7,\ \xi^4 - \xi^6,\ 2\xi + \xi^5 - 2\xi^7).$$

(5) En virtud del apartado anterior, E es el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio

$$p(\mathtt{t}) := (\mathtt{t}^2 + 1) \cdot (\mathtt{t}^4 + \mathtt{t}^3 + \mathtt{t}^2 + \mathtt{t} + 1) \cdot (\mathtt{t}^4 - 5),$$

luego la extensión $E|\mathbb{Q}$ es de Galois. Veamos que $[E : \mathbb{Q}(\xi)] = 2$, lo que implica que

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\xi)] \cdot [\mathbb{Q}(\xi) : \mathbb{Q}] = 2 \cdot 8 = 16.$$

Por un lado, las raíces de $\mathtt{t}^4 - 5$ son $\sqrt[4]{5}, -\sqrt[4]{5}, \sqrt[4]{5}i, -\sqrt[4]{5}i$ y, como $i \in \mathbb{Q}(\xi)$,

$$E = \mathbb{Q}(\xi)(\sqrt[4]{5}, -\sqrt[4]{5}, \sqrt[4]{5}i, -\sqrt[4]{5}i) = \mathbb{Q}(\xi)(\sqrt[4]{5}, \sqrt[4]{5}i) = \mathbb{Q}(\xi)(\sqrt[4]{5}, i) = \mathbb{Q}(\xi)(\sqrt[4]{5}).$$

En consecuencia, $[E : \mathbb{Q}(\xi)] = \deg(P_{\mathbb{Q}(\xi),\sqrt[4]{5}})$, así que basta probar que el polinomio mínimo de $\sqrt[4]{5}$ sobre $\mathbb{Q}(\xi)$ tiene grado 2.

Como $\mathtt{t}^2 - \sqrt{5} \in \mathbb{Q}(\xi)[\mathtt{t}]$ tiene a $\sqrt[4]{5}$ por raíz, basta probar que $\sqrt[4]{5} \notin \mathbb{Q}(\xi)$. En caso contrario, $\mathbb{Q}(\sqrt[4]{5})|\mathbb{Q}$ sería una subextensión de grado 4 de $\mathbb{Q}(\xi)|\mathbb{Q}$, luego coincidiría con una de las tres subextensiones $K_4|\mathbb{Q}$, $K_5|\mathbb{Q}$ o $K_6|\mathbb{Q}$ de grado 4 calculadas en el apartado anterior. Esto es imposible ya que $\mathbb{Q}(\sqrt[4]{5}) \subset \mathbb{R}$, mientras que tanto K_4 como K_5 y K_6 contienen números complejos no reales, pues

$$i \in K_4 \setminus \mathbb{R}, \quad \eta \in K_5 \setminus \mathbb{R} \quad \& \quad 2\xi + \xi^5 - 2\xi^7 \in K_6 \setminus \mathbb{R}.$$

Veamos que $2\xi + \xi^5 - 2\xi^7 \in \mathbb{C} \setminus \mathbb{R}$. En caso contrario, como $-\xi^7 = \xi^{-3} = \overline{\xi^3}$, se tiene

$$0 = \Im(2\xi+\xi^5-2\xi^7) = 2\Im(\xi)+1-2\Im(\xi^7) = 2\Im(\xi)+1+2\Im(\xi^{-3}) = 2\Im(\xi)+1+2\Im(\overline{\xi^3}),$$

donde $\Im(z)$ denota la parte imaginaria del número complejo $z \in \mathbb{C}$. Por tanto,

$$\begin{aligned} 1/2 &= -\Im(\xi) - \Im(\overline{\xi^3}) = -\Im(\xi) + \Im(\xi^3) = \operatorname{sen}(3\pi/10) - \operatorname{sen}(\pi/10) \\ &= 2\cos(2\pi/5)\operatorname{sen}(\pi/10) = 2\operatorname{sen}(\pi/2 - 2\pi/5)\operatorname{sen}(\pi/10) = 2\operatorname{sen}^2(\pi/10) \end{aligned}$$

luego $\operatorname{sen}(\pi/10) = 1/2$, y esto es falso.

Veamos por último que el grupo de Galois $G(E : \mathbb{Q})$ no es abeliano. Si lo fuera todos sus subgrupos serían normales, por lo que todas las subextensiones de $E|\mathbb{Q}$ serían de Galois. Pero esto es falso, pues $\mathbb{Q}(\sqrt[4]{5})|\mathbb{Q}$ no es de Galois, ya que $\sqrt[4]{5}i$ es una raíz del polinomio $\mathtt{t}^4 - 5 = P_{\mathbb{Q},\sqrt[4]{5}}(\mathtt{t})$ y, sin embargo, $\sqrt[4]{5}i \notin \mathbb{Q}(\sqrt[4]{5})$. □

Número IV.14 Sean $p \in \mathbb{Z}$ primo y L un cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^4 - p$. Probar que el grupo de Galois $G(L : \mathbb{Q})$ es isomorfo al grupo diedral $\mathcal{D}_4$ de orden 8 y calcular elementos primitivos de todas las subextensiones $E|\mathbb{Q}$ de $L|\mathbb{Q}$.

Solución. Vamos a calcular las raíces de f en $\mathbb{C}$. Denotemos $\rho := \sqrt[4]{p}$ el único número real positivo cuya potencia cuarta es p. Entonces $f(\rho) = 0$, y si η es otra raíz de f en $\mathbb{C}$ se tiene $\rho^4 = p = \eta^4$. En consecuencia, $(\eta/\rho)^4 = 1$, luego existe un entero $k > 0$ tal que $\eta/\rho = i^k$, donde $i := \sqrt{-1}$. Como $i^4 = 1$, se deduce que las raíces de f en $\mathbb{C}$ son $\{\rho, \rho i, -\rho, -\rho i\}$. En consecuencia,

$$L = \mathbb{Q}(\rho, \rho i, -\rho, -\rho i) = \mathbb{Q}(\rho, i).$$

El orden del grupo $G(L : \mathbb{Q})$ es el grado $[L : \mathbb{Q}]$ de la extensión $L|\mathbb{Q}$. Por tanto, si denotamos $F := \mathbb{Q}(\rho)$ se tiene $L = F(i)$, luego

$$\operatorname{ord}(G(L : \mathbb{Q})) = [L : \mathbb{Q}] = [F(i) : \mathbb{Q}] = [F(i) : F] \cdot [F : \mathbb{Q}] = [F(i) : F] \cdot [\mathbb{Q}(\rho) : \mathbb{Q}].$$

Observamos que $[F(i) : F] = \deg(\mathtt{t}^2 + 1) = 2$ ya que $F \subset \mathbb{R}$ e $i \in \mathbb{C} \setminus \mathbb{R}$ es raíz del polinomio $\mathtt{t}^2 + 1$. Por otro lado, f es irreducible en $\mathbb{Z}[\mathtt{t}]$, por el Criterio de Eisenstein, luego también es irreducible en $\mathbb{Q}[\mathtt{t}]$. En consecuencia, $[\mathbb{Q}(\rho) : \mathbb{Q}] = \deg(f) = 4$, por lo que, finalmente, $\operatorname{ord}(G(L : \mathbb{Q})) = 8$.

Se trata ahora de identificar el grupo $G(L : \mathbb{Q})$. Los automorfismos de L quedan determinados por las imágenes de ρ e i. Cada automorfismo transforma estos elementos en raíces de su polinomio mínimo, lo que da un máximo de $4 \cdot 2 = 8$ posibilidades. Como sabemos que $\operatorname{ord}(G(L : \mathbb{Q})) = 8$ todas esas asignaciones inducen automorfismos de L, y entre ellas elegimos

$$\sigma : L \to L,\ \rho \to \rho i;\ i \to i \quad \& \quad \tau : L \to L,\ \rho \to \rho;\ i \to -i.$$

Se comprueba inmediatamente que σ tiene orden 4 mientras que τ tiene orden 2. Además $\sigma\tau\sigma = \tau$, luego por la Proposición II.2.3, vol. I, $\langle\sigma,\tau\rangle = \mathcal{D}_4$ es el grupo diedral de orden 8. Como $\langle\sigma,\tau\rangle$ es un subgrupo de $G(L:\mathbb{Q})$ y ambos grupos tienen orden 8, coinciden, esto es, $G(L:\mathbb{Q}) = \mathcal{D}_4$.

Para la segunda parte observamos que los elementos de $G := G(L:\mathbb{Q})$ son

$$G = \{\mathrm{id}_L, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\},$$

de los que σ y σ^3 son los únicos de orden 4, mientras que los demás tienen orden 2, salvo la identidad. Comenzamos estudiando las subextensiones de $L|\mathbb{Q}$ de grado 4. Los subgrupos de orden 2 de G son

$$H_1 := \langle\sigma^2\rangle, \quad H_2 := \langle\tau\rangle, \quad H_3 := \langle\sigma\tau\rangle, \quad H_4 := \langle\sigma^2\tau\rangle \quad \& \quad H_5 := \langle\sigma^3\tau\rangle.$$

El cuerpo fijo $E_i := \mathrm{Fix}(H_i)$ de H_i cumple que $[E_i:\mathbb{Q}] = 8/\operatorname{ord}(H_i) = 4$, y vamos a calcular un elemento primitivo de cada extensión $E_i|\mathbb{Q}$.

Como $\sigma^2(\rho) = \sigma(\rho i) = \sigma(\rho)i = \rho i^2 = -\rho$ resulta $\sigma^2(\rho^2) = \rho^2$, y también $\sigma^2(i) = i$. Por tanto $\mathbb{Q}(\rho^2, i) \subset E_1$, y de hecho se da la igualdad. Para probarlo basta ver que $[\mathbb{Q}(\rho^2,i):\mathbb{Q}] = 4$. Como $\rho^2 \in \mathbb{R}$ y el polinomio mínimo de ρ^2 sobre $\mathbb{Q}$ es $\mathtt{t}^2 - p$, se tiene:

$$[\mathbb{Q}(\rho^2,i):\mathbb{Q}] = [\mathbb{Q}(\rho^2)(i):\mathbb{Q}(\rho^2)]\cdot[\mathbb{Q}(\rho^2):\mathbb{Q}] = 2\cdot 2 = 4.$$

De la demostración del Teorema del elemento primitivo se desprende que

$$E_1 = \mathbb{Q}(\rho^2, i) = \mathbb{Q}(\rho^2 + i).$$

Por otro lado, $\mathbb{Q}(\rho) \subset E_2$ pues $\tau(\rho) = \rho$, y como $[\mathbb{Q}(\rho):\mathbb{Q}] = \deg(f) = 4 = [E_2:\mathbb{Q}]$ concluimos que $E_2 = \mathbb{Q}(\rho)$. Para encontrar un elemento primitivo de la extensión $E_3|\mathbb{Q}$ observamos que

$$\sigma\tau(\rho) = \tau(\sigma(\rho)) = \tau(\rho i) = \tau(\rho)\tau(i) = -\rho i \quad \& \quad \sigma\tau(i) = \tau(\sigma(i)) = \tau(i) = -i,$$

por lo que $\sigma\tau(\rho i) = (-\rho i)(-i) = -\rho$. En consecuencia, $\sigma\tau(\rho - \rho i) = \rho - \rho i$, es decir, $\mathbb{Q}(\rho - \rho i) \subset E_3$, y para probar la igualdad basta ver que $[\mathbb{Q}(\rho - \rho i):\mathbb{Q}] = 4$. Denotamos $\alpha := \rho - \rho i$, que cumple

$$p = \rho^4 = \alpha^4/(1-i)^4 = -\alpha^4/4.$$

Por tanto, el polinomio mínimo de α sobre $\mathbb{Q}$ es $\mathtt{t}^4 + 4p$, así que $[\mathbb{Q}(\rho - \rho i):\mathbb{Q}] = 4$.

En cuanto a la extensión $E_4|\mathbb{Q}$ observamos que

$$\sigma^2\tau(\rho i) = \tau(\sigma^2(\rho i)) = \tau(\sigma^2(\rho)\sigma^2(i)) = \tau(-\rho i) = \rho i,$$

luego $\rho i \in E_4$. Como, además, $[E_4:\mathbb{Q}] = 4 = \deg(f) = \deg(P_{\mathbb{Q},\rho i}) = 4$, resulta $E_4 = \mathbb{Q}(\rho i)$. Para terminar con las subextensiones de grado 4 calculamos

$$\sigma^3\tau(\rho) = \tau(\sigma^3(\rho)) = \tau(-\rho i) = \rho i \quad \& \quad \sigma^3\tau(i) = \tau(\sigma^3(i)) = \tau(i) = -i,$$

así que $\sigma^3\tau(\rho i) = \rho i \cdot (-i) = \rho$. Por ello, $\sigma^3\tau(\rho + \rho i) = \rho + \rho i$, es decir, $\mathbb{Q}(\rho + \rho i) \subset E_5$, y para probar la igualdad es suficiente demostrar que $[\mathbb{Q}(\rho + \rho i) : \mathbb{Q}] = 4$. Denotamos $\mu := \rho + \rho i$, que cumple

$$p = \rho^4 = \mu^4/(1+i)^4 = -\mu^4/4.$$

Por tanto, el polinomio mínimo de μ sobre $\mathbb{Q}$ es $\mathtt{t}^4 + 4p$, luego $[\mathbb{Q}(\rho + \rho i) : \mathbb{Q}] = 4$ y, en consecuencia, $E_5 = \mathbb{Q}(\rho + \rho i)$.

Por último, estudiamos las subextensiones de grado 2. Los subgrupos de orden 4 de $G(L : \mathbb{Q})$ son

$$M_1 := \langle \sigma \rangle, \quad M_2 := \langle \sigma^2, \tau \rangle \quad \text{y} \quad M_3 := \langle \sigma^2, \sigma\tau \rangle,$$

y denotamos $F_i = \mathrm{Fix}(M_i)$ para $i = 1, 2, 3$. Sabemos que $[F_i : \mathbb{Q}] = 8/\operatorname{ord}(M_i) = 2$, y vamos a calcular un elemento primitivo de cada extensión $F_i|\mathbb{Q}$. Es inmediato que $F_1 = \mathbb{Q}(i)$ porque $\sigma(i) = i$, mientras que $F_2 = \mathbb{Q}(\rho^2)$, pues $\sigma^2(\rho^2) = \rho^2 = \tau(\rho^2)$. Finalmente,

$$\sigma^2(\rho^2 i) = \sigma^2(\rho^2)\sigma^2(i) = \rho^2 i \quad \& \quad \sigma\tau(\rho^2 i) = \tau(\sigma(\rho)^2\sigma(i)) = \tau(-\rho^2 i) = \rho^2 i,$$

luego $F_3 = \mathbb{Q}(\rho^2 i)$. □

Número IV.15 (1) Probar que $h(\mathtt{t}) := \mathtt{t}^4 + 1$ es un polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$.

(2) Sea L un cuerpo de descomposición de h sobre $\mathbb{Q}$. Encontrar un elemento primitivo de la extensión $L|\mathbb{Q}$.

(3) ¿Cuál es el orden del grupo de Galois $G(L : \mathbb{Q})$? Demostrar que es abeliano y calcular sus coeficientes de torsión.

(4) Encontrar elementos primitivos de todas las subextensiones no triviales de $L|\mathbb{Q}$ y determinar cuáles son de Galois.

Solución. (1) Tras la sustitución $\mathtt{t} \mapsto \mathtt{t} + 1$ se obtiene el polinomio

$$h(\mathtt{t}+1) = \mathtt{t}^4 + 4\mathtt{t}^3 + 6\mathtt{t}^2 + 4\mathtt{t} + 2,$$

que es irreducible en $\mathbb{Z}[\mathtt{t}]$, y por tanto en $\mathbb{Q}[\mathtt{t}]$, por el Criterio de Eisenstein. Esto implica que también h es irreducible en $\mathbb{Q}[\mathtt{t}]$.

(2) Sea $u \in \mathbb{C}$ raíz de h. También $-u$ es raíz, ya que $h(-u) = h(u) = 0$. Además $u \neq 0$, luego $u \neq -u$, y se tiene

$$h(1/u) = 1 + 1/u^4 = (u^4+1)/u^4 = h(u)/u^4 = 0,$$

así que $1/u$ es otra raíz de h y, por lo que acabamos de ver, también $-1/u$ lo es.

Se comprueba inmediatamente que, además, los números $u, -u, 1/u$ y $-1/u$ son distintos dos a dos ya que $u^2 \neq \pm 1$, pues $u^4 = -1$. Así,

$$h(\mathtt{t}) = (\mathtt{t} - u)(\mathtt{t} + u)(\mathtt{t} - 1/u)(\mathtt{t} + 1/u),$$

y esto implica que $L := \mathbb{Q}(u)$ es un cuerpo de descomposición de h sobre $\mathbb{Q}$ y u es un elemento primitivo de la extensión $L|\mathbb{Q}$. Para calcular u explícitamente observamos que $(u^2)^2 = -1$, luego podemos suponer que $u^2 = \sqrt{-1} := i$ que es el número complejo de módulo 1 y argumento $\pi/2$, una de cuyas raíces cuadradas u tiene módulo 1 y argumento $\pi/4$, es decir,

$$u := \cos(\pi/4) + i\,\mathrm{sen}(\pi/4)i = \sqrt{2}(1+i)/2.$$

(3) Como la extensión $L|\mathbb{Q}$ es de Galois, se tiene

$$\mathrm{ord}(G(L:\mathbb{Q})) = [L:\mathbb{Q}] = [\mathbb{Q}(u):\mathbb{Q}] = \deg(h) = 4.$$

Esto ya prueba que el grupo $G(L:\mathbb{Q})$ es abeliano, pues todos los grupos de orden 4 lo son. Cada $\mathbb{Q}$-automorfismo de $\mathbb{Q}(u)$ queda determinado por la imagen del elemento primitivo u, luego los elementos del grupo de Galois $G(L:\mathbb{Q})$ son los automorfismos determinados por las siguientes asignaciones:

$$\varphi_1 : u \mapsto u, \quad \varphi_2 : u \mapsto -u, \quad \varphi_3 : u \mapsto 1/u, \quad \varphi_4 : u \mapsto -1/u.$$

En los cuatro casos $\varphi_j^2(u) = u$, luego $G(L:\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, ya que el grupo $G(L:\mathbb{Q})$ no tiene elementos de orden cuatro. Los coeficientes de torsión de este grupo son $(2,2)$.

(4) El grupo $G(L:\mathbb{Q})$ posee tres elementos de orden 2, que son los automorfismos φ_2, φ_3 y φ_4, por lo que sus subgrupos no triviales son $H_j := \langle \varphi_j \rangle$ para $j = 2, 3, 4$.

Por el Teorema fundamental sus cuerpos fijos $K_j := \mathrm{Fix}(H_j) = \mathrm{Fix}(\varphi_j)$ son los cuerpos intermedios entre $\mathbb{Q}$ y L, luego $L|\mathbb{Q}$ tiene tres subextensiones propias, que son $K_j|\mathbb{Q}$, con $j = 2, 3, 4$. Todas ellas son normales porque su grado es 2. Para obtener elementos primitivos de estas subextensiones observamos en primer lugar que

$$\varphi_2(u^2) = (\varphi_2(u))^2 = (-u)^2 = u^2,$$

luego $\mathbb{Q} \subset \mathbb{Q}(u^2) \subset K_2$. Además u^2 es raíz del polinomio $g_2(\mathtt{t}) := \mathtt{t}^2 + 1 \in \mathbb{Q}[\mathtt{t}]$, que es irreducible en $\mathbb{Q}[\mathtt{t}]$, por lo que $[\mathbb{Q}(u^2):\mathbb{Q}] = \deg(g_2) = 2$, y en consecuencia,

$$2 = [K_2:\mathbb{Q}] = [K_2:\mathbb{Q}(u^2)] \cdot [\mathbb{Q}(u^2):\mathbb{Q}] = 2 \cdot [K_2:\mathbb{Q}(u^2)],$$

luego $[K_2:\mathbb{Q}(u^2)] = 1$, es decir, $K_2 = \mathbb{Q}(u^2) = \mathbb{Q}(i)$.

Para encontrar un elemento primitivo de la extensión $K_3|\mathbb{Q}$ observamos que

$$\varphi_3(1/u) = 1/\varphi_3(u) = 1/(1/u) = u,$$

y por tanto $v := u + 1/u$ queda fijo por φ_3, pues

$$\varphi_3(v) = \varphi_3(u) + \varphi_3(1/u) = (1/u) + u = v.$$

Así, $\mathbb{Q} \subset \mathbb{Q}(v) \subset K_3$, y para demostrar que la segunda inclusión es una igualdad es suficiente, por la transitividad del grado, comprobar que $[\mathbb{Q}(v) : \mathbb{Q}] = [K_3 : \mathbb{Q}] = 2$. Ahora bien,

$$v^2 = \frac{(u^2+1)^2}{u^2} = \frac{u^4+1+2u^2}{u^2} = \frac{2u^2}{u^2} = 2,$$

por lo que el polinomio $g_3(\mathtt{t}) := \mathtt{t}^2 - 2 \in \mathbb{Q}[\mathtt{t}]$, que es irreducible en $\mathbb{Z}[\mathtt{t}]$, luego en $\mathbb{Q}[\mathtt{t}]$, por el Criterio de Eisenstein, tiene a v por raíz, así que $[\mathbb{Q}(v) : \mathbb{Q}] = \deg(g_3) = 2$. Así, $K_3 = \mathbb{Q}(v)$. Podemos calcular explícitamente v como sigue. El módulo de u es 1 pues $|u|^4 = |u^4| = |-1| = 1$, así que $u\overline{u} = 1$, luego $v = u + 1/u = u + \overline{u} = \sqrt{2}$, es decir, $K_3 = \mathbb{Q}(\sqrt{2})$.

Por último, los cálculos precedentes muestran que $i, \sqrt{2} \in L$, luego $w := i\sqrt{2} \in L$ y como $w^2 + 2 = 0$, el polinomio mínimo de w sobre $\mathbb{Q}$ es $g_4(\mathtt{t}) := \mathtt{t}^2 + 2$, que tiene grado 2. A fortiori deducimos que $K_4 = \mathrm{Fix}(\varphi_4) = \mathbb{Q}(i\sqrt{2})$. □

Número IV.16 (1) Probar que los polinomios $g(\mathtt{t}) := \mathtt{t}^2 + 4$, $h(\mathtt{t}) := \mathtt{t}^3 + 4$ y $f(\mathtt{t}) := \mathtt{t}^6 + 4$ son irreducibles en $\mathbb{Q}[\mathtt{t}]$.

(2) Demostrar que $L := \mathbb{Q}(\sqrt{3}, i, \sqrt[3]{2})$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$.

(3) Calcular el grado de la extensión $L|\mathbb{Q}$.

(4) ¿Cuál es el orden del grupo de Galois $G(L : \mathbb{Q})$? Probar que es un grupo diedral.

(5) Encontrar generadores de todas las subextensiones no triviales de $L|\mathbb{Q}$ y determinar cuáles son de Galois.

Solución. (1) Para demostrar que $g(\mathtt{t}) := \mathtt{t}^2 + 4$ es irreducible en $\mathbb{Q}[\mathtt{t}]$ es suficiente probar, ya que $\deg(g) = 2$, que g carece de raíces en $\mathbb{Q}$, lo que es obvio pues sus raíces en $\mathbb{C}$ son $\pm\sqrt{2}i \in \mathbb{C} \setminus \mathbb{Q}$. Supongamos ahora que h es reducible en $\mathbb{Q}[\mathtt{t}]$. Entonces, puesto que $\deg(h) = 3$, tendría una raíz racional y, como h es mónico, existiría $z \in \mathbb{Z}$ tal que $z^3 = -4$. Por ello $1 < |z| < 2$, y esto es imposible.

Por último, la irreducibilidad de f se deduce de lo anterior y el Ejercicio II.3.

(2) Sea $L \subset \mathbb{C}$ un cuerpo de descomposición de f sobre $\mathbb{Q}$. Con las notaciones anteriores, $(2i)^2 = -4 = u^6 = (u^3)^2$, luego $2i = \pm u^3 \in L$, así que $i \in L$. También

$$\xi := e^{2\pi i/6} = e^{\pi i/3} = \cos(\pi/3) + i\,\mathrm{sen}(\pi/3) = (1 + \sqrt{3}i)/2$$

pertenece a L, pues para cada exponente entero j el producto $u\xi^j$ es raíz de f, ya que

$$f(u\xi^j) = (u\xi^j)^6 + 4 = u^6(\xi^6)^j + 4 = u^6 + 4 = 0.$$

En particular $u, u\xi \in L$, por lo que $\xi = u\xi/u \in L$, lo que implica que $L = \mathbb{Q}(u, \xi)$. Por otro lado, $\sqrt{3} = (2\xi - 1)/i \in L$, mientras que u es una de las raíces cúbicas de $2i = 2(\cos\pi/2 + i\,\mathrm{sen}\,\pi/2)$, luego podemos suponer que

$$u := \sqrt[3]{2}(\cos\pi/6 + i\,\mathrm{sen}\,\pi/6) = \sqrt[3]{2}(\sqrt{3} + i)/2.$$

Como $\sqrt{3}, i \in L$ concluimos que $\sqrt[3]{2} \in L$. En consecuencia $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$.

(3) Como el polinomio mínimo $P_{\mathbb{Q},\sqrt[3]{2}}(\mathtt{t}) := \mathtt{t}^3 - 2$ de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ tiene grado 3 y la extensión $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$ tiene grado 4, y $\mathrm{mcd}(3, 4) = 1$, deducimos que

$$[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i)(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{3}, i)] \cdot [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 3 \cdot 4 = 12.$$

(4) Como la extensión $L|\mathbb{Q}$ es de Galois el grupo de automorfismos $G(L : \mathbb{Q})$ tiene orden 12, y los $\mathbb{Q}$-automorfismos de L quedan determinados por las imágenes de los generadores $\sqrt[3]{2}, \sqrt{3}$ e i de la extensión $L|\mathbb{Q}$. Las imágenes de $\rho := \sqrt[3]{2}$ son las raíces de su polinomio mínimo $P_{\mathbb{Q},\rho}(\mathtt{t}) = \mathtt{t}^3 - 2$ sobre $\mathbb{Q}$, que son ρ, $\rho\zeta$ y $\rho\zeta^2$, donde

$$\zeta := e^{2\pi i/3} = \cos(2\pi/3) + i\,\mathrm{sen}(2\pi/3) = (-1 + \sqrt{3}i)/2.$$

Las imágenes de $\sqrt{3}$ e i son las raíces de sus polinomios mínimos $P_{\mathbb{Q},\sqrt{3}}(\mathtt{t}) := \mathtt{t}^2 - 3$ y $P_{\mathbb{Q},i}(\mathtt{t}) := \mathtt{t}^2 + 1$ sobre $\mathbb{Q}$, es decir, $\pm\sqrt{3}$ y $\pm i$, respectivamente. En conclusión,

$$G(L : \mathbb{Q}) = \{\varphi_{jk\ell} :\ 0 \le j \le 2,\ 0 \le k, \ell \le 1\},$$

donde $\varphi_{jk\ell}$ es el $\mathbb{Q}$-automorfismo de L inducido por la asignación

$$\rho \mapsto \rho\zeta^j, \quad \sqrt{3} \mapsto (-1)^k\sqrt{3} \quad \& \quad i \mapsto (-1)^\ell i.$$

Conviene observar que $\zeta^{-1} = -(\sqrt{3}i + 1)/2$, luego

$$\varphi_{jk\ell}(\zeta) = \frac{-1 + (-1)^{k+\ell}\sqrt{3}i}{2} = \begin{cases} \zeta & \text{si } k + \ell \text{ es par} \\ 1/\zeta & \text{si } k + \ell \text{ es impar.} \end{cases}$$

Para demostrar que $G(L : \mathbb{Q})$ es isomorfo al grupo diedral $\mathcal{D}_6$ es suficiente probar que $\sigma := \varphi_{1,1,1}$ tiene orden 6, $\tau := \varphi_{0,0,1}$ tiene orden 2 y $\sigma \cdot \tau \cdot \sigma = \tau$. Esto prueba que el subgrupo $\langle \sigma, \tau \rangle$ de $G(L : \mathbb{Q})$ es isomorfo a $\mathcal{D}_6$ y como $\mathrm{ord}(G(L : \mathbb{Q})) = 12$ se concluye que $G(L : \mathbb{Q}) = \langle \sigma, \tau \rangle \cong \mathcal{D}_6$. Nótese que $\sigma(\zeta) = \zeta$, luego

$$\sigma^2(\rho) = \rho\zeta^2, \ \ \sigma^2(\sqrt{3}) = \sqrt{3} \ \text{ y } \ \sigma^2(i) = i$$

por lo que $o(\sigma) \neq 2$, mientras que por ser $\zeta^3 = 1$, $\sigma^3(\rho) = \rho$, $\sigma^3(\sqrt{3}) = -\sqrt{3}$ y $\sigma^3(i) = -i$, lo que demuestra que $o(\sigma) \neq 3$. De hecho estas igualdades muestran que $o(\sigma) = 6$. Por otro lado, las igualdades $\tau(\rho) = \rho$, $\tau(\sqrt{3}) = \sqrt{3}$ y $\tau(i) = -i$ prueban que $o(\tau) = 2$. Además $\tau(\zeta) = 1/\zeta$, y en consecuencia,

$$\begin{aligned} (\sigma \cdot \tau \cdot \sigma)(\rho) &= (\tau \cdot \sigma)(\rho\zeta) = \sigma(\rho/\zeta) = \rho = \tau(\rho), \\ (\sigma \cdot \tau \cdot \sigma)(\sqrt{3}) &= (\tau \cdot \sigma)(-\sqrt{3}) = \sigma(-\sqrt{3}) = \sqrt{3} = \tau(\sqrt{3}), \\ (\sigma \cdot \tau \cdot \sigma)(i) &= (\tau \cdot \sigma)(-i) = \sigma(i) = -i = \tau(i), \end{aligned}$$

lo que demuestra la igualdad buscada $\sigma \cdot \tau \cdot \sigma = \tau$.

(5) Por el apartado anterior el grupo de Galois de la extensión $L|\mathbb{Q}$ es

$$G(L : \mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \tau\sigma^4, \tau\sigma^5\},$$

y los órdenes de cada uno de sus elementos son:

$$o(\mathrm{id}) = 1,\ o(\sigma) = o(\sigma^5) = 6,\ o(\sigma)^2 = o(\sigma^4) = 3 \quad \& \quad o(\sigma^3) = o(\tau\sigma^j) = 2,$$

donde $0 \leq j \leq 5$. En particular $G(L:\mathbb{Q})$ posee, exactamente, tres subgrupos de orden 6, que son

$$H_1 := \langle\sigma\rangle \cong \mathbb{Z}_6, \quad H_2 := \langle\sigma^2, \tau\rangle \cong \mathcal{D}_3 \quad \& \quad H_3 := \langle\sigma^2, \tau\sigma\rangle \cong \mathcal{D}_3.$$

Existen por tanto, exactamente, tres subextensiones de $L|\mathbb{Q}$ de grado 2 que denotamos $K_1|\mathbb{Q}$, $K_2|\mathbb{Q}$ y $K_3|\mathbb{Q}$. Como en el apartado (3) vimos que $\sqrt{3},\ i \in L$, deducimos que $K_1 := \mathbb{Q}(i)$, $K_2 := \mathbb{Q}(\sqrt{3})$ y $K_3 := \mathbb{Q}(\sqrt{3}i)$. Las tres extensiones $K_i|\mathbb{Q}$ con $i = 1, 2, 3$ son de Galois pues tienen grado 2.

Buscamos a continuación las subextensiones de grado 3, que se corresponden con los subgrupos de $G(L:\mathbb{Q})$ de orden 4. Como ninguno de sus elementos tiene orden 4 todos los subgrupos de orden 4 de $G(L:\mathbb{Q})$ son isomorfos a $\mathbb{Z}_2 \times \mathbb{Z}_2$, y están formados por la identidad y 3 elementos de orden 2. Como σ^3 conmuta con todos los elementos del grupo $G(L:\mathbb{Q})$, se tienen los siguientes subgrupos de orden 4:

$$H_3 := \{\mathrm{id}, \sigma^3, \tau, \tau\sigma^3\}, \quad H_4 := \{\mathrm{id}, \sigma^3, \tau\sigma, \tau\sigma^4\} \quad \& \quad H_5 := \{\mathrm{id}, \sigma^3, \tau\sigma^2, \tau\sigma^5\}.$$

Y de hecho estos son todos. En efecto, si $\tau\sigma^j$ y $\tau\sigma^k$ con $0 \leq j < k \leq 5$ son elementos de orden 2 que pertenecen a un subgrupo de $G(L:\mathbb{Q})$ de orden 4 han de conmutar, esto es, $(\tau\sigma^j)\cdot(\tau\sigma^k) = (\tau\sigma^k)\cdot(\tau\sigma^j)$, de donde se deduce que $\sigma^{k-j} = \sigma^{j-k}$, o sea, $\sigma^{2(k-j)} = \mathrm{id}$, o equivalentemente $k - j = 3$, es decir, $\tau\sigma^k = \tau\sigma^{j+3}$, como queríamos probar. Existen por tanto, exactamente, tres subextensiones de grado 3 de $L|\mathbb{Q}$. Dichas extensiones son $K_3|\mathbb{Q}$, $K_4|\mathbb{Q}$ y $K_5|\mathbb{Q}$, donde

$$K_3 := \mathbb{Q}(\rho), \quad K_4 := \mathbb{Q}(\rho\zeta) \quad \& \quad K_5 := \mathbb{Q}(\rho\zeta^2).$$

Estos tres cuerpos son distintos dos a dos, pues en caso contrario $\mathbb{Q}(\rho)$ contendría a ζ, y esto es imposible ya que $\zeta \in \mathbb{C} \setminus \mathbb{R}$ y $\mathbb{Q}(\rho) \subset \mathbb{R}$.

Ninguna de las subextensiones $K_j|\mathbb{Q}$ con $j = 3, 4, 5$ es de Galois, pues los subgrupos H_3, H_4 y H_5 no son normales, ya que son 2-subgrupos de Sylow de $\mathcal{D}_6$ distintos.

El grupo $G(L:\mathbb{Q})$ posee un único subgrupo H_6 de orden 3 ya que tiene, exactamente, dos elementos de orden 3. Como H_6 es un 3-subgrupo de Sylow de $G(L:\mathbb{Q})$ se deduce que H_6 es subgrupo normal de $G(L:\mathbb{Q})$. En consecuencia, $L|\mathbb{Q}$ posee una única subextensión $K_6|\mathbb{Q}$ de grado 4, que además es de Galois. Vimos en el apartado (3) que $\sqrt{3}, i \in L$ por lo que el cuerpo $K_6 := \mathbb{Q}(\sqrt{3}, i)$ cumple que $K_6|\mathbb{Q}$ es la única subextensión de grado 4 de $L|\mathbb{Q}$.

Buscamos, finalmente, las subextensiones de grado 6 de $L|\mathbb{Q}$, que son los cuerpos fijos de los elementos de orden 2 del grupo $G(L:\mathbb{Q})$. Hay, por tanto, exactamente siete, y el único de ellos que es normal es $H_7 := \langle\sigma^3\rangle$, porque $\langle\sigma^3\rangle$ es el centro del grupo diedral $\mathcal{D}_6$, o lo que es igual, σ^3 es el único elemento de orden 2 de $G(L:\mathbb{Q})$ que genera un subgrupo normal. Ya hemos calculado previamente que $\sigma^3(\rho) = \rho$, mientras

que de las igualdades $\sigma^3(\sqrt{3}) = -\sqrt{3}$ y $\sigma^3(i) = -i$ se deduce que $\sigma^3(\sqrt{3}i) = \sqrt{3}i$. Por tanto, $K_7 := \mathrm{Fix}(\sigma^3) = \mathbb{Q}(\rho, \sqrt{3}i)$, y la extensión $K_7|_{\mathbb{Q}}$ es la única subextensión de Galois de grado 6 de $L|\mathbb{Q}$.

Para proseguir la búsqueda de subextensiones de grado 6 observamos que dados elementos $a, b \in \mathbb{C}$ algebraicos sobre $\mathbb{Q}$ tales que $[\mathbb{Q}(a) : \mathbb{Q}] = 3$ y $[\mathbb{Q}(b) : \mathbb{Q}] = 2$ se deduce del Ejemplo I.2.4 que la extensión $\mathbb{Q}(a, b)|\mathbb{Q}$ tiene grado 6. En particular, como $\rho, \rho\zeta$ y $\rho\zeta^2$ tienen a $\mathtt{t}^3 - 2$ por polinomio mínimo sobre $\mathbb{Q}$, mientras que i y $\sqrt{3}$ son elementos de grado 2 sobre $\mathbb{Q}$, obtenemos las siguientes seis subextensiones de $L|\mathbb{Q}$ de grado 6:

$$K_8 := \mathbb{Q}(\rho, i), \quad K_9 := \mathbb{Q}(\rho, \sqrt{3}), \quad K_{10} := \mathbb{Q}(\rho\zeta, i)$$
$$K_{11} := \mathbb{Q}(\rho\zeta, \sqrt{3}), \quad K_{12} := \mathbb{Q}(\rho\zeta^2, i) \quad \& \quad K_{13} := \mathbb{Q}(\rho\zeta^2, \sqrt{3}).$$

□

Número IV.17 Sean K un cuerpo de característica 0 tal que todo polinomio de $K[\mathtt{t}]$ de grado impar tiene alguna raíz en K, y $L|K$ una extensión de Galois. Demostrar que el orden del grupo de Galois $G(L : K)$ es potencia de 2.

Solución. Escribimos $\mathrm{ord}(G(L : K)) = 2^m n$ donde $m \geq 0$ y $n \geq 1$ son enteros y n es impar, y se trata de probar que $n = 1$. Por el Teorema de Sylow existe un subgrupo H de $G(L : K)$ de orden 2^m, y consideramos su cuerpo fijo $F := \mathrm{Fix}(H)$. Se cumple que $[L : F] = [L : \mathrm{Fix}(H)] = \mathrm{ord}(H) = 2^m$ y, como la extensión $L|K$ es de Galois, se tiene

$$[F : K] = \frac{[L : K]}{[L : F]} = \frac{\mathrm{ord}(G(L : K))}{2^m} = n.$$

Por el Teorema del elemento primitivo existe $u \in F$ tal que $F := K(u)$, y el grado del polinomio mínimo $P_{K,u}$ de u sobre K es $[K(u) : K] = n$, que es impar. Por hipótesis, $P_{K,u} \in K[\mathtt{t}]$ tiene una raíz en K y esto implica, por ser $P_{K,u}$ irreducible en $K[\mathtt{t}]$, que su grado es $n = 1$, como queríamos demostrar. □

Número IV.18 Sean $\overline{K}$ un cierre algebraico de un cuerpo K de característica 0 y un automorfismo $\sigma \in G(\overline{K} : K)$. Probar que el conjunto

$$E := \{x \in \overline{K} : \sigma(x) = x\}$$

es un subcuerpo de $\overline{K}$ que contiene a K y que toda extensión finita $L|E$ es de Galois y cíclica, esto es, su grupo de Galois $G(L : E)$ es un grupo cíclico.

Solución. La inclusión $K \subset E$ es obvia, pues por hipótesis σ fija cada elemento de K. Además E es subcuerpo de $\overline{K}$, pues si $x, y \in E$ se tiene

$$\sigma(x - y) = \sigma(x) - \sigma(y) = x - y \quad \& \quad \sigma(xy) = \sigma(x)\sigma(y) = xy,$$

por lo que $x-y, xy \in E$, y si $x \in E \setminus \{0\}$ se tiene

$$x\sigma(x^{-1}) = \sigma(x)\sigma(x^{-1}) = \sigma(xx^{-1}) = \sigma(1) = 1 \quad \Longrightarrow \quad \sigma(x^{-1}) = x^{-1},$$

o sea, $\sigma(x^{-1}) = x^{-1}$, es decir, $x^{-1} \in E$, así que E es un subcuerpo de $\overline{K}$.

Para la segunda parte, sea $L|E$ una extensión finita y denotemos $F|E$ la clausura de Galois de $L|E$. Vamos a demostrar que el grupo $G(F:E)$ es cíclico. Por el teorema del elemento primitivo existe $\alpha \in F$ tal que $F := E(\alpha)$, y denotamos

$$f(\mathtt{t}) := \mathtt{t}^n + a_1\mathtt{t}^{n-1} + \cdots + a_n = P_{E,\alpha}(\mathtt{t}) \in E[\mathtt{t}]$$

el polinomio mínimo de α sobre E. Como cada $\sigma(a_i) = a_i$, resulta

$$\begin{aligned} 0 = \sigma(0) = \sigma(f(\alpha)) = \sigma\Big(\alpha^n + \sum_{i=1}^{n} a_i\alpha^{n-1}\Big) &= \sigma(\alpha)^n + \sum_{i=1}^{n} \sigma(a_i)\sigma(\alpha)^{n-i} \\ &= \sigma(\alpha)^n + \sum_{i=1}^{n} a_i\sigma(\alpha)^{n-i} = f(\sigma(\alpha)), \end{aligned}$$

luego $\beta := \sigma(\alpha)$ es una raíz de f. Como la extensión $F|E$ es de Galois y el polinomio $f \in E[\mathtt{t}]$ posee una raíz $\alpha \in F$, también $\beta \in F$. En consecuencia, la restricción

$$\tau := \sigma|_F : F = E(\alpha) \to F = E(\beta)$$

es un E-automorfismo de F, y vamos a demostrar que el grupo $G(F:E)$ es el grupo cíclico $H = \langle\tau\rangle$ generado por τ. Observamos que $E = \mathrm{Fix}(H)$ porque

$$E \subset \mathrm{Fix}(H) = \{x \in F : \tau(x) = x\} = \{x \in F : \sigma(x) = x\} \subset \{x \in \overline{K} : \sigma(x) = x\} = E.$$

Así, como la extensión $F|E$ es de Galois, resulta que $\mathrm{Fix}(H) = E = \mathrm{Fix}(G(F:E))$, y por el Teorema fundamental, $G(F:E) = H = \langle\tau\rangle$ es un grupo cíclico.

Para acabar observamos que, por ser $G(F:E)$ un grupo cíclico, sus subgrupos son normales. Así, por el Teorema fundamental, todas las subextensiones de $F|E$ son de Galois, luego $L|E$ lo es. Por tanto $L = F$ y $G(L:E) = G(F:E) = \langle\tau\rangle$ es un grupo cíclico. □

Número IV.19 Sean E_1 y E_2 dos subcuerpos de $\mathbb{C}$ tales que las extensiones $E_1|\mathbb{Q}$ y $E_2|\mathbb{Q}$ son de Galois y $G(E_1:\mathbb{Q}) \cong \mathbb{Z}_6 \cong G(E_2:\mathbb{Q})$. Supongamos además que $[E_1 \cap E_2 : \mathbb{Q}] = 2$.

(1) Sea F el menor subcuerpo de $\mathbb{C}$ que contiene a E_1 y E_2. ¿Es de Galois la extensión $F|\mathbb{Q}$? ¿Cuál es su grado?

(2) Demostrar que el grupo de Galois $G(F:\mathbb{Q})$ es abeliano. Calcular sus coeficientes de torsión. ¿Cuántas subextensiones propias y no triviales tiene $F|\mathbb{Q}$?

Solución. (1) Se demuestra en el Corolario IV.2.5 que la extensión $F|\mathbb{Q}$ es de Galois, y que si denotamos $L := E_1 \cap E_2$,

$$\begin{aligned}[F:\mathbb{Q}]\cdot[L:\mathbb{Q}] &= [E_1:\mathbb{Q}]\cdot[E_2:\mathbb{Q}] = \operatorname{ord}(G(E_1:\mathbb{Q}))\cdot\operatorname{ord}(G(E_2:\mathbb{Q}))\\ &= \operatorname{ord}(\mathbb{Z}_6)\cdot\operatorname{ord}(\mathbb{Z}_6) = 36.\end{aligned}$$

Como $[L:\mathbb{Q}] = 2$ se deduce de lo anterior que $[F:\mathbb{Q}] = 18$.

(2) Como la extensión $F|K$ es de Galois y el homomorfismo

$$G(F:\mathbb{Q}) \to G(E_1:\mathbb{Q}) \times G(E_2:\mathbb{Q}) \cong \mathbb{Z}_6 \times \mathbb{Z}_6,\ \sigma \mapsto (\sigma|_{E_1}, \sigma|_{E_2})$$

es inyectivo, $G(F:\mathbb{Q})$ es un grupo de orden $[F:\mathbb{Q}] = 18$ isomorfo a un subgrupo de $\mathbb{Z}_6 \times \mathbb{Z}_6$, luego se deduce del teorema de estructura de los grupos abelianos finitos, VI.1.5, vol. I, que $G(F:\mathbb{Q})$ es isomorfo al producto $\mathbb{Z}_6 \times \mathbb{Z}_3$. En particular los coeficientes de torsión de $G(F:\mathbb{Q})$ son 6 y 3.

El número de subextensiones propias y no triviales de la extensión $F|\mathbb{Q}$ coincide con el número de subgrupos propios y no triviales del grupo $G(F:\mathbb{Q}) \cong \mathbb{Z}_6 \times \mathbb{Z}_3$. El único elemento de orden 2 de $\mathbb{Z}_6 \times \mathbb{Z}_3$ es $\zeta_1 := (3+6\mathbb{Z}, 0+3\mathbb{Z})$, así que $H_1 := \langle\zeta_1\rangle$ es el único subgrupo de orden 2 de $\mathbb{Z}_6 \times \mathbb{Z}_3$. Los elementos de orden 3 de $\mathbb{Z}_6 \times \mathbb{Z}_3$ son

$$\begin{aligned}&\zeta_2 := (0+6\mathbb{Z}, 1+3\mathbb{Z}), \quad \zeta_3 := (0+6\mathbb{Z}, 2+3\mathbb{Z}), \quad \zeta_4 := (2+6\mathbb{Z}, 1+3\mathbb{Z}),\\ &\zeta_5 := (4+6\mathbb{Z}, 2+3\mathbb{Z}), \quad \zeta_6 := (2+6\mathbb{Z}, 2+3\mathbb{Z}), \quad \zeta_7 := (4+6\mathbb{Z}, 1+3\mathbb{Z}),\\ &\zeta_8 := (2+6\mathbb{Z}, 0+3\mathbb{Z}) \quad \& \quad \zeta_9 := (4+6\mathbb{Z}, 0+3\mathbb{Z}),\end{aligned}$$

lo que proporciona cuatro subgrupos de orden 3, que son

$$H_2 := \langle\zeta_2\rangle, \quad H_3 := \langle\zeta_4\rangle, \quad H_4 := \langle\zeta_6\rangle \quad \& \quad H_5 := \langle\zeta_8\rangle.$$

Los subgrupos de orden 6 de $\mathbb{Z}_6 \times \mathbb{Z}_3$ son abelianos, luego isomorfos a $\mathbb{Z}_6$. Los elementos de orden 6 de $\mathbb{Z}_6 \times \mathbb{Z}_3$ son

$$\begin{aligned}&\zeta_{10} := (1+6\mathbb{Z}, 0+3\mathbb{Z}), \quad \zeta_{11} := (5+6\mathbb{Z}, 0+3\mathbb{Z}), \quad \zeta_{12} := (1+6\mathbb{Z}, 1+3\mathbb{Z}),\\ &\zeta_{13} := (5+6\mathbb{Z}, 2+3\mathbb{Z}), \quad \zeta_{14} := (1+6\mathbb{Z}, 2+3\mathbb{Z}), \quad \zeta_{15} := (5+6\mathbb{Z}, 1+3\mathbb{Z})\\ &\zeta_{16} := (3+6\mathbb{Z}, 1+3\mathbb{Z}) \quad \& \quad \zeta_{17} := (3+6\mathbb{Z}, 2+3\mathbb{Z}),\end{aligned}$$

luego $\mathbb{Z}_6 \times \mathbb{Z}_3$ tiene cuatro subgrupos de orden 6, a saber, $H_6 := \langle\zeta_9\rangle$, $H_7 := \langle\zeta_{12}\rangle$, $H_8 := \langle\zeta_{14}\rangle$ y $H_9 := \langle\zeta_{16}\rangle$. Por último, se deduce del tercer teorema de Sylow que todo grupo de orden 18 tiene un único subgrupo de orden 9, que en nuestro caso es $H_{10} := \langle 2+6\mathbb{Z}\rangle \times \mathbb{Z}_3$.

Concluimos que $G(F:\mathbb{Q})$ posee, exactamente, 10 subgrupos propios no triviales, lo que por el Teorema fundamental de la teoría de Galois implica que $F|\mathbb{Q}$ posee, exactamente, 10 subextensiones propias no triviales. □

Soluciones a los ejercicios del Capítulo V

Número V.1 Sean $\omega := e^{2\pi i/3}$ y $A := \{a + b\omega : a, b \in \mathbb{Z}\}$.

(1) Comprobar que el polinomio mínimo $f := P_{\mathbb{Q},\omega}$ de ω sobre $\mathbb{Q}$ tiene coeficientes enteros y demostrar que A es un subanillo de $\mathbb{C}$ cerrado respecto de la conjugación de números complejos.

(2) Demostrar que la función

$$\|\cdot\| : A \to \mathbb{N},\ a + b\omega \mapsto a^2 + b^2 - ab$$

es una norma que dota al anillo A de estructura de dominio euclídeo. ¿Cuáles son las unidades de A?

(3) Sea $p \in \mathbb{Z}$ un número primo y denotemos $\widehat{f}$ la imagen de f por el epimorfismo canónico $\mathbb{Z}[\mathtt{t}] \to \mathbb{Z}_p[\mathtt{t}]$ que transforma $\mathtt{t}$ en $\mathtt{t}$ y cada $k \in \mathbb{Z}$ en su clase $\widehat{k} = k \bmod p$. Sea $\mathfrak{a}$ el ideal de $\mathbb{Z}_p[\mathtt{t}]$ generado por $\widehat{f}$. Demostrar que la aplicación

$$\varphi : A \to \mathbb{Z}_p[\mathtt{t}]/\mathfrak{a},\ a + b\omega \mapsto (\widehat{a} + \widehat{b}\mathtt{t}) + \mathfrak{a}$$

es un epimorfismo de anillos. Calcular un generador del núcleo de φ.

(4) Probar que un número primo $p \in \mathbb{Z}$ es irreducible en A si y sólo si $p \equiv 2 \bmod 6$ o $p \equiv 5 \bmod 6$.

(5) ¿Cuántos elementos tiene el cuerpo $K := A/2A$?

Solución. (1) Observamos que $\omega^3 = e^{2\pi i} = 1$, luego

$$0 = \omega^3 - 1 = (\omega - 1)(1 + \omega + \omega^2)$$

y, como $\omega \neq 1$, se deduce que $f(\omega) = 0$, donde $f(\mathtt{t}) := 1 + \mathtt{t} + \mathtt{t}^2 \in \mathbb{Z}[\mathtt{t}]$ es irreducible, pues es el polinomio ciclotómico Φ_3. Por ello $f = P_{\mathbb{Q},\omega}$, y su raíz distinta de ω es su conjugado $\overline{\omega} = 1/\omega \neq \omega$. En particular,

$$\omega^2 = -(1 + \omega), \quad \omega + \overline{\omega} = -1 \quad \& \quad \omega\overline{\omega} = 1.$$

Al sumar y multiplicar dos elementos $x := a + b\omega$ e $y := c + d\omega$ de A resulta

$$x + y = (a + c) + (b + d)\omega \in A$$
$$xy = ac + (ad + bc)\omega + bd\omega^2 = (ac - bd) + (ad + bc - bd)\omega \in A,$$

lo que prueba que A es un subanillo de $\mathbb{C}$. Además, para cada $x = a + b\omega \in A$, también su conjugado $\overline{x} = a + b\overline{\omega} = (a - b) - b\omega \in A$.

(2) En cuanto a la función $\|\cdot\|$, observamos que dado $x := a + b\omega \in A$ resulta

$$x\overline{x} = (a + b\omega)(a + b\overline{\omega}) = a^2 + ab(\omega + \overline{\omega}) + b^2\omega\overline{\omega} = a^2 + b^2 - ab = \|x\|,$$

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

$$\|xy\| = (xy)\cdot\overline{(xy)} = (x\overline{x})\cdot(y\overline{y}) = \|x\|\cdot\|y\|.$$

Para probar que $\|\cdot\|$ dota al anillo A de estructura de dominio euclídeo sólo falta ver que existe división. Sean $x := a + b\omega,\ y := c + d\omega \in A$ tales que $y \neq 0$. Dividiendo como números complejos,

$$x/y = x\overline{y}/y\overline{y} = (u + v\omega)/r,$$

donde $u, v, r \in \mathbb{Z}$ y $r = \|y\| > 0$. Tanto $q_1 = u/r$ como $q_2 = v/r$ son números reales, luego existen $\alpha, \beta \in \mathbb{Z}$ tales que $|q_1 - \alpha| \leq 1/2$ y $|q_2 - \beta| \leq 1/2$. Denotando $r_1 := q_1 - \alpha$ y $r_2 := q_2 - \beta$ resulta

$$x = (q_1 + q_2\omega)y \quad \& \quad q_1 + q_2\omega = \alpha + \beta\omega + (r_1 + r_2\omega)$$

con $|r_1| \leq 1/2$ y $|r_2| \leq 1/2$. En consecuencia,

$$x = (\alpha + \beta\omega)y + (r_1 + r_2\omega)y,$$

y todo se reduce a comprobar que la norma de

$$s + t\omega = (r_1 + r_2\omega)y = x - (\alpha + \beta\omega)y \in A$$

es menor que la de y. Ahora bien,

$$\begin{aligned}\|s + t\omega\| &= (s + t\omega)\overline{(s + t\omega)} = (r_1 + r_2\omega)y\overline{(r_1 + r_2\omega)y} \\ &= y\overline{y}\cdot(r_1 + r_2\omega)\cdot\overline{(r_1 + r_2\omega)} = \|y\|\cdot(r_1^2 + r_2^2 - r_1r_2) \leq 3\|y\|/4 < \|y\|.\end{aligned}$$

Por la Proposición IV.1.11, vol. II, las unidades de A son sus elementos de norma 1. En consecuencia, $u := a + b\omega \in A$ es unidad si y sólo si

$$1 = \|u\| = a^2 - ab + b^2 = (a - b/2)^2 + 3b^2/4,$$

esto es, $(2a - b)^2 + 3b^2 = 4$, y por tanto, $b^2 = 0, 1$. Si $b^2 = 0$, entonces $b = 0$ y $a^2 = 1$, es decir, $u = \pm 1$. Por su parte, si $b^2 = 1$, entonces $(2a - b)^2 = 1$, luego $2a = b \pm 1$. Si $b = 1$, entonces $a = 0, 1$, mientras que si $b = -1$, entonces $a = 0, -1$. Por tanto, las unidades de A son los números $\{\pm 1,\ \pm\omega,\ \pm(1 + \omega)\}$.

(3) Comprobemos que φ preserva sumas. Dados $x := a + b\omega,\ y := c + d\omega \in A$ su suma es $z := (a + c) + (b + d)\omega \in A$, y se tiene

$$\begin{aligned}\varphi(x + y) = \varphi(z) &= \big(\widehat{(a + c)} + \widehat{(b + d)}\mathtt{t}\big) + \mathfrak{a} \\ &= ((\widehat{a} + \widehat{b}\mathtt{t}) + \mathfrak{a}) + ((\widehat{c} + \widehat{d}\mathtt{t}) + \mathfrak{a}) = \varphi(x) + \varphi(y).\end{aligned}$$

En cuanto al producto, ya vimos que $xy = (ac - bd) + (ad + bc - bd)\omega$, luego

$$\varphi(xy) = \big(\widehat{(ac - bd)} + \widehat{(ad + bc - bd)}\mathtt{t}\big) + \mathfrak{a}.$$

Por otro lado, como $1+\mathtt{t}+\mathtt{t}^2 \in \mathfrak{a}$ resulta que $\mathtt{t}^2+\mathfrak{a} = -(1+\mathtt{t})+\mathfrak{a}$, por lo que

$$\begin{aligned}\varphi(x)\cdot\varphi(y) &= ((\widehat{a}+\widehat{b}\mathtt{t})+\mathfrak{a})\cdot((\widehat{c}+\widehat{d}\mathtt{t})+\mathfrak{a}) = (\widehat{a}+\widehat{b}\mathtt{t})(\widehat{c}+\widehat{d}\mathtt{t})+\mathfrak{a}\\ &= (\widehat{ac}+(\widehat{ad+bc})\mathtt{t}+\widehat{bd}\mathtt{t}^2)+\mathfrak{a} = (\widehat{ac}+(\widehat{ad+bc})\mathtt{t}+\mathfrak{a})-(\widehat{bd}(1+\mathtt{t})+\mathfrak{a})\\ &= ((\widehat{ac-bd})+(\widehat{ad+bc-bd})\mathtt{t})+\mathfrak{a},\end{aligned}$$

lo que demuestra que $\varphi(xy) = \varphi(x)\cdot\varphi(y)$.

Para la sobreyectividad, dado $g \in \mathbb{Z}_p[\mathtt{t}]$ existen $q, r \in \mathbb{Z}_p[\mathtt{t}]$ tales que $g := q\widehat{f}+r$ y $\deg(r) < \deg(\widehat{f}) = 2$, es decir, $q = u+v\mathtt{t}$ con $u, v \in \mathbb{Z}_p$. Sean $a, b \in \mathbb{Z}$ tales que $\widehat{a} = u$, $\widehat{b} = v$ y consideremos $z := a+b\omega \in A$. Como $\widehat{f} \in \mathfrak{a}$ se tiene

$$\varphi(z) = (\widehat{a}+\widehat{b}\mathtt{t})+\mathfrak{a} = (u+v\mathtt{t})+\mathfrak{a} = r+\mathfrak{a} = g+\mathfrak{a},$$

y esto demuestra que la aplicación φ es sobreyectiva.

Para terminar este apartado calculamos $\ker\varphi$. Nótese que $x := a+b\omega \in \ker\varphi$ si y sólo si $\widehat{a}+\widehat{b}\mathtt{t} \in \mathfrak{a} = (\widehat{f})$. Como $\deg(\widehat{f}) = 2$ esta condición equivale a que $\widehat{a}+\widehat{b}\mathtt{t}$ sea el polinomio nulo, o lo que es lo mismo, $a, b \in p\mathbb{Z}$. Esto significa que existen $s, t \in \mathbb{Z}$ tales que $a = ps$ y $b = pt$, o lo que es igual, $x = p(s+t\omega) \in pA$. Por tanto, $\ker\varphi = pA$ es el ideal generado por p.

(4) Por el Primer Teorema de isomorfía, $A/pA \cong \mathbb{Z}_p[\mathtt{t}]/\mathfrak{a}$. Como A y $\mathbb{Z}_p[\mathtt{t}]$ son dominios DFU y $\mathfrak{a} = (\widehat{f})$ está generado por un polinomio de grado 2,

$$\begin{aligned}&p \text{ es irreducible en } A \iff A/pA \text{ es dominio} \iff \mathbb{Z}_p[\mathtt{t}]/\mathfrak{a} \text{ es dominio}\\ &\iff \widehat{f} \text{ es irreducible en } \mathbb{Z}_p[\mathtt{t}] \iff \widehat{f} \text{ carece de raíces en } \mathbb{Z}_p.\end{aligned}$$

Supongamos que $p \not\equiv 2, 5 \bmod 6$. Hemos de probar que en este caso $\widehat{f}$ tiene alguna raíz en $\mathbb{Z}_p$. Puesto que p es primo, o bien $p = 3$ o bien $p \equiv 1 \bmod 6$. En el primer caso $\widehat{f}(\widehat{1}) = 1+1+1 = 0 \in \mathbb{Z}_3$, luego $\widehat{f}$ tiene una raíz en $\mathbb{Z}_p$. En el segundo, $3|(p-1)$. Pero $p-1$ es el orden del grupo multiplicativo $\mathbb{Z}_p^*$ de los elementos no nulos de $\mathbb{Z}_p$ y, por el Teorema de Cauchy, IV.2.1, vol. I, el grupo $\mathbb{Z}_p^*$ contiene un elemento u de orden 3, esto es, $u^3 = 1$ y $u \neq 1$. Por tanto,

$$0 = u^3-1 = (u-1)(1+u+u^2) = (u-1)\widehat{f}(u),$$

luego $\widehat{f}(u) = 0$ y así también en este caso $\widehat{f}$ tiene una raíz en $\mathbb{Z}_p$.

Para demostrar el recíproco hemos de probar que si $\widehat{f}$ tiene alguna raíz $u \in \mathbb{Z}_p$, entonces, $p = 3$ o $p \equiv 1 \bmod 6$. Observamos que

$$u^3-1 = (u-1)(1+u+u^2) = (u-1)\widehat{f}(u) = 0,$$

por lo que $u^3 = 1$. Si $u = 1$, entonces $0 = \widehat{f}(u) = \widehat{3}$, o sea, $p = 3$. Por otro lado, si $u \neq 1$ entonces el orden de u en grupo multiplicativo $\mathbb{Z}_p^*$ es 3, así que el orden $p-1$

de $\mathbb{Z}_p^*$ es múltiplo de 3. En particular $p \neq 2$, luego $p-1$ es par, y por tanto $p-1$ es múltiplo de 6, o lo que es lo mismo, $p \equiv 1 \bmod 6$, como queríamos probar.

(5) Cada elemento $x \in A$ se escribe, dividiendo entre 2 en el dominio euclídeo A, como $x = 2q + r$, donde $q, r \in A$ y $\|r\| < \|2\| = 4$. Por supuesto, $x + 2A = r + 2A$, y basta encontrar los elementos de norma $0, 1, 2$ y 3. El único elemento de A de norma 0 es 0 y los elementos de norma 1 son las unidades calculadas en el apartado (2).

Ningún elemento de A tiene norma 2. En efecto, si $x := a + b\omega \in A$ tuviese norma 2, entonces $a^2 + b^2 - ab = 2$, o sea $(a - b/2)^2 + 3b^2/4 = 2$, o lo que es igual, $(2a - b)^2 + 3b^2 = 8$. Esto implica que $3b^2 \leq 8$, es decir, $b^2 = 0, 1$. Pero si $b^2 = 0$, entonces $a^2 = 2$, que es imposible, y si $b^2 = 1$ entonces $(2a-b)^2 = 5$, que es imposible también.

Por último, la condición $\|x\| = 3$ equivale a $(2a - b)^2 + 3b^2 = 12$, por lo que $b = 0, \pm 1, \pm 2$. En el primer caso $a^2 = 3$, lo que no es posible. Si $b = \pm 1$ entonces $(2a-b) = \pm 3$, luego $b = 1$, y en tal caso $a = 2$ o $a = -1$, o $b = -1$, lo que proporciona $a = 1$ y $a = -2$. Así, los elementos de A de norma 3 son $\pm(2 + \omega)$ y $\pm(1 - \omega)$. Del análisis anterior se desprende que

$$K = \{0_K,\ \pm(1+2A),\ \pm(\omega+2A),\ \pm((1+\omega)+2A),\ \pm((2+\omega)+2A),\ \pm((1-\omega)+2A)\}.$$

Ahora bien, para cada $x \in A$ se tiene $x+2A = -x+2A$, lo que reduce la lista anterior a la mitad:

$$K = \{0_K,\ 1 + 2A,\ \omega + 2A,\ (1 + \omega) + 2A,\ (2 + \omega) + 2A,\ (1 - \omega) + 2A\}.$$

Además, $(2+\omega)+2A = \omega+2A$ y $(1+\omega)+2A = (1-\omega)+2A$, por lo que, finalmente,

$$K = \{0_K,\ 1 + 2A,\ \omega + 2A, (1 + \omega) + 2A\},$$

lo que demuestra que K consta de cuatro elementos. □

Número V.2 Probar que el polinomio $f(\mathtt{t}) := \mathtt{t}^3 + 2\mathtt{t} + 2 \in \mathbb{F}_3[\mathtt{t}]$ es irreducible y sea u una raíz de f en una extensión de $\mathbb{F}_3$. Hallar las raíces cúbicas de $u+2$ en $\mathbb{F}_3(u)$.

Solución. El polinomio f no tiene raíces en $\mathbb{F}_3$, ya que $f(0) = f(1) = f(2) = 2$, luego es irreducible en $\mathbb{F}_3[\mathtt{t}]$. Como $u^3 = -2u - 2 = u + 1$ se tiene, puesto que $\mathrm{char}(\mathbb{F}_3) = 3$,

$$u + 2 = u^3 + 1 = u^3 + 3u^2 + 3u + 1 = (u + 1)^3,$$

así que $a := u+1$ es una raíz cúbica de $u+2$, esto es, a es raíz del polinomio $\mathtt{t}^3-(u+2)$. Para calcular las demás raíces dividimos

$$\mathtt{t}^3 - (u + 2) = (\mathtt{t} - a)(\mathtt{t}^2 + a\mathtt{t} + a^2) = (\mathtt{t} - a)(\mathtt{t}^2 - 2a\mathtt{t} + a^2) = (\mathtt{t} - a)^3$$

luego la única raíz cúbica de $u + 2$ en $\mathbb{F}_3(u)$ es $u + 1$. □

Número V.3 (1) Sea $A := \mathbb{Z}[i]$ el anillo de los enteros de Gauss. Demostrar que el cociente $E := A/7A$ es un cuerpo finito y calcular cuántos elementos tiene.

(2) Determinar el cuerpo primo K de E y un elemento primitivo ξ de la extensión $E|K$. Calcular el polinomio mínimo de ξ sobre K.

Solución. (1) El número primo 7 es irreducible en $\mathbb{Z}[i]$, en virtud de la Proposición IV.1.13, vol. II, porque no es congruente con 1 mod 4. Como el anillo de enteros de Gauss es un dominio euclídeo, el ideal $\mathfrak{a} := 7A$ es maximal, luego el cociente $E = A/\mathfrak{a}$ es un cuerpo y, por el Ejercicio IV.14 vol. II, el cuerpo E tiene 49 elementos.

(2) Como el cuerpo E tiene característica 7 su cuerpo primo es $K := \mathbb{F}_7$. La aplicación

$$\mathbb{F}_7 \to E,\ \ell + 7\mathbb{Z} \mapsto \ell + \mathfrak{a}$$

es un homomorfismo de cuerpos, e identificamos $\mathbb{F}_7$ y su imagen. Sea $\xi := i + \mathfrak{a}$, que no pertenece a $\mathbb{F}_7$ ya que $\xi^2 + 1 = 0$ y sin embargo -1 no es un cuadrado en $\mathbb{F}_7$ pues

$$0^2 = 0,\ \ 1^2 = 6^2 = 1,\ \ 2^2 = 5^2 = 4 \quad \& \quad 3^2 = 4^2 = 2.$$

Por tanto $\mathbb{F}_7 \subsetneq \mathbb{F}_7(\xi)$, luego $[\mathbb{F}_7(\xi) : \mathbb{F}_7] \geq 2$. Por la transitividad del grado,

$$2 = \log_7 49 = [E : \mathbb{F}_7] = [E : \mathbb{F}_7(\xi)] \cdot [\mathbb{F}_7(\xi) : \mathbb{F}_7],$$

luego $[E : \mathbb{F}_7(\xi)] = 1$, esto es, $E = \mathbb{F}_7(\xi)$. Por último $f(\mathtt{t}) = \mathtt{t}^2 + 1$ es el polinomio mínimo de ξ sobre K porque $\deg(f) = 2 = [K(\xi) : K]$ y $f(\xi) = 0$. □

Número V.4 (1) Sean $p \in \mathbb{Z}$ primo y $f \in \mathbb{F}_p[\mathtt{t}]$. Probar que $(f(\mathtt{t}))^p = f(\mathtt{t}^p)$ y que si α es raíz de f entonces también lo es α^{p^n} para cada $n \in \mathbb{Z}^+$.

(2) Hallar los polinomios mínimos de β^2 y β^3 sobre $\mathbb{F}_2$ sabiendo que $\beta^4 + \beta + 1 = 0$.

Solución. (1) Argumentamos por inducción sobre $n := \deg(f)$. Si $n = 0$ entonces $f \in \mathbb{F}_p$ y, por el Pequeño Teorema de Fermat, VI.2.5, vol. I,

$$f(\mathtt{t}^p) = f = f^p = (f(\mathtt{t}))^p.$$

Sea ahora f de grado $n > 0$ y supongamos probado el resultado para polinomios de grado menor que n. Existen $a \in \mathbb{F}_p$ y $g \in \mathbb{F}_p[\mathtt{t}]$ tales que $f(\mathtt{t}) = a\mathtt{t}^n + g(\mathtt{t})$ y $\deg(g) < n$, luego por la hipótesis de inducción,

$$f(\mathtt{t}^p) = a\mathtt{t}^{np} + g(\mathtt{t}^p) = a\mathtt{t}^{np} + (g(\mathtt{t}))^p.$$

Por otro lado, por la Fórmula del binomio de Newton, y puesto que $\binom{p}{i} \in p\mathbb{Z}$ para $0 < i < p$, según demostramos en el Ejemplo VI.2.7, vol. II, se tiene

$$(f(\mathtt{t}))^p = (a\mathtt{t}^n + g(\mathtt{t}))^p = \sum_{i=0}^{p} \binom{p}{i} a^i \mathtt{t}^{ni} (g(\mathtt{t}))^{p-i} = a^p \mathtt{t}^{np} + (g(\mathtt{t}))^p = a\mathtt{t}^{np} + (g(\mathtt{t}))^p,$$

lo que proporciona la igualdad buscada.

También probamos por inducción la segunda parte de este primer apartado. Es obvio el caso $n = 0$ mientras que para $n = 1$ se tiene, por lo probado anteriormente, $f(\alpha^p) = (f(\alpha))^p = 0^p = 0$. Si admitimos el resultado para exponentes menores que $n \geq 2$ y $\gamma := \alpha^{p^{n-1}}$ la hipótesis de inducción nos dice que $f(\gamma) = 0$, luego

$$f(\alpha^{p^n}) = f(\gamma^p) = f(\gamma)^p = 0.$$

(2) El polinomio $f(\mathtt{t}) := \mathtt{t}^4+\mathtt{t}+1$ es irreducible en $\mathbb{F}_2[\mathtt{t}]$. En efecto, si f fuese reducible sería producto de dos polinomios mónicos de grado 2, ya que $f(0) = f(1) = 1$, luego existirían $a, b \in \mathbb{F}_2$ tales que

$$f(\mathtt{t}) = (\mathtt{t}^2 + a\mathtt{t} + 1)(\mathtt{t}^2 + b\mathtt{t} + 1),$$

y como el coeficiente de $\mathtt{t}^3$ de f es nulo, mientras que el de $\mathtt{t}$ es 1 se tiene $0 = a+b = 1$, lo que es absurdo. Por lo demostrado en el apartado anterior, $f(\beta^2) = f(\beta)^2 = 0$, así que $f = P_{\mathbb{F}_2,\beta^2}$. En cuanto a $\beta^3 := u$ observamos que, puesto que f es irreducible en $\mathbb{F}_2[\mathtt{t}]$, es el polinomio mínimo de β sobre $\mathbb{F}_2$, así que la extensión $\mathbb{F}_2(\beta)|\mathbb{F}_2$ tiene grado 4. En consecuencia, el grupo multiplicativo K^* formado por los elementos no nulos del cuerpo $K := \mathbb{F}_2(\beta)$ tiene orden 15, y se deduce del Teorema de Lagrange que $\beta^5 = 1$, es decir, $u^5 = 1$, luego

$$0 = u^5 - 1 = (u - 1)(1 + u + u^2 + u^3 + u^4).$$

Por tanto u es raíz del polinomio $g(\mathtt{t}) := 1+\mathtt{t}+\mathtt{t}^2+\mathtt{t}^3+\mathtt{t}^4$, que de hecho es el polinomio mínimo de β^3 sobre $\mathbb{F}_2$. Para comprobarlo basta demostrar la irreducibilidad de g en $\mathbb{F}_2[\mathtt{t}]$. Como $g(0) = g(1) = 1$, los posibles factores de g en $\mathbb{Z}_2[\mathtt{t}]$ tienen grado 2. Supongamos que

$$g(\mathtt{t}) = (\mathtt{t}^2 + c\mathtt{t} + 1)(\mathtt{t}^2 + d\mathtt{t} + 1)$$

para ciertos $c, d \in \mathbb{F}_2$. Al igualar coeficientes resulta que $c + d = 1 = cd$, y esto es imposible. En conclusión, $g = P_{\mathbb{F}_2,\beta^3}$. □

Número V.5 Sea K un cuerpo finito con q elementos. Determinar el número de polinomios mónicos e irreducibles de grado 3 en $K[\mathtt{t}]$.

Solución. El número de polinomios mónicos de grado 3 en $K[\mathtt{t}]$ es q^3, y vamos a calcular el número $i_q(3)$ de polinomios mónicos e irreducibles de $K[\mathtt{t}]$ de grado 3 como resta $i_q(3) = q^3 - r_q(3)$, donde $r_q(3)$ es el número de polinomios mónicos y reducibles de grado 3 en $K[\mathtt{t}]$. Puesto que $K[\mathtt{t}]$ es un DFU y K es un cuerpo, los polinomios mónicos y reducibles f de grado 3 en $K[\mathtt{t}]$ son de una de las formas siguientes:

$$f = f_1^3, \text{ donde } f_1 := \mathtt{t} - a; \quad f = f_1^2 \cdot f_2 \text{ donde } f_1 := \mathtt{t} - a, \ f_2 := \mathtt{t} - b,$$
$$f = f_1 \cdot f_2 \cdot f_3, \text{ donde } f_1 := \mathtt{t} - a, \ f_2 := \mathtt{t} - b, \ f_3 := \mathtt{t} - c,$$

siendo $a, b, c \in K$ con $a \neq b \neq c \neq a$, y por último $f = f_1 \cdot f_2$, donde $f_1 := \mathtt{t} - a$ con $a \in K$ y f_2 es un polinomio mónico e irreducible en $K[\mathtt{t}]$ de grado 2. Existen por tanto 4 tipos esencialmente distintos de factorizaciones de los polinomios mónicos y reducibles de $K[\mathtt{t}]$ de grado 3 en producto de irreducibles, salvo para $q = 2$, en el que no hay factorizaciones del tercer tipo, pues $\mathbb{F}_2$ no contiene tres elementos distintos.

Vamos a contar el número de polinomios de cada uno de estos tipos, teniendo en cuenta que el orden en que aparecen los factores es irrelevante. Hay q del primer tipo, $q(q-1)$ del segundo y, si $q \geq 3$, hay $\binom{q}{3}$ del tercero, mientras que el número de factorizaciones del cuarto tipo es $q \cdot i_q(2)$, donde $i_q(2) = \binom{q}{2}$ es, según vimos en V.1.1, el número de polinomios mónicos e irreducibles de grado 2 en $K[\mathtt{t}]$. En consecuencia,

$$r_q(3) = q + q(q-1) + \binom{q}{3} + q\binom{q}{2} = q^2 + q\binom{q}{2} + \binom{q}{3}, \text{ si } q \neq 2,$$

así que el número $i_q(3)$ de polinomios mónicos e irreducibles de $K[\mathtt{t}]$ de grado 3 es

$$i_q(3) = q^3 - r_q(3) = q^2(q-1) - q\binom{q}{2} - \binom{q}{3} = \frac{q^2(q-1)}{2} - \frac{q(q-1)(q-2)}{6} = \frac{q(q^2-1)}{3}.$$

Para $q = 2$ resulta $r_2(3) = 2 + 2 + 2\binom{2}{2} = 6$, luego $i_2(3) = 2^3 - 6 = 2$ es el número de polinomios irreducibles de grado 3 en $\mathbb{F}_2[\mathtt{t}]$. □

Número V.6 Sean $p \in \mathbb{Z}$ un número primo mayor que 3 y L_f un cuerpo de descomposición del polinomio $f(\mathtt{t}) := \mathtt{t}^p - 3$ sobre $\mathbb{F}_p$. Calcular el grado $[L_f : \mathbb{F}_p]$.

Solución. Puesto que $p > 3$ se tiene, por el Pequeño Teorema de Fermat, $3^p = 3$, luego $f(\mathtt{t}) := \mathtt{t}^p - 3^p = (\mathtt{t} - 3)^p$, así que f factoriza en $\mathbb{F}_p[\mathtt{t}]$ en producto de factores de grado 1. En consecuencia, $L_f = \mathbb{F}_p$, es decir, $[L_f : \mathbb{F}_p] = 1$. □

Número V.7 ¿Son isomorfos los cuerpos de descomposición sobre el cuerpo $\mathbb{F}_3$ de los polinomios

$$f(\mathtt{t}) := \mathtt{t}^3 + 2\mathtt{t} + 1 \quad \& \quad g(\mathtt{t}) := \mathtt{t}^3 + \mathtt{t}^2 + \mathtt{t} + 2?$$

Si lo son, definir un isomorfismo entre ellos.

Solución. Sea u una raíz de f en un cuerpo de descomposición suyo sobre $\mathbb{F}_3$. Así $0 = f(u)^3 = f(u^3)$, luego tambien $u^3 = -2u - 1 = u + 2$ es raíz de f. Como la suma de las raíces de este polinomio es nula su tercera raíz es $-(u + u + 2) = u + 1$. En consecuencia

$$f(\mathtt{t}) = (\mathtt{t} - u) \cdot (\mathtt{t} - (u+1))(\mathtt{t} - (u+2)),$$

y un cuerpo de descomposición de f sobre $\mathbb{F}_3$ es $\mathbb{F}_3(u)$. Como f es irreducible en $\mathbb{F}_3[\mathtt{t}]$, pues carece de raíces en $\mathbb{F}_3$, resulta que $[\mathbb{F}_3(u) : \mathbb{F}_3] = \deg(f) = 3$.

Análogamente, si v es una raíz de g en un cuerpo de descomposición suyo sobre $\mathbb{F}_3$, se tiene $0 = g(v)^3 = g(v^3)$, luego $v^3 = 2v^2 + 2v + 1 \in \mathbb{F}_3(v)$ es otra raíz de g y la tercera también pertenece a $\mathbb{F}_3(v)$ porque vale, por las Fórmulas de Cardano-Vieta, $-1 - v - (2v^2 + 2v + 1) = 1 + v^2$.

En consecuencia, $\mathbb{F}_3(v)$ es un cuerpo de descomposición sobre $\mathbb{F}_3$ del polinomio g, que es irreducible en $\mathbb{F}_3[\mathtt{t}]$, por lo que $[\mathbb{F}_3(v) : \mathbb{F}_3] = \deg(g) = 3$. Se deduce de lo anterior que tanto $\mathbb{F}_3(u)$ como $\mathbb{F}_3(v)$ tienen $27 = 3^3$ elementos, luego por el Teorema V.1.2 son isomorfos. Vamos a definir un isomorfismo $\varphi : \mathbb{F}_3(u) \to \mathbb{F}_3(v)$ cuya restricción a $\mathbb{F}_3$ sea la identidad, para lo que basta decidir cuál es la imagen de u, que será de la forma $\varphi(u) = a + bv + cv^2$ para ciertos $a, b, c \in \mathbb{F}_3$. Por el Pequeño Teorema de Fermat se tiene $a^3 = a$, $b^3 = b$ y $c^3 = c$, y se debe cumplir que

$$\begin{aligned}(a+2) + bv + cv^2 = \varphi(u+2) = \varphi(u^3) = (\varphi(u))^3 = (a + bv + cv^2)^3 = a^3 + b^3v^3 \\ + c^3v^6 = a + b(2v^2 + 2v + 1) + c(2v^2 + 2v + 1)^2 = (a + b) + 2bv \\ + 2bv^2 + c(v^4 + v^2 + 1 + 2v^3 + v^2 + v) = (a + b + c) + (2b + c)v \\ + 2(b + c)v^2 + 2c(2v^2 + 2v + 1) + c(2v^3 + 2v^2 + v) = (a + b) \\ + 2bv + 2(b + c)v^2 + 2c(2v^2 + 2v + 1) = (a + b + 2c) \\ + (2b + c)v + 2bv^2,\end{aligned}$$

y como $1, v$ y v^2 son linealmente independientes sobre $\mathbb{F}_3$ resulta

$$\begin{cases} b & + & 2c & = & 2 \\ b & + & c & = & 0 \\ 2b & - & c & = & 0 \end{cases}$$

es decir, $b = 1$ y $c = 2$. Esto no impone ninguna condición sobre a así que tomamos, por ejemplo $a = 0$, esto es, $\varphi(u) = v + 2v^2$. Por tanto, la aplicación

$$\varphi : \mathbb{F}_3(u) \to \mathbb{F}_3(v),\ x_1 + x_2u + x_3u^2 \mapsto x_1 + x_2(v + 2v^2) + x_3(v + 2v^2)^2.$$

es un isomorfismo entre $\mathbb{F}_3(u)$ y $\mathbb{F}_3(v)$. □

Número V.8 (1) Factorizar $\mathtt{t}^{16} - \mathtt{t}$ como producto de polinomios irreducibles en $\mathbb{F}_2[\mathtt{t}]$.

(2) Factorizar como producto de polinomios irreducibles en $\mathbb{F}_3[\mathtt{t}]$ el polinomio $\mathtt{t}^9 - \mathtt{t}$.

Solución. (1) Este es un caso particular del Corolario V.1.4 con $p = 2$ y $n = 4$. El conjunto de divisores positivos de 4 es $D_4 := \{1, 2, 4\}$, y sea $\Sigma := \Sigma_1 \sqcup \Sigma_2 \sqcup \Sigma_4$ donde cada Σ_d es el conjunto de polinomios mónicos e irreducibles en $\mathbb{F}_2[\mathtt{t}]$ de grado d. En el Corolario V.1.4 hemos visto que

$$\mathtt{t}^{16} - \mathtt{t} = \prod_{f \in \Sigma} f = \Big(\prod_{f \in \Sigma_1} f\Big) \cdot \Big(\prod_{f \in \Sigma_2} f\Big) \cdot \Big(\prod_{f \in \Sigma_4} f\Big).$$

Los polinomios mónicos de grado 1 en $\mathbb{F}_2[\mathtt{t}]$ son $\mathtt{t}$ y $\mathtt{t}-1$, y ambos son irreducibles. Los polinomios mónicos de grado 2 en $\mathbb{F}_2[\mathtt{t}]$ son $\mathtt{t}^2$, $\mathtt{t}^2+\mathtt{t}=\mathtt{t}(\mathtt{t}+1)$, $\mathtt{t}^2+1=(\mathtt{t}+1)^2$ y $\mathtt{t}^2+\mathtt{t}+1$, y sólo el último es irreducible, pues carece de raíces en $\mathbb{F}_2$.

Por último, se desprende del Corolario V.1.5 que el número de polinomios mónicos e irreducibles en $\mathbb{F}_2[\mathtt{t}]$ de grado 4 es

$$N_4^2 = \frac{\mu(4)2 + \mu(2)2^2 + \mu(1)2^4}{4} = \frac{16-4}{4} = 3,$$

y vamos a calcularlos. Si f es uno de ellos $f(0)=1$, pues $f(0)\neq 0$, y así

$$f(\mathtt{t}) := \mathtt{t}^4 + a_1\mathtt{t}^3 + a_2\mathtt{t}^2 + a_3\mathtt{t} + 1,$$

con $a_i \in \{0,1\}$. Como $a_1+a_2+a_3 = f(1) \neq 0$, el número de a_i's que valen 1 es 1 o 3. Además,

$$(\mathtt{t}^2+\mathtt{t}+1)^2 = \mathtt{t}^4+\mathtt{t}^2+1$$

es reducible, luego los tres polinomios mónicos e irreducibles en $\mathbb{F}_2[\mathtt{t}]$ de grado 4 son

$$\mathtt{t}^4+\mathtt{t}^3+1,\ \ \mathtt{t}^4+\mathtt{t}+1 \quad \& \quad \mathtt{t}^4+\mathtt{t}^3+\mathtt{t}^2+\mathtt{t}+1.$$

Así, la factorización de $\mathtt{t}^{16}-\mathtt{t}$ como producto de polinomios mónicos e irreducibles en $\mathbb{F}_2[\mathtt{t}]$ es:

$$\mathtt{t}^{16}-\mathtt{t} = \mathtt{t}\cdot(\mathtt{t}-1)\cdot(\mathtt{t}^2+\mathtt{t}+1)\cdot(\mathtt{t}^4+\mathtt{t}^3+1)\cdot(\mathtt{t}^4+\mathtt{t}+1)\cdot(\mathtt{t}^4+\mathtt{t}^3+\mathtt{t}^2+\mathtt{t}+1).$$

(2) Este también es un caso particular del Corolario V.1.4, ahora con $p=3$ y $n=2$. El conjunto de divisores de 2 es $D_2=\{1,2\}$, mientras que $\Sigma := \Sigma_1 \sqcup \Sigma_2$ y cada Σ_d es el conjunto de polinomios mónicos e irreducibles en $\mathbb{F}_3[\mathtt{t}]$ de grado d.

En el Corolario V.1.4 hemos visto que

$$\mathtt{t}^9-\mathtt{t} = \prod_{f\in\Sigma} f = \Big(\prod_{f\in\Sigma_1} f\Big)\cdot\Big(\prod_{f\in\Sigma_2} f\Big).$$

Los polinomios mónicos de grado 1 en $\mathbb{F}_3[\mathtt{t}]$ son $\mathtt{t}$, $\mathtt{t}-1$ y $\mathtt{t}-2$, y todos ellos son irreducibles. En $\mathbb{F}_3[\mathtt{t}]$ hay nueve polinomios mónicos de grado 2, de los que los seis siguientes son reducibles:

$$\mathtt{t}^2,\quad \mathtt{t}^2+\mathtt{t}=\mathtt{t}(\mathtt{t}+1),\ \ \mathtt{t}^2+2\mathtt{t}=\mathtt{t}(\mathtt{t}+2),\ \ \mathtt{t}^2+2=(\mathtt{t}+1)(\mathtt{t}+2)$$
$$\mathtt{t}^2+2\mathtt{t}+1=(\mathtt{t}+1)^2 \quad \& \quad \mathtt{t}^2+\mathtt{t}+1=(\mathtt{t}+2)^2.$$

Sin embargo son irreducibles en $\mathbb{F}_3[\mathtt{t}]$, pues carecen de raíces en $\mathbb{F}_3$, los polinomios

$$\mathtt{t}^2+1,\ \ \mathtt{t}^2+\mathtt{t}+2 \ \text{ y } \ \mathtt{t}^2+2\mathtt{t}+2.$$

Resulta así la siguiente factorizacion en producto de polinomios irreducibles en $\mathbb{F}_3[\mathtt{t}]$:

$$\mathtt{t}^9-\mathtt{t} = \mathtt{t}\cdot(\mathtt{t}-1)\cdot(\mathtt{t}-2)\cdot(\mathtt{t}^2+1)\cdot(\mathtt{t}^2+\mathtt{t}+2)\cdot(\mathtt{t}^2+2\mathtt{t}+2).$$

□

Número V.9 Escribir las tablas de sumar y multiplicar del cuerpo de 9 elementos.

Solución. El cuerpo $\mathbb{F}_9$ de nueve elementos es el cuerpo de descomposición sobre $\mathbb{F}_3$ del polinomio $\mathtt{t}^9-\mathtt{t}$. Se desprende de la factorización obtenida en el Ejercicio anterior que $\mathbb{F}_9$ consiste en los elementos 0, 1, $2=-1$, y las dos raíces de cada uno de los polinomios $\mathtt{t}^2+1$, $\mathtt{t}^2+\mathtt{t}+2$ y $\mathtt{t}^2+2\mathtt{t}+2$.

El grupo $\mathbb{F}_9^*=\mathbb{F}_9\setminus\{0\}$ es cíclico de orden 8, y tiene, por tanto, $\varphi(8)=4$ generadores, donde φ es la función de Euler. Nótese que 1 tiene orden 1, mientras que -1 tiene orden 2 y las dos raíces de $\mathtt{t}^2+1$ tienen orden 4, pues si $t^2+1=0$, entonces $t^2\neq 1$ pero $t^4=(t^2)^2=(-1)^2=1$. En consecuencia, cualquiera de las raíces del producto $(\mathtt{t}^2+\mathtt{t}+2)\cdot(\mathtt{t}^2+2\mathtt{t}+2)$ es un generador de $\mathbb{F}_9^*$. Elegimos, por ejemplo, $\alpha\in\mathbb{F}_9$ tal que $\alpha^2+\alpha+2=0$, es decir, $\alpha^2=1+2\alpha$, y sabemos que $\alpha^8=1$ y

$$\mathbb{F}_9=\{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7\}.$$

Para obtener la tabla de sumar efectuamos dos cálculos previos. Observamos en primer lugar que $\alpha^4=-1=2$, pues α tiene orden 8. Además,

$$1+1=2=\alpha^4,\quad \alpha^2=1+2\alpha,\quad \alpha^3=\alpha^2\cdot\alpha=(1+2\alpha)\cdot\alpha=\alpha-\alpha^2=2+2\alpha,$$
$$\alpha^5=\alpha^4\cdot\alpha=2\alpha,\quad \alpha^6=2\alpha^2=2+\alpha,\quad \alpha^7=2\alpha^3=1+\alpha.$$

Con esta información calculamos las sumas $1+\alpha^k$ para $1\leq k\leq 7$:

$$1+\alpha=\alpha^7,\quad 1+\alpha^2=2+2\alpha=\alpha^3,\quad 1+\alpha^3=2\alpha=\alpha^5,\quad 1+\alpha^4=1+2=0,$$
$$1+\alpha^5=1+2\alpha=\alpha^2,\quad 1+\alpha^6=1+(2+\alpha)=\alpha\quad\&\quad 1+\alpha^7=2+\alpha=\alpha^6.$$

Dados $0\leq i<j\leq 7$ se tiene $\alpha^i+\alpha^j=\alpha^i(1+\alpha^{j-i})$ y ambos factores son potencias de α ya calculadas, mientras que $\alpha^j+\alpha^j=2\alpha^j=\alpha^4\cdot\alpha^j=\alpha^{4+j}$. Se tiene así:

$+$	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7
0	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7
1	1	α^4	α^7	α^3	α^5	0	α^2	α^7	α^6
α	α	α^7	α^5	1	α^4	α^6	0	α^3	α^2
α^2	α^2	α^3	1	α^6	α	α^5	α^7	0	α^4
α^3	α^3	α^5	α^4	α	α^7	α^2	α^6	1	0
α^4	α^4	0	α^6	α^5	α^2	1	α^3	α^7	α
α^5	α^5	α^2	0	α^7	α^6	α^3	α	α^4	1
α^6	α^6	α	α^3	0	1	α^7	α^4	α^2	α^5
α^7	α^7	α^6	α^2	α^4	0	α	1	α^5	α^3

Por su parte, la tabla de multiplicar se calcula directamente empleando que $\alpha^8=1$:

$\cdot$	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7
0	0	0	0	0	0	0	0	0	0
1	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7
α	0	α	α^2	α^3	α^4	α^5	α^6	α^7	1
α^2	0	α^2	α^3	α^4	α^5	α^6	α^7	1	α
α^3	0	α^3	α^4	α^5	α^6	α^7	1	α	α^2
α^4	0	α^4	α^5	α^6	α^7	1	α	α^2	α^3
α^5	0	α^5	α^6	α^7	1	α	α^2	α^3	α^4
α^6	0	α^6	α^7	1	α	α^2	α^3	α^4	α^5
α^7	0	α^7	1	α	α^2	α^3	α^4	α^5	α^6

□

Número V.10 Sean p y q dos números primos. Calcular el número de polinomios mónicos e irreducibles en $\mathbb{F}_p[\mathtt{t}]$ de grados 4, 6 y q.

Solución. Vimos en el Corolario V.1.5 que si $D(n)$ es el conjunto de divisores positivos de n y μ es la función de Möbius, el número N_n^p de polinomios mónicos e irreducibles en $\mathbb{F}_p[\mathtt{t}]$ de grado n cumple la igualdad

$$nN_n^p = \sum_{d\in D(n)} \mu(n/d)p^d. \tag{V.11}$$

Aplicándola con $n = 4$, cuyos divisores positivos son 1, 2 y 4, se tiene

$$4N_4^p = \mu(4)p + \mu(2)p^2 + \mu(1)p^4 = p^4 - p^2 \quad \Longrightarrow \quad N_4^p = p^2(p-1)(p+1)/4.$$

Como los divisores positivos de 6 son 1, 2, 3 y 6, empleando la fórmula (V.11) se tiene

$$6N_6^p = \mu(6)p + \mu(3)p^2 + \mu(2)p^3 + \mu(1)p^6 = p^6 - p^3 - p^2 + p,$$

así que $N_6^p = (p^6 - p^3 - p^2 + p)/6$. Por fin, los divisores positivos del primo q son 1 y q, luego $qN_q^p = \mu(q)p + \mu(1)p^q$, es decir, $N_q^p = (p^q - p)/q$. □

Número V.11 Sea F un cuerpo finito de característica $p > 0$. Describir su cierre algebraico y demostrar que es un cuerpo numerable y no finito.

Solución. Sabemos que F contiene a su cuerpo primo, que es el cuerpo $\mathbb{F}_p$ con p elementos. El cierre algebraico $\mathbb{F}_\infty$ de $\mathbb{F}_p$ es también cierre algebraico de F, por lo que podemos suponer desde el principio que $F := \mathbb{F}_p$. En efecto, $\mathbb{F}_\infty$ es algebraicamente cerrado y contiene a F, en virtud de II.1.12 (1) ya que la extensión $F|\mathbb{F}_p$ es algebraica por ser finita. Además $\mathbb{F}_\infty|F$ es una extensión algebraica, por serlo $\mathbb{F}_\infty|\mathbb{F}_p$. Ambos hechos demuestran que $\mathbb{F}_\infty$ es un cierre algebraico de F.

Como $k!$ divide a $n!$ para $1 \le k \le n$, se deduce de V.1.3 (4) que el cuerpo $\mathbb{F}_{p^{k!}}$ con $p^{k!}$ elementos está contenido en el cuerpo $\mathbb{F}_{p^{n!}}$ con $p^{n!}$ elementos, luego se deduce de la

Proposición I.1.9 (1) que la unión $\mathbb{F}_\infty := \bigcup_{n\in\mathbb{Z}^+} \mathbb{F}_{p^{n!}}$ es un cuerpo que contiene a $\mathbb{F}_p$. De hecho la extensión $\mathbb{F}_\infty|\mathbb{F}_p$ es algebraica porque lo es cada una de las subextensiones $\mathbb{F}_{p^{n!}}|\mathbb{F}_p$, que son finitas, y sólo falta demostrar que el cuerpo $\mathbb{F}_\infty$ es algebraicamente cerrado.

En virtud de la Proposición II.1.5 basta probar que cada polinomio $f \in \mathbb{F}_p[\mathtt{t}]$ de grado ≥ 1 factoriza en $\mathbb{F}_\infty[\mathtt{t}]$ en producto de factores de grado 1, y para ello es suficiente hacerlo en el caso en que f es irreducible en $\mathbb{F}_p[\mathtt{t}]$. Ahora bien, si $n := \deg(f)$ se prueba en el Corolario V.1.4 que f divide a $\mathtt{t}^{p^n} - \mathtt{t}$. Como este último polinomio factoriza en $F_{p^n}[\mathtt{t}] \subset \mathbb{F}_{p^{n!}}[\mathtt{t}] \subset \mathbb{F}_\infty[\mathtt{t}]$ en producto de factores de grado 1, también f lo hace. Para la segunda parte, $\mathbb{F}_\infty$ es numerable, por ser unión numerable de conjuntos finitos. Si $\mathbb{F}_\infty$ fuese finito y tiene k elementos, existe $n \in \mathbb{Z}^+$ tal que $k < p^{n!}$, y esto es una contradicción porque $\mathbb{F}_{p^{n!}} \subset \mathbb{F}_\infty$. □

Número V.12 Demostrar que toda raíz α del polinomio $f(\mathtt{t}) := \mathtt{t}^3 + \mathtt{t} + 1 \in \mathbb{F}_2[\mathtt{t}]$ en un cierre algebraico de $\mathbb{F}_2$ es un generador del grupo multiplicativo $\mathbb{F}_{2^3}^*$ formado por los elementos no nulos del cuerpo con 8 elementos.

Solución. Dividiendo como en la enseñanza secundaria, esto es, mediante una caja que contiene al divisor, y puesto que trabajamos en cuerpos de característica 2, resulta la igualdad

$$\mathtt{t}^7 - 1 = (\mathtt{t}^3 + \mathtt{t} + 1) \cdot (\mathtt{t}^4 + \mathtt{t}^2 + \mathtt{t} + 1),$$

y como $f(\alpha) = 0$ se deduce que $\alpha^7 = 1$, así que α es raíz del polinomio $g(\mathtt{t}) := \mathtt{t}^{2^3} - \mathtt{t}$. Esto prueba que $\alpha \in \mathbb{F}_8$, pues este cuerpo está formado por las raíces de g en un cierre algebraico de $\mathbb{F}_2$. El grupo $\mathbb{F}_{2^3}^*$ está generado por cualquiera de sus elementos distintos de 1, pues su orden 7 es primo. Pero $\alpha \neq 1$, pues $f(1) = 1 \neq 0$, así que $\mathbb{F}_{2^3}^* = \langle\alpha\rangle$, como queremos. □

Número V.13 Sean K un cuerpo finito y $\mathtt{t}$ una indeterminada sobre K. Demostrar que para cada automorfismo $\varphi : K(\mathtt{t}) \to K(\mathtt{t})$ se cumple que $\varphi(K) = K$.

Solución. Basta probar que $\varphi(K) \subset K$, pues aplicando esto al automorfismo φ^{-1} se tiene $\varphi^{-1}(K) \subset K$, y por tanto

$$K = \varphi(\varphi^{-1}(K)) \subset \varphi(K) \subset K.$$

Si $p = \mathrm{char}(K)$ la extensión $K|\mathbb{F}_p$ es finita, luego algebraica. Para cada $x \in K$ existe, por ser algebraico sobre $\mathbb{F}_p$, un polinomio no nulo $f(\mathtt{t}) := \sum_{j=0}^n a_j \mathtt{t}^j \in \mathbb{F}_p[\mathtt{t}]$ tal que $f(x) = 0$. Como la restricción $\varphi|_{\mathbb{F}_p} : \mathbb{F}_p \to K(\mathtt{t})$ es la inclusión, por V.1.9, se tiene

$$0 = \varphi(0) = \varphi\Big(\sum_{j=0}^n a_j x^j\Big) = \sum_{j=0}^n \varphi(a_j)\varphi(x^j) = \sum_{j=0}^n a_j \varphi(x)^j = f(\varphi(x)).$$

Por tanto $\varphi(x) \in K(\mathtt{t})$ es algebraico sobre $\mathbb{F}_p$, luego también sobre K. Esto implica, por III.1.2 (2), que $\varphi(x) \in K$. □

Número V.14 Sean p un número primo, K un cuerpo finito de característica p y α una raíz del polinomio $f(\mathtt{t}) := \mathtt{t}^p - \mathtt{t} - a \in K[\mathtt{t}]$, donde $a \in K^* := K \setminus \{0\}$.

(1) Demostrar que $K(\alpha)$ es cuerpo de descomposición de f sobre K y expresar en función de α las restantes raíces de f.

(2) Probar que si no es trivial el grupo de Galois $G(K(\alpha) : K)$ es cíclico de orden p.

(3) Demostrar que si f es reducible en $K[\mathtt{t}]$ entonces factoriza en $K[\mathtt{t}]$ como producto de factores de grado 1.

(4) Demostrar que si $a \in \mathbb{F}_p \setminus \{0\}$ entonces f es irreducible en $\mathbb{F}_p[\mathtt{t}]$.

Solución. (1) Por el Pequeño Teorema de Fermat $x^p = x$ para cada $x \in \mathbb{F}_p$, luego

$$\begin{aligned} f(\alpha + x) = (\alpha + x)^p - (\alpha + x) - a &= \alpha^p + x^p - \alpha - x - a \\ &= (\alpha^p - \alpha - a) + (x^p - x) = f(\alpha) = 0. \end{aligned}$$

Como f tiene a lo sumo p raíces en K concluimos que efectivamente las tiene y que son los elementos del conjunto $\{\alpha + x : \ x \in \mathbb{F}_p\} \subset K(\alpha)$. En particular $K(\alpha)$ es un cuerpo de descomposición de f sobre K.

(2) En el Teorema V.1.11 vimos que el grupo de Galois $G(K(\alpha) : K)$ es cíclico y que la extensión $K(\alpha)|K$ es de Galois. Por eso el grupo $G(K(\alpha) : K)$ es trivial si y sólo si lo es la extensión $K(\alpha)|K$, o sea, $\alpha \in K$. Supongamos que no es éste el caso y observamos que. por el Lema II.1.1, existe $\sigma \in G(K(\alpha) : K)$ tal que $\sigma(\alpha) = \alpha + 1$, donde estamos escribiendo en forma aditiva $\mathbb{F}_p := \{0, 1, \ldots, p-1\}$. El automorfismo σ tiene orden p. En efecto, $\sigma^j(\alpha) = \alpha + j$ para $1 \leq j \leq p-1$, y en consecuencia $\sigma^p(\alpha) = \alpha + p = \alpha$, mientras que $\sigma^j(\alpha) = \alpha + j \neq \alpha$.

Comprobamos que $G(K(\alpha) : K) = \langle\sigma\rangle$. Dado $\psi \in G(K(\alpha) : K)$, y puesto que $f(\alpha) = 0$ y $f \in K[\mathtt{t}]$, se deduce del Lema II.1.1 que también $\psi(\alpha)$ es raíz de f. Por tanto existe $k = [k]_p \in \mathbb{F}_p$ tal que $\psi(\alpha) = \alpha + k = \sigma^k(\alpha)$, es decir $\psi = \sigma^k \in \langle\sigma\rangle$.

(3) El polinomio f factoriza en $K[\mathtt{t}]$ en producto de factores de grado 1 si y sólo si $\alpha \in K$, o lo que es igual, el grupo $G(K(\alpha) : K)$ es trivial. Si no estamos en este caso hemos visto en el apartado anterior que este grupo tiene orden p. Entonces, como $f(\alpha) = 0$ y

$$\deg(f) = p = \operatorname{ord}(G(K(\alpha) : K)) = [K(\alpha) : K],$$

concluimos que $f = P_{K,\alpha}$, y en particular f es irreducible en $K[\mathtt{t}]$.

(4) Por el apartado anterior es suficiente demostrar que f carece de raíces en $\mathbb{F}_p$. Ahora bien, para cada $x \in \mathbb{F}_p$ se tiene $f(x) = x^p - x - a = -a \neq 0$. □

Número V.15 Sean K un cuerpo con 2^{10} elementos y $\alpha \in K^*$ un generador del grupo multiplicativo $K^* := K \setminus \{0\}$. Encontrar un elemento primitivo de cada subextensión de $K|\mathbb{F}_2$.

Solución. Como $[K : \mathbb{F}_2] = \log_2 2^{10} = 10$, el grupo de Galois $G(K : \mathbb{F}_2)$ tiene 10 elementos y está generado por el automorfismo de Frobenius $\phi : K \to K : x \mapsto x^2$.

El grupo cíclico $\langle\phi\rangle$ de orden 10 tiene dos subgrupos, que son $H_1 := \langle\phi^5\rangle$ de orden 2 y $H_2 := \langle\phi^2\rangle$ de orden 5. En consecuencia, la extensión $K|\mathbb{F}_2$ tiene dos subextensiones propias $K_j|\mathbb{F}_2$ para $j = 1, 2$, donde $K_j := \mathrm{Fix}(H_j)$. Buscamos elementos primitivos α_j de las extensiones $K_j|\mathbb{F}_2$.

Debe cumplirse que $\phi^5(\alpha_1) = \alpha_1$ y $\phi^2(\alpha_2) = \alpha_2$, es decir $\alpha_1^{32} = \alpha_1$ y $\alpha_2^4 = \alpha_2$, o lo que es igual, $\alpha_1^{31} = 1$ y $\alpha_2^3 = 1$. Como cada $\alpha_j \neq 1$ y los enteros 3 y 31 son primos, lo anterior equivale a que los órdenes de α_1 y α_2 en K^* sean 31 y 3, respectivamente. Ahora bien, el orden de α es

$$2^{10} - 1 = (2^5 - 1)(2^5 + 1) = 31 \cdot 3 \cdot 11$$

así que $\alpha_1 = \alpha^{33}$ tiene orden 31 y $\alpha_2 = \alpha^{341}$ tiene orden 3. Por tanto, las subextensiones propias de $K|\mathbb{F}_2$ son $\mathbb{F}_2(\alpha^{33})|\mathbb{F}_2$ y $\mathbb{F}_2(\alpha^{341})|\mathbb{F}_2$. □

Número V.16 Demostrar que $f(\mathtt{t}) := \mathtt{t}^4 + 1$ es irreducible como polinomio en $\mathbb{Z}[\mathtt{t}]$ pero es reducible en $\mathbb{F}_p[\mathtt{t}]$ para cada primo p.

Solución. Supongamos que f es reducible en $\mathbb{Z}[\mathtt{t}]$. Como carece de raíces enteras existen $a, b \in \mathbb{Z}$ tales que

$$\mathtt{t}^4 + 1 = (\mathtt{t}^2 + a\mathtt{t} + b)(\mathtt{t}^2 - a\mathtt{t} + b) = \mathtt{t}^4 + (2b - a^2)\mathtt{t}^2 + b^2$$

luego $b^2 = 1$ y $2b = a^2 \geq 0$, así que $b = 1$ y $a^2 = 2$, que es imposible.

Para $p = 2$ se tiene $\mathtt{t}^4 + 1 = (\mathtt{t} + 1)^4$, así que en lo sucesivo suponemos que el primo p es impar, y distinguimos varios casos. Si $p \equiv 1 \bmod 4$ se deduce del Corolario V.2.3 que existe $b \in \mathbb{F}_p$ tal que $b^2 = -1$, y por ello

$$(\mathtt{t}^2 + b)(\mathtt{t}^2 - b) = t^4 - b^2 = \mathtt{t}^4 + 1,$$

luego f es reducible en $\mathbb{F}_p[\mathtt{t}]$. Suponemos ahora que $p \equiv 3 \bmod 4$ y tratamos primero el caso en que $p - 1$ o $p + 1$ es múltiplo de 8. Entonces, por el Corolario V.2.7 existe $a \in \mathbb{F}_p$ tal que $a^2 = 2$, por lo que

$$(\mathtt{t}^2 + a\mathtt{t} + 1)(\mathtt{t}^2 - a\mathtt{t} + 1) = (\mathtt{t}^2 + 1)^2 - a^2\mathtt{t}^2 = (\mathtt{t}^2 + 1)^2 - 2\mathtt{t}^2 = \mathtt{t}^4 + 1,$$

luego f es reducible en $\mathbb{F}_p[\mathtt{t}]$. Sólo falta abordar el caso en que $p \equiv 3 \bmod 4$ y ni $p - 1$ ni $p+1$ son múltiplos de 8. Deducimos de los Corolarios V.2.3 y V.2.7 que $\left(\frac{-1}{p}\right) = -1$ y $\left(\frac{2}{p}\right) = -1$, así que

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

luego existe $a \in \mathbb{F}_p$ tal que $a^2 = -2$. En consecuencia,

$$(\mathtt{t}^2 + a\mathtt{t} - 1)(\mathtt{t}^2 - a\mathtt{t} - 1) = (\mathtt{t}^2 - 1)^2 - a^2\mathtt{t}^2 = (\mathtt{t}^2 - 1)^2 + 2\mathtt{t}^2 = \mathtt{t}^4 + 1,$$

por lo que también en este caso f es reducible en $\mathbb{F}_p[\mathtt{t}]$. □

Número V.17 ¿Tiene alguna raíz el polinomio $f(\mathtt{t}) := \mathtt{t}^2 - [7]_{23} \in \mathbb{F}_{23}[\mathtt{t}]$ en el cuerpo $\mathbb{F}_{23}$?

Solución. Se trata de decidir si el símbolo de Legendre $\left(\frac{7}{23}\right)$ es 1 o -1. Puesto que $23 \equiv 7 \equiv 3 \bmod 4$, se deduce del Corolario V.2.7 y el Teorema V.2.9 que

$$\left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -(-1)^{(7^2-1)/8} = -1,$$

luego f carece de raíces en $\mathbb{F}_{23}$. □

Número V.18 ¿Tiene alguna raíz en el cuerpo finito $\mathbb{F}_{97}$ con 97 elementos el polinomio $f(\mathtt{t}) := \mathtt{t}^2 - [2002]_{97} \in \mathbb{F}_{97}[\mathtt{t}]$?

Solución. Se trata de calcular el símbolo de Legendre $\left(\frac{2002}{97}\right)$. Se tiene

$$2002 = 20 \cdot 97 + 62 \quad \& \quad 97 \equiv 1 \bmod 8,$$

En particular $97 \equiv 1 \bmod 4$, y se deduce de V.2.4 (2.1) y (2.4), el Corolario V.2.7 y la Ley de reciprocidad cuadrática V.2.8, que

$$\left(\frac{2002}{97}\right) = \left(\frac{62}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{31}{97}\right) = \left(\frac{31}{97}\right) = \left(\frac{97}{31}\right) = \left(\frac{3 \cdot 31 + 2^2}{31}\right) = \left(\frac{2}{31}\right)^2 = 1,$$

luego el polinomio f tiene alguna raíz en el cuerpo $\mathbb{F}_{97}$. □

Número V.19 ¿Existe algún número entero x tal que $x^2 + 4x + 3 \equiv 7 \bmod 11$?

Solución. La condición del enunciado equivale a que $x^2 + 4x \equiv 4 \bmod 11$, esto es, $(x+2)^2 \equiv 8 \bmod 11$, y denotando $t := x + 2$ esto equivale a que $t^2 \equiv 8 \bmod 11$. Se trata por tanto de decidir si 8 es un residuo cuadrático $\bmod 11$. Ahora bien, por V.2.4 (2.5) y el Corolario V.2.7,

$$\left(\frac{8}{11}\right) = \left(\frac{2^3}{11}\right) = \left(\frac{2}{11}\right)^3 = (-1)^{3(11^2-1)/8} = (-1)^{45} = -1,$$

luego 8 no es un residuo cuadrático $\bmod 11$, así que la ecuación inicial carece de solución. □

Número V.20 Sean $K := \mathbb{F}_{31}$ y $f(\mathtt{x},\mathtt{y}) := 317\mathtt{x}^2 - 151\mathtt{xy} + 40\mathtt{y}^2$. Decidir si existe algún punto $(a,b) \in K^2$ con alguna coordenada no nula en el que se anula la forma cuadrática f.

Solución. Observamos que $f(\mathtt{x},\mathtt{y}) = 7\mathtt{x}^2 + 4\mathtt{xy} + 9\mathtt{y}^2 \in K[\mathtt{x},\mathtt{y}]$, sin más que dividir entre 31 los coeficientes de f, y como $9 \cdot 7 = 63 \equiv 1 \bmod 31$, remplazamos f por

$$\begin{aligned} g(\mathtt{x},\mathtt{y}) := 9f(\mathtt{x},\mathtt{y}) = \mathtt{x}^2 + 36\mathtt{xy} + 81\mathtt{y}^2 &= (\mathtt{x}+18\mathtt{y})^2 + (81-18^2)\mathtt{y}^2 \\ &= (\mathtt{x}+18\mathtt{y})^2 - 243\mathtt{y}^2 = (\mathtt{x}+18\mathtt{y})^2 + 5\mathtt{y}^2. \end{aligned}$$

Denotando $\mathtt{z} := \mathtt{x}+18\mathtt{y}$ se trata de averiguar si la forma cuadrática $h(\mathtt{z},\mathtt{y}) := \mathtt{z}^2+5\mathtt{y}^2$ se anula en algún punto de K^2 con alguna coordenada no nula. En efecto, si existiese un punto $(a,b) \in K^2 \setminus \{(0,0)\}$ tal que $f(a,b) = 0$, entonces

$$(z,y) := (a+18b,b) \neq (0,0) \quad \& \quad h(z,y) = 0.$$

Necesariamente $y \neq 0$, luego $t := z/y \in K$ es raíz del polinomio $\mathtt{t}^2 + [5]_{31} \in K[\mathtt{t}]$. Esto significa que $\left(\frac{-5}{31}\right) = 1$. Sin embargo, empleando V.2.4 (2.1), (2.4) y (2.6) y el Teorema V.2.9, deducimos que

$$\left(\frac{-5}{31}\right) = \left(\frac{-1}{31}\right) \cdot \left(\frac{5}{31}\right) = (-1)^{(31-1)/2} \left(\frac{31}{5}\right) = (-1)^{15} \left(\frac{1}{5}\right) = -1.$$

Por fin, el origen de coordenadas es el único punto de K^2 en que f se anula. □

Número V.21 ¿Para qué primos p tiene $[-7]_p$ raíz cuadrada en el cuerpo $\mathbb{F}_p$?

Solución. Todos los elementos de $\mathbb{F}_2$ son, por el Lema V.2.1, un cuadrado en $\mathbb{F}_2$, luego -7 tiene raíz cuadrada en $\mathbb{F}_2$. Además, $[-7]_7 = [0]_7$, luego $[-7]_7$ tiene raíz cuadrada en $\mathbb{F}_7$. En lo sucesivo suponemos que el primo p es impar y distinto de 7, y vamos a calcular el símbolo de Legendre

$$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{7}{p}\right) = (-1)^{(p-1)/2} \left(\frac{7}{p}\right), \tag{V.12}$$

donde hemos empleado V.2.4 (2.4) y (2.6). Como $7 \equiv 3 \bmod 4$ se deduce del Teorema V.2.9 que $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$ si $p \equiv 1 \bmod 4$, y en tal caso $(p-1)/2$ es par, mientras que $\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$ si $p \equiv 3 \bmod 4$, y entonces $(p-1)/2$ es impar. En ambos casos se deduce de (V.12) que

$$\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right). \tag{V.13}$$

Denotando r el resto de la división de p entre 7 se deduce de V.2.4 (2.1) y (V.13) que

$$\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right) = \left(\frac{r}{7}\right)$$

para todo primo $p \neq 2, 7$. Los cuadrados no nulos de $\mathbb{F}_7$ son las clases $[1]_7$, $[2]_7$ y $[4]_7$, luego $[-7]_p$ tiene raíz cuadrada en el cuerpo $\mathbb{F}_p$ si y sólo si $p = 2, 7$ o p es congruente mod 7 con 1, 2 o 4. □

Número V.22 Calcular, para cada primo impar $p \neq 3$, el símbolo de Legendre $\left(\frac{3}{p}\right)$.

Solución. Por la Ley de reciprocidad cuadrática,

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{si } p \equiv 1 \bmod 4, \\ -\left(\frac{p}{3}\right) & \text{si } p \equiv 3 \bmod 4. \end{cases}$$

Por otro lado, $[1]_3$ es un cuadrado en $\mathbb{F}_3$, mientras que $[2]_3$ no lo es, es decir,

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \bmod 3, \\ -1 & \text{si } p \equiv 2 \bmod 3. \end{cases}$$

En consecuencia,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \bmod 4 \ \ \& \ \ p \equiv 1 \bmod 3 \ \text{ o si } p \equiv 3 \bmod 4 \ \ \& \ \ p \equiv 2 \bmod 3 \\ -1 & \text{si } p \equiv 1 \bmod 4 \ \ \& \ \ p \equiv 2 \bmod 3 \ \text{ o si } p \equiv 3 \bmod 4 \ \ \& \ \ p \equiv 1 \bmod 3. \end{cases}$$

La expresión anterior se puede simplificar como sigue. Por un lado, p es congruente con 1 módulo 3 y módulo 4 si y sólo si es congruente con 1 módulo 12. Por otro, las condiciones $p \equiv 3 \bmod 4$ y $p \equiv 2 \bmod 3$ equivalen, multiplicando la primera por 3 y la segunda por 4, a que $3p \equiv 9 \bmod 12$ y $4p \equiv 8 \bmod 12$. Esto implica, restando, que $p \equiv -1 \bmod 12$. El recíproco es evidente, esto es, si $p \equiv -1 \bmod 12$, entonces $p+1$ es múltiplo de 3 y de 4, luego $p \equiv 3 \bmod 4$ y $p \equiv 2 \bmod 3$. Esto prueba que

$$\left(\frac{3}{p}\right) = 1 \quad \Longleftrightarrow \quad p \equiv \pm 1 \bmod 12.$$

Obsérvese, por otro lado, que puesto que p no es mútiplo ni de 2 ni de 3, necesariamente es congruente con ± 1 o ± 5 módulo 12, así que

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \bmod 12, \\ -1 & \text{si } p \equiv \pm 5 \bmod 12. \end{cases}$$

□

Número V.23 (1) Sea p un primo tal que $q := 2p + 1$ es primo y $p \equiv 3 \bmod 4$. Demostrar que $2^p \equiv 1 \bmod q$.

(2) ¿Es primo el número $2^{59} - 1$?

Solución. (1) En virtud de V.2.4 (2.3) se tiene $\left(\frac{2}{q}\right) \equiv 2^{(q-1)/2} \equiv 2^p \bmod q$. Por otro lado, existe $s \in \mathbb{Z}$ tal que $p = 3 + 4s$, y así $q = 2p + 1 = 7 + 8s$, por lo que

$$q^2 - 1 = (q-1)(q+1) = 8(q-1)(s+1),$$

y por el Corolario V.2.7 se tiene

$$\left(\frac{2}{q}\right) = (-1)^{(q^2-1)/8} = (-1)^{(q-1)(s+1)} = (-1)^{2p(s+1)} = 1.$$

En conclusión, $2^p \equiv 1 \bmod q$, como pretendemos demostrar.

(2) Como $p = 59$ es primo congruente con 3 $\bmod 4$ y $q = 119 = 2p + 1$ es primo también, se deduce del apartado anterior que $2^{59} - 1 \in q\mathbb{Z}$, luego $2^{59} - 1$ no es primo. □

Número V.24 ¿Para qué primos p existen $x, y \in \mathbb{Z}$ tales que $p = x^2 + 7y^2$?

Solución. Desde luego $7 = 0^2 + 7 \cdot 1^2$, luego $p = 7$ admite una representación como la del enunciado. En lo sucesivo suponemos que $p \neq 7$ y $p = x^2 + 7y^2$ para ciertos $x, y \in \mathbb{Z}$. En tal caso $x, y \neq 0$, y en particular $p \neq 2$. Además $y \notin p\mathbb{Z}$, pues en caso contrario existiría $z \in \mathbb{Z}$ tal que $y = pz$, luego $p = x^2 + 7p^2z^2$. Esto implica que $x^2 = p(1 - 7pz^2) \in p\mathbb{Z}$, por lo que $p|x^2$, así que $p|x$. Existe por tanto $s \in \mathbb{Z}$ tal que $x = ps$, de donde $p = p^2(s^2 + 7z^2)$, lo que es imposible.

Tomando clases $\bmod p$ se tiene $-[x]_p^2 = [7]_p[y]_p^2$, y como $[y]_p \neq 0$, el cociente $t := [x]_p/[y]_p \in \mathbb{F}_p$ cumple que $t^2 = -7$, o lo que es igual, $\left(\frac{-7}{p}\right) = 1$. En virtud del Ejercicio V.21 los números p buscados son $p = 7$ y aquellos primos $p > 7$ congruentes con 1, 2 o 4 $\bmod 7$. □

Número V.25 (1) Sean p un primo impar, $a \in \mathbb{Z} \setminus p\mathbb{Z}$ y $k \geq 2$ un entero. Demostrar que el número de soluciones de la ecuación $\mathtt{x}^2 \equiv a \bmod p$ coincide con el número de soluciones de la ecuación $\mathtt{x}^2 \equiv a \bmod p^k$.

(2) Encontrar las soluciones de la ecuación $\mathtt{x}^2 \equiv 14 \bmod 625$.

Solución. (1) Si la ecuación $\mathtt{x}^2 \equiv a \bmod p$ carece de solución, entonces $x^2 - a \notin p\mathbb{Z}$ para cada entero x, luego $x^2 - a \notin p^k\mathbb{Z}$ para todo $x \in \mathbb{Z}$, es decir, tampoco la ecuación $\mathtt{x}^2 \equiv a \bmod p^k$ tiene solución.

Supongamos ahora que la ecuación $\mathtt{x}^2 \equiv a \bmod p$ tiene alguna solución. Esto significa que el polinomio $\mathtt{t}^2 - [a]_p \in \mathbb{F}_p[\mathtt{t}]$ tiene alguna raíz $\zeta := z + p\mathbb{Z} \in \mathbb{F}_p$, luego tiene exactamente dos raíces, ζ y $-\zeta$, porque el número de raíces es menor o igual que el grado, ya que $\mathbb{F}_p$ es un cuerpo.

Se trata por tanto de demostrar que el polinomio $\mathtt{t}^2 - [a]_{p^k} \in \mathbb{Z}_{p^k}[\mathtt{t}]$ tiene, exactamente, dos raíces en el anillo $\mathbb{Z}_{p^k}$. Comenzamos demostrando que tiene alguna, y antes de nada observemos que $p \not| z$, porque $p \not| a$ y $z^2 - a \in p\mathbb{Z}$.

Sean $\xi := z + \sqrt{a} \in \mathbb{Z}[\sqrt{a}]$ y para cada entero positivo j su potencia j-ésima, que es un elemento del anillo $\mathbb{Z}[\sqrt{a}]$, es decir, existen enteros $u_j, v_j \in \mathbb{Z}$ tales que

$$u_j + v_j\sqrt{a} = (z + \sqrt{a})^j = \xi^j.$$

Se comprueba inmediatamente que la aplicación

$$\tau : \mathbb{Z}[\sqrt{a}] \to \mathbb{Z}[\sqrt{a}],\ \alpha + \beta\sqrt{a} \mapsto \alpha - \beta\sqrt{a}$$

es un homomorfismo de anillos, luego

$$u_j - v_j\sqrt{a} = \tau(u_j + v_j\sqrt{a}) = \big(\tau(z + \sqrt{a})\big)^j = (z - \sqrt{a})^j.$$

Por supuesto, $u_1 = z$ y $v_1 = 1$. Además,

$$\begin{aligned} u_j + v_j\sqrt{a} = \xi^j &= \xi^{j-1} \cdot \xi = (u_{j-1} + v_{j-1}\sqrt{a})(z + \sqrt{a}) \\ &= (zu_{j-1} + av_{j-1}) + (u_{j-1} + zv_{j-1})\sqrt{a}, \end{aligned}$$

y en consecuencia,

$$\begin{cases} u_j &= zu_{j-1} + av_{j-1} \\ v_j &= u_{j-1} + zv_{j-1}. \end{cases} \tag{V.14}$$

En particular, como $p|(a - z^2)$ se deduce que $u_j - zv_j = (a - z^2)v_{j-1} \equiv 0 \bmod p$, mientras que $u_j + zv_j = 2zu_{j-1} + (a + z^2)v_{j-1}$. Vamos a probar, por inducción sobre j, las siguientes igualdades:

$$u_j^2 - av_j^2 \equiv (z^2 - a)^j \equiv 0 \bmod p^j \quad \& \quad u_j + zv_j \equiv (2z)^j \bmod p. \tag{V.15}$$

Para la primera de ellas observamos que, para $j = 1$,

$$u_1^2 - av_1^2 = z^2 - a \equiv 0 \bmod p,$$

y si suponemos probado que $u_{j-1}^2 - av_{j-1}^2 \equiv (z^2 - a)^{j-1} \equiv 0 \bmod p^{j-1}$ entonces, empleando las igualdades (V.14),

$$\begin{aligned} u_j^2 - av_j^2 &= (zu_{j-1} + av_{j-1})^2 - a(u_{j-1} + zv_{j-1})^2 = z^2u_{j-1}^2 + a^2v_{j-1}^2 + 2azu_{j-1}v_{j-1} \\ &\quad - a(u_{j-1}^2 + z^2v_{j-1}^2 + 2zu_{j-1}v_{j-1}) = (z^2 - a)u_{j-1}^2 + (a^2 - az^2)v_{j-1}^2 \\ &= (z^2 - a)(u_{j-1}^2 - av_{j-1}^2). \end{aligned}$$

Como $z^2 - a \equiv 0 \bmod p$ y $u_{j-1}^2 - av_{j-1}^2 \equiv (z^2 - a)^{j-1} \equiv 0 \bmod p^{j-1}$, al multiplicar resulta

$$u_j^2 - av_j^2 \equiv (z^2 - a)(u_{j-1}^2 - av_{j-1}^2) \equiv (z^2 - a)^j \equiv 0 \bmod p^j,$$

que es la primera de las igualdades que queríamos probar.

Para la segunda, que es obvia para $j = 1$, ya que $u_1 = z$ y $v_1 = 1$, suponemos probado que $u_{j-1} + zv_{j-1} \equiv (2z)^{j-1} \bmod p$. Entonces, por (V.14),

$$u_j + zv_j = zu_{j-1} + av_{j-1} + zu_{j-1} + z^2 v_{j-1} = 2zu_{j-1} + (a + z^2)v_{j-1}, \qquad \text{(V.16)}$$

y puesto que $z^2 \equiv a \bmod p$ tenemos $a + z^2 \equiv 2z^2 \bmod p$, lo que sustituido en (V.16) completa el argumento inductivo:

$$\begin{aligned} u_j + zv_j &= 2zu_{j-1} + (a + z^2)v_{j-1} \equiv 2zu_{j-1} + 2z^2 v_{j-1} \\ &\equiv 2z(u_{j-1} + zv_{j-1}) \bmod p \equiv (2z)^j \bmod p. \end{aligned}$$

En particular p no divide a $u_j + zv_j$, pues ya hemos señalado que $p \nmid z$, lo que por ser p primo impar implica que $p \nmid (2z)^j$. Sin embargo hemos demostrado que p divide a $u_j - zv_j$, luego p no divide a la resta $2zv_j = (u_j + zv_j) - (u_j - zv_j)$, y por ello $p \nmid v_j$.

En particular $\mcd(v_j, p^j) = 1$, luego por la Identidad de Bezout existen $a_j, b_j \in \mathbb{Z}$ tales que $1 = a_j p^j + b_j v_j$, es decir, $b_j v_j \equiv 1 \bmod p^j$. Así, multiplicando por b_k la primera de las igualdades (V.15) con $j := k$, y denotando $x_k := b_k u_k$ se tiene

$$x_k^2 = b_k^2 u_k^2 \equiv a b_k^2 v_k^2 \equiv a(b_k v_k)^2 \equiv a \bmod p^k,$$

lo que demuestra que la ecuación $\mathtt{x}^2 \equiv a \bmod p^k$ también tiene solución.

Ya sólo queda comprobar que tiene exactamente dos soluciones. Si denotamos $\eta := x_k + p^k\mathbb{Z}$ a la que hemos encontrado, es obvio que $-\eta = -x_k + p^k\mathbb{Z}$ es otra, y hemos de ver que son las únicas. Antes observamos que $x_k \notin p\mathbb{Z}$. En caso contrario $x_k^2 \in p\mathbb{Z}$, y como $x_k^2 - a \in p^k\mathbb{Z} \subset p\mathbb{Z}$ deducimos que la resta $a = x_k^2 - (x_k^2 - a) \in p\mathbb{Z}$, y esto es falso.

Denotemos $\rho := x + p^k\mathbb{Z}$ una raíz del polinomio $\mathtt{t}^2 - [a]_{p^k} \in \mathbb{Z}_{p^k}[\mathtt{t}]$. Entonces $\rho^2 = [a]_{p^k} = \eta^2$, o sea,

$$(x - x_k)(x + x_k) = x^2 - x_k^2 \in p^k\mathbb{Z} \subset p\mathbb{Z},$$

luego bien $x - x_k \in p\mathbb{Z}$, bien $x + x_k \in p\mathbb{Z}$. Pero no pueden darse ambas condiciones simultáneamente, pues en tal caso la resta $2x_k = (x + x_k) - (x - x_k) \in p\mathbb{Z}$, es decir, $p|x_k$, y ya hemos visto que esto es falso. Por tanto, sin pérdida de generalidad podemos suponer que p no divide a $x + x_k$, lo que unido a la condición $(x - x_k)(x + x_k) \in p^k\mathbb{Z}$ implica que $x - x_k \in p^k\mathbb{Z}$, es decir $\rho = \eta$.

(2) Se trata de un caso particular del apartado (1) donde $p = 5$, $k = 4$ y $a = 14$. Hemos probado que las soluciones son $\pm(x_4 + 625\mathbb{Z})$, donde $x_4 = b_4 u_4$, así que tenemos que calcular b_4 y u_4. Nótese que una solución de la ecuación $\mathtt{x}^2 \equiv 14 \bmod 5$ es $\zeta := 2 + 5\mathbb{Z}$, luego con las notaciones del apartado anterior $z = 2$. Por tanto,

$$u_4 + v_4\sqrt{14} = (2 + \sqrt{14})^4 = 548 + 144\sqrt{14},$$

luego $u_4 = 548$. Además $v_4 = 144$, y una Identidad de Bezout para v_4 y $p^4 = 625$ es $1 = (-47) \cdot 625 + 204 \cdot 144$, es decir, $b_4 = 204$. Al multiplicar, $x_4 = b_4 u_4 = 111792$, y reduciendo $\bmod 5$ obtenemos las soluciones

$$\rho = x_4 + 625\mathbb{Z} = 111792 + 625\mathbb{Z} = 542 + 625 = -83 + 625\mathbb{Z} \quad \& \quad -\rho = 83 + 625\mathbb{Z}.$$

□

Número V.26 Sean K un cuerpo finito de característica distinta de 2 y tres elementos $a, b, c \in K^*$. Demostrar que existen $x, y \in K$ tales que $c = ax^2 + by^2$.

Solución. En virtud del Corolario D.3 del Teorema de Chevalley-Warning la forma cuadrática $f(\mathtt{x}, \mathtt{y}, \mathtt{z}) := a\mathtt{x}^2 + b\mathtt{y}^2 - c\mathtt{z}^2$ tiene alguna solución $(x_0, y_0, z_0) \neq (0, 0, 0)$. Si $z_0 \neq 0$ resulta

$$a(x_0/z_0)^2 + b(y_0/z_0)^2 = (ax_0^2 + by_0^2)/z_0^2 = cz_0^2/z_0^2 = c,$$

luego existen $x := x_0/z_0 \in K$ e $y := y_0/z_0 \in K$ tales que $ax^2 + by^2 = c$.

Supongamos ahora que $z_0 = 0$, lo que implica que $ax_0^2 + by_0^2 = 0$ y $(x_0, y_0) \neq (0, 0)$. De hecho $x_0 \neq 0 \neq y_0$, ya que tanto a como b son no nulos. Entonces $-b/a = (x_0/y_0)^2$, luego existe $t_0 := x_0/y_0 \in K$ tal que $-b/a = t_0^2$, esto es, $b = -at_0^2$, por lo que la ecuación a resolver es

$$c := a\mathtt{x}^2 + b\mathtt{y}^2 = a\mathtt{x}^2 - at_0^2\mathtt{y}^2 = a(\mathtt{x}^2 - t_0^2\mathtt{y}^2) = a(\mathtt{x} - t_0\mathtt{y})(\mathtt{x} + t_0\mathtt{y}).$$

Una solución de esta ecuación es la del sistema de ecuaciones lineales

$$\begin{cases} \mathtt{x} & - & t_0\mathtt{y} & = & 1 \\ \mathtt{x} & + & t_0\mathtt{y} & = & c/a, \end{cases}$$

y al resolverlo obtenemos $x := (1 + c/a)/2$ e $y := (c/a - 1)/2t_0$. □

Número V.27 Sea p un número primo. Determinar el número de puntos del conjunto

$$X := \{(x, y, z) \in \mathbb{F}_p^3 : x^2 + y^2 + z^2 = 0\}.$$

Solución. Tratamos primero el caso $p = 2$. El producto $\mathbb{F}_2^3$ tiene 8 puntos y sólo la mitad están en X; aquéllos en los que el número de coordenadas iguales a 1 es par, esto es,

$$(0, 0, 0),\ (1, 1, 0),\ (1, 0, 1) \quad \& \quad (0, 1, 1).$$

En lo sucesivo suponemos que $p > 2$ y vamos a demostrar que $\mathrm{Card}(X) = p^2$. Para cada pareja $(x, y) \in \mathbb{F}_p^2$ existen a lo sumo dos valores $z \in \mathbb{F}_p$ tales que $x^2 + y^2 + z^2 = 0$.

En efecto, si $a = -(x^2 + y^2)$ es un cuadrado $\mathsf{mod}\ p$ el polinomio $\mathtt{t}^2 - a$ tiene dos raíces $z, -z \in \mathbb{F}_p$ (que son sólo una si $a = 0$), mientras que si a no es un cuadrado $\mathsf{mod}\ p$ el polinomio $\mathtt{t}^2 - a$ no tiene ninguna raíz en $\mathbb{F}_p$ y la ecuación $\mathtt{x}^2 + \mathtt{y}^2 + \mathtt{z}^2 = 0$ carece de solución en $\mathbb{F}_p$.

Abreviaremos lo anterior diciendo que el par (x, y) proporciona, a lo sumo, dos puntos en X. Como en $\mathbb{F}_p^2$ hay p^2 pares (x, y) deducimos que el número n de puntos de X cumple $n \leq 2p^2$.

Además n es múltiplo de p, por el Teorema de Chevalley-Warning D.2, luego $n-p \in p\mathbb{Z}$. Consideramos en el conjunto $Z := X \setminus \{(0,0,0)\}$ la siguiente relación de equivalencia: dos ternas $(x_1,y_1,z_1),(x_2,y_2,z_2) \in Z$ están relacionadas si son proporcionales, esto es, si existe $t \in \mathbb{F}_p^*$ tal que $(x_1,y_1,z_1) = (tx_2,ty_2,tz_2)$. Cada clase de equivalencia consta de $p-1$ elementos, tantos como $\mathbb{F}_p^*$, y si s es el número de clases resulta que $n-1 = s(p-1)$. Por ello

$$n-p = n-1-(p-1) = s(p-1)-(p-1) = (s-1)(p-1),$$

luego $(n-p) \in (p-1)\mathbb{Z}$. Por tanto $n-p$ es múltiplo de p y de $p-1$, así que es múltiplo de su mínimo común múltiplo, que es $p(p-1)$ ya que $\mathrm{mcd}(p,p-1)=1$.

Hemos probado hasta ahora que $n-p$ es un múltiplo de $p(p-1)$ y que es menor o igual que

$$2p^2-p = 2p(p-1)+p < 3p(p-1).$$

Así, $n-p \in \{0,\, p(p-1),\, 2p(p-1)\}$. Veremos que $n-p = p(p-1)$, es decir, $n = p^2$, y para ello comprobaremos que $n-p$ no vale ni 0 ni $2p(p-1)$, esto es, $p \neq n \neq 2p^2-p$.

Si $n = p$ entonces X consiste en las ternas $\{t(a,b,c) : t \in \mathbb{F}_p^*\}$ proporcionales a una solución no nula $(a,b,c) \in X$ y la solución nula. Podemos suponer que $a \neq 0$, y entonces $(-a,b,c) \in X$ pero no es proporcional a la terna (a,b,c); si lo fuera existiría $t \in \mathbb{F}_p^*$ tal que $(-a,b,c) = (ta,tb,tc)$, luego $t=-1$, así que $b=-b$ y $c=-c$. Como $p \neq 2$ esto implica que $b=c=0$, y en consecuencia $a=0$, lo que es falso.

Por tanto $n \geq p+1$, y sólo falta comprobar que $n < 2p^2-p$. Para ello distinguimos dos casos, según que p sea congruente con 1 o $3 \bmod 4$.

Si $p \equiv 1 \bmod 4$, entonces la ecuación $\mathtt{x}^2+\mathtt{y}^2=0$ tiene $2p-1$ soluciones. En efecto, -1 es un resto cuadrático $\bmod p$, por ser $p \equiv 1 \bmod 4$, y en consecuencia el conjunto $R := \{t \in \mathbb{F}_p : t^2 = -1\}$ tiene dos elementos, y las fibras de la aplicación

$$M := \{(x,y) \in \mathbb{F}_p^2 : xy \neq 0 \quad \& \quad x^2+y^2=0\} \to R,\ (x,y) \mapsto x/y$$

tienen $p-1$ elementos, pues dos pares tienen la misma imagen si y sólo si son proporcionales. Esto demuestra que $\mathrm{Card}(M) = 2(p-1)$ y, añadiendo la solución nula, deducimos que hay exactamente $2p-1$ pares (x,y) tales que $x^2+y^2=0$. Para dichos pares el único elemento $z \in \mathbb{F}_p$ tal que $x^2+y^2+z^2=0$ es $z=0$, por lo que la estimación inicial sobre el número de elementos de X se puede mejorar; de los p^2 pares $(x,y) \in \mathbb{F}_p^2$ hay al menos $2p-1$ que sólo proporcionan un elemento en X, que es $(x,y,0)$, luego

$$n \leq 2(p^2-(2p-1))+2p-1 = 2p^2-2p+1 < 2p^2-p.$$

Por último, si $p \equiv 3 \bmod 4$, no existe ninguna terna $(x,0,z) \in X$ con $x \neq 0$, ya que -1 no es un resto cuadrático $\bmod p$ en ese caso. Por eso sólo $p^2-(p-1)$ de los pares $(x,y) \in \mathbb{F}_p^2$ proporcionan una terna $(x,y,z) \in X$, así que

$$n \leq 2(p^2-(p-1)) = 2p^2-2p+2 < 2p^2-p.$$

En consecuencia, para cada primo p se cumple que $\mathrm{Card}(X) = p^2$. □

Número V.28 (Teorema de Erdös-Ginzburg-Ziv) Sean p un número primo y $a_1, \ldots, a_{2p-1} \in \mathbb{Z}$. Demostrar que existe un subconjunto I de $\{1, \ldots, 2p-1\}$ con p elementos tal que $\sum_{i\in I} a_i \equiv 0 \bmod p$.

Solución. Sean $K := \mathbb{F}_p$, $b_i := a_i + p\mathbb{Z} \in K$ y los polinomios $f_1, f_2 \in K[\mathtt{x}_1, \ldots, \mathtt{x}_{2p-1}]$ definidos por

$$f_1(\mathtt{x}) := \sum_{i=1}^{2p-1} \mathtt{x}_i^{p-1} \quad \& \quad f_2(\mathtt{x}) := \sum_{i=1}^{2p-1} a_i \mathtt{x}_i^{p-1}.$$

El término independiente de f_1 y de f_2 es nulo, luego el conjunto

$$\mathcal{Z} = \{x := (x_1, \ldots, x_{2p-1}) \in K^{2p-1} : f_1(x) = 0,\ f_2(x) = 0\}$$

no es vacío, pues contiene al origen $(0, \ldots, 0) \in K^{2p-1}$. Se deduce del Teorema de Chevalley-Warning que $\mathrm{Card}(\mathcal{Z}) \geq p$, y por tanto existe $x := (x_1, \ldots, x_{2p-1}) \in \mathcal{Z}$ alguna de cuyas coordenadas no es nula. El subconjunto I buscado es

$$I = \{1 \leq i \leq 2p-1 :\ x_i \neq 0\},$$

que por lo anterior no es vacío. Como $f_1(x) = 0 = f_2(x)$ se tienen las igualdades

$$\sum_{i\in I} x_i^{p-1} = 0 \quad \& \quad \sum_{i\in I} b_i x_i^{p-1} = 0.$$

Por el Pequeño Teorema de Fermat, $x^{p-1} = 1$ para todo $x \in \mathbb{F}_p^*$, luego las igualdades anteriores se reescriben así:

$$\sum_{i\in I} 1 = 0 \quad \& \quad \sum_{i\in I} b_i = 0.$$

La primera dice que $\mathrm{Card}(I)$ es múltiplo de p y, como $0 < \mathrm{Card}(I) < 2p$, se deduce que $\mathrm{Card}(I) = p$, y la segunda es

$$\sum_{i\in I} (a_i + p\mathbb{Z}) = 0 + p\mathbb{Z},$$

esto es, $\sum_{i\in I} a_i \equiv 0 \bmod p$. □

Soluciones a los ejercicios del Capítulo VI

Número VI.1 Sean m y n enteros positivos primos entre sí y $\zeta_m, \zeta_n \in \mathbb{C}$ raíces primitivas m-ésima y n-ésima de la unidad, respectivamente. Probar la igualdad $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

Solución. Vamos a comprobar en primer lugar que $\zeta := \zeta_m\zeta_n$ es una raíz primitiva mn-ésima de la unidad. En efecto, ζ es raíz mn-ésima de la unidad ya que

$$\zeta^{mn} = ((\zeta_m)^m)^n \cdot ((\zeta_n)^n)^m = 1 \cdot 1 = 1.$$

Por tanto, basta demostrar que el orden de ζ, como elemento del grupo multiplicativo $\mathbb{C}^*$ de los números complejos no nulos, es mn. Ahora bien, como $\mathbb{C}^*$ es abeliano, al aplicar el Lema I.2.6 vol. I, se tiene $o(\zeta_m\zeta_n) = o(\zeta_m)o(\zeta_n) = mn$.

Comprobemos ahora que $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_m, \zeta_n)$. El contenido $\mathbb{Q}(\zeta) \subset \mathbb{Q}(\zeta_m, \zeta_n)$ es evidente, pues $\zeta = \zeta_m\zeta_n$. Para el recíproco, observamos que

$$o(\zeta^m) = o(\zeta)/\operatorname{mcd}(o(\zeta), m) = mn/m = n$$

y, análogamente $o(\zeta^n) = m$, luego $\zeta_m \in \mathcal{U}_m = \langle\zeta^n\rangle$ y $\zeta_n \in \mathcal{U}_n = \langle\zeta^m\rangle$, lo que implica que $\zeta_m \in \mathbb{Q}(\zeta)$ y $\zeta_n \in \mathbb{Q}(\zeta)$. Esto prueba que $\mathbb{Q}(\zeta_m, \zeta_n) \subset \mathbb{Q}(\zeta)$ y con ello la igualdad $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_m, \zeta_n)$.

Denotamos $K := \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$, que es un cuerpo que contiene a $\mathbb{Q}$, y para probar la igualdad del enunciado hemos de demostrar que $[K : \mathbb{Q}] = 1$. Comprobemos que $\mathbb{Q}(\zeta_m) = K(\zeta_m)$. En efecto, es evidente que $\mathbb{Q}(\zeta_m) \subset K(\zeta_m)$ porque $\mathbb{Q} \subset K$, y para el contenido recíproco basta observar que $\mathbb{Q}(\zeta_m)$ contiene tanto a K como a ζ_m.

Como $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_n)$, los polinomios mínimos $P_{\mathbb{Q}(\zeta_n),\zeta_m}$, P_{K,ζ_m} y $P_{\mathbb{Q},\zeta_m}$ cumplen que $P_{\mathbb{Q}(\zeta_n),\zeta_m}$ divide a P_{K,ζ_m} y P_{K,ζ_m} divide a $P_{\mathbb{Q},\zeta_m}$. En consecuencia, si $\varphi : \mathbb{N} \to \mathbb{N}$ es la función de Euler,

$$\begin{aligned}[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta_n)] &= [\mathbb{Q}(\zeta_n)(\zeta_m) : \mathbb{Q}(\zeta_n)] \\ &= \deg(P_{\mathbb{Q}(\zeta_n),\zeta_m}) \leq \deg(P_{K,\zeta_m}) \leq \deg(P_{\mathbb{Q},\zeta_m}) = \varphi(m).\end{aligned} \tag{VI.17}$$

Como m y n son primos entre sí se tiene $\varphi(mn) = \varphi(m)\varphi(n)$, en virtud de la Proposición VI.2.2 vol. I., y así

$$\begin{aligned}[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta_n)] \cdot [\mathbb{Q}(\zeta_n) : \mathbb{Q}] &= [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(mn) \\ &= \varphi(m)\varphi(n) = [\mathbb{Q}(\zeta_m) : \mathbb{Q})] \cdot [\mathbb{Q}(\zeta_n) : \mathbb{Q}].\end{aligned}$$

Simplificando obtenemos la igualdad $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta_n)] = [\mathbb{Q}(\zeta_m) : \mathbb{Q})] = \varphi(m)$, lo que remplazado en (VI.17) nos proporciona

$$\varphi(m) = [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta_n)] \leq \deg(P_{K,\zeta_m}) = [K(\zeta_m) : K] \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m),$$

y de aquí la igualdad $[K(\zeta_m) : K] = \varphi(m)$. Como ya señalamos que $K(\zeta_m) = \mathbb{Q}(\zeta_m)$, resulta finalmente, por la transitividad del grado,

$$[K(\zeta_m) : K] \cdot [K : \mathbb{Q}] = [K(\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m) = [K(\zeta_m) : K],$$

o lo que es igual, $[K : \mathbb{Q}] = 1$. □

Número VI.2 (1) Hallar el polinomio ciclotómico Φ_9 y su grupo de Galois $G_{\mathbb{Q}}(\Phi_9)$.

(2) Sea $L \subset \mathbb{C}$ un cuerpo de descomposición de Φ_9 sobre $\mathbb{Q}$. Expresar como extensiones simples las subextensiones de $L|\mathbb{Q}$ y en cada caso encontrar el polinomio mínimo sobre $\mathbb{Q}$ de un elemento primitivo.

Solución. (1) Como $\Phi_3(\mathtt{t}) = \mathtt{t}^2 + \mathtt{t} + 1$ y, por VI.1.12, $\Phi_9(\mathtt{t}) = \Phi_3(\mathtt{t}^3)$, resulta que

$$\Phi_9(\mathtt{t}) = (\mathtt{t}^3)^2 + \mathtt{t}^3 + 1 = \mathtt{t}^6 + \mathtt{t}^3 + 1.$$

En cuanto al grupo de Galois, se sigue del Teorema VI.1.11 que $G_{\mathbb{Q}}(\Phi_9)$ es isomorfo al grupo multiplicativo $\mathbb{Z}_9^*$ de unidades del anillo $\mathbb{Z}_9$ que, por el Ejercicio VI.20, vol. I, es un grupo cíclico de orden $\varphi(9) = 6$, donde $\varphi : \mathbb{N} \to \mathbb{N}$ es la función de Euler. En consecuencia $G_{\mathbb{Q}}(\Phi_9) = \mathbb{Z}_6$.

(2) El grupo cíclico $\mathbb{Z}_6$ tiene, exactamente, dos subgrupos propios; uno de orden 2 y otro de orden 3, luego $L|\mathbb{Q}$ tiene dos subextensiones propias, una de grado 2 y otra de grado 3. Denotemos $\zeta := e^{2\pi i/9}$, que es una raíz primitiva novena de la unidad. Entonces, $L = \mathbb{Q}(\zeta)$ y $\mathbb{Q}(\zeta^3)|\mathbb{Q}$ es la única subextensión de grado 2 de $L|\mathbb{Q}$, ya que

$$(\zeta^3)^2 + \zeta^3 + 1 = 0 \quad \Longrightarrow \quad P_{\mathbb{Q},\zeta^3}(\mathtt{t}) = \mathtt{t}^2 + \mathtt{t} + 1 = \Phi_2(\mathtt{t}),$$

pues Φ_2 es irreducible en $\mathbb{Q}[\mathtt{t}]$. Por otro lado, $\eta := \zeta + (1/\zeta) \in \mathbb{Q}(\zeta)$ y $\zeta^6 + \zeta^3 + 1 = 0$, así que η es raíz del polinomio $f(\mathtt{t}) := \mathtt{t}^3 - 3\mathtt{t} + 1$, pues

$$\eta^3 = \zeta^3 + 3(\zeta + 1/\zeta) + 1/\zeta^3 = 3\eta + (\zeta^6 + 1)/\zeta^3 = 3\eta - 1.$$

Además f es irreducible en $\mathbb{Z}[\mathtt{t}]$, luego en $\mathbb{Q}[\mathtt{t}]$, pues no tiene raíces enteras. Así, $\mathbb{Q}(\eta)|\mathbb{Q}$ es la única subextensión de grado 3 de $L|\mathbb{Q}$ y $P_{\mathbb{Q},\eta}(\mathtt{t}) = \mathtt{t}^3 - 3\mathtt{t} + 1$. □

Número VI.3 Sean n y k dos números enteros positivos tales que, o bien n es impar o bien tanto n como k son pares. Utilizar, si se desea, el Teorema del número primo de Dirichlet para demostrar que existen números enteros u, v tales que

$$\mathrm{mcd}(u, n) = \mathrm{mcd}(v, n) = 1 \quad \& \quad k = u + v.$$

Solución. Si $n = 1$ basta elegir $u = 1$ y $v = k - 1$. Suponemos $n \geq 2$ y sean $p_1 < \cdots < p_r$ los divisores primos de n. Para $1 \leq i \leq r$ existe un entero k_i tal que $k_i \not\equiv 0, k \bmod p_i$. En efecto, esto es evidente si $p_i > 2$, porque en tal caso $\mathbb{Z}_{p_i}$ tiene al menos 3 elementos, mientras que si $p_1 = 2$ entonces n, y por tanto k, es par, por lo que basta elegir $k_1 = 1$.

Por el Teorema chino de los restos, II.2.5, vol. II, existe un número entero x tal que $x \equiv k_i \bmod p_i$ para $1 \leq i \leq r$. En particular $x \not\equiv 0 \bmod p_i$ para $1 \leq i \leq r$, luego $\mathrm{mcd}(x, n) = 1$. Entonces, por el Teorema del número primo de Dirichlet, la progresión aritmética $\{x + \ell n : \ell \in \mathbb{N}\}$ contiene infinitos primos. En particular, existe $\ell \in \mathbb{N}$ tal que $p := x + \ell n > n$ es primo.

Los enteros $u = p$ y $v = k - p$ cumplen que $k = u + v$ y $\mathrm{mcd}(u, n) = 1$, y sólo falta comprobar que $\mathrm{mcd}(v, n) = 1$. En caso contrario alguno de los primos p_i dividiría a $v = k - p = k - x - \ell n$, luego $p_i | (k - x)$, esto es, $k_i \equiv x \equiv k \bmod p_i$, lo que es falso. □

Número VI.4 ¿Es finito el conjunto formado por los números primos p para los que existe algún entero n tal que $p|(n^2 + 1)$?

Solución. La condición $p|(n^2 + 1)$ para algún entero n equivale a que -1 es un resto cuadrático $\bmod p$, o lo que es lo mismo, en virtud de la Proposición V.2.4 (2.6), $1 = \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, esto es, $p \equiv 1 \bmod 4$. Por la forma débil del Teorema del número primo de Dirichlet, VI.1.14, existen infinitos números primos congruentes con $1 \bmod 4$, por lo que el conjunto de primos del enunciado no es finito. □

Número VI.5 (1) Probar que un primo impar $p \equiv \pm 1 \bmod 5$ si y sólo si 5 es un resto cuadrático $\bmod p$.

(2) Sea p un primo impar. Probar que alguno de los números 2, 5 y 10 es un resto cuadrático $\bmod p$.

(3) Demostrar que existen infinitos números primos impares p tales que 2, 5 y 10 son restos cuadráticos $\bmod p$ y encontrar uno de ellos.

Solución. (1) Como $5 \equiv 1 \bmod 4$ se deduce del Teorema V.2.9 que $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, luego 5 es un resto cuadrático $\bmod p$ si y sólo si p es un resto cuadrático $\bmod 5$. Los restos cuadráticos no nulos $\bmod 5$ son 1 y 4, luego 5 es un resto cuadrático $\bmod p$ si y sólo si $p \equiv \pm 1 \bmod 5$.

(2) Supongamos que ni 2 ni 5 son restos cuadráticos $\bmod p$. Entonces, el símbolo de Legendre $\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right) = -1$, y por V.2.4 (2.4),

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = (-1)^2 = 1,$$

luego 10 es un resto cuadrático $\bmod p$.

(3) Los primos impares p tales que $\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right) = 1$ cumplen también que

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = 1^2 = 1.$$

La condición $\left(\frac{2}{p}\right) = 1$ equivale, por el Corolario V.2.7, a que $p^2 - 1$ sea múltiplo de 16. Además, por el apartado (1), $\left(\frac{5}{p}\right) = 1$ si y sólo si $p \equiv \pm 1 \bmod 5$. El particular,

los primos p tales que $p-1$ es múltiplo de $80 = 16 \cdot 5$ cumplen que

$$p^2 - 1 = (p+1)(p-1) \in 80\mathbb{Z} \subset 16\mathbb{Z} \quad \& \quad p - 1 \in 5\mathbb{Z} \quad \Longrightarrow \quad \left(\frac{2}{p}\right) = 1 = \left(\frac{5}{p}\right).$$

Por la forma débil del Teorema del número primo de Dirichlet, VI.1.14, existen infinitos números primos congruentes con 1 mod 80, y para cualquiera de ellos 2, 5 y 10 son restos cuadráticos mod p. Por ejemplo, $p = 161$ lo cumple. □

Número VI.6 Sea $L_f \subset \mathbb{C}$ un cuerpo de descomposición sobre $\mathbb{Q}$ de un polinomio irreducible $f \in \mathbb{Q}[\mathtt{t}]$. Probar que si $[L_f : \mathbb{Q}]$ es impar entonces $L_f \subset \mathbb{R}$.

Solución. Supongamos, por reducción al absurdo, que $L_f \not\subset \mathbb{R}$. Existe por tanto una raíz $\alpha \in \mathbb{C} \setminus \mathbb{R}$ de f. Como $f \in \mathbb{R}[\mathtt{t}]$ la conjugada de cada raíz de f es también raíz de f, y en consecuencia la restricción

$$\tau : L_f \to L_f,\ z \mapsto \overline{z}$$

a L_f de la conjugación compleja tiene orden 2, pues $\tau^2 = \mathrm{id}$ y $\tau(\alpha) \neq \alpha$. Por ello el orden del grupo de Galois es par, al ser múltiplo del orden de τ, y esto es una contradicción, ya que

$$[L_f : \mathbb{Q}] = \mathrm{ord}(G_K(f)) \in 2\mathbb{Z},$$

contra la hipótesis. □

Número VI.7 Sean K un cuerpo de característica 0 y $f \in K[\mathtt{t}]$ un polinomio irreducible cuyo grupo de Galois $G_K(f)$ es cíclico. Probar que el discriminante $\Delta(f)$ es el cuadrado de un elemento de K si y sólo si el orden de $G_K(f)$ es impar.

Solución. Sean L_f un cuerpo de descomposición de f sobre K y $\delta \in L_f$ una de las dos raíces cuadradas de $\Delta(f)$. Si $\delta \in L_f \setminus K$, entonces el polinomio mínimo de δ sobre K es $\mathtt{t}^2 - \Delta(f)$, y aplicando la transitividad del grado a la torre de cuerpos $K \subset K(\delta) \subset L_f$ resulta

$$\mathrm{ord}(G_K(f)) = [L_f : K] = [L_f : K(\delta)] \cdot [K(\delta) : K] = 2 \cdot [L_f : K(\delta)],$$

luego el orden de $G_K(f)$ es par. Suponemos ahora que el grupo cíclico $G_K(f) = \langle \sigma \rangle$ tiene orden par n y sea $u \in L_f$ una raíz de f. Por tanto, el conjunto de raíces de f en L_f es $\{\sigma^j(u) : 0 \leq j \leq n-1\}$ y una raíz cuadrada del discriminante $\Delta(f)$ en L_f es

$$\delta := \prod_{0 \leq i < j \leq n-1} (\sigma^i(u) - \sigma^j(u)).$$

Hay que probar que $\delta \notin K$ y, como la extensión $L_f|K$ es de Galois con grupo de Galois $G_K(f) = \langle\sigma\rangle$, basta ver que $\sigma(\delta) \neq \delta$, pues $K = \mathrm{Fix}(G_K(f)) = \mathrm{Fix}(\sigma)$. Pero,

$$\begin{aligned}
\sigma(\delta) &= \sigma\Big(\prod_{0\le i<j\le n-1}(\sigma^i(u)-\sigma^j(u))\Big) = \prod_{0\le i<j\le n-1}(\sigma^{i+1}(u)-\sigma^{j+1}(u)) \\
&= \prod_{1\le k<\ell\le n}(\sigma^k(u)-\sigma^\ell(u)) = \prod_{1\le k<\ell\le n-1}(\sigma^k(u)-\sigma^\ell(u)) \prod_{1\le k\le n-1}(\sigma^k(u)-\sigma^n(u)) \\
&= \prod_{1\le k<\ell\le n-1}(\sigma^k(u)-\sigma^\ell(u)) \prod_{1\le k\le n-1}(\sigma^k(u)-\sigma^0(u)) \\
&= (-1)^{n-1}\prod_{1\le k<\ell\le n-1}(\sigma^k(u)-\sigma^\ell(u)) \prod_{1\le \ell\le n-1}(\sigma^0(u)-\sigma^\ell(u)) \\
&= (-1)^{n-1}\prod_{0\le k<\ell\le n-1}(\sigma^k(u)-\sigma^\ell(u)) = -\delta,
\end{aligned}$$

luego $\sigma(\delta) = -\delta \neq \delta$, pues al ser f irreducible $\Delta(f)$ es no nulo. □

Número VI.8 Sean K un cuerpo de característica 0 y $f \in K[\mathtt{t}]$ un polinomio irreducible de grado 3. Sea L_f un cuerpo de descomposición de f sobre K. ¿Qué se puede decir acerca del número de extensiones $L_f|E$ de grado 2, donde $K \subset E \subset L_f$?

Solución. El número de extensiones intermedias de $L_f|K$ de grado 2 coincide con el número de elementos de orden 2 del grupo $G_K(f)$. Hemos visto en la tabla de la Proposición VI.3.2 que dicho grupo es $\mathbb{Z}_3$ o $\mathcal{S}_3$. El primero de estos grupos no tiene ningún elemento de orden 2 y el segundo tiene tres. Así, el número de extensiones intermedias $L_f|E$ de $L_f|K$ de grado 2 es tres o cero. □

Número VI.9 Sean u, v y w las raíces en $\mathbb{C}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^3 - 3\mathtt{t} + 1$. Sean $a := u^2v^2$, $b := u^2w^2$ y $c := v^2w^2$.

(1) Hallar los coeficientes de $g(\mathtt{t}) := (\mathtt{t}-a)(\mathtt{t}-b)(\mathtt{t}-c)$. ¿Es g irreducible en $\mathbb{Q}[\mathtt{t}]$?

(2) Calcular el discriminante de g y el grupo de Galois $G_{\mathbb{Q}}(g)$.

Solución. (1) Las relaciones de Cardano-Vieta aplicadas al polinomio

$$\mathtt{t}^3 - 3\mathtt{t} + 1 = (\mathtt{t}-u)(\mathtt{t}-v)(\mathtt{t}-w)$$

se leen

$$u+v+w = 0, \;\; uv+uw+vw = -3 \quad \& \quad uvw = -1.$$

Por otro lado,

$$g(\mathtt{t}) = \mathtt{t}^3 - (a+b+c)\mathtt{t}^2 + (ab+ac+bc)\mathtt{t} - abc,$$

luego los coeficientes de g valen

$$\begin{aligned} a+b+c &= u^2v^2+u^2w^2+v^2w^2 = (uv+uw+vw)^2-2(u^2vw+v^2uw+w^2uv)\\ &= 9-2uvw(u+v+w) = 9,\\ ab+ac+bc &= u^4v^2w^2+v^4u^2w^2+w^4u^2v^2 = u^2v^2w^2(u^2+v^2+w^2)\\ &= (u+v+w)^2-2(uv+uw+vw) = 6 \quad \&\\ abc &= u^4v^4w^4 = 1, \end{aligned}$$

por lo que $g(\mathtt{t}) = \mathtt{t}^3 - 9\mathtt{t}^2 + 6\mathtt{t} - 1$. Este polinomio carece de raíces enteras, ya que $g(1) = -3$ y $g(-1) = -17$, luego es irreducible en $\mathbb{Z}[\mathtt{t}]$ y por tanto en $\mathbb{Q}[\mathtt{t}]$.

(2) En virtud de la Proposición VII.2.11, vol. II, el discriminante de g coincide con el del polinomio

$$h(\mathtt{t}) := g(\mathtt{t}+3) = \mathtt{t}^3 - 21\mathtt{t} - 37,$$

luego $\Delta(g) = \Delta(h) = 4\cdot 21^3 - 27\cdot 37^2 = 81 = 9^2$. De la tabla de la Proposición VI.3.2 se sigue que $G_{\mathbb{Q}}(g) = \mathbb{Z}_3$. □

Número VI.10 Calcular la resolvente cúbica g de $f(\mathtt{t}) := \mathtt{t}^4 - 2\mathtt{t}^2 - 1$ y el grupo de Galois $G_{\mathbb{Q}}(g)$.

Solución. Para estudiar el grupo de Galois de los polinomios de grado 4 en VI.3.3 introdujimos la resolvente cúbica g del polinomio

$$f(\mathtt{t}) := \mathtt{t}^4 + a\mathtt{t}^3 + b\mathtt{t}^2 + c\mathtt{t} + d$$

definida por

$$g(\mathtt{t}) := \mathtt{t}^3 - 2b\mathtt{t}^2 + (b^2+ac-4d)\mathtt{t} + (da^2+c^2-abc),$$

lo que en nuestro caso nos proporciona el polinomio reducible

$$g(\mathtt{t}) = \mathtt{t}^3 + 4\mathtt{t}^2 + 8\mathtt{t} = \mathtt{t}(\mathtt{t}^2+4\mathtt{t}+8).$$

Como $\mathtt{t}^2+4\mathtt{t}+8 = (\mathtt{t}+2)^2+4$ no tiene raíces reales éste polinomio es irreducible en $\mathbb{Q}[\mathtt{t}]$, así que el discriminante de g, que es el de f, no es un cuadrado en $\mathbb{Q}$, lo que en virtud de la Proposición VI.3.2 implica que el grupo $G_{\mathbb{Q}}(f) \cong \mathbb{Z}_2$. □

Número VI.11 Sean K un cuerpo de característica 0 y para cada $s \in K$ consideramos el polinomio

$$f_s(\mathtt{t}) := \mathtt{t}^3 - s\mathtt{t}^2 + (s-3)\mathtt{t} + 1 \in K[\mathtt{t}].$$

(1) Probar que f_s es reducible en $K[\mathtt{t}]$ si y sólo si existe $u \in K$ tal que

$$u^3 - 3u + 1 = su(u-1).$$

(2) Calcular el discriminante $\Delta(f_s)$ de f_s y demostrar que es el cuadrado de un elemento de K. Deducir que f_s tiene alguna raíz múltiple en un cierre algebraico $\overline{K}$ de K si y sólo si $s^2-3s+9=0$, y que en tal caso $f_s(\mathtt{t})=(\mathtt{t}-s/3)^3$.

(3) Sea $s\in K$ tal que f_s es irreducible en $K[\mathtt{t}]$. Calcular el grupo de Galois $G_K(f_s)$ y demostrar que si α es una raíz de f_s en $\overline{K}$, las otras dos raíces de f_s en $\overline{K}$ se pueden expresar como cocientes de expresiones polinómicas en α cuyos coeficientes no dependen de s.

(4) Sea $L|K$ una extensión de Galois de grado 3. Demostrar que existen $\alpha\in L$ y $s\in K$ tales que $L=K(\alpha)$ y el polinomio mínimo de α sobre K es

$$P_{K,\alpha}(\mathtt{t})=f_s(\mathtt{t})=\mathtt{t}^3-s\mathtt{t}^2+(s-3)\mathtt{t}+1.$$

Solución. (1) Como $\deg(f_s)=3$, es reducible en $K[\mathtt{t}]$ si y sólo si tiene alguna raíz u en K, es decir, existe $u\in K$ tal que $u^3-su^2+(s-3)u+1=0$ o, equivalentemente,

$$u^3-3u+1=su^2-su=su(u-1).$$

(2) Vimos en el Ejemplo VII.2.12, vol. II que denotando $\delta_s:=s^2-3s+9\in K$, el discriminante $\Delta(f_s)$ del polinomio f_s es

$$\begin{aligned}\Delta(f_s)&=-4(s-3)^3+s^2(s-3)^2-18s(s-3)+4s^3-27=-4(s^3-9s^2+27s-27)\\&\quad+s^2(s-3)^2-18(s-3)+4s^3-27\\&=s^4-6s^3+27s^2-54s+81=(s^2-3s+9)^2=\delta_s^2.\end{aligned}$$

Esto prueba que $\Delta(f_s)$ es el cuadrado de un elemento de K. Además, f_s tiene una raíz múltiple en $\overline{K}$ si y sólo su discriminante es nulo, es decir, si y sólo si $s^2-3s+9=0$. En tal caso, $s^2=3s-9$ y $-s^3=-3s^2+9s=-3(3s-9)+9s=27$, por lo que

$$(\mathtt{t}-s/3)^3=\mathtt{t}^3-s\mathtt{t}^2+(s^2/3)\mathtt{t}-s^3/27=\mathtt{t}^3-s\mathtt{t}^2+(s-3)\mathtt{t}+1=f_s.$$

(3) Se deduce directamente de la Proposición VI.3.2 que $G_K(f_s)=\mathbb{Z}_3$, ya que $\delta_s\in K$ y estamos suponiendo que f_s es irreducible en $K[\mathtt{t}]$. Sean $\beta,\gamma\in\overline{K}$ las raíces de f_s distintas de α. Por las Fórmulas de Cardano-Vieta se tiene

$$\left\{\begin{array}{ccccccc}\alpha&+&\beta&+&\gamma&=&s\,,\\ \alpha\beta&+&\alpha\gamma&+&\beta\gamma&=&s-3\\ \alpha\beta\gamma&&&&&=&-1\,.\end{array}\right. \tag{VI.18}$$

De las dos primeras ecuaciones se deduce que

$$\begin{aligned}(\beta+\gamma)(1-\alpha)+\alpha-\beta\gamma&=(\beta+\gamma+\alpha)-\alpha(\beta+\gamma)-\beta\gamma\\&=s-(\alpha\beta+\alpha\gamma+\beta\gamma)=s-(s-3)=3.\end{aligned}$$

Nótese que $\alpha\neq 1$, pues f_s es irreducible en $K[\mathtt{t}]$, lo que nos permite despejar $\beta+\gamma$. De hecho, empleando la igualdad que acabamos de obtener y la tercera de (VI.18)

resulta que

$$\beta+\gamma=\frac{3-\alpha+\beta\gamma}{1-\alpha}=\frac{3-\alpha-1/\alpha}{1-\alpha}=\frac{-\alpha^2+3\alpha-1}{\alpha(1-\alpha)}=\frac{(1-\alpha)(\alpha-1)+\alpha}{\alpha(1-\alpha)}$$
$$=\Big(\frac{\alpha-1}{\alpha}\Big)+\Big(\frac{1}{1-\alpha}\Big).$$

Por tanto, si denotamos $\alpha_1:=(\alpha-1)/\alpha$ y $\alpha_2:=1/(1-\alpha)$, hemos probado que

$$\begin{cases}\beta & + & \gamma & = & \alpha_1 & + & \alpha_2,\\ & & \beta\gamma & = & \alpha_1\alpha_2, & & \end{cases}$$

y esto implica que $\beta=\alpha_1$ y $\gamma=\alpha_2$, o al revés, esto es, las raíces de f_s son α, $(\alpha-1)/\alpha$ y $1/(1-\alpha)$.

(4) Sea $u\in L\setminus K$ un elemento primitivo de la extensión $L|K$. Su polinomio mínimo sobre K tiene grado 3, luego existen $x_1,x_2,x_3\in K$ tales que $u^3=x_1u^2+x_2u+x_3$. Veamos que cada elemento $v\in L\setminus K$ se escribe como $v=(au+b)/(cu+d)$ para cierta matriz

$$A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\mathcal{M}_2(K),\tag{VI.19}$$

cuyo determinante es no nulo. En efecto, como $\{1,u,u^2\}$ es base de L como K-espacio vectorial, existen $z_1,z_2,z_3\in K$ tales que $v=z_1u^2+z_2u+z_3$. La igualdad buscada $v=(au+b)/(cu+d)$ equivale a que

$$\begin{aligned}au+b=v(cu+d)&=(z_1u^2+z_2u+z_3)(cu+d)=z_1cu^3+(dz_1+cz_2)u^2\\&+(dz_2+cz_3)u+dz_3=z_1c(x_1u^2+x_2u+x_3)+(dz_1+cz_2)u^2+(dz_2+cz_3)u\\&+dz_3=(cx_1z_1+dz_1+cz_2)u^2+(cx_2z_1+dz_2+cz_3)u+(cx_3z_1+dz_3).\end{aligned}$$

Por ser $\{1,u,u^2\}$ base de L, lo anterior equivale a

$$\begin{cases}cx_1z_1+dz_1+cz_2 & = & 0\\ cx_2z_1+dz_2+cz_3 & = & a\\ cx_3z_1+dz_3 & = & b\end{cases}\tag{VI.20}$$

Elegimos $c=-z_1$ y $d=z_2+x_1z_1$, lo que hace que se cumpla la primera igualdad del sistema (VI.20) y elegimos a y b para que se satisfagan las igualdades segunda y tercera, es decir,

$$\begin{cases}a & = & cx_2z_1+dz_2+cz_3 & = & -x_2z_1^2+z_2(z_2+x_1z_1)-z_1z_3\\ b & = & cx_3z_1+dz_3 & = & -x_3z_1^2+x_1z_1z_3+z_2z_3\end{cases}$$

A fortiori, $\det(A)\neq 0$, pues en caso contrario los vectores (a,b) y (c,d) de K^2 serían proporcionales, esto es, existiría $\lambda\in K$ tal que $a=\lambda c$ y $b=\lambda d$, por lo que

$$v=(au+b)/(cu+d)=\lambda\in K,$$

y esto es falso. Como la extensión $L|K$ es de Galois de grado 3 su grupo de Galois es cíclico $G(L:K) := \langle\sigma\rangle$ de orden 3, y en particular $\sigma(u) \in L \setminus K$. Por lo que acabamos de probar existe una matriz A como en (VI.19) tal que $\sigma(u) = (au+b)/(cu+d)$.

Por conveniencia notacional denotamos este último cociente por $\sigma(u) = A \cdot u$, y señalemos que es inmediato comprobar que si $B \in \mathcal{M}_2(K)$ es otra matriz cuadrada de orden 2 con determinante no nulo, entonces

$$(AB) \cdot u = A \cdot (B \cdot u).$$

Denotemos $\mathrm{GL}_2(K)$ el grupo multiplicativo de las matrices cuadradas de orden 2 con coeficientes en K y determinante no nulo, $\mathcal{H}$ su subgrupo formado por las matrices de la forma

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \text{ con } \lambda \in K \setminus \{0\},$$

y el cociente $\mathrm{PGL}_2(K) := \mathrm{GL}_2(K)/\mathcal{H}$, que se llama *grupo proyectivo lineal general* sobre K.

Como σ tiene orden 3 también la clase $[A] \in \mathrm{PGL}_2(K)$ tiene orden 3. En efecto, $u = \sigma^3(u) = A^3 \cdot u$, luego $[A]^3 = [I_3]$, donde I_3 es la matriz identidad de orden 2. Esto implica que el orden de $[A] \in \mathrm{PGL}_2(K)$ es 3, pues en caso contrario $[A] = [I_3]$, es decir, $\sigma(u) = A \cdot u = u$, y σ sería la identidad, lo que es falso.

El endomorfismo $\varphi : K^2 \to K^2$ cuya matriz respecto de la base estándar de K^2 es A, no es una homotecia, pues $[A] \neq [I_3]$. En particular, existe un vector $\omega_1 \in K^2$ tal que $\mathcal{B} := \{\omega_1, \omega_2 = \varphi(\omega_1)\}$ es base de K^2, y la matriz de φ respecto de $\mathcal{B}$, definida como aquélla cuyas *filas* son las coordenadas respecto de $\mathcal{B}$ de los vectores $\varphi(\omega_1)$ y $\varphi(\omega_2)$, tiene la forma

$$B := \begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K).$$

Como las matrices A y B son conjugadas en $\mathrm{GL}_2(K)$ también son conjugadas sus clases $[A], [B] \in \mathrm{PGL}_2(K)$, y en particular $[B]$ tiene orden 3. Al calcular B^3 resulta

$$B^3 = B \cdot B^2 = \begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix} \begin{pmatrix} c & d \\ cd & c+d^2 \end{pmatrix} = \begin{pmatrix} cd & c+d^2 \\ c(c+d^2) & 2cd+d^3 \end{pmatrix},$$

y que $[B]$ tenga orden 3 equivale a que $c + d^2 = 0$ y $cd = 2cd + d^3$. La primera de estas condiciones implica la segunda, luego existe $d \in K^* := K \setminus \{0\}$ tal que

$$B = \begin{pmatrix} 0 & 1 \\ -d^2 & d \end{pmatrix}.$$

Como las matrices A y B son semejantes existe una matriz $P \in \mathrm{GL}_2(K)$ tal que $B = PAP^{-1}$. Como P tiene determinante no nulo, $\beta := P \cdot u \in L \setminus K$, luego es un elemento primitivo de la extensión $L|K$ ya que el grado de ésta es primo. Además,

$$\sigma(\beta) = \sigma(P \cdot u) = P \cdot (A \cdot u) = (PA) \cdot u = PA \cdot (P^{-1} \cdot \beta) = (PAP^{-1}) \cdot \beta = B \cdot \beta,$$

es decir, $\sigma(\beta) = 1/(-d^2\beta + d)$. Así, también $\alpha = d\beta$ es elemento primitivo de $L|K$ y vamos a demostrar que su polinomio mínimo sobre K adopta la forma del enunciado. Nótese que

$$\sigma(\alpha) = d\sigma(\beta) = \frac{1}{1-d\beta} = \frac{1}{1-\alpha} \quad \Longrightarrow \quad \sigma^2(\alpha) = \frac{1}{1-\sigma(\alpha)} = \frac{1}{1-\frac{1}{1-\alpha}} = \frac{\alpha-1}{\alpha}.$$

Vamos a comprobar que

$$f(\mathtt{t}) := (\mathtt{t}-\alpha)(\mathtt{t}-\sigma(\alpha))(\mathtt{t}-\sigma^2(\alpha)),$$

pertenece a $K[\mathtt{t}]$, por lo que será el polinomio mínimo de α sobre K, y que $f = f_s$ para un $s \in K$ adecuado. Su término independiente es

$$f(0) = -\alpha \cdot \sigma(\alpha) \cdot \sigma^2(\alpha) = -\alpha \cdot \Big(\frac{1}{1-\alpha}\Big) \cdot \Big(\frac{\alpha-1}{\alpha}\Big) = 1,$$

el coeficiente $-s = -\big(\alpha + \sigma(\alpha) + \sigma^2(\alpha)\big)$ de $\mathtt{t}^2$ de f pertenece a K, al ser invariante por σ, pues

$$\sigma(s) = \sigma\big(\alpha + \sigma(\alpha) + \sigma^2(\alpha)\big) = \sigma(\alpha) + \sigma^2(\alpha) + \sigma^3(\alpha) = \sigma(\alpha) + \sigma^2(\alpha) + \alpha = s,$$

mientras que el coeficiente de $\mathtt{t}$ es

$$\begin{aligned}\alpha\sigma(\alpha) + \alpha\sigma^2(\alpha) + \sigma(\alpha)\sigma^2(\alpha) &= \Big(\frac{\alpha}{1-\alpha}\Big) + (\alpha-1) - \frac{1}{\alpha} = (\alpha-1) \\ &+ \Big(\frac{\alpha-1}{1-\alpha}\Big) + \Big(\frac{1}{1-\alpha}\Big) + \Big(\frac{\alpha-1}{\alpha}\Big) - 1 = \alpha + \Big(\frac{1}{1-\alpha}\Big) \\ &+ \Big(\frac{\alpha-1}{\alpha}\Big) - 3 = \alpha + \sigma(\alpha) + \sigma^2(\alpha) - 3 = s - 3.\end{aligned}$$

En consecuencia, existe $s \in K$ tal que

$$\begin{aligned}P_{K,\alpha}(\mathtt{t}) &= (\mathtt{t}-\alpha)(\mathtt{t}-\sigma(\alpha))(\mathtt{t}-\sigma^2(\alpha)) = \mathtt{t}^3 - \big(\alpha + \sigma(\alpha) + \sigma^2(\alpha)\big)\mathtt{t}^2 \\ &+ \big(\alpha\sigma(\alpha) + \alpha\sigma^2(\alpha) + \sigma(\alpha)\sigma^2(\alpha)\big)\mathtt{t} - \alpha \cdot \sigma(\alpha) \cdot \sigma^2(\alpha) \\ &= \mathtt{t}^3 - s\mathtt{t}^2 + (s-3)\mathtt{t} + 1.\end{aligned}$$

□

Número VI.12 Encontrar polinomios $f \in \mathbb{Q}[\mathtt{t}]$ de grado 3 cuyo grupo de Galois $G_{\mathbb{Q}}(f)$ coincida con los que aparecen en la tabla de la Proposición VI.3.2.

Solución. El polinomio $f_1(\mathtt{t}) := \mathtt{t}(\mathtt{t}-1)(\mathtt{t}+1) = \mathtt{t}^3 - \mathtt{t}$ es reducible en $\mathbb{Q}[\mathtt{t}]$ y su discriminante es $\Delta(f_1) = 4$. Con las notaciones de la Proposición VI.3.2, $\delta = 2 \in \mathbb{Q}$, luego $G_{\mathbb{Q}}(f_1) = \{1\}$.

También es reducible en $\mathbb{Q}[\mathtt{t}]$ el polinomio $f_2(\mathtt{t}) := \mathtt{t}(\mathtt{t}^2+1) = \mathtt{t}^3 + \mathtt{t}$, pero en este caso $\Delta(f_2) = -4$, así que $\delta = 2\sqrt{-1} \notin \mathbb{Q}$, luego $G_{\mathbb{Q}}(f_2) = \mathbb{Z}_2$.

El polinomio $f_3(\mathtt{t}) := \mathtt{t}^3 - 3\mathtt{t} + 1$ es irreducible en $\mathbb{Z}[\mathtt{t}]$, y por tanto en $\mathbb{Q}[\mathtt{t}]$, porque no tiene raíces enteras, ya que $f_3(1) = -1$ y $f_3(-1) = 3$. Además, su discriminante es $\Delta(f_3) = 4 \cdot 3^3 - 27 \cdot 1^2 = 81$, por lo que $\delta = 9 \in \mathbb{Q}$ y, de acuerdo con la Proposición VI.3.2, $G_{\mathbb{Q}}(f_3) = \mathbb{Z}_3$. Hemos elegido este polinomio haciendo $s := 0$ en el polinomio f_s del Ejercicio anterior.

Por fin, $f_4(\mathtt{t}) := \mathtt{t}^3 - 4\mathtt{t} + 1$ es irreducible en $\mathbb{Q}[\mathtt{t}]$ pues $f_4(1) = -2$ y $f_4(-1) = 4$, pero $\Delta(f_4) = 4 \cdot 4^3 - 27 \cdot 1^2 = 229$, luego $\delta := \sqrt{\Delta(f_4)} = \sqrt{229} \notin \mathbb{Q}$ y $G_{\mathbb{Q}}(f_4) = \mathcal{S}_3$. □

Número VI.13 Encontrar una extensión $K|\mathbb{Q}$ de grado 2 y un polinomio $f \in \mathbb{Q}[\mathtt{t}]$ de grado 3 tales que f es irreducible en $K[\mathtt{t}]$ y los grupos de Galois $G_{\mathbb{Q}}(f)$ y $G_K(f)$ no sean isomorfos.

Solución. Elegimos $f := \mathtt{t}^3 - 4\mathtt{t} + 1$, cuyo grupo de Galois $G_{\mathbb{Q}}(f)$ es isomorfo, según hemos probado en el Ejercicio anterior, al grupo simétrico $\mathcal{S}_3$. Tomamos $\delta = \sqrt{229}$, que según hemos visto en el Ejercicio anterior cumple $\delta^2 = \Delta(f)$, y el cuerpo $K := \mathbb{Q}(\delta)$. Nótese que $[K : \mathbb{Q}] = [\mathbb{Q}(\delta) : \mathbb{Q}] = 2$ pues $P_{\mathbb{Q},\delta}(\mathtt{t}) = \mathtt{t}^2 - 229$.

Por último, sea $\alpha \in \mathbb{C}$ una raíz de f. Entonces $f = P_{\mathbb{Q},\alpha}$, por lo que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Como $[\mathbb{Q}(\delta) : \mathbb{Q}] = 2$ y $\mathrm{mcd}(2, 3) = 1$, se deduce del Ejemplo I.2.4 que $[K(\alpha) : K] = 3$, luego $f = P_{K,\alpha}$ y, en particular, f es irreducible en $K[\mathtt{t}]$. Como $\delta = \sqrt{229} \in K$, se desprende de la tabla de la Proposición VI.3.2 que $G_K(f) \cong \mathbb{Z}_3$. □

Número VI.14 Sean p un número primo y supongamos que el grupo de Galois $G_{\mathbb{Q}}(f)$ es cíclico, donde $f(\mathtt{t}) := \mathtt{t}^3 - p\mathtt{t} + p$. Demostrar que $p \equiv 1 \bmod 3$.

Solución. El polinomio f es irreducible en $\mathbb{Z}[\mathtt{t}]$, luego en $\mathbb{Q}[\mathtt{t}]$, por el Criterio de Eisenstein. Por tanto, a la vista de la Proposición VI.3.2, su grupo de Galois sobre $\mathbb{Q}$ es $\mathbb{Z}_3$ o $\mathcal{S}_3$, según que su discriminante $\Delta(f) = 4p^3 - 27p^2$ sea o no el cuadrado de un número racional o, equivalentemente, a la vista del Corolario V.2.12 vol. II, el cuadrado de un número entero. En consecuencia,

$$G_{\mathbb{Q}}(f) \text{ es cíclico} \iff \Delta(f) = p^2(4p - 27) \text{ es el cuadrado de un número entero.}$$

Ahora bien, si existe $z \in \mathbb{Z}$ tal que $p^2(4p - 27) = z^2$, el primo p divide a z^2, luego a z, así que existe $x \in \mathbb{Z}$ tal que $z = px$, por lo que $p^2(4p - 27) = z^2 = p^2x^2$, esto es $4p - 27 = x^2$. Tomando clases $\bmod 3$ resulta

$$p \equiv 4p - 27 \bmod 3 \equiv x^2 \bmod 3.$$

Los elementos que son un cuadrado en $\mathbb{F}_3$ son $0 + 3\mathbb{Z}$ y $1 + 3\mathbb{Z}$. Pero como p es primo, si fuese congruente con $0 \bmod 3$ sería $p = 3$ y $4p - 27 = -15$ no es un cuadrado en $\mathbb{Z}$. En consecuencia, $p \equiv 1 \bmod 3$. □

Número VI.15 Sean K un cuerpo de característica 0 y $f \in K[\mathtt{t}]$ un polinomio de grado 4 cuyo grupo de Galois $G_K(f)$ es el grupo alternado $\mathcal{A}_4$. ¿Cuál es el grupo de Galois sobre K de la resolvente cúbica g del polinomio f?

Solución. Por la tabla en la Proposición VI.3.3, si δ es una raíz cuadrada del discriminante común $\Delta(f) = \Delta(g)$ de f y g, deducimos que g es irreducible en $K[\mathtt{t}]$ y $\delta \in K$. Entonces, por la tabla en la Proposición VI.3.2, $G_K(g) = \mathbb{Z}_3$. □

Número VI.16 Sean $K \subset \mathbb{R}$ un cuerpo y $f \in K[\mathtt{t}]$ un polinomio irreducible de grado 4 que tiene, exactamente, dos raíces reales. Probar que su grupo de Galois $G_K(f)$ es $\mathcal{D}_4$ o $\mathcal{S}_4$.

Solución. Por el Ejercicio VII.13, vol. II, $\Delta(f) < 0$, y en particular $K \subset \mathbb{R}$ no contiene ninguna raíz cuadrada del discriminante de f. Se deduce entonces de la tabla VI.3.3, que $G_K(g)$ es $\mathbb{Z}_4$, $\mathcal{D}_4$ o $\mathcal{S}_4$, y es suficiente descartar la primera opción. Supongamos, por reducción al absurdo, que $G_K(f) = \mathbb{Z}_4$ y sean $u \in \mathbb{R}$ una raíz de f y L_f un cuerpo de descomposición de f sobre K. Entonces,

$$[L_f : K(u)] = \frac{[L_f : K]}{[K(u) : K]} = \frac{\operatorname{ord}(G_K(f))}{\deg(P_{K,u})} = \frac{\operatorname{ord}(\mathbb{Z}_4)}{\deg(f)} = \frac{4}{4} = 1,$$

es decir, $L_f = K(u) \subset \mathbb{R}$, lo que significa que las cuatro raíces de f son reales, contra la hipótesis. □

Número VI.17 Sean $p > 5$ un número primo y $f_p(\mathtt{t}) := \mathtt{t}^4 + p\mathtt{t} + p \in \mathbb{Q}[\mathtt{t}]$. Determinar el grupo de Galois $G_{\mathbb{Q}}(f_p)$.

Solución. El polinomio f_p es irreducible en $\mathbb{Z}[\mathtt{t}]$, luego en $\mathbb{Q}[\mathtt{t}]$, por el Criterio de Eisenstein. Además, su resolvente cúbica es $g_p(\mathtt{t}) := \mathtt{t}^3 - 4p\mathtt{t} + p^2$, según la Proposición VI.3.3. Vamos a demostrar que g_p es irreducible en $\mathbb{Q}[\mathtt{t}]$, lo que equivale a que no tenga raíces enteras. Éstas han de dividir al término independiente, luego las posibles raíces enteras de g_p son $1, -1, p, -p, p^2, -p^2$. Nótese que

$$g_p(1) = 1 - 4p + p^2 = p(p-4) + 1 \neq 0 \quad \& \quad g_p(-1) = -1 + 4p + p^2 = p(p+4) - 1 \neq 0,$$

mientras que al evaluar en $\pm p^2$ se tiene

$$\begin{aligned} g_p(p^2) = p^6 - 4p^3 + p^2 = p^2(p^4 - 4p + 1) = p^2\big(p(p^3 - 4) + 1\big) \neq 0 \quad \& \\ g_p(-p^2) = -p^6 + 4p^3 + p^2 = p^2(-p^4 + 4p + 1) \\ = p^2\big(p(4 - p^3) + 1\big) \neq 0. \end{aligned}$$

Por último, y puesto que estamos suponiendo $p \neq 3, 5$, evaluando en $\pm p$ se obtiene

$$g_p(p) = p^3 - 3p^2 = p^2(p-3) \neq 0 \quad \& \quad g_p(-p) = -p^3 + 5p^2 = p^2(5-p) \neq 0.$$

Por tanto, g_p es irreducible en $\mathbb{Q}[\mathtt{t}]$. En cuanto al discriminante de f_p, que es el de g_p, se tiene

$$\Delta(f_p) = \Delta(g_p) = (-4)(-4p)^3 - 27p^4 = p^3(256 - 27p).$$

Así, si $\Delta(f_p)$ es un cuadrado en $\mathbb{Q}$ lo es en $\mathbb{Z}$, y esto implica que $p|(256 - 27p)$, luego $p|256 = 2^8$, así que $p = 2$, y esto está descartado por hipótesis. En conclusión, para cada primo $p > 5$ el polinomio g_p es irreducible y $\Delta(f_p)$ no es un cuadrado en $\mathbb{Q}$. Se deduce de la Proposición VI.3.3 que el grupo de Galois de f_p sobre $\mathbb{Q}$ es el grupo alternado $\mathcal{A}_4$ de orden 12. □

Número VI.18 Sean K un cuerpo de característica 0 y $E|K$ una extensión de grado 4. Demostrar que las siguientes afirmaciones son equivalentes:

(1) $E|K$ es de Galois y $G(E : K) = \mathbb{Z}_4$.

(2) Existen un elemento primitivo α de la extensión $E|K$ y $a \in K^* := K \setminus \{0\}$, $s, u \in K$ tales que el polinomio mínimo de α sobre K adopta una de las siguientes formas:

$$P_{K,\alpha}(\mathtt{t}) = \mathtt{t}^4 - 4u(4s^2+1)\mathtt{t}^2 + 4u^2(4s^2+1), \text{ o bien } P_{K,\alpha}(\mathtt{t}) = \mathtt{t}^4 - a,$$

la segunda tan sólo en el caso en que -1 es un cuadrado en K.

Solución. (1) $\Longrightarrow$ (2) Sea $E|K$ una extensión de grado 4 con grupo de Galois $\mathbb{Z}_4$. Este grupo posee un único subgrupo propio, que tiene orden 2, luego la extensión $E|K$ posee una única subextensión propia $L|K$, y $[L : K] = 2$, y si σ es un generador de $G(E : K)$, entonces $L = \mathrm{Fix}(\sigma^2)$. Sea $\omega \in L \setminus K$, cuyo polinomio mínimo sobre K es de la forma $P_{K,\omega} := \mathtt{t}^2 - 2b\mathtt{t} + c \in K[\mathtt{t}]$. Entonces $\omega = b \pm \sqrt{b^2 - c}$, luego existe $\Delta := b^2 - c \in K$ tal que $L = K(\omega) = K(\sqrt{\Delta})$. Por la misma razón, existe $\gamma \in L$ que no es un cuadrado en L tal que $E = L(\sqrt{\gamma})$. Vamos a comprobar que $\alpha := \sqrt{\gamma} \in E$ satisface las condiciones del enunciado.

Comenzamos probando que es un elemento primitivo de $E|K$ y calculando su polinomio mínimo sobre K. Como $\{1, \sqrt{\Delta}\}$ es una base de L como K-espacio vectorial, existen $x_1, x_2 \in K$ tales que $\gamma = x_1 + x_2\sqrt{\Delta}$, por lo que

$$(\alpha^2 - x_1)^2 = (\gamma - x_1)^2 = \Delta x_2^2,$$

es decir, el polinomio $f(\mathtt{t}) := (\mathtt{t}^2 - x_1)^2 - \Delta x_2^2 \in K[\mathtt{t}]$ cumple $f(\alpha) = 0$. Para demostrar que f es irreducible en $K[\mathtt{t}]$, y puesto que $\deg(f) = 4 = [E : K]$, es suficiente comprobar que $E = K(\alpha)$. Esto se deduce de que $L|K$ es la única subextensión no trivial de $E|K$ y $L \neq K(\alpha)$ ya que $\alpha \notin L$ porque γ no es un cuadrado en L.

Para terminar la prueba de esta implicación hemos de ver que f adopta la forma del polinomio $P_{K,\alpha}$ del enunciado. Es evidente que $-\alpha$ es también raíz de f y, puesto que σ tiene orden 4, otra raíz de f, distinta de α y $-\alpha$, es $\beta := \sigma(\alpha)$, así que

$$(\mathtt{t}^2 - x_1)^2 - \Delta x_2^2 = f(\mathtt{t}) = (\mathtt{t} - \alpha)(\mathtt{t} + \alpha)(\mathtt{t} - \beta)(\mathtt{t} + \beta) \in K[\mathtt{t}].$$

Esto implica que $\sigma(\beta) = -\alpha$. En efecto, $\sigma(\beta)$ es raíz de f y como $E = K(\beta)$, necesariamente $\sigma(\beta) \neq \beta, -\beta$ porque en caso contrario σ^2 es la identidad. Lo mismo sucede si $\sigma(\beta) = \alpha$, pues entonces $\sigma^2(\beta) = \sigma(\alpha) = \beta$. En consecuencia, $\eta := \alpha\beta$ queda fijo por σ^2, por lo que $L = K(\eta)$, ya que $\sigma(\eta) = \sigma(\alpha)\sigma(\beta) = -\alpha\beta = -\eta$. En particular, existen $z_1, z_2 \in K$ tales que $\eta = z_1 + z_2\sqrt{\Delta}$ y, elevando al cuadrado,

$$z_1^2 + \Delta z_2^2 + 2z_1z_2\sqrt{\Delta} = (z_1 + z_2\sqrt{\Delta})^2 = \eta^2 = \alpha^2\beta^2 = f(0) \in K.$$

Como $\{1, \sqrt{\Delta}\}$ son K-linealmente independientes, lo anterior implica que $z_1z_2 = 0$. Pero $z_2 \neq 0$ pues en caso contrario $\eta = z_1 \in K$, y esto es falso ya que $\sigma(\eta) = -\eta \neq \eta$. Así, $z_1 = 0$, luego

$$\Delta z_2^2 = f(0) = x_1^2 - \Delta x_2^2 \quad \Longrightarrow \quad \Delta(x_2^2 + z_2^2) = x_1^2. \tag{VI.21}$$

Si $x_2^2 + z_2^2 \neq 0$ definimos $s := x_2/2z_2 \in K$ y $u := x_1z_2^2/2(x_2^2 + z_2^2) \in K$. Entonces, los coeficientes del polinomio $P_{K,\alpha}$ del enunciado son

$$\begin{aligned} 4u(4s^2 + 1) = (2x_1z_2^2)(1 + x_2^2/z_2^2)/(x_2^2 + z_2^2) = 2x_1 \quad \& \\ 4u^2(4s^2 + 1) = 2ux_1 = x_1^2z_2^2/(x_2^2 + z_2^2) = x_1^2 - \Delta x_2^2, \end{aligned}$$

y así resulta la igualdad anunciada

$$\begin{aligned} f(\mathtt{t}) = (\mathtt{t}^2 - x_1)^2 - \Delta x_2^2 &= \mathtt{t}^4 - 2x_1\mathtt{t}^2 + (x_1^2 - \Delta x_2^2) \\ &= \mathtt{t}^4 - 4u(4s^2 + 1)\mathtt{t}^2 + 4u^2(4s^2 + 1) = P_{K,\alpha}(\mathtt{t}). \end{aligned}$$

Analizamos ahora el caso en que $x_2^2 + z_2^2 = 0$. Ya hemos probado que $z_2 \neq 0$, así que $(x_2/z_2)^2 = -1$, luego este caso sólo se presenta si -1 es un cuadrado en K. De la igualdad (VI.21) se sigue que $x_1 = 0$, por lo que denotando $a := \Delta x_2^2 \in K$ el polinomio mínimo de α sobre K es $f(\mathtt{t}) := \mathtt{t}^4 - a$.

(2) $\Longrightarrow$ (1) Se trata de probar que si existe un elemento primitivo α de la extensión $E|K$ cuyo polinomio mínimo sobre K tiene la forma del enunciado, entonces el grupo de Galois $G(E : K)$ es cíclico de orden 4. Si $P_{K,\alpha}(\mathtt{t}) := \mathtt{t}^4 - a$, donde $a \in K^*$ y existe $i \in K$ tal que $i^2 = -1$, las raíces de $P_{K,\alpha}$ en un cierre algebraico de K son $\alpha, -\alpha, \alpha i$ y $-\alpha i$. El K-automorfismo σ de E que cumple $\sigma(\alpha) = \alpha i$ tiene orden 4, ya que $\sigma(i) = i$, pues $i \in K$, y por ello $\sigma^2(\alpha) = \sigma(\alpha i) = \sigma(\alpha)i = -\alpha$.

Suponemos ahora que -1 no es un cuadrado en K y existen $\alpha \in E$ y $s, u \in K$ tales que $E = K(\alpha)$ y el polinomio mínimo de α sobre K es

$$P_{K,\alpha}(\mathtt{t}) := \mathtt{t}^4 - 4u(4s^2 + 1)\mathtt{t}^2 + 4u^2(4s^2 + 1).$$

Nótese que $\rho := \sqrt{4s^2 + 1} \in E \setminus K$, pues en caso contrario

$$\begin{aligned} P_{K,\alpha}(\mathtt{t}) &= (\mathtt{t}^2 - 2u(4s^2 + 1))^2 - 16\rho^2s^2u^2 \\ &= (\mathtt{t}^2 - 2u(4s^2 + 1) - 4\rho su)(\mathtt{t}^2 - 2u(4s^2 + 1) + 4\rho su), \end{aligned} \tag{VI.22}$$

y $P_{K,\alpha}$ sería reducible en $K[\mathtt{t}]$, lo cual es falso.

Empleando la fórmula para el discriminante de un polinomio de grado 4 que aparece en VII.2.12, vol. II, el del polinomio $P_{K,\alpha}$ resulta ser

$$\Delta(P_{K,\alpha}) = \left(2^9 \cdot u^3 s^2 (4s^2+1)\right)^2 (4s^2+1),$$

que no es un cuadrado en K, ya que $\rho = \sqrt{4s^2+1} \in E \setminus K$.

Además, si denotamos $\delta_1 := 2^9 \cdot \rho u^3 s^2 (4s^2+1)$ una raíz del discriminante $\Delta(P_{K,\alpha})$, se deduce de (VI.22) que el polinomio $P_{K,\alpha}$ es reducible en $K(\delta_1)[\mathtt{t}]$, luego por la Proposición VI.3.3 el grupo de Galois de la extensión $E|K$ es $\mathbb{Z}_4$. □

Número VI.19 Sea $E|K$ una extensión de cuerpos de grado 4. Demostrar que las siguientes afirmaciones son equivalentes:

(1) $E|K$ es de Galois y $G(E:K) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

(2) Existen un elemento primitivo α de la extensión $E|K$ y $s, u \in K$ tales que

$$P_{K,\alpha}(\mathtt{t}) = \mathtt{t}^4 - 2(s+u)\mathtt{t}^2 + (s-u)^2.$$

Solución. (1) $\Longrightarrow$ (2) Supongamos que $E|K$ es una extensión de Galois cuyo grupo de Galois es $G(E:K) = \mathbb{Z}_2 \times \mathbb{Z}_2$. Este grupo tiene tres elementos de orden 2, luego se deduce del Teorema fundamental de la teoría de Galois que $E|K$ admite tres subextensiones de grado 2. Consideramos dos de ellas $L|K$ y $F|K$, y sean $s, u \in K$ que no son cuadrados en K tales que $L := K(\sqrt{s})$ y $F := K(\sqrt{u})$. Se deduce del Ejercicio II.4 que $\alpha := \sqrt{s} + \sqrt{u}$ es un elemento primitivo de $E|K$, y elevando al cuadrado,

$$s = (\alpha - \sqrt{u})^2 = \alpha^2 + u - 2\alpha\sqrt{u} \quad \Longrightarrow \quad 2\alpha\sqrt{u} = \alpha^2 + u - s.$$

Elevando al cuadrado de nuevo se tiene

$$4u\alpha^2 = (\alpha^2 + u - s)^2 = \alpha^4 + 2(u-s)\alpha^2 + (u-s)^2.$$

Por tanto, α es raíz del polinomio

$$f(\mathtt{t}) := \mathtt{t}^4 - 2(s+u)\mathtt{t}^2 + (s-u)^2 \in K[\mathtt{t}],$$

y de hecho $f = P_{K,\alpha}$ es el polinomio mínimo de α sobre K puesto que

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

(2) $\Longrightarrow$ (1) Supongamos ahora que $E|K$ es una extensión de grado 4 y que existe un elemento primitivo α de $E|K$ cuyo polinomio mínimo sobre K es

$$P_{K,\alpha}(\mathtt{t}) := \mathtt{t}^4 - 2(s+u)\mathtt{t}^2 + (s-u)^2$$

para ciertos $s, u \in K$. El discriminante del polinomio $P_{K,\alpha}$ es, por VII.2.12, vol. II,

$$\begin{aligned}\Delta(P_{K,\alpha}) &= 256(s-u)^6 - 512(s+u)^2(s-u)^4 + 256(s+u)^4(s-u)^2 \\ &= 256(s-u)^2((s-u)^2 - (s+u)^2)^2 = \delta^2,\end{aligned}$$

donde $\delta := 16(s-u)((s-u)^2-(s+u)^2)$. Además, la resolvente cúbica de f es, por VI.3.3,

$$g(\mathtt{t}) := \mathtt{t}^3 - 4(s+u)\mathtt{t}^2 + 8su\mathtt{t} = \mathtt{t}\big(\mathtt{t}^2 - 4(s+u)\mathtt{t} + 8su\big),$$

que es reducible en $K[\mathtt{t}]$, y por la Proposición VI.3.3, $G(E:K) = \mathbb{Z}_2 \times \mathbb{Z}_2$. □

Número VI.20 Calcular el grupo de Galois $G_{\mathbb{Q}}(f_i)$ para $i = 1, 2$, donde

$$f_1(\mathtt{t}) := \mathtt{t}^4 + 3\mathtt{t}^3 - 3\mathtt{t} - 2 \quad \& \quad f_2(\mathtt{t}) := \mathtt{t}^4 + \mathtt{t}^2 - 2\mathtt{t} + 1.$$

Solución. Veamos que el polinomio f_1 es irreducible en $\mathbb{Z}[\mathtt{t}]$ y, por tanto, en $\mathbb{Q}[\mathtt{t}]$. Como $f_1(1) = -1 = f_1(-1)$ mientras que $f_1(2) = 32$ y $f_1(-2) = -4$, deducimos que f_1 no tiene raíces enteras. Por ello, si f_1 fuese reducible en $\mathbb{Z}[\mathtt{t}]$ existirían números enteros a, b, c y d tales que

$$f_1(\mathtt{t}) := (\mathtt{t}^2 + a\mathtt{t} + b)(\mathtt{t}^2 + c\mathtt{t} + d) \implies \begin{cases} a + c = 3 \\ ac + b + d = 0 \\ ad + bc = -3 \\ bd = -2 \end{cases}$$

De la primera igualdad se deduce que a o c es par, luego también lo es $b + d = -ac$, así que, b y d tienen la misma paridad. Esto es incompatible con la igualdad $bd = -2$, ya que si b y d son impares su producto también lo es, mientras que si son pares su producto es múltiplo de 4.

Empleando la Proposición VI.3.3 la resolvente cúbica de f_1 es $g_1(\mathtt{t}) := \mathtt{t}^3 - \mathtt{t} - 9$, cuyo discriminante, que coincide con el de f_1 vale, según el Ejemplo VII.2.12, vol. II,

$$\Delta(f_1) = \Delta(g_1) = 4 - 27 \cdot 9^2 < 0 \implies \delta_1 = \sqrt{\Delta(f_1)} \notin \mathbb{Q}.$$

Además g_1 es irreducible en $\mathbb{Z}[\mathtt{t}]$, luego en $\mathbb{Q}[\mathtt{t}]$, pues tiene grado 3 y no tiene raíces enteras. En efecto, $g_1(1) = -9 = g_1(-1)$, $g_1(3) = 15$, $g_1(-3) = -33$, $g_1(9) = 711$ y $g_1(-9) = -729$.

Por ser f_1 y g_1 irreducibles en $\mathbb{Q}[\mathtt{t}]$ y $\delta_1 \notin \mathbb{Q}$, se sigue de la tabla que aparece en la Proposición VI.3.3 que $G_{\mathbb{Q}}(f_1) = \mathcal{S}_4$.

Respecto del polinomio f_2, que carece de raíces enteras puesto que $f_2(1) = 1$ y $f_2(-1) = 5$, es irreducible en $\mathbb{Z}[\mathtt{t}]$, luego también en $\mathbb{Q}[\mathtt{t}]$. En caso contrario, y puesto que el coeficiente de $\mathtt{t}^3$ en f_2 es nulo, existirían $a, b, c \in \mathbb{Z}$ tales que

$$f_2(\mathtt{t}) := (\mathtt{t}^2 + a\mathtt{t} + b)(\mathtt{t}^2 - a\mathtt{t} + c) \implies \begin{cases} b + c - a^2 = 1 \\ a(b-c) = 2 \\ bc = 1 \end{cases}$$

Esto no es posible, pues la tercera igualdad implica que $b = c = \pm 1$, por lo que $2 = a(b-c) = 0$. La resolvente cúbica g_2 de f_2 es reducible en $\mathbb{Q}[\mathtt{t}]$ ya que, por VI.3.3,

$$g_2(\mathtt{t}) := \mathtt{t}^3 - 2\mathtt{t}^2 - 3\mathtt{t} + 4 = (\mathtt{t} - 1)(\mathtt{t}^2 - \mathtt{t} - 4).$$

Por último, el discriminante de f vale $\Delta(f_2) = -235 < 0$, por el Ejemplo VII.2.12, vol. II, por lo que $\delta_2 := \sqrt{\Delta(f_2)} \notin \mathbb{Q}$. Se sigue de la Proposición VI.3.3 que $G_{\mathbb{Q}}(f_2) = \mathcal{D}_4$. □

Número VI.21 Encontrar polinomios irreducibles $f \in \mathbb{Q}[\mathtt{t}]$ de grado 4 cuyo grupo de Galois $G_{\mathbb{Q}}(f)$ coincida con los que aparecen en la tabla de la Proposición VI.3.3.

Solución. Vimos en VII.2.12, vol. II que el discriminante del polinomio,

$$f(\mathtt{t}) := \mathtt{t}^4 + b\mathtt{t}^2 + c\mathtt{t} + d \in \mathbb{Q}[\mathtt{t}]$$

viene dado por

$$\Delta(f) = 256d^3 - 128b^2d^2 + 144bc^2d + 16b^4d - 4b^3c^2 - 27c^4,$$

y por la Proposición VI.3.3 su resolvente cúbica es

$$g(\mathtt{t}) := \mathtt{t}^3 - 2b\mathtt{t}^2 + (b^2 - 4d)\mathtt{t} + c^2 \in \mathbb{Q}[\mathtt{t}].$$

Vimos en VI.2.13, vol. II, que el polinomio $f(\mathtt{t}) := \mathtt{t}^4 - 10\mathtt{t}^2 + 1$ es irreducible en $\mathbb{Q}[\mathtt{t}]$. Este polinomio es de la forma $f(\mathtt{t}) := \mathtt{t}^4 - 2(s+u)\mathtt{t}^2 + (s-u)^2$ con $s := 3$ y $u := 2$, luego $G_{\mathbb{Q}}(f) = \mathbb{Z}_2 \times \mathbb{Z}_2$, según hemos probado en el Ejercicio VI.19.

Consideremos ahora el polinomio $f := \mathtt{t}^4 - 20\mathtt{t}^2 + 20$ que es irreducible en $\mathbb{Z}[\mathtt{t}]$ por el Criterio de Eisenstein, y por tanto en $\mathbb{Q}[\mathtt{t}]$, que se obtiene para los valores $s = u = 1$ en el polinomio

$$\mathtt{t}^4 - 4u(4s^2+1)\mathtt{t}^2 + 4u^2(4s^2+1) \in \mathbb{Q}[\mathtt{t}]$$

del Ejercicio VI.18. En virtud de lo probado en dicho Ejercicio, $G_{\mathbb{Q}}(f) = \mathbb{Z}_4$.

Además, hemos probado en el Ejercicio VI.20 que el grupo de Galois $G_{\mathbb{Q}}(f)$ del polinomio $f(\mathtt{t}) := \mathtt{t}^4 + \mathtt{t}^2 - 2\mathtt{t} + 1$ es isomorfo al grupo diedral $\mathcal{D}_4$ de orden 8, y según vimos en el Ejercicio VI.17, $G_{\mathbb{Q}}(f) = \mathcal{A}_4$ para el polinomio $f(\mathtt{t}) := \mathtt{t}^4 + 7\mathtt{t} + 7 \in \mathbb{Q}[\mathtt{t}]$.

Finalmente, el grupo de Galois $G_{\mathbb{Q}}(f)$ del polinomio $f(\mathtt{t}) := \mathtt{t}^4 + 3\mathtt{t}^3 - 3\mathtt{t} - 2$ es el grupo simétrico $\mathcal{S}_4$, según hemos visto en el Ejercicio VI.20. □

Número VI.22 Sean K un cuerpo de característica 0 y $a, b \in K$ tales que el polinomio $f(\mathtt{t}) := \mathtt{t}^4 + a\mathtt{t}^2 + b$ es irreducible en $K[\mathtt{t}]$. Hallar, en función de los valores de a y b, el grupo de Galois de f sobre K.

Solución. La resolvente cúbica de f es $g(\mathtt{t}) = \mathtt{t}^3 - 2a\mathtt{t}^2 + (a^2 - 4b)\mathtt{t},$, por VI.3.3, que es reducible en $K[\mathtt{t}]$. Se deduce entonces de la tabla de la Proposición VI.3.3 que $G_K(f)$ es uno de los siguientes tres grupos: $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ o el diedral $\mathcal{D}_4$. Además, $\Delta(f) = 16b(4b - a^2)^2$, en virtud de VII.2.12 vol. II. Por tanto, si b es un cuadrado

en K también $\Delta(f)$ lo es y se deduce de la tabla en VI.3.3 que $G_K(f) = \mathbb{Z}_2 \times \mathbb{Z}_2$. Suponemos en lo sucesivo que b no es un cuadrado en K, por lo que tampoco $\Delta(f)$ lo es, así que $G_K(f)$ es $\mathbb{Z}_4$ o $\mathcal{D}_4$.

Para decidir cuál de estos dos grupos es $G_K(f)$ hemos de estudiar la irreducibilidad de f en $K(\delta)[\mathtt{t}]$, donde $\delta := 4\sqrt{b}(4b - a^2)$ es una de las raíces cuadradas de $\Delta(f)$. La reducibilidad de f equivale a que sea producto de dos factores de grado 2 o que tenga una raíz, digamos $u \in K(\delta)$. Pero entonces, como f es irreducible en $K[\mathtt{t}]$,

$$4 = \deg(f) = \deg(P_{K,u}) = [K(u) : K] \leq [K(\delta) : K] = 2,$$

que es falso. Se trata por tanto de estudiar bajo qué condiciones f es producto de dos polinomios de grado 2 en $K(\delta)[\mathtt{t}]$. Nótese que $K(\delta) = K(\sqrt{b})$, y factorizamos f completando cuadrados:

$$f(\mathtt{t}) = (\mathtt{t}^2 + a/2)^2 - (a^2 - 4b)/4 = (\mathtt{t}^2 + a/2 - \sqrt{a^2 - 4b}/2)(\mathtt{t}^2 + a/2 + \sqrt{a^2 - 4b}/2).$$

Sean $\overline{K}$ un cierre algebraico de K y $c \in \overline{K}$ tal que $c^2 = a^2 - 4b$. Así,

$$f(\mathtt{t}) = (\mathtt{t}^2 + a/2 - c/2)(\mathtt{t}^2 + a/2 + c/2).$$

Por tanto, atendiendo a la tabla de VI.3.3, se tiene:

$$\begin{aligned} G_K(f) = \mathbb{Z}_4 &\iff f \text{ es reducible en } K(\sqrt{b})[\mathtt{t}] \\ &\iff c \in K(\sqrt{b}) \iff \sqrt{a^2 - 4b} \in K(\sqrt{b}). \end{aligned}$$

Finalmente, el grupo $G_K(f)$ se calcula de acuerdo a la siguiente tabla:

$\sqrt{b} \in K$	$\sqrt{a^2 - 4b} \in K(\sqrt{b})$	$G_K(f)$
SI	–	$\mathbb{Z}_2 \times \mathbb{Z}_2$
NO	SI	$\mathbb{Z}_4$
NO	NO	$\mathcal{D}_4$

□

Número VI.23 Sean $f_1(\mathtt{t}) := \mathtt{t}^4 - 2\mathtt{t}^2 + 2, f_2(\mathtt{t}) := \mathtt{t}^3 + 9\mathtt{t} + 18$, L_i el cuerpo de descomposición de f_i sobre $\mathbb{Q}$ y L el menor subcuerpo de $\mathbb{C}$ que contiene a L_1 y L_2.

(1) Probar que el grupo de Galois $G_{\mathbb{Q}}(f_1)$ es isomorfo al grupo diedral $\mathcal{D}_4$ de orden 8.

(2) Sean v y w dos raíces de f_1 en L_1 que no son opuestas. Calcular el polinomio mínimo de w sobre $\mathbb{Q}(v)$.

(3) Probar que f_2 tiene tres raíces distintas u_1, u_2 y u_3 en L_2, que el grupo de Galois $G_{\mathbb{Q}}(f_2) \cong \mathcal{S}_3$ y que $G_{L_1}(f_2)$ es isomorfo a $\mathbb{Z}_3$.

(4) Demostrar que $[L:\mathbb{Q}] = 24$.

(5) Probar que $L_1|\mathbb{Q}$ es la única subextensión de $L|\mathbb{Q}$ de grado 8.

(6) Demostrar que $\mathbb{Q}(u_i)|\mathbb{Q}$, con $i = 1, 2, 3$ son todas las subextensiones de grado 3 de la extensión $L|\mathbb{Q}$.

(7) Demostrar que existe un único automorfismo $\rho \in G(L:\mathbb{Q})$ tal que $\rho(v) = w$, $\rho(w) = -v$ y $\rho(u_1) = u_2$. Calcular el grado $[F:\mathbb{Q}]$, donde $F = \mathrm{Fix}(\rho)$ es el cuerpo fijo de ρ.

(8) Hallar un elemento primitivo θ de la extensión $F|\mathbb{Q}$ y el polinomio mínimo de θ sobre $\mathbb{Q}$.

Solución. (1) Aplicamos los resultados que arroja la tabla del ejercicio anterior. En nuestro caso $a = -2$ y $b = 2$, por lo que $\sqrt{b} = \sqrt{2} \notin \mathbb{Q}$ y $\sqrt{a^2 - 4b} = \sqrt{-4} \notin \mathbb{Q}(\sqrt{b})$, por lo que $G_{\mathbb{Q}}(f_1) \cong \mathcal{D}_4$.

(2) Las raíces de f_1 son $v, -v, w$ y $-w$, así que $L_1 = \mathbb{Q}(v, w)$, luego

$$\begin{aligned} 8 = \mathrm{ord}(\mathcal{D}_4) = [L_1:\mathbb{Q}] &= [\mathbb{Q}(v)(w):\mathbb{Q}(v)] \cdot [\mathbb{Q}(v):\mathbb{Q}] \\ &= [\mathbb{Q}(v)(w):\mathbb{Q}(v)] \cdot \deg(f_1) = 4 \cdot [\mathbb{Q}(v)(w):\mathbb{Q}(v)], \end{aligned}$$

de donde $[\mathbb{Q}(v)(w):\mathbb{Q}(v)] = 2$, esto es, el polinomio mínimo $P_{\mathbb{Q}(v),w}$ de w sobre $\mathbb{Q}(v)$ tiene grado 2. Por otro lado, v^2 y w^2 son las raíces del polinomio $\mathtt{t}^2 - 2\mathtt{t} + 2$, luego $w^2 + v^2 = 2$, así que w es raíz del polinomio $h(\mathtt{t}) := \mathtt{t}^2 + v^2 - 2 \in \mathbb{Q}(v)[\mathtt{t}]$, que tiene grado 2. En conclusión, $P_{\mathbb{Q}(v),w} = h$.

(3) El polinomio f_2 es irreducible en $\mathbb{Q}[\mathtt{t}]$, lo que garantiza que posee tres raíces distintas en L_2. Para verlo basta observar que

$$g(\mathtt{x}) = f_2(3\mathtt{x}) = 27\mathtt{x}^3 + 27\mathtt{x} + 18 = 9(3\mathtt{x}^3 + 3\mathtt{x} + 2)$$

y el polinomio $3\mathtt{x}^3 + 3\mathtt{x} + 2$ es irreducible en $\mathbb{Z}[\mathtt{x}]$, por el Criterio de Eisenstein modificado, VI.2.8, vol. II. Esto implica que es irreducible en $\mathbb{Q}[\mathtt{x}]$, así que también $g(\mathtt{x})$ lo es, luego f_2 es irreducible en $\mathbb{Q}[\mathtt{t}]$. En caso contrario tendría una raíz $q \in \mathbb{Q}$, por lo que $g(q/3) = f_2(q) = 0$, contra la irreducibilidad de g en $\mathbb{Q}[\mathtt{x}]$. Ahora, para calcular el grupo de Galois $G_{\mathbb{Q}}(f_2)$ empleamos la tabla de VI.3.2. Vimos en el Ejemplo VII.2.12 (2), vol. II que el discriminante del polinomio $\mathtt{t}^3 + p\mathtt{t} + q$ es $\Delta = -4p^3 - 27q^2$, luego en nuestro caso

$$\Delta(f_2) = -4 \cdot 9^3 - 27 \cdot 18^2 = -16 \cdot 3^6 = -108^2,$$

una de cuyas raíces cuadradas es $\delta = 108i$, donde $i := \sqrt{-1}$. Como $\delta \notin \mathbb{Q}$ se desprende de VI.3.3 que $G_{\mathbb{Q}}(f_2) \cong \mathcal{S}_3$.

Comprobemos ahora que f_2 es irreducible en $L_1[\mathtt{t}]$. En caso contrario, y puesto que $\deg(f_2) = 3$, el cuerpo L_1 contendría a alguna de sus raíces, digamos u_1. Entonces, $\mathbb{Q} \subset \mathbb{Q}(u_1) \subset L_1$, y por tanto

$$8 = [L_1:\mathbb{Q}] = [L_1:\mathbb{Q}(u_1)] \cdot [\mathbb{Q}(u_1):\mathbb{Q}] = \deg(P_{\mathbb{Q},u_1}) \cdot [L_1:\mathbb{Q}(u_1)] = 3 \cdot [L_1:\mathbb{Q}(u_1)],$$

luego 8 es múltiplo en $\mathbb{Z}$ de 3, y esto es falso. Además,

$$0 = f_1(v) = v^4 - 2v^2 + 2 = (v^2-1)^2 + 1 \quad \Longrightarrow \quad i = \varepsilon(v^2-1) \in \mathbb{Q}(v) \subset L_1, \ \text{(VI.23)}$$

para cierto $\varepsilon \in \{-1, +1\}$, de donde $\delta = 108i \in L_1$. Se deduce así de la tabla de VI.3.2 que $G_{L_1}(f_2) \cong \mathbb{Z}_3$.

(4) Como $L_1 = \mathbb{Q}(v, w)$ y $L_2 = \mathbb{Q}(u_1, u_2, u_3)$ resulta $L = \mathbb{Q}(v, w, u_1, u_2, u_3)$. Esto prueba, por un lado, que la extensión $L|\mathbb{Q}$ es de Galois, ya que L es el cuerpo de descomposición sobre $\mathbb{Q}$ del producto $f_1 f_2$, y por otro que $L = L_1(u_1, u_2, u_3)$ es el cuerpo de descomposición de f_2 sobre L_1. En consecuencia,

$$[L : \mathbb{Q}] = [L : L_1] \cdot [L_1 : \mathbb{Q}] = 8 \cdot \mathrm{ord}(G(L : L_1)) = 8 \cdot \mathrm{ord}(G_{L_1}(f_2)) = 8 \cdot 3 = 24.$$

(5) Como la extensión $L_1|\mathbb{Q}$ es de Galois y tiene grado 8, el subgrupo $G(L : L_1)$ de $G(L : \mathbb{Q})$ es un subgrupo normal de orden 3 de $G(L : \mathbb{Q})$. Es por tanto el único 3-subgrupo de Sylow de $G(L : \mathbb{Q})$, ya que $\mathrm{ord}(G(L : \mathbb{Q})) = [L : \mathbb{Q}] = 8 \cdot 3$, lo que por el teorema fundamental de la teoría de Galois implica que $L_1|\mathbb{Q}$ es la única subextensión de grado 8 de $L|\mathbb{Q}$.

(6) Veamos en primer lugar que las subextensiones $\mathbb{Q}(u_i)|\mathbb{Q}$, con $i = 1, 2, 3$, son distintas dos a dos. En caso contrario se tendría, por ejemplo, $\mathbb{Q}(u_1) = \mathbb{Q}(u_2)$. En tal caso, $u_2 \in \mathbb{Q}(u_1)$ y también $u_3 = -(u_1 + u_2) \in \mathbb{Q}(u_1)$, por lo que $L_2 = \mathbb{Q}(u_1)$, y esto es falso ya que

$$[\mathbb{Q}(u_1) : \mathbb{Q}] = \deg(P_{\mathbb{Q},u_1}) = \deg(f_2) = 3 \quad \& \quad [L_2 : \mathbb{Q}] = \mathrm{ord}(G_{\mathbb{Q}}(f_2)) = \mathrm{ord}(\mathcal{S}_3) = 6.$$

Para acabar este apartado basta probar que la extensión $L|\mathbb{Q}$ no posee más de 3 subextensiones de grado 3 o, equivalentemente, que el grupo $G(L : \mathbb{Q})$ no posee más de 3 subgrupos de orden 8. Esto es consecuencia inmediata del tercer teorema de Sylow ya que $\mathrm{ord}(G(L : \mathbb{Q})) = [L : \mathbb{Q}] = 8 \cdot 3$.

(7) Como v^2 y w^2 son las raíces del polinomio $\mathtt{t}^2 - 2\mathtt{t} + 2$ se tiene $v^2 w^2 = 2$, así que $vw = \sqrt{2}$. En particular $L_1 = \mathbb{Q}(v, w) = \mathbb{Q}(v, \sqrt{2})$. Por otro lado, hemos probado en el apartado (3) que $f_2 = P_{L_1,u_1}$, así que $L_1 \subset L_1(u_1) \subset L$ y

$$[L_1(u_1) : L_1] = \deg(f_2) = 3 = \mathrm{ord}(G_{L_1}(f_2)) = [L : L_1],$$

así que $L = L_1(u_1)$. En conclusión, $L = L_1(u_1) = \mathbb{Q}(v, \sqrt{2}, u_1)$. Así, cada automorfismo $\varphi \in G(L : \mathbb{Q})$ queda determinado por las imágenes de $v, \sqrt{2}$ y u_1. Además,

$$\varphi(v) \in \{v, -v, w, -w\}, \quad \varphi(\sqrt{2}) = \pm\sqrt{2} \quad \& \quad \varphi(u_1) \in \{u_1, u_2, u_3\}.$$

Como esto proporciona un máximo de $24 = 4 \cdot 2 \cdot 3$ posibles automorfismos de $L|\mathbb{Q}$ y hemos probado en el apartado (6) que $\mathrm{ord}(G(L : \mathbb{Q})) = 24$, todas estas asignaciones inducen automorfismos de $L|\mathbb{Q}$. En particular existe un (único) automorfismo ρ de $L|\mathbb{Q}$ determinado por las condiciones

$$\rho(v) = w, \quad \rho(\sqrt{2}) = -\sqrt{2} \quad \& \quad \rho(u_1) = u_2.$$

Éste es el automorfismo buscado, ya que $\rho(w) = \rho(\sqrt{2}/v) = -\sqrt{2}/w = -v$.

Para calcular el grado $[F : \mathbb{Q}]$ vamos a demostrar antes que $\rho(u_2) = u_1$, lo que implica que $\rho(u_3) = u_3$. En efecto, en caso contrario $\rho(u_2) = u_3$ y $\rho(u_3) = u_1$, luego el producto

$$108i = \delta = \sqrt{\Delta(f_2)} = (u_1 - u_2)(u_1 - u_3)(u_2 - u_3)$$

cumpliría que

$$\begin{aligned} 108\rho(i) = \rho(108i) = \rho(\delta) &= (\rho(u_1) - \rho(u_2))(\rho(u_1) - \rho(u_3))(\rho(u_2) - \rho(u_3)) \\ &= (u_2 - u_3)(u_2 - u_1)(u_3 - u_1) = \delta = 108i, \end{aligned}$$

es decir, $\rho(i) = i$. Pero esto es falso pues por la igualdad (VI.23) y $v^2 + w^2 = 2$,

$$\begin{aligned} \rho(i) = \varepsilon\rho(v^2 - 1) &= \varepsilon((\rho(v))^2 - 1) = \varepsilon(w^2 - 1) \\ &= \varepsilon(2 - v^2 - 1) = \varepsilon(1 - v^2) = -i. \end{aligned}$$

Hemos probado que $\rho(u_2) = u_1$, así que el orden de ρ es 4, porque, por un lado,

$$\rho^2(v) = \rho(w) = -v, \quad \rho^2(\sqrt{2}) = -\rho(\sqrt{2}) = \sqrt{2} \quad \& \quad \rho^2(u_1) = \rho(u_2) = u_1,$$

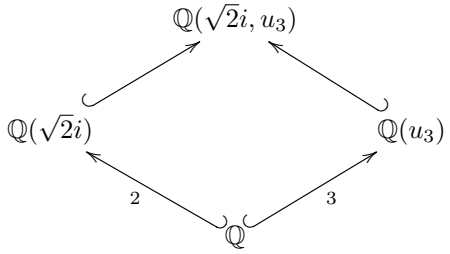
por lo que el orden de ρ no es 2, mientras que

$$\rho^4(v) = \rho^2(\rho^2(v)) = \rho^2(-v) = -\rho^2(v) = v, \quad \rho^4(\sqrt{2}) = \sqrt{2} \quad \& \quad \rho^4(u_1) = u_1,$$

así que ρ tiene orden 4. Por el Teorema fundamental de la teoría de Galois,

$$[L : F] = [L : \mathrm{Fix}(\rho)] = o(\rho) = 4 \quad \Longrightarrow \quad [F : \mathbb{Q}] = [L : \mathbb{Q}]/[L : F] = 24/4 = 6.$$

(8) Ya hemos señalado en el apartado anterior que $\rho(u_3) = u_3$, luego $u_3 \in \mathrm{Fix}(\rho) = F$. Además $\rho(i) = -i$ y $\rho(\sqrt{2}) = -\sqrt{2}$, por lo que $\rho(\sqrt{2}i) = \sqrt{2}i$. Así, $\mathbb{Q}(\sqrt{2}i, u_3) \subset F$, y esta inclusión es una igualdad. Para ello basta ver que $[\mathbb{Q}(\sqrt{2}i, u_3) : \mathbb{Q}] = 6$, lo que se deduce de lo visto en el Ejemplo I.2.4, puesto que $\mathrm{mcd}(2, 3) = 1$ y



Por la prueba del teorema del elemento primitivo, $\theta = u_3 + \sqrt{2}i$ es un elemento primitivo de $F|\mathbb{Q}$, y hemos de calcular su polinomio mínimo. Para esto basta hallar un polinomio de grado 6 con coeficientes en $\mathbb{Q}$ que tenga a θ por raíz. Se tiene

$$(\theta - \sqrt{2}i)^3 + 9(\theta - \sqrt{2}i) + 18 = f_2(u_3) = 0,$$

y desarrollando el cubo,

$$\theta^3 - 3\sqrt{2}i\theta^2 - 6\theta + 2\sqrt{2}i + 9\theta - 9\sqrt{2}i + 18 = 0.$$

Esta igualdad equivale a

$$\theta^3 + 3\theta + 18 = \sqrt{2}i(3\theta^2 + 7) \quad \Longrightarrow \quad (\theta^3 + 3\theta + 18)^2 = -2(3\theta^2 + 7)^2.$$

Desarrollando ambos cuadrados y simplificando resulta

$$\theta^6 + 6\theta^4 + 36\theta^3 + 111\theta^2 + 108\theta + 422,$$

y esto demuestra que el polinomio mínimo de θ sobre $\mathbb{Q}$ es

$$P_{\mathbb{Q},\theta}(\mathtt{t}) = \mathtt{t}^6 + 6\mathtt{t}^4 + 36\mathtt{t}^3 + 111\mathtt{t}^2 + 108\mathtt{t} + 422.$$

□

Número VI.24 (1) Hallar un polinomio irreducible $f \in \mathbb{Q}[\mathtt{t}]$ de grado 4 tal que $G_{\mathbb{Q}}(f) = \mathcal{D}_4$ mientras que $G_{\mathbb{Q}(i)}(f) = \mathbb{Z}_2 \times \mathbb{Z}_2$, donde $i := \sqrt{-1}$.

(2) Encontrar un polinomio irreducible $f \in \mathbb{Q}[\mathtt{t}]$ de grado 4 cuyo grupo de Galois sobre $\mathbb{Q}$ sea el grupo cíclico $\mathbb{Z}_4$ mientras que $G_{\mathbb{Q}(\sqrt{2})}(f) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Solución. (1) En el Ejercicio VI.21 hemos probado que $G_{\mathbb{Q}}(f) = \mathcal{D}_4$ para el polinomio $f(\mathtt{t}) := \mathtt{t}^4 - 2\mathtt{t}^2 - 1$, que es irreducible en $\mathbb{Q}[\mathtt{t}]$. Allí demostramos que $\Delta(f) = -32^2$, cuya raíz cuadrada es $\delta = 32i \in K := \mathbb{Q}(i)$. También vimos que f es irreducible en $K[\mathtt{t}] = K(\delta)[\mathtt{t}]$, y es obvio que $\delta \in K$. La tabla de la Proposición VI.3.3 nos dice que $G_K(f) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(2) En el Ejercicio VI.21 hemos probado que el polinomio $f(\mathtt{t}) := \mathtt{t}^4 - 4\mathtt{t}^2 + 2$ es irreducible en $\mathbb{Q}[\mathtt{t}]$ y que $G_{\mathbb{Q}}(f) = \mathbb{Z}_4$. También señalamos allí que

$$f(\mathtt{t}) = (\mathtt{t}^2 - 2 - \sqrt{2}) \cdot (\mathtt{t}^2 - 2 + \sqrt{2}),$$

luego f es reducible en $\mathbb{Q}(\sqrt{2})[\mathtt{t}]$. Por VI.3.4, $G_{\mathbb{Q}(\sqrt{2})}(f) = \mathbb{Z}_2 \times \mathbb{Z}_2$, pues f carece de raíces en $\mathbb{Q}(\sqrt{2})$. En efecto, si existiese $\alpha \in \mathbb{Q}(\sqrt{2})$ con $f(\alpha) = 0$, y como f es irreducible en $\mathbb{Q}[\mathtt{t}]$, sería $f = P_{\mathbb{Q},\alpha}$, así que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 4$, mientras que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. En consecuencia, $\alpha \notin \mathbb{Q}(\sqrt{2})$. □

Número VI.25 Sean $K := \mathbb{Q}(\sqrt{-3})$ y $f(\mathtt{t}) := (\mathtt{t}^3 - 2)(\mathtt{t}^2 - 5)$. Hallar el grupo de Galois $G_K(f)$.

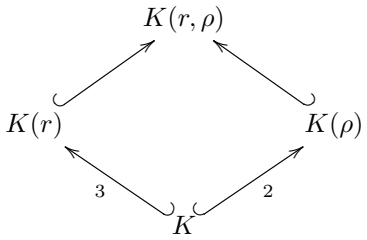
Solución. Comenzamos calculando generadores de la extensión $L_f|K$, donde $L_f \subset \mathbb{C}$ es un cuerpo de descomposición de f sobre K. Sean $r := \sqrt[3]{2} \in \mathbb{R}$ la única raíz real del polinomio $\mathtt{t}^3 - 2$ y

$$\xi = e^{2\pi i/3} = \frac{-1 + \sqrt{3}i}{2} = \frac{-1 + \sqrt{-3}}{2} \in K.$$

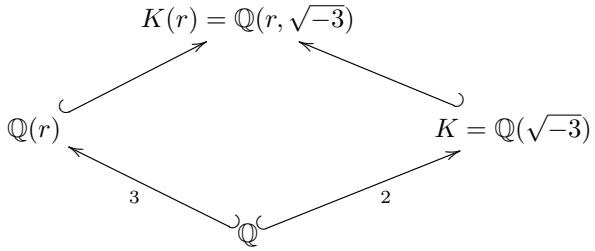
Las raíces de $\mathtt{t}^3-2$ en $\mathbb{C}$ son r, ξr y $\xi^2 r$, mientras que las de $\mathtt{t}^2-5$ son $\rho := \sqrt{5}$ y $-\rho$. Por tanto

$$L_f = K(r,\xi,\rho) = K(r,\rho) \quad \& \quad [L_f : K] = 6.$$

En efecto, la última igualdad se desprende del Ejemplo I.2.4 si vemos que



Ahora bien, como $[\mathbb{Q}(r):\mathbb{Q}] = \deg(P_{\mathbb{Q},r}) = \deg(\mathtt{t}^3-2) = 3$ y $[K:\mathbb{Q}] = 2$ tenemos



se deduce de I.2.4 que $[K(r):K] = 3$. Por otro lado, $[K(\rho):K] \leq \deg(\mathtt{t}^2-5) = 2$, y esta desigualdad es una igualdad. En caso contrario $K = K(\rho)$, y por ello

$$\mathbb{Q} \subset \mathbb{Q}(\rho) \subset K(\rho) = K = \mathbb{Q}(\sqrt{-3}). \tag{VI.24}$$

Pero las extensiones $\mathbb{Q}(\rho)|\mathbb{Q}$ y $\mathbb{Q}(\sqrt{-3})|\mathbb{Q}$ tienen grado 2 ya que $P_{\mathbb{Q},\rho}(\mathtt{t}) = \mathtt{t}^2-5$ y $P_{\mathbb{Q}(\rho),\sqrt{-3}}(\mathtt{t}) = \mathtt{t}^2+3$, y se deduce de (VI.24) que $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\rho) \subset \mathbb{R}$, que es falso.

Como la extensión $L_f|K$ es de Galois el grupo $G_K(f)$ tiene 6 elementos, luego es isomorfo al grupo cíclico $\mathbb{Z}_6$ o al grupo simétrico $\mathcal{S}_3$.

Consideremos el K-automorfismo ϕ de $L_f = K(r,\rho)$ que satisface las condiciones $\phi(r) := \xi r$ y $\phi(\rho) := -\rho$. El orden de ϕ no es ni 2 ni 3 ya que

$$\phi^2(r) = \phi(\xi r) = \xi\phi(r) = \xi^2 r \neq r \quad \& \quad \phi^3(\rho) = -\rho \neq \rho,$$

por lo que $o(\phi) = 6$, o sea, $G_K(f) = \mathbb{Z}_6$. □

Número VI.26 Sean p un número primo, $f(\mathtt{t}) := \mathtt{t}^5 - p$ y $L_f \subset \mathbb{C}$ un cuerpo de descomposición de f sobre el cuerpo $\mathbb{Q}$ de los números racionales.

(1) Determinar el grupo de Galois $G_{\mathbb{Q}}(f)$ de f sobre $\mathbb{Q}$.

(2) ¿Contiene $G_{\mathbb{Q}}(f)$ alguna transposición visto como subgrupo de $\mathcal{S}_5$?

(3) ¿Es abeliano el grupo $G_{\mathbb{Q}}(f)$?

(4) Calcular, para cada divisor n del orden del grupo $G_{\mathbb{Q}}(f)$, el número de elementos de orden n.

(5) Encontrar un elemento primitivo de cada subextensión propia de Galois de $L_f|\mathbb{Q}$.

Solución. (1) Se probó en VI.4.7 (3) que $G_{\mathbb{Q}}(f) = \mathcal{F}_5$ es el subgrupo afín de orden 20.

(2) Si el grupo $G_{\mathbb{Q}}(f)$ contuviese una transposición coincidiría, en virtud de la Proposición III.2.7, vol. I, con $\mathcal{S}_5$, lo que es absurdo porque su orden es 20.

(3) El grupo $\mathcal{F}_5$ no es abeliano; presentamos una prueba *ad hoc* para describir adecuadamente los elementos de $G_{\mathbb{Q}}(f)$, lo que emplearemos en la resolución de los siguientes apartados. Cada $\mathbb{Q}$-automorfismo de L_f queda determinado por las imágenes de $r := \sqrt[5]{p}$ y $\zeta := e^{2\pi i/5}$ pues el cuerpo de descomposición L_f de f sobre $\mathbb{Q}$ es

$$L_f = \mathbb{Q}(r, r\zeta, r\zeta^2, r\zeta^3, r\zeta^4) = \mathbb{Q}(r, \zeta).$$

Las posibles imágenes de r son las raíces $r\zeta^j$, con $0 \leq j \leq 4$, de su polinomio mínimo f, mientras que las de ζ son las raíces ζ^k, con $1 \leq k \leq 4$, de su polinomio mínimo Φ_5. Esto da un total de 20 posibles automorfismos y, como hemos visto en el apartado (1) que el orden de $G_{\mathbb{Q}}(f)$ es 20, cada asignación

$$r \mapsto r\zeta^j \quad \& \quad \zeta \mapsto \zeta^k, \ \text{ con } \ 0 \leq j \leq 4, \ \ 1 \leq k \leq 4$$

induce un automorfismo $\psi_{jk} \in G_{\mathbb{Q}}(f)$ que cumple $\psi_{jk}(r) = r\zeta^j$ y $\psi_{jk}(\zeta) = \zeta^k$. Nótese que $\psi_{0,1}$ es la identidad y que $G_{\mathbb{Q}}(f)$ no es abeliano, ya que

$$(\psi_{12} \cdot \psi_{11})(r) = \psi_{11}(r\zeta) = \psi_{11}(r)\psi_{11}(\zeta) = r\zeta^2 \quad \& \\ (\psi_{11} \cdot \psi_{12})(r) = \psi_{12}(r\zeta) = \psi_{12}(r)\psi_{12}(\zeta) = r\zeta^3,$$

lo que implica que $\psi_{12} \cdot \psi_{11} \neq \psi_{11} \cdot \psi_{12}$.

(4) Toda permutación $\sigma \in \mathcal{S}_5$ es, por la Proposición III.1.6, vol. I, producto de ciclos disjuntos de longitudes $\ell_1, \ldots, \ell_r$, de modo que $\ell_1 + \cdots + \ell_r \leq 5$ y, por el Corolario III.1.11, vol. I, el orden de σ es el mínimo común múltiplo de $\ell_1, \ldots, \ell_r$. El valor máximo de este mínimo común múltiplo es 6, que se obtiene para $r = 2$, $\ell_1 = 2$ y $\ell_2 = 3$, luego en $\mathcal{S}_5$ no hay elementos de orden mayor que 6, y lo mismo sucede en el subgrupo $G_{\mathbb{Q}}(f)$ de $\mathcal{S}_5$. Por tanto, si para cada divisor n de 20 denotamos $\nu(n)$ el número de elementos de orden n en el grupo $G_{\mathbb{Q}}(f)$, lo anterior demuestra que $\nu(20) = \nu(10) = 0$. Además $\nu(1) = 1$, pues la identidad es el único elemento de orden 1 de $G_{\mathbb{Q}}(f)$.

Según vimos en el Ejemplo V.1.8 (1), vol. I, el grupo $G_{\mathbb{Q}}(f)$ contiene un único subgrupo H_5 de orden 5, así que los elementos de orden 5 de $G_{\mathbb{Q}}(f)$ son, precisamente, los elementos de H_5 distintos del neutro, luego $\nu(5) = 4$. Para obtener $\nu(2)$ efectuamos

un cálculo directo, esto es, determinamos para qué pares (j,k) distintos de $(0,1)$ el automorfismo ψ_{jk} cumple que $\psi_{jk}^2(r) = r$ y $\psi_{jk}^2(\zeta) = \zeta$. Estas condiciones equivalen a

$$r = \psi_{jk}(\psi_{jk}(r)) = \psi_{jk}(r\zeta^j) = \psi_{jk}(r)\psi_{jk}(\zeta^j) = r\zeta^j\zeta^{kj} = r\zeta^{j(k+1)} \quad \&$$
$$\zeta = \psi_{jk}(\psi_{jk}(\zeta)) = \psi_{jk}(\zeta^k) = \zeta^{k^2} \quad \Longleftrightarrow \quad \zeta^{k^2-1} = 1.$$

Estas dos condiciones equivalen a que $\zeta^{j(k+1)} = \zeta^{k^2-1} = 1$, o sea, tanto $j(k+1)$ como k^2-1 han de ser múltiplos de 5. La última de estas dos condiciones se puede reescribir diciendo que $5|(k+1)(k-1)$ y, como 5 es primo, esto equivale a que $5|(k+1)$, en cuyo caso $5|j(k+1)$, o $5|(k-1)$, luego $k = 1$, por lo que necesariamente $5|j$.

Como $0 \leq j \leq 4$ y $1 \leq k \leq 4$ lo anterior equivale a que $k = 4$ o $(j,k) = (0,1)$. Este último caso corresponde al automorfismo identidad, que es $\psi_{0,1}$. Por tanto, los elementos de orden 2 del grupo de Galois $G_{\mathbb{Q}}(f)$ son $\{\psi_{j4} : 0 \leq j \leq 4\}$, así que $\nu(2) = 5$. Por la Fórmula de Lagrange, los órdenes de los elementos de $G_{\mathbb{Q}}(f)$ son 1, 2, 5, 10 o 20, luego

$$\nu(4) = 20 - \big(\nu(1) + \nu(2) + \nu(5) + \nu(10) + \nu(20)\big) = 10.$$

(5) Por la segunda parte del Teorema fundamental de la teoría de Galois las subextensiones de Galois $E|\mathbb{Q}$ de $L_f|\mathbb{Q}$ están en correspondencia biyectiva con los subgrupos normales de $G_{\mathbb{Q}}(f)$, así que comenzamos por determinar éstos. Ya hemos señalado que $G_{\mathbb{Q}}(f)$ posee un único subgrupo H_5 de orden 5, que por tanto es normal.

Sin embargo si $G_{\mathbb{Q}}(f)$ contuviese un subgrupo normal de orden 4 éste sería, por el Primer Teorema de Sylow, V.1.1 vol. I, su único subgrupo de orden 4, luego contendría a todos los elementos de orden 4 de $G_{\mathbb{Q}}(f)$. Pero esto es imposible pues acabamos de ver que $\nu(4) = 10$.

Si $G_{\mathbb{Q}}(f)$ contuviese un subgrupo normal H_2 de orden 2 la intersección $H_2 \cap H_5$ sería trivial porque $\mathrm{mcd}(2,5) = 1$ y esto implica, por el Ejemplo II.2.10 (2), vol. I, que

$$H_2H_5 \cong H_2 \times H_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \cong \mathbb{Z}_{10},$$

por lo que $G_{\mathbb{Q}}(f)$ contendría algún elemento de orden 10, y ya hemos señalado en el apartado (4) que esto es falso.

Por último $G_{\mathbb{Q}}(f)$ contiene, por el Segundo Teorema de Sylow, algún subgrupo K de orden 2, por lo que $H_{10} = KH_5$ es, en virtud de II.1.1 (3) y la Proposición I.2.1 vol. I, un subgrupo de $G_{\mathbb{Q}}(f)$ de orden 10. El índice $[G_{\mathbb{Q}}(f) : H_{10}] = 2$, y esto implica, según el Ejemplo II.1.2 (3) vol. I, que H_{10} es subgrupo normal de $G_{\mathbb{Q}}(f)$. De hecho es el único subgrupo de orden 10 pues si existiese otro, digamos M, y puesto que ni M ni H_{10} contienen elementos de orden 4, resulta

$$20 = \mathrm{ord}(G_{\mathbb{Q}}(f)) \geq \nu(4) + \mathrm{Card}(H_{10} \cup M) = \nu(4) + \mathrm{ord}(H_{10})$$
$$+ \mathrm{ord}(M) - \mathrm{ord}(H_{10} \cap M) = 30 - \mathrm{ord}(H_{10} \cap M) \geq 30 - 5 = 25,$$

y esto es imposible.

Resumiendo, el grupo $G_{\mathbb{Q}}(f)$ posee, exactamente, dos subgrupos normales propios H_5 y H_{10} de órdenes 5 y 10, respectivamente, luego $\mathrm{Fix}(H_5)|\mathbb{Q}$ y $\mathrm{Fix}(H_{10})|\mathbb{Q}$ son las únicas subextensiones propias de Galois de $L_f|\mathbb{Q}$, de grados $[\mathrm{Fix}(H_5):\mathbb{Q}] = 20/5 = 4$ y $[\mathrm{Fix}(H_{10}):\mathbb{Q}] = 20/10 = 2$.

Actuando ortodoxamente, el cálculo de las subextensiones de Galois de $L_f|\mathbb{Q}$ exigiría determinar los cuerpos fijos $\mathrm{Fix}(H_5)$ y $\mathrm{Fix}(H_{10})$, pero éste no es el modo más eficiente de proceder. Sabemos que $\mathrm{Fix}(H_5)|\mathbb{Q}$ es la única subextensión de grado 4, y que el polinomio mínimo de ζ sobre $\mathbb{Q}$ es el ciclotómico Φ_5, de grado 4, por lo que $\mathrm{Fix}(H_5) = \mathbb{Q}(\zeta)$, luego $\mathbb{Q}(\zeta)|\mathbb{Q}$ es la única subextensión de $L_f|\mathbb{Q}$ de grado 4, y es de Galois.

En cuanto a la subextensión de Galois de grado 2 es suficiente encontrar un elemento $u \in L_f$ cuyo polinomio mínimo sobre $\mathbb{Q}$ tenga grado 2, pues en tal caso $\mathbb{Q}(u)|\mathbb{Q}$ es una subextensión de $L_f|\mathbb{Q}$ de grado 2, por lo que es de Galois y, a fortiori, $\mathbb{Q}(u) = \mathrm{Fix}(H_{10})$, ya que $L_f|\mathbb{Q}$ admite una única subextrensión de grado 2. Denotamos $u := \zeta^2 + \zeta^3$ y, puesto que $\zeta^5 = 1$,

$$u^2 = (\zeta^2 + \zeta^3)^2 = \zeta^4 + \zeta^6 + 2\zeta^5 = \zeta^4 + \zeta + 2.$$

Sumando resulta que

$$u^2 + u = (\zeta^4 + \zeta + 2) + (\zeta^2 + \zeta^3) = (\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1) + 1 = 1.$$

Como el polinomio $g(\mathtt{t}) := \mathtt{t}^2 + \mathtt{t} - 1$ es irreducible en $\mathbb{Q}[\mathtt{t}]$ y $g(u) = 0$, la extensión $\mathbb{Q})(u)|\mathbb{Q}$ tiene grado 2 y por tanto es de Galois. □

Número VI.27 Denotemos $\mathtt{x} := (\mathtt{x}_1, \mathtt{x}_2, \mathtt{x}_3, \mathtt{x}_4, \mathtt{x}_5)$ y consideremos el polinomio

$$\mathtt{q}(\mathtt{x}) := \mathtt{x}_1\mathtt{x}_2 + \mathtt{x}_2\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_1 - \mathtt{x}_1\mathtt{x}_3 - \mathtt{x}_3\mathtt{x}_5 - \mathtt{x}_5\mathtt{x}_2 - \mathtt{x}_2\mathtt{x}_4 - \mathtt{x}_4\mathtt{x}_1.$$

Calcular el estabilizador $\mathrm{Stab}_{\mathcal{S}_5}(\mathtt{q})$ para la acción de $\mathcal{S}_5$ sobre $K[\mathtt{x}]$ introducida en VI.2.3.

Solución. Hemos probado en VI.4.2 que el estabilizador del polinomio $\mathtt{p} := \mathtt{q}^2$ es el grupo afín $\mathcal{F}_5$ de orden 20, y desde luego $\mathrm{Stab}_{\mathcal{S}_5}(\mathtt{q})$ es un subgrupo de $\mathrm{Stab}_{\mathcal{S}_5}(\mathtt{p}) = \mathcal{F}_5$, ya que si $\sigma \in \mathcal{S}_5$ cumple que $\widetilde{\sigma}(\mathtt{q}) = \mathtt{q}$, entonces

$$\widetilde{\sigma}(\mathtt{p}) = \widetilde{\sigma}(\mathtt{q}^2) = (\widetilde{\sigma}(\mathtt{q}))^2 = \mathtt{q}^2 = \mathtt{p}.$$

Por otro lado, vimos en el Apéndice A.2 vol. I. que la intersección $\mathcal{F}_5 \cap \mathcal{A}_5$ del grupo afín $\mathcal{F}_5$ con el grupo alternado $\mathcal{A}_5$ es el grupo diedral $\mathcal{D}_5$ generado por $\sigma := (1,2,3,4,5)$ y $\tau := (1,4)(2,3)$. Escribimos $\mathtt{q} := \mathtt{q}_1 - \mathtt{q}_2$, donde

$$\mathtt{q}_1(\mathtt{x}) := \mathtt{x}_1\mathtt{x}_2 + \mathtt{x}_2\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_1 \quad \& \quad \mathtt{q}_2(\mathtt{x}) := \mathtt{x}_1\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_2 + \mathtt{x}_2\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_1.$$

Entonces,

$$\begin{aligned}
\widetilde{\sigma}(\mathtt{q}_1) &= \mathtt{x}_2\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_1 + \mathtt{x}_1\mathtt{x}_2 = \mathtt{q}_1,\\
\widetilde{\sigma}(\mathtt{q}_2) &= \mathtt{x}_2\mathtt{x}_4 + \mathtt{x}_4\mathtt{x}_1 + \mathtt{x}_1\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_2 = \mathtt{q}_2,\\
\widetilde{\tau}(\mathtt{q}_1) &= \mathtt{x}_4\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_2 + \mathtt{x}_2\mathtt{x}_1 + \mathtt{x}_1\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_4 = \mathtt{q}_1,\\
\widetilde{\tau}(\mathtt{q}_2) &= \mathtt{x}_4\mathtt{x}_2 + \mathtt{x}_2\mathtt{x}_5 + \mathtt{x}_5\mathtt{x}_3 + \mathtt{x}_3\mathtt{x}_1 + \mathtt{x}_1\mathtt{x}_4 = \mathtt{q}_2,
\end{aligned}$$

luego $\widetilde{\sigma}(\mathtt{q}) = \widetilde{\tau}(\mathtt{q}) = \mathtt{q}$, por lo que $\mathcal{D}_5 \subset \mathrm{Stab}_{\mathcal{S}_5}(\mathtt{q})$.

Además $\gamma := (1,2,4,3) \in \mathcal{F}_5 \setminus \mathrm{Stab}_{\mathcal{S}_5}(\mathtt{q})$, pues vimos en VI.4.2 que $\widetilde{\gamma}(\mathtt{q}) = -\mathtt{q}$. Así, $\mathcal{D}_5 \subset \mathrm{Stab}_{\mathcal{S}_5}(\mathtt{q}) \subsetneq \mathcal{F}_5$ y, como $[\mathcal{F}_5 : \mathcal{D}_5] = 2$, resulta $\mathcal{D}_5 = \mathrm{Stab}_{\mathcal{S}_5}(\mathtt{q})$. □

Número VI.28 Hallar el grupo de Galois de $f(\mathtt{t}) := \mathtt{t}^5 - 2$ sobre $K := \mathbb{Q}(\sqrt{5})$.

Solución. El discriminante de f es $\Delta(f) = 5^5 \cdot 2^4 = (100\sqrt{5})^2$, en virtud de VII.2.12, vol. II, y es un cuadrado en K. Además, la resolvente séxtica de f tiene a $0 \in K$ por raíz, porque

$$R_{f,\mathtt{p}}(\mathtt{t}) = \mathtt{t}^6 - 2^{14} \cdot 5^5\mathtt{t}.$$

Se sigue de la tabla VI.4.5 que $G_K(f)$ es cíclico o diedral. Pero f tiene una única raíz real, y se deduce del Corolario VI.4.4 que $G_K(f) = \mathcal{D}_5$. □

Número VI.29 Sean $a, b \in \mathbb{Q}$ tales que $f(\mathtt{t}) := \mathtt{t}^5 + a\mathtt{t}^3 + (a^2/5)\mathtt{t} + b$ es irreducible en $\mathbb{Q}[\mathtt{t}]$. Calcular el grupo de Galois de f sobre $\mathbb{Q}$.

Solución. El discriminante de f es $\Delta(f) = (4a^5 + 3125b^2)^2/5^5$, que no es el cuadrado de un número racional, pues $\sqrt{5} \notin \mathbb{Q}$. Además, la resolvente séxtica de f es

$$R_{f,\mathtt{p}}(\mathtt{t}) = (\mathtt{t}^3 - 7a^2\mathtt{t}^2 + 11a^4\mathtt{t} + (3/25)a^6 + 4000ab^2)^2 - 2^{10}\Delta(f)\mathtt{t},$$

que tiene a $5a^2 \in \mathbb{Q}$ por raíz. Se deduce de la tabla VI.4.5 que $G_{\mathbb{Q}}(f) = \mathcal{F}_5$. □

Número VI.30 Sean K un cuerpo de característica cero, $K_1|K$ una extensión de Galois y $f \in K[\mathtt{t}]$.

(1) Demostrar que el grupo de Galois $G_{K_1}(f)$ de f sobre el cuerpo K_1 es isomorfo a un subgrupo normal H del grupo de Galois $G_K(f)$ de f sobre K.

(2) Probar que el cociente $G_K(f)/H$ es isomorfo a un cociente del grupo $G(K_1 : K)$.

Solución. (1) Sean E un cuerpo de descomposición de f sobre K y E_1 un cuerpo de descomposición de f sobre K_1 que contiene a E. Por definición, $G_K(f) = G(E : K)$ y $G_{K_1}(f) = G(E_1 : K_1)$. Por el teorema del elemento primitivo existe $\alpha \in K_1$ tal que $K_1 := K(\alpha)$, luego $E_1 = E(\alpha)$. En particular, la extensión $E_1|K$ es de Galois, por

ser E_1 un cuerpo de descomposición de $f \cdot P_{K,\alpha}$ sobre K. Las subextensiones $K_1|K$ y $E|K$ son de Galois; la primera por hipótesis, y la segunda por ser E un cuerpo de descomposición sobre K.

Sea $F := E \cap K_1$ y vamos a demostrar, empleando el Teorema fundamental de la teoría de Galois IV.2.4, que la extensión $F|K$ es de Galois. Sea $\phi \in G(E_1 : K)$. Por ser de Galois tanto $K_1|K$ como $E|K$, resulta que $\phi(K_1) \subset K_1$ y $\phi(E) \subset E$, luego

$$\phi(F) = \phi(E \cap K_1) = \phi(E) \cap \phi(K_1) \subset E \cap K_1 = F, \tag{VI.25}$$

y esto equivale a que la extensión $F|K$ es de Galois. Empleando de nuevo el Teorema fundamental deducimos que $H := G(E : F)$ es un subgrupo normal del grupo de Galois $G(E : K) = G_K(f)$, y todo se reduce a demostrar que $G_{K_1}(f)$ es isomorfo a H. Vamos a comprobar que la aplicación

$$\Psi : G_{K_1}(f) = G(E_1 : K_1) \to H = G(E : F),\ \varphi \mapsto \varphi|_E$$

es un isomorfismo de grupos. En primer lugar hemos de comprobar que ésta es una aplicación bien definida. Dado $\varphi \in G(E_1 : K_1) \subset G(E_1 : K)$ ya hemos señalado que, por ser la extensión $E|K$ de Galois, $\varphi(E) \subset E$. De hecho se da la igualdad $\varphi(E) = E$, pues aplicando lo anterior al automorfismo φ^{-1} se tiene $\varphi^{-1}(E) \subset E$, por lo que $E = \varphi(\varphi^{-1}(E)) \subset \varphi(E) \subset E$. Por tanto $\varphi|_E$ es un automorfismo de E, y fija cada elemento de F, pues φ deja fijos todos los elementos de K_1.

De lo anterior se desprende que Ψ es un homomorfismo bien definido. Veamos que es inyectivo. Si la restricción $\varphi|_E$ de un automorfismo $\varphi \in G(E_1 : K_1)$ es la identidad en E entonces, $\varphi|_{E \cup K_1}$ es la identidad. Pero

$$E_1 = E(\alpha) \subset E \cup K(\alpha) = E \cup K_1 \subset E_1,$$

luego $\varphi = \mathrm{id}_{E_1}$. Así, para terminar este apartado basta demostrar que el homomorfismo Ψ es sobreyectivo. Supongamos, por reducción al absurdo, que $H_1 = \operatorname{im} \Psi \subsetneq H$. Entonces, como la extensión $E|F$ es de Galois por serlo $E|K$, resulta que

$$F = \mathrm{Fix}(G(E : F)) = \mathrm{Fix}(H) \subsetneq \mathrm{Fix}(H_1),$$

luego existe $\beta \in \mathrm{Fix}(H_1) \setminus F$. Como H_1 es subgrupo de $G(E : F)$, resulta que $\mathrm{Fix}(H_1) \subset E$, así que $\beta \in E \setminus E \cap K_1$, por lo que $\beta \in E_1 \setminus K_1$. Pero $E_1|K_1$ es una extensión de Galois, por lo que $K_1 = \mathrm{Fix}(G(E_1 : K_1))$, así que existe un automorfismo $\varphi \in G(E_1 : K_1)$ tal que $\varphi(\beta) \neq \beta$. Por tanto, la restricción $\varphi|_E \in \operatorname{im} \Psi = H_1$ pero $\varphi(\beta) \neq \beta$, y esto contradice la hipótesis de que $\beta \in \mathrm{Fix}(H_1)$.

(2) Por el Teorema fundamental, y puesto que las extensiones $E|K$, $K_1|K$ y $F|K$ son de Galois,

$$G_K(f)/H = G(E : K)/G(E : F) \cong G(F : K) \cong G(K_1 : K)/G(K_1 : F).$$

□

Soluciones a los ejercicios del Capítulo VII

Número VII.1 Sean K un cuerpo y los polinomios de $K[\mathtt{t}]$ de grado n

$$f(\mathtt{t}) := \sum_{i=0}^{n} a_i \mathtt{t}^i \quad \& \quad g(\mathtt{t}) := \sum_{i=0}^{n} a_{n-i} \mathtt{t}^i.$$

Demostrar que f es resoluble por radicales sobre K si y sólo si g lo es.

Solución. Las raíces de g son las inversas de las raíces de f pues $g(\mathtt{t}) = \mathtt{t}^n f(1/\mathtt{t})$. En consecuencia, las raíces de f son expresables mediante radicales sobre K si y sólo si lo son las de g. □

Número VII.2 (1) Estudiar si el polinomio $f(\mathtt{t}) := \mathtt{t}^6 - 3\mathtt{t}^4 + 6\mathtt{t}^2 - 3$ es resoluble por radicales.

(2) Sea $\alpha \in \mathbb{C}$ una raíz de f. Calcular el polinomio mínimo de $\alpha^2 - 1$ sobre $\mathbb{Q}$.

Solución. (1) El polinomio auxiliar $g(\mathtt{t}) := \mathtt{t}^3 - 3\mathtt{t}^2 + 6\mathtt{t} - 3$ es resoluble por radicales al ser de grado 3, en virtud del Corolario VII.1.12. Como $f(\mathtt{t}) = g(\mathtt{t}^2)$, también f es resoluble por radicales.

(2) El polinomio g es irreducible en $\mathbb{Q}[\mathtt{t}]$, por el Criterio de Eisenstein, luego $g = P_{\mathbb{Q},\alpha^2}$ es el polinomio mínimo de α^2 sobre $\mathbb{Q}$. Denotamos $u := \alpha^2 - 1$, que cumple

$$[\mathbb{Q}(u) : \mathbb{Q}] = [\mathbb{Q}(\alpha^2) : \mathbb{Q}] = \deg(g) = 3.$$

Por otro lado, sustituyendo $\alpha^2 = u + 1$ en la igualdad $g(\alpha^2) = 0$ obtenemos

$$0 = g(u+1) = (u+1)^3 - 3(u+1)^2 + 6(u+1) - 3 = u^3 + 3u + 1,$$

y por tanto $P_{\mathbb{Q},\alpha^2-1}(\mathtt{t}) = \mathtt{t}^3 + 3\mathtt{t} + 1$. □

Número VII.3 Sean $f, g \in \mathbb{Q}[\mathtt{t}]$ dos polinomios resolubles por radicales.

(1) ¿Se puede asegurar que también $f + g$ es resoluble por radicales?

(2) ¿Se puede asegurar que fg es resoluble por radicales?

Solución. (1) Los polinomios $f(\mathtt{t}) := \mathtt{t}^5$ y $g(\mathtt{t}) = -10\mathtt{t} - 2$ son resolubles por radicales sobre $\mathbb{Q}$; el primero por tener a 0 por única raíz y el segundo porque su única raíz es $-1/5$. Sin embargo su suma $h(\mathtt{t}) := f(\mathtt{t}) + g(\mathtt{t}) = \mathtt{t}^5 - 10\mathtt{t} - 2$ no es resoluble por radicales, ya que vimos en el Ejemplo VI.4.7 que su grupo de Galois sobre $\mathbb{Q}$ es el grupo simétrico $\mathcal{S}_5$, que no es resoluble.

(2) Sea $\overline{\mathbb{Q}} \subset \mathbb{C}$ un cierre algebraico de $\mathbb{Q}$ y factorizamos en $\overline{\mathbb{Q}}[\mathtt{t}]$ los polinomios f y g:

$$f(\mathtt{t}) := a\prod_{j=1}^{m}(\mathtt{t}-u_j) \;\;\&\;\; g(\mathtt{t}) := b\prod_{k=1}^{n}(\mathtt{t}-v_k) \;\;\Longrightarrow\;\; f(\mathtt{t})g(\mathtt{t}) = ab\prod_{j,k}(\mathtt{t}-u_j)(\mathtt{t}-v_k).$$

Así, $L_f := \mathbb{Q}(u_1,\ldots,u_m)$ y $L_g := \mathbb{Q}(v_1,\ldots,v_n)$ son cuerpos de descomposición de f y g contenidos en $\overline{\mathbb{Q}}$, por lo que $L_{fg} = \mathbb{Q}(u_1,\ldots,u_m,v_1,\ldots,v_n)$ es un cuerpo de descomposición de fg sobre $\mathbb{Q}$.

Las extensiones $L_f|\mathbb{Q}$ y $L_g|\mathbb{Q}$ son quasiradicales pues los polinomios f y g son resolubles por radicales. Existen por tanto extensiones radicales $K_f|\mathbb{Q}$ y $K_g|\mathbb{Q}$ tales que $L_f \subset K_f$ y $L_g \subset K_g$. En consecuencia, existen $\alpha_1,\ldots,\alpha_r,\beta_1,\ldots,\beta_s$ tales que

$$K_f := \mathbb{Q}(\alpha_1,\ldots,\alpha_r) \quad \& \quad K_g := \mathbb{Q}(\beta_1,\ldots,\beta_s),$$

de modo que α_1 y β_1 son raíces de los polinomios $\mathtt{t}^{m_1} - a_1 \in K[\mathtt{t}]$ y $\mathtt{t}^{n_1} - b_1 \in K[\mathtt{t}]$, respectivamente, y α_i es raíz de un polinomio del tipo $\mathtt{t}^{m_i} - a_i \in \mathbb{Q}(\alpha_1,\ldots,\alpha_{i-1})[\mathtt{t}]$ para $2 \le i \le r$, mientras que β_j es, para $2 \le j \le s$, raíz de un polinomio del tipo $\mathtt{t}^{n_j} - b_j \in \mathbb{Q}(\beta_1,\ldots,\beta_{j-1})[\mathtt{t}]$. En consecuencia,

$$L_{fg} = \mathbb{Q}(u_1,\ldots,u_m,v_1,\ldots,v_n) \subset K = \mathbb{Q}(\alpha_1,\ldots,\alpha_r,\beta_1,\ldots,\beta_s)$$

y, como la extensión $K|\mathbb{Q}$ es radical, su subextensión $L_{fg}|\mathbb{Q}$ es quasiradical, por lo que el producto fg es resoluble por radicales. □

Número VII.4 Sean $\xi := e^{2\pi i/7}$ y $L := \mathbb{Q}(\xi)$.

(1) ¿Cuántas subextensiones de grado dos posee la extensión $L|\mathbb{Q}$? Obtener elementos primitivos de dichas subextensiones y los polinomios mínimos sobre $\mathbb{Q}$ de dichos elementos.

(2) ¿Contiene L a $i := \sqrt{-1}$? Sea $\gamma := e^{\pi i/7}$. Demostrar que $\mathbb{Q}(\xi) = \mathbb{Q}(\gamma)$.

(3) ¿Es resoluble por radicales sobre $\mathbb{Q}$ el polinomio

$$h(\mathtt{t}) := \mathtt{t}^6 - \mathtt{t}^5 + \mathtt{t}^4 - \mathtt{t}^3 + \mathtt{t}^2 - \mathtt{t} + 1?$$

Solución. (1) El polinomio ciclotómico $\Phi_7(\mathtt{t}) := \sum_{j=1}^{6}\mathtt{t}^j$, cuyas raíces son las potencias $\{\xi^j : 1 \le j \le 6\}$ es el polinomio mínimo de ξ sobre $\mathbb{Q}$. Como cada $\xi^j \in L$ la extensión $L|\mathbb{Q}$ es de Galois, ya que L es un cuerpo de descomposición de Φ_7 sobre $\mathbb{Q}$. En particular, por el Teorema VI.1.11, el grupo de Galois

$$G(L:\mathbb{Q}) = G_{\mathbb{Q}}(\Phi_7) \cong \mathbb{Z}_7^* \cong \mathbb{Z}_6$$

es el grupo cíclico de orden 6. De hecho está generado por el único $\mathbb{Q}$-automorfismo $\phi : L \to L$ que cumple $\phi(\xi) = \xi^3$. En efecto,

$$\phi^2(\xi) = \phi(\xi^3) = (\phi(\xi))^3 = \xi^9 = \xi^2 \neq \xi \quad \&$$
$$\phi^3(\xi) = \phi(\phi^2(\xi)) = \phi(\xi^2) = (\phi(\xi))^2 = \xi^6 \neq \xi,$$

luego el orden de ϕ no es ni 2 ni 3, y por tanto es 6. Por ser cíclico, $G(L:\mathbb{Q})$ contiene un único subgrupo $H := \langle\phi^2\rangle$ de orden 3, y en consecuencia, si denotamos $E := \mathrm{Fix}(H)$, la extensión $E|\mathbb{Q}$ es la única subextensión de $L|\mathbb{Q}$ de grado 2.

Para obtener un elemento primitivo de $E|\mathbb{Q}$ recordamos que $\phi^2(\xi) = \xi^2$, y buscamos un elemento $\eta \in L$ fijo por ϕ^2 como sigue.

Una base del $\mathbb{Q}$-espacio vectorial L es $\mathcal{B} := \{1, \xi, \xi^2, \xi^3, \xi^4, \xi^5\}$, luego existen números racionales a_j con $0 \le j \le 5$, tales que $\eta := \sum_{j=0}^{5} a_j \xi^j$, y se debe cumplir la igualdad $\phi^2(\eta) = \eta$. Como

$$\begin{aligned}&\phi^2(\xi) = \xi^2, \quad \phi^2(\xi^2) = \xi^4, \quad \phi^2(\xi^3) = \xi^6 = -(1+\xi+\xi^2+\xi^3+\xi^4+\xi^5),\\ &\phi^2(\xi^4) = \phi^2(\xi^2)\phi^2(\xi^2) = \xi^8 = \xi \quad \& \quad \phi^2(\xi^5) = \phi^2(\xi)\phi^2(\xi^4) = \xi^3,\end{aligned}$$

tenemos

$$\begin{aligned}a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4\xi^4 + a_5\xi^5 &= \eta = \phi^2(\eta)\\ &= a_0 + a_1\xi^2 + a_2\xi^4 - a_3(1+\xi+\xi^2+\xi^3+\xi^4+\xi^5) + a_4\xi + a_5\xi^3.\end{aligned}$$

Agrupando términos en potencias de ξ resulta

$$a_3+(a_1+a_3-a_4)\xi+(-a_1+a_2+a_3)\xi^2+(2a_3-a_5)\xi^3+(-a_2+a_3+a_4)\xi^4+(a_3+a_5)\xi^5 = 0.$$

Esto implica, por ser $\mathcal{B}$ base, que $a_3 = 0$, y sustituyendo este valor en los demás sumandos y dividiendo por ξ obtenemos

$$(a_1 - a_4) + (a_2 - a_1)\xi - a_5\xi^2 + (a_4 - a_2)\xi^3 + a_5\xi^4 = 0.$$

De aquí se sigue que también $a_5 = 0$, y por tanto

$$(a_1 - a_4) + (a_2 - a_1)\xi + (a_4 - a_2)\xi^3 = 0,$$

y esto equivale a que $a_1 = a_2 = a_4$. Así, salvo multiplicación por un número racional, $\eta := \xi + \xi^2 + \xi^4$, por lo que $\mathbb{Q}(\eta)|\mathbb{Q}$ es la única subextensión de $L|\mathbb{Q}$ de grado 2.

El polinomio mínimo de η tiene grado 2, luego para calcularlo es suficiente expresar η^2 en función de la base $\mathcal{B}$. Ahora bien,

$$\begin{aligned}\eta^2 &= \xi^2(1+\xi+\xi^3)^2 = \xi^2(1+2\xi+\xi^2+2\xi^3++2\xi^4+\xi^6)\\ &= \xi^2(1+\xi+\xi^2+\xi^3+\xi^4+\xi^6) + \xi^2(\xi+\xi^3+\xi^4)\\ &= -\xi^2\xi^5 + \xi^3 + \xi^5 - (1+\xi+\xi^2+\xi^3+\xi^4+\xi^5)\\ &= -2 - (\xi+\xi^2+\xi^4) = -\eta - 2\end{aligned}$$

luego $P_{\mathbb{Q},\eta}(\mathtt{t}) = \mathtt{t}^2 + \mathtt{t} + 2$.

(2) Vamos a demostrar que $i \notin L$ y suponemos lo contrario. Entonces $\mathbb{Q}(i)|\mathbb{Q}$ sería una subextensión de $L|\mathbb{Q}$ de grado 2. Como acabamos de probar que $\mathbb{Q}(\eta)|\mathbb{Q}$ es la única, han de coincidir, esto es, $\mathbb{Q}(i) = \mathbb{Q}(\eta)$, y en particular $\eta \in \mathbb{Q}(i)$. Existen por

tanto $a, b \in \mathbb{Q}$ tales que $\eta = a + bi$ y $b \neq 0$ porque $\eta \notin \mathbb{Q}$. Elevando al cuadrado, $\eta^2 = (a^2 - b^2) + 2abi$. Por tanto,

$$0 = \eta^2 + \eta + 2 = (a^2 - b^2) + 2abi + a + bi + 2 = (a^2 - b^2 + a + 2) + b(2a + 1)i,$$

y como b es no nulo, necesariamente $a = -1/2$. Entonces $b^2 = a^2 + a + 2 = 7/4$, y esto implica que $\sqrt{7} = \pm 2b \in \mathbb{Q}$, lo que es absurdo. Queda pues probado que $i \notin L$.

Por otro lado $\xi = \gamma^2$, luego $\mathbb{Q}(\xi) \subset \mathbb{Q}(\gamma)$. Para probar el contenido recíproco observamos que $\xi^{14} = \gamma^{14} = (-1)^{14} = 1$, esto es $-1, \xi$ y γ pertenecen al grupo $\mathfrak{U}_{14}$ de raíces 14-ésimas de la unidad. Un generador de este grupo es $-\xi = (-1)\cdot\xi$ ya que -1 tiene orden 2, ξ tiene orden 7 y por tanto el orden de $-\xi$ es $\mathrm{mcm}(2, 7) = 14$, que es el orden de $\mathfrak{U}_{14}$. Existe por tanto $k \in \mathbb{Z}$ tal que $\gamma = (-\xi)^k \in \mathbb{Q}(\xi)$ lo que demuestra el contenido $\mathbb{Q}(\gamma) \subset \mathbb{Q}(\xi)$, y con ello la igualdad.

(3) Como $\mathtt{t}^7 + 1 = (\mathtt{t} + 1)h(\mathtt{t})$, las raíces de h son las raíces séptimas de -1 que no son -1, o sea,

$$\{\gamma, \gamma^3, \gamma^5, \gamma^9, \gamma^{11}, \gamma^{13}\}.$$

Por tanto un cuerpo de descomposición de h sobre $\mathbb{Q}$ es $L_h := \mathbb{Q}(\gamma) = \mathbb{Q}(\xi) = L$, así que el grupo

$$G_{\mathbb{Q}}(h) = G(L : \mathbb{Q}) \cong \mathbb{Z}_6$$

es resoluble. Por el Teorema de Galois, h es resoluble por radicales sobre $\mathbb{Q}$. □

Número VII.5 Sean K un cuerpo de característica 0 y $a, b, c, d \in K$. ¿Es resoluble por radicales sobre K el polinomio

$$f(\mathtt{t}) := \mathtt{t}^8 + a\mathtt{t}^7 + b\mathtt{t}^6 + c\mathtt{t}^5 + d\mathtt{t}^4 + c\mathtt{t}^3 + b\mathtt{t}^2 + a\mathtt{t} + 1?$$

Solución. Como $f(0) \neq 0$, las raíces de f en un cierre algebraico $\overline{K}$ de K son las del cociente

$$\frac{f(\mathtt{t})}{\mathtt{t}^4} = \mathtt{t}^4 + \frac{1}{\mathtt{t}^4} + a\Big(\mathtt{t}^3 + \frac{1}{\mathtt{t}^3}\Big) + b\Big(\mathtt{t}^2 + \frac{1}{\mathtt{t}^2}\Big) + c\Big(\mathtt{t} + \frac{1}{\mathtt{t}}\Big) + d.$$

Además, podemos escribir

$$\mathtt{t}^2 + \frac{1}{\mathtt{t}^2} = \Big(\mathtt{t} + \frac{1}{\mathtt{t}}\Big)^2 - 2 \quad \& \quad \mathtt{t}^3 + \frac{1}{\mathtt{t}^3} = \Big(\mathtt{t} + \frac{1}{\mathtt{t}}\Big)^3 - 3\Big(\mathtt{t} + \frac{1}{\mathtt{t}}\Big),$$

mientras que para las potencias cuartas se tiene,

$$\mathtt{t}^4 + \frac{1}{\mathtt{t}^4} = \Big(\mathtt{t} + \frac{1}{\mathtt{t}}\Big)^4 - 4\Big(\mathtt{t}^2 + \frac{1}{\mathtt{t}^2}\Big) - 6 = \Big(\mathtt{t} + \frac{1}{\mathtt{t}}\Big)^4 - 4\Big(\mathtt{t} + \frac{1}{\mathtt{t}}\Big)^2 + 2.$$

Por ello, denotando $\mathtt{u} := \mathtt{t} + 1/\mathtt{t}$ reescribimos

$$\begin{aligned} f(\mathtt{t})/\mathtt{t}^4 &= \mathtt{u}^4 - 4\mathtt{u}^2 + 2 + a(\mathtt{u}^3 - 3\mathtt{u}) + b(\mathtt{u}^2 - 2) + c\mathtt{u} + d \\ &= \mathtt{u}^4 + a\mathtt{u}^3 + (b - 4)\mathtt{u}^2 + (c - 3a)\mathtt{u} + (d + 2 - 2b) := g(\mathtt{u}). \end{aligned}$$

Por el Corolario VII.1.12 el polinomio g es resoluble por radicales, pues $\deg(g) = 4$. Si u_1, u_2, u_3 y u_4 son las raíces de g en $\overline{K}$, las soluciones de las ecuaciones polinómicas $\mathtt{t}+1/\mathtt{t} = \mathtt{u}_i$ son las raíces de f en $\overline{K}$. La ecuación anterior es $\mathtt{t}^2 - u_i\mathtt{t} + 1 = 0$, que tiene por raíces a $t_i := (u_i \pm \sqrt{u_i^2 - 4})/2$, lo que prueba la resolubilidad por radicales de f. □

Número VII.6 (1) Sea $f \in \mathbb{Q}[\mathtt{t}]$ un polinomio irreducible cuyo grado es un número primo. Supongamos que f posee al menos dos raíces reales y alguna raíz en $\mathbb{C} \setminus \mathbb{R}$. ¿Es f resoluble por radicales sobre $\mathbb{Q}$?

(2) Sean $p \equiv 1 \bmod 4$ un número primo y $f \in \mathbb{Q}[\mathtt{t}]$ un polinomio irreducible de grado p cuyo discriminante es negativo. Probar que f no es resoluble por radicales sobre $\mathbb{Q}$.

Solución. (1) Sean $a, b \in \mathbb{R}$ y $\omega \in \mathbb{C} \setminus \mathbb{R}$ tres raíces de f. Si f fuese resoluble por radicales el cuerpo $\mathbb{Q}(a, b) \subset \mathbb{R}$ sería, por el Corolario VII.1.10, un cuerpo de descomposición de f sobre $\mathbb{Q}$. Pero esto es falso ya que $\omega \notin \mathbb{Q}(a, b)$ es raíz de f. Por tanto, f no es resoluble por radicales sobre $\mathbb{Q}$.

(2) Como el discriminante $\Delta(f) < 0$, se deduce del Ejercicio VII.13, vol. II que el número n de raíces de f en $\mathbb{C} \setminus \mathbb{R}$ no es múltiplo de 4. En particular $0 \neq n \neq p - 1$. Además $n \neq p$, por el Teorema de Bolzano. Dicho de otro modo, $1 \leq n \leq p - 2$, luego estamos en las condiciones del apartado anterior, así que f no es resoluble por radicales sobre $\mathbb{Q}$. □

Número VII.7 (1) Sean K un cuerpo de característica 0 y $a, b \in K$ tales que $a \neq 0$ y $f(\mathtt{t}) := \mathtt{t}^5 + a\mathtt{t} + b$ es irreducible en $K[\mathtt{t}]$. Probar que f es resoluble por radicales sobre K si y sólo si existen $u, v \in K$ tales que

$$a = \frac{3125uv^4}{(u-1)^4(u^2-6u+25)} \quad \& \quad b = \frac{3125uv^5}{(u-1)^4(u^2-6u+25)}.$$

(2) Sean $p \equiv 3 \bmod 4$ un número primo y $f(\mathtt{t}) := \mathtt{t}^5 + 2p\mathtt{t} + 2p^2$. ¿Es f resoluble por radicales sobre $\mathbb{Q}$?

Solución. (1) Como los grupos $\mathcal{A}_5$ y $\mathcal{S}_5$ no son resolubles, se desprende de la tabla VI.4.5 y del Teorema de Galois VII.1.1 que f es resoluble por radicales sobre K si y sólo si el grupo de Galois $G_K(f)$ es isomorfo a $\mathbb{Z}_5$, $\mathcal{D}_5$ o el grupo afín $\mathcal{F}_5$. En la citada tabla se observa que esto equivale a que la resolvente séxtica de f, que vale

$$R_{f,\mathtt{p}}(\mathtt{t}) = (\mathtt{t}^3 - 20a\mathtt{t}^2 + 240a^2\mathtt{t} + 320a^3)^2 - 2^{10}(256a^5 + 3125b^4)\mathtt{t},$$

posee alguna raíz $\omega \in K$. Como $a \neq 0$ definimos $u := \omega/a$ y $v := b/a$, y vamos a comprobar que se cumplen las igualdades del enunciado. Por un lado,

$$0 = R_{f,\mathtt{p}}(\omega) = \big((au)^3 - 20a(au)^2 + 240a^2(au) + 320a^3\big)^2 - 2^{10}\big(256a^5 + 3125(av)^4\big)(au).$$

Tras simplificar, y puesto que $a \neq 0$ la igualdad anterior se reescribe

$$u^6 - 10u^5 + 55u^4 - 140u^3 + 175u^2 - 160u + 25 = (u-1)^4(u^2 - 6u + 25).$$

Ahora basta despejar a y luego emplear que $b = av$ para obtener

$$a = \frac{3125uv^4}{(u-1)^4(u^2-6u+25)} \quad \& \quad b = \frac{3125uv^5}{(u-1)^4(u^2-6u+25)}.$$

(2) Supongamos que f es resoluble por radicales. Se deduce del apartado anterior que existen $u, v \in \mathbb{Q}$ tales que

$$2p = \frac{3125uv^4}{(u-1)^4(u^2-6u+25)} \quad \& \quad 2p^2 = \frac{3125uv^5}{(u-1)^4(u^2-6u+25)}.$$

Al dividir resulta $v = p$, lo que sustituído en la primera de las igualdades anteriores y dividiendo por p se tiene

$$2(u-1)^4(u^2-6u+25) = 5^5up^3.$$

Sean $x, y \in \mathbb{Z}$ primos entre sí tales que $u := x/y$, con lo que

$$2(x-y)^4(x^2-6xy+25y^2) = 5^5y^5xp^3 \quad \Longrightarrow \quad p|(x^2-6xy+25y^2) \quad \text{o} \quad p|(x-y).$$

Veamos que lo primero no puede darse. Según vimos en IV.1.13, vol. II, el primo p es irreducible en el anillo $\mathbb{Z}[i]$ de los enteros de Gauss, y denotando $\alpha := x - 3y \in \mathbb{Z}$ y $\beta := 4y \in \mathbb{Z}$,

$$x^2 - 6xy + 25y^2 = (x-3y)^2 + 16y^2 = \alpha^2 + \beta^2 = (\alpha + i\beta)(\alpha - i\beta).$$

Si $p|(x^2-6xy+25y^2) = (\alpha+i\beta)(\alpha-i\beta)$, entonces $p|(\alpha+i\beta)$ o $p|(\alpha-i\beta)$ en $\mathbb{Z}[i]$, así que $p|\alpha$ y $p|\beta$, es decir, $p|(x-3y)$ y $p|y$. Esto implica que p divide a x e y, lo que es falso ya que $\mathrm{mcd}(x,y) = 1$. Por tanto $p|(x-y)$, luego el primo p aparece elevado al exponente 4 en la factorización en $\mathbb{Z}$ de

$$5^5y^5xp^3 = 2(x-y)^4(x^2-6xy+25y^2),$$

y como $p \neq 5$, deducimos que p divide a xy^5. Por tanto $p|x$ o $p|y$, lo que unido a que $p|(x-y)$ implica que p divide a x y a y, lo que es falso ya que $\mathrm{mcd}(x,y) = 1$. Por fin, f no es resoluble por radicales sobre $\mathbb{Q}$. □

Número VII.8 Sean $\mathtt{x}, \mathtt{y}$ indeterminadas sobre $\mathbb{Q}$ y el polinomio

$$f(\mathtt{t}) := \mathtt{t}^5 + \frac{5\mathtt{y}^4(\mathtt{x}^2+1)^2(\mathtt{x}^2+\mathtt{x}-1)(\mathtt{x}^2-\mathtt{x}-1)}{4}\mathtt{t} + \frac{\mathtt{y}^5(\mathtt{x}^2+1)^3(\mathtt{x}^2+\mathtt{x}-1)(2\mathtt{x}-1)(\mathtt{x}+2)}{2}.$$

Demostrar que el grupo de Galois sobre $K := \mathbb{Q}(\mathtt{x}, \mathtt{y})$ del polinomio $f \in K[\mathtt{t}]$ es resoluble.

Solución. Obsérvese que $p := \mathtt{x}^2 + \mathtt{x} - 1$ es un elemento irreducible de $\mathbb{Q}[\mathtt{x}, \mathtt{y}]$ porque, como polinomio en $\mathbb{Q}[\mathtt{y}][\mathtt{x}]$, carece de raíces en $\mathbb{Q}[\mathtt{y}]$. Se deduce del Criterio de Eisenstein que f es irreducible en $\mathbb{Q}[\mathtt{x}, \mathtt{y}][\mathtt{t}]$ y, como $\mathbb{Q}[\mathtt{x}, \mathtt{y}]$ es un dominio de factorización única, el Lema de Gauss implica que f es irreducible en $K[\mathtt{t}]$.

Vamos a utilizar el Ejercicio anterior VII.7 para probar que el grupo $G_K(f)$ es resoluble. Esto equivale a que existan $u, v \in K$ tales que

$$\begin{aligned} \frac{5\mathtt{y}^4(\mathtt{x}^2+1)^2(\mathtt{x}^2+\mathtt{x}-1)(\mathtt{x}^2-\mathtt{x}-1)}{4} &= \frac{3125uv^4}{(u-1)^4(u^2-6u+25)} \quad \& \\ \frac{\mathtt{y}^5(\mathtt{x}^2+1)^3(\mathtt{x}^2+\mathtt{x}-1)(2\mathtt{x}-1)(\mathtt{x}+2)}{2} &= \frac{3125uv^5}{(u-1)^4(u^2-6u+25)}. \end{aligned} \tag{VII.26}$$

Al dividir miembro a miembro se obtiene

$$\frac{2\mathtt{y}(\mathtt{x}^2+1)(2\mathtt{x}-1)(\mathtt{x}+2)}{5(\mathtt{x}^2-\mathtt{x}-1)} = v \quad \Longrightarrow \quad \mathtt{y} = \frac{5v(\mathtt{x}^2-\mathtt{x}-1)}{2(\mathtt{x}^2+1)(2\mathtt{x}-1)(\mathtt{x}+2)}. \tag{VII.27}$$

Al sustituir este valor de $\mathtt{y}$ en la primera de las igualdades de (VII.26) y simplificar se obtiene

$$(\mathtt{x}^2+\mathtt{x}-1)(\mathtt{x}^2-\mathtt{x}-1)^5(u-1)^4(u^2-6u+25) = 64u(\mathtt{x}^2+1)^2(2\mathtt{x}-1)^4(\mathtt{x}+2)^4. \tag{VII.28}$$

Vamos a encontrar explícitamente $u \in K$ satisfaciendo la igualdad anterior y tomando como v la fracción racional que aparece en (VII.27) se obtiene una solución de (VII.26), y por ello $G_K(f)$ es resoluble.

La igualdad (VII.28) implica que u pertenece al cierre algebraico de $\mathbb{Q}(\mathtt{x})$ en K, esto es, $u \in \mathbb{Q}(\mathtt{x})$. Escribimos $u := g(\mathtt{x})/h(\mathtt{x})$ donde $g, h \in \mathbb{Q}[\mathtt{x}]$ son polinomios primos entre sí. Al sustituir esta expresión de u en (VII.28) y multiplicar ambos miembros por h^6 se tiene

$$(\mathtt{x}^2+\mathtt{x}-1)(\mathtt{x}^2-\mathtt{x}-1)^5(g-h)^4(g^2-6gh+25h^2) = 64gh^5(\mathtt{x}^2+1)^2(2\mathtt{x}-1)^4(\mathtt{x}+2)^4. \tag{VII.29}$$

Sea h_1 un factor irreducible y mónico de h en $\mathbb{Q}[\mathtt{x}]$. Como h_1 no divide a g tampoco divide a $g-h$ ni a $g^2-6gh+25h^2$, luego bien $h_1 = \mathtt{x}^2+\mathtt{x}-1$, bien $h_1 = \mathtt{x}^2-\mathtt{x}-1$. En el primer caso h_1 sería un factor de multiplicidad 1 del miembro de la izquierda en (VII.29) y de multiplicidad al menos 5 del miembro de la derecha, y esto es falso. En consecuencia, el único factor mónico irreducible de h es $h_1 := \mathtt{x}^2-\mathtt{x}-1$, y sin más que contar la multiplicidad de este factor en los dos miembros de (VII.29) deducimos que $h = \lambda h_1$ para cierto $\lambda \in \mathbb{Q}$. Simplificando resulta que

$$(\mathtt{x}^2+\mathtt{x}-1)(g-h)^4(g^2-6gh+25h^2) = 64\lambda^5 g(\mathtt{x}^2+1)^2(2\mathtt{x}-1)^4(\mathtt{x}+2)^4. \tag{VII.30}$$

Sea g_1 un factor mónico e irreducible de g en $\mathbb{Q}[\mathtt{x}]$. Como g_1 no divide a h tampoco divide a $g-h$ ni a $g^2-6gh+25h^2$, luego $g_1 := \mathtt{x}^2+\mathtt{x}-1$, y como aparece con

multiplicidad 1 en los dos miembros de (VII.30) deducimos que existe $\mu \in \mathbb{Q}$ tal que $g = \mu g_1$. Simplificando de nuevo,

$$(g-h)^4(g^2-6gh+25h^2) = 64\lambda^5\mu(\mathtt{x}^2+1)^2(2\mathtt{x}-1)^4(\mathtt{x}+2)^4. \qquad \text{(VII.31)}$$

Como el polinomio $g^2-6gh+25h^2 = (g-3h)^2+16h^2$ no tiene raíces reales, se sigue de (VII.31) que $g-h$ se anula en $\mathtt{x} := 1/2$ y $\mathtt{x} := -2$, luego es múltiplo del producto $(2\mathtt{x}-1)(\mathtt{x}+2)$. Contando multiplicidades deducimos que existe $\alpha \in \mathbb{Q}$ tal que

$$g-h = \alpha(2\mathtt{x}-1)(\mathtt{x}+2) = 2\alpha\mathtt{x}^2+3\alpha\mathtt{x}-2\alpha.$$

Por otro lado,

$$g-h = \mu g_1 - \lambda h_1 = \mu(\mathtt{x}^2+\mathtt{x}-1) - \lambda(\mathtt{x}^2-\mathtt{x}-1) = (\mu-\lambda)\mathtt{x}^2+(\mu+\lambda)\mathtt{x}+(\lambda-\mu),$$

e igualando las dos expresiones obtenidas para $g-h$ resulta

$$(\mu-\lambda)\mathtt{x}^2+(\mu+\lambda)\mathtt{x}+(\lambda-\mu) = g-h = 2\alpha\mathtt{x}^2+3\alpha\mathtt{x}-2\alpha.$$

Por tanto, $3(\mu-\lambda) = 2(\mu+\lambda)$, esto es, $\mu = 5\lambda$, y por (VII.31) existe $\beta \in \mathbb{Q}$ tal que

$$g^2-6gh+25h^2 = \beta(x^2+1)^2.$$

Ahora bien,

$$\begin{aligned} g^2-6gh+25h^2 &= \mu^2g_1^2-6\lambda\mu g_1h_1+25\lambda^2h_1^2 = 25\lambda^2(g_1^2+h_1^2)-30\lambda^2g_1h_1 \\ &= 5\lambda^2(10(\mathtt{x}^4-\mathtt{x}^2+1)-6(\mathtt{x}^4-3\mathtt{x}^2+1)) \\ &= 5\lambda^2(4\mathtt{x}^4+8\mathtt{x}^2+4) = 20\lambda^2(\mathtt{x}^2+1)^2, \end{aligned}$$

así que basta tomar $\lambda = 1$, $\mu = 5$ y $\beta = 20$, esto es,

$$u = \frac{g}{h} = \frac{\mu g_1}{\lambda h_1} = \frac{5(\mathtt{x}^2+\mathtt{x}-1)}{\mathtt{x}^2-\mathtt{x}-1} \quad \& \quad v = \frac{2\mathtt{y}(\mathtt{x}^2+1)(2\mathtt{x}-1)(\mathtt{x}+2)}{5(\mathtt{x}^2-\mathtt{x}-1)}.$$

□

Número VII.9 Sean $K := \mathbb{Q}(\mathtt{x})$ y $f(\mathtt{t}) := \mathtt{t}^5+5(5\mathtt{x}^2-1)\mathtt{t}+4(5\mathtt{x}^2-1)$. Calcular el grupo de Galois $G_K(f)$.

Solución. El polinomio f es irreducible en $\mathbb{Q}[\mathtt{x}][\mathtt{t}]$, luego en $K[\mathtt{t}]$, por el Criterio de Eisenstein, ya que $5\mathtt{x}^2-1$ es irreducible en $\mathbb{Q}[\mathtt{x}]$. Un cálculo sencillo muestra que el discriminante de f es

$$\begin{aligned} \Delta(f) &= 4^4\cdot 5^5(5\mathtt{x}^2-1)^5+4^4\cdot 5^5(5\mathtt{x}^2-1)^4 = 4^4\cdot 5^5(5\mathtt{x}^2-1)^4(5\mathtt{x}^2-1+1) \\ &= 4^4\cdot 5^6\cdot(5\mathtt{x}^2-1)^4\cdot\mathtt{x}^2 = (4^2\cdot 5^3\cdot(5\mathtt{x}^2-1)^2\cdot\mathtt{x})^2, \end{aligned}$$

que es un cuadrado en K. Esto implica, por VI VI.4.5, que $G_K(f)$ es el grupo alternado $\mathcal{A}_5$, el grupo diedral $\mathcal{D}_5$ o el grupo cíclico $\mathbb{Z}_5$. Probaremos que estamos en el primer

caso, para lo que basta demostrar que $G_K(f)$ no es resoluble. Si lo fuera existirían, en virtud del Ejercicio VII.7, $u, v \in K$ tales que

$$5(5\mathtt{x}^2-1) = \frac{3125uv^4}{(u-1)^4(u^2-6u+25)} \quad \& \quad 4(5\mathtt{x}^2-1) = \frac{3125uv^5}{(u-1)^4(u^2-6u+25)}.$$

Dividiendo se deduce que $v = 4/5$, luego estas condiciones implican que existe $u \in K$ tal que

$$(5\mathtt{x}^2-1)(u-1)^4(u^2-6u+25) = 256u. \tag{VII.32}$$

Esta igualdad muestra que $u \notin \mathbb{Q}[\mathtt{x}]$, pues en tal caso se tendría, contando grados,

$$2 + 4\deg(u) + 2\deg(u) = \deg(u),$$

que es imposible. Existen por tanto polinomios $g, h \in \mathbb{Q}[\mathtt{x}]$ primos entre sí tales que $\deg(h) \geq 1$ y $u = g/h$, y reemplazando este valor en (VII.32) se tiene

$$(5\mathtt{x}^2-1)(g-h)^4(g^2-6gh+25h^2) = 256gh^5. \tag{VII.33}$$

Sea h_1 un factor mónico e irreducible de h en $\mathbb{Q}[\mathtt{x}]$. Este polinomio no divide a $g-h$ ni a $g^2-6gh+25h^2$, luego necesariamente $h_1 = \mathtt{x}^2 - 1/5$. Si $\deg(g) \geq 1$ tomamos un factor mónico e irreducible g_1 de g en $\mathbb{Q}[\mathtt{x}]$ y el argumento anterior implica que $g_1 = \mathtt{x}^2 - 1/5$, lo que es imposible ya que g y h son primos entre sí. Podemos por tanto suponer que $g = 1$, y contando grados en la igualdad (VII.33) se obtiene una contradicción:

$$2 + 4\deg(h) + 2\deg(h) = 5\deg(h).$$

□

Número VII.10 Sean K un cuerpo de característica 0 y $\mathtt{t}, \mathtt{x}_1, \ldots, \mathtt{x}_n$ indeterminadas sobre K. Denotamos $\mathtt{s}_1, \ldots, \mathtt{s}_n$ las formas simétricas elementales en las indeterminadas $\mathtt{x}_1, \ldots, \mathtt{x}_n$ y consideramos el polinomio

$$f(\mathtt{t}) := \mathtt{t}^n + \sum_{j=0}^{n-1}(-1)^{n-j}\mathtt{s}_{n-j}\mathtt{t}^j = \prod_{k=1}^{n}(\mathtt{t}-\mathtt{x}_k)$$

y el cuerpo $L := K(\mathtt{s}_1, \ldots, \mathtt{s}_n)$. Demostrar que si $c_1, \ldots, c_n$ son elementos de K distintos dos a dos y $E := K(\mathtt{x}_1, \ldots, \mathtt{x}_n)$, entonces $u := \sum_{k=1}^n c_k\mathtt{x}_k$ es un elemento primitivo de la extensión $E|L$.

Solución. El contenido $L(u) \subset L(\mathtt{x}_1, \ldots, \mathtt{x}_n) = E$ es evidente, y para demostrar el recíproco se trata de ver que $[E : L(u)] = 1$. Como la extensión $E|L$ es de Galois también lo es $E|L(u)$, luego

$$[E : L(u)] = \operatorname{ord}\big(G(E : L(u))\big),$$

por lo que se trata de demostrar que el único L-automorfismo de E que deja fijo u es la identidad.

Por el Teorema de Abel, VI.2.2, el grupo de Galois $G(E:L)$ es el grupo simétrico $\mathcal{S}_n$, identificando cada permutación $\sigma \in \mathcal{S}_n$ con el L-automorfismo $\widetilde{\sigma}$ que cumple $\widetilde{\sigma}(\mathtt{x}_k) = \mathtt{x}_{\sigma(k)}$. Hemos de probar que si $\sigma \in \mathcal{S}_n$ y $\widetilde{\sigma}(u) = u$, entonces $\sigma = \mathrm{id}$. Sea $\tau := \sigma^{-1}$ y escribimos

$$\widetilde{\sigma}(u) = \widetilde{\sigma}\Big(\sum_{k=1}^{n} c_k \mathtt{x}_k\Big) = \sum_{k=1}^{n} c_k \mathtt{x}_{\sigma(k)} = \sum_{k=1}^{n} c_{\tau(k)} \mathtt{x}_k,$$

por lo que $\widetilde{\sigma}(u) = u$ si y sólo si

$$0 = u - \widetilde{\sigma}(u) = \sum_{k=1}^{n} c_k \mathtt{x}_k - \sum_{k=1}^{n} c_{\tau(k)} \mathtt{x}_k = \sum_{k=1}^{n} (c_k - c_{\tau(k)}) \mathtt{x}_k. \tag{VII.34}$$

Los elementos $\{\mathtt{x}_1, \ldots, \mathtt{x}_n\}$ son K-independientes, pues son K-algebraicamente independientes, de modo que de la igualdad (VII.34) se deduce que $c_k = c_{\tau(k)}$ para $1 \leq k \leq n$. Como los coeficientes c_k son distintos dos a dos lo anterior significa que τ es la permutación identidad. Por ello $\sigma = \mathrm{id}$ y $\widetilde{\sigma}$ es el automorfismo identidad. □

Número VII.11 (Lema de Artin) Sean G un grupo y K un cuerpo. Un *carácter* de G a valores en K es un homomorfismo de grupos $\chi : G \to K^*$.

(1) Probar que cualesquiera caracteres $\chi_1, \ldots, \chi_n$ de G a valores en K distintos dos a dos son linealmente independientes sobre K, o sea, para cada n-upla $(a_1, \ldots, a_n) \in K^n$ donde algún $a_i \neq 0$ existe $g \in G$ tal que

$$\sum_{k=1}^{n} a_k \chi_k(g) \neq 0.$$

(2) Sean $\alpha_1, \ldots, \alpha_\ell \in K$ no nulos y distintos dos a dos y $a_1, \ldots, a_\ell \in K$ tales que

$$\sum_{k=1}^{\ell} a_k \alpha_k^n = 0 \quad \forall\, n \in \mathbb{Z}.$$

Demostrar que $a_k = 0$ para $1 \leq k \leq \ell$.

Solución. (1) Supongamos, por reducción al absurdo, que existen $a_1, \ldots, a_n \in K^*$ tales que

$$\sum_{k=1}^{n} a_k \chi_k(g) = 0 \quad \forall\, g \in G, \tag{VII.35}$$

y el número n de sumandos es mínimo entre los que cumplen esta condición. Necesariamente $n \geq 2$, pues los caracteres toman valores en K^*. Vamos a llegar a contradicción

obteniendo una relación como la anterior en la que el número de sumandos es menor que n. Como $\chi_1 \neq \chi_2$ existe $g_1 \in G$ tales que $\chi_1(g_1) \neq \chi_2(g_1)$. Entonces,

$$\sum_{k=1}^{n} a_k \chi_k(g_1)\chi_k(g) = \sum_{k=1}^{n} a_k \chi_k(gg_1) = 0 \quad \forall\, g \in G.$$

Dividiendo por $\chi_1(g_1)$ obtenemos

$$a_1\chi_1(g) + \sum_{k=2}^{n} a_k \frac{\chi_k(g_1)\chi_k(g)}{\chi_1(g_1)} = 0 \quad \forall\, g \in G. \tag{VII.36}$$

Al restar las igualdades (VII.35) y (VII.36) resulta

$$\sum_{k=2}^{n} a_k \Big(\frac{\chi_k(g_1)}{\chi_1(g_1)} - 1\Big)\chi_k(g) \quad \forall\, g \in G.$$

Ésta es una relación entre los caracteres $\chi_2, \ldots, \chi_n$ y, por la minimalidad de n, todos los coeficientes han de ser nulos. Esto es falso, ya que por ser $a_2 \neq 0$ y $\chi_1(g_1) \neq \chi_2(g_1)$ se tiene

$$a_2\Big(\frac{\chi_2(g_1)}{\chi_1(g_1)} - 1\Big) \neq 0.$$

(2) Para $1 \leq k \leq \ell$ la aplicación $\chi_k : \mathbb{Z} \to K^*, n \mapsto \alpha_k^n$ es un carácter, ya que dados números enteros m, n se tiene

$$\chi_k(m+n) = \alpha_k^{m+n} = \alpha_k^m \cdot \alpha_k^n = \chi_k(m) \cdot \chi_k(n).$$

La hipótesis dice que

$$\sum_{k=1}^{\ell} a_k \chi_k(n) = 0 \quad \forall\, n \in \mathbb{Z},$$

y del apartado anterior se deduce que $a_k = 0$ para $1 \leq k \leq \ell$. □

Número VII.12 Sea K un cuerpo con q elementos y $\mathtt{t}$ una indeterminada sobre K.

(1) Calcular el orden del grupo de Galois $G(K(\mathtt{t}) : K)$.

(2) Para cada $a \in K^* = K \setminus \{0\}$ consideramos los K-automorfismos

$$\phi_a : K(\mathtt{t}) \to K(\mathtt{t}),\ \mathtt{t} \mapsto a\mathtt{t} \quad \& \quad \psi_a : K(\mathtt{t}) \to K(\mathtt{t}),\ \mathtt{t} \mapsto \mathtt{t} + a.$$

Sea $\gamma \in G\big(K(\mathtt{t}) : K\big)$ definido por $\gamma(\mathtt{t}) := 1/\mathtt{t}$. Demostrar que el grupo $G(K(\mathtt{t}) : K)$ está generado por el conjunto $S := \{\gamma, \phi_a, \psi_a : a \in K^*\}$.

(3) Sean L el cuerpo fijo de $G(K(\mathtt{t}) : K)$ y

$$u := \frac{(\mathtt{t}^{q^2} - \mathtt{t})^{q+1}}{(\mathtt{t}^q - \mathtt{t})^{q^2+1}}.$$

Demostrar que u es un elemento primitivo de la extensión $L|K$.

Solución. (1) Según se demuestra en IV.1.3, si $\mathrm{GL}_2(K)$ es el grupo multiplicativo de las matrices cuadradas de orden 2 con coeficientes en K y determinante no nulo y $\mathcal{H}$ su subgrupo formado por las matrices de la forma

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},$$

donde $\lambda \in K \setminus \{0\}$, entonces $G(K(\mathtt{t}) : K) \cong \mathrm{GL}_2(K)/\mathcal{H}$. Por tanto,

$$\mathrm{ord}(G(K(\mathtt{t}) : K)) = \mathrm{ord}(\mathrm{GL}_2(K))/\,\mathrm{ord}(\mathcal{H}) = \mathrm{ord}(\mathrm{GL}_2(K))/(q-1).$$

Las matrices de $\mathrm{GL}_2(K)$ tienen, por primera fila, cualquier vector no nulo de K^2, luego existen q^2-1 primeras filas de matrices en $\mathrm{GL}_2(K)$. Para cada una de ellas, la segunda fila ha de ser no múltiplo de la primera. Como cada fila no nula tiene, exactamente, q múltiplos distintos, el número de no múltiplos es q^2-q, por lo que

$$\mathrm{ord}(\mathrm{GL}_2(K) = (q^2-1)(q^2-q).$$

En consecuencia,

$$\mathrm{ord}(G(K(\mathtt{t}) : K)) = \frac{\mathrm{ord}(\mathrm{GL}_2(K))}{q-1} = \frac{(q^2-1)(q^2-q)}{q-1} = (q-1)q(q+1).$$

(2) La inclusión $\{\gamma, \phi_a, \psi_a : a \in K^*\} \subset G(K(\mathtt{t}) : K)$ es obvia, pues estas aplicaciones se corresponden con las matrices no singulares

$$\gamma \rightsquigarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \phi_a \rightsquigarrow \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \quad \& \quad \psi_a \rightsquigarrow \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

Para probar que generan el grupo $G(K(\mathtt{t}) : K)$ sean

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K) \quad \& \quad \beta \in G(K(\mathtt{t}) : K)$$

tales que $\beta(\mathtt{t}) := (a\mathtt{t}+b)/(c\mathtt{t}+d)$. Distinguimos varios casos.

Caso 1. Si $c = 0$, entonces $ad = \det(A) \neq 0$, luego $d \neq 0$ y

$$\beta(\mathtt{t}) = (a/d)\mathtt{t} + (b/d) = (\psi_{b/d} \cdot \phi_{a/d})(\mathtt{t}) \quad \Longrightarrow \quad \beta = \psi_{b/d} \cdot \phi_{a/d}.$$

Caso 2. Si $c \neq 0$ y $a = 0$, entonces $-bc = \det(A) \neq 0$, por lo que b y c son no nulos. Así, si $c_1 = c/b$ y $d_1 = d/c$ resulta

$$\beta(\mathtt{t}) = b/(c\mathtt{t}+d) = 1/(c_1\mathtt{t}+d_1) = (\gamma \cdot \phi_{c_1} \cdot \psi_{d_1})(\mathtt{t}) \quad \Longrightarrow \quad \beta = \gamma \cdot \phi_{c_1} \cdot \psi_{d_1}.$$

Caso 3. Si $ac \neq 0$ y $d = 0$, entonces $-bc = \det(A) \neq 0$. En consecuencia, $c \neq 0$ y denotando $a_1 := a/c$, $b_1 := b/c$ y $c_1 := a/b$ se tiene

$$\begin{aligned} \beta(\mathtt{t}) &= (a\mathtt{t}+b)/c\mathtt{t} = a_1 + b_1/\mathtt{t} = \gamma(b_1\mathtt{t}+a_1) = \gamma(\psi_{c_1}(b_1\mathtt{t})) \\ &= \gamma(\psi_{c_1}(\phi_{b_1}(\mathtt{t}))) = (\phi_{b_1} \cdot \psi_{c_1} \cdot \gamma)(\mathtt{t}) \quad \Longrightarrow \quad \beta = \phi_{b_1} \cdot \psi_{c_1} \cdot \gamma. \end{aligned}$$

Caso 4. Sólo queda analizar el caso en que tanto a como c y d son no nulos. Sea $r := ad - bc = \det(A) \neq 0$, y consideramos los K-automorfismos β_1 y β_2 definidos por

$$\beta_1(\mathtt{t}) := \frac{\mathtt{t} + b/a}{r/ad} \quad \& \quad \beta_2(\mathtt{t}) := \frac{a}{d\mathtt{t} + c},$$

que pertenecen al grupo $\langle S \rangle$ generado por S según hemos probado en los casos 1 y 2. Además,

$$(\beta_2 \cdot \gamma \cdot \beta_1)(\mathtt{t}) = (\gamma \cdot \beta_1)\Big(\frac{a}{d\mathtt{t} + c}\Big) = \beta_1\Big(\frac{a}{d/\mathtt{t} + c}\Big) = \beta_1\Big(\frac{a\mathtt{t}}{c\mathtt{t} + d}\Big) = \frac{a\big(\frac{\mathtt{t}+b/a}{r/ad}\big)}{c\big(\frac{\mathtt{t}+b/a}{r/ad}\big) + d}$$
$$= \frac{a\mathtt{t} + b}{c\mathtt{t} + (cb + r)/a} = \frac{a\mathtt{t} + b}{c\mathtt{t} + d} = \beta(\mathtt{t}),$$

por lo que también en este caso el automorfismo β pertenece al subgrupo $\langle S \rangle$.

(3) Por el apartado anterior, para probar que $u \in \mathrm{Fix}(G(K(\mathtt{t}) : K))$ basta probar que

$$\gamma(u) = u, \quad \phi_a(u) = u \quad \& \quad \psi_a(u) = u$$

para cada $a \in K^*$. Ahora bien, como $q^2 + 1$ y $q + 1$ tienen la misma paridad,

$$\gamma(u) = \frac{\Big(\frac{1}{\mathtt{t}^{q^2}} - \frac{1}{\mathtt{t}}\Big)^{q+1}}{\Big(\frac{1}{\mathtt{t}^q} - \frac{1}{\mathtt{t}}\Big)^{q^2+1}} = \frac{(\mathtt{t} - \mathtt{t}^{q^2})^{q+1}}{(\mathtt{t} - \mathtt{t}^q)^{q^2+1}} = \frac{(\mathtt{t}^{q^2} - \mathtt{t})^{q+1}}{(\mathtt{t}^q - \mathtt{t})^{q^2+1}} = u.$$

Por otro lado dado $a \in K^*$, y puesto que éste es un grupo multiplicativo de orden $q - 1$, se tiene

$$a^{q-1} = 1, \quad a^{q^2-1} = (a^{q-1})^{q+1} = 1 \quad \& \quad a^{q+1}/a^{q^2+1} = 1/a^{q^2-q} = (1/a^{q-1})^q = 1.$$

En consecuencia, $a^{q+1} = a^2 \cdot a^{q-1} = a^2 = a^2 \cdot a^{q^2-1} = a^{q^2+1}$, luego

$$\phi_a(u) = \frac{\big((a\mathtt{t})^{q^2} - a\mathtt{t}\big)^{q+1}}{\big((a\mathtt{t})^q - a\mathtt{t}\big)^{q^2+1}} = \frac{(a\mathtt{t}^{q^2} - a\mathtt{t})^{q+1}}{(a\mathtt{t}^q - a\mathtt{t})^{q^2+1}}$$
$$= \frac{a^{q+1}(\mathtt{t}^{q^2} - \mathtt{t})^{q+1}}{a^{q^2+1}(\mathtt{t}^q - \mathtt{t})^{q^2+1}} = \frac{\big(\mathtt{t}^{q^2} - \mathtt{t}\big)^{q+1}}{\big(\mathtt{t}^q - \mathtt{t}\big)^{q^2+1}} = u.$$

Por último se tiene

$$(\mathtt{t} + a)^q = \mathtt{t}^q + a \quad \& \quad (\mathtt{t} + a)^{q^2} = \mathtt{t}^{q^2} + a.$$

En efecto si $p := \mathrm{char}(K)$ existe un entero $s \geq 1$ tal que $q := p^s$, luego si denotamos $\phi : K(\mathtt{t}) \to K(\mathtt{t})$, $x \mapsto x^p$ el automorfismo de Frobenius de $K(\mathtt{t})$, cada potencia $\phi^n = \phi \circ \overset{n)}{\cdots} \circ \phi$ es un automorfismo de $K(\mathtt{t})$, por lo que

$$(\mathtt{t} + a)^q = \phi^s(\mathtt{t} + a) = \phi^s(\mathtt{t}) + \phi^s(a) = \mathtt{t}^{p^s} + a^{p^s} = \mathtt{t}^q + a^q = \mathtt{t}^q + a$$

y, análogamente, como $q^2 = p^{2s}$, se tiene

$$(\mathtt{t}+a)^{q^2} = \phi^{2s}(\mathtt{t}+a) = \phi^{2s}(\mathtt{t}) + \phi^{2s}(a) = \mathtt{t}^{p^{2s}} + a^{p^{2s}} = \mathtt{t}^{q^2} + a^{q^2} = \mathtt{t}^{q^2} + a.$$

En consecuencia, para cada $a \in K^*$ se cumple

$$\psi_a(u) = \frac{\big((\mathtt{t}+a)^{q^2} - (\mathtt{t}+a)\big)^{q+1}}{\big((\mathtt{t}+a)^q - (\mathtt{t}+a)\big)^{q^2+1}} = \frac{(\mathtt{t}^{q^2} - \mathtt{t})^{q+1}}{(\mathtt{t}^q - \mathtt{t})^{q^2+1}} = u.$$

Denotando $L := \mathrm{Fix}\big(G(K(\mathtt{t}) : K)\big)$ hemos demostrado que $K(u) \subset L$, y para probar la igualdad $L = K(u)$ basta ver que $[L : K(u)] = 1$. Aplicando la transitividad del grado a la cadena de cuerpos $K(u) \subset L \subset K(\mathtt{t})$ se tiene

$$[K(\mathtt{t}) : K(u)] = [K(\mathtt{t}) : L] \cdot [L : K(u)],$$

luego hemos de comprobar que $[K(\mathtt{t}) : K(u)] = [K(\mathtt{t}) : L]$, y para ello es suficiente ver que $[K(\mathtt{t}) : K(u)] \leq [K(\mathtt{t}) : L]$. Acotamos el grado de la extensión $K(\mathtt{t})|K(u)$ mediante el Teorema de Lüroth. Denotamos $\mathtt{x} := \mathtt{t}^{q-1}$, de modo que

$$f(\mathtt{t}) := \frac{\mathtt{t}^{q^2-1} - 1}{\mathtt{t}^{q-1} - 1} = \frac{\big(\mathtt{t}^{q-1}\big)^{q+1} - 1}{\mathtt{t}^{q-1} - 1} = \frac{\mathtt{x}^{q+1} - 1}{\mathtt{x} - 1} = \sum_{k=0}^{q} \mathtt{x}^k = \sum_{k=0}^{q} \mathtt{t}^{k(q-1)},$$

por lo que $f \in K[\mathtt{t}]$ es un polinomio de grado $q(q-1)$. En consecuencia,

$$f^{q+1} \in K[\mathtt{t}] \quad \& \quad \deg(f^{q+1}) = q(q-1)(q+1) = q(q^2-1).$$

Escribimos ahora

$$\begin{aligned} u := \frac{(\mathtt{t}^{q^2} - \mathtt{t})^{q+1}}{(\mathtt{t}^q - \mathtt{t})^{q^2+1}} &= \frac{\mathtt{t}^{q+1}(\mathtt{t}^{q^2-1} - 1)^{q+1}}{\mathtt{t}^{q^2+1}(\mathtt{t}^{q-1} - 1)^{q^2+1}} \\ &= \frac{(\mathtt{t}^{q^2-1} - 1)^{q+1}}{\mathtt{t}^{q^2-q}(\mathtt{t}^{q-1} - 1)^{q+1}(\mathtt{t}^{q-1} - 1)^{q^2-q}} = \frac{f^{q+1}(\mathtt{t})}{\big(\mathtt{t}^q - \mathtt{t}\big)^{q^2-q}}, \end{aligned}$$

y por la Observación III.1.2,

$$\begin{aligned} [K(\mathtt{t}) : K(u)] &\leq \max\{\deg(f^{q+1}), \deg\big((\mathtt{t}^q - \mathtt{t})^{q^2-q}\big)\} \\ &= \max\{q(q^2-1), q(q^2-q)\} = q^3 - q. \end{aligned}$$

Para terminar es suficiente probar que $s := q^3 - q \leq [K(\mathtt{t}) : L]$. Recordemos que en el primer apartado hemos demostrado que $\mathrm{ord}\big(G(K(\mathtt{t}) : K)\big) = s$, y suponemos, por reducción al absurdo, que $[K(\mathtt{t}) : L] := r < s$.

Denotemos $G(K(\mathtt{t}) : K) = \{\sigma_1, \ldots, \sigma_s\}$ y $\mathcal{B} = \{\zeta_1, \ldots, \zeta_r\}$ una base de $K(\mathtt{t})$ como L-espacio vectorial. Denotamos $a_{ij} := \sigma_j(\zeta_i) \in K(\mathtt{t})$ y consideramos el sistema homogéneo de ecuaciones lineales

$$\begin{cases} a_{11}x_1 & + & \cdots & + & a_{1s}x_s & = & 0 \\ \vdots & & & & \vdots & & \vdots \\ a_{r1}x_1 & + & \cdots & + & a_{rs}x_s & = & 0 \end{cases}$$

Como el sistema tiene más incógnitas que ecuaciones admite una solución no trivial, que denotamos $c_1, \dots, c_s$, y vamos a demostrar que $\sum_{j=1}^{s} c_j\sigma_j = 0$, lo que contradice el Lema de Artin-Dedekind, VII.1.7. En efecto, dado $\zeta \in K(\mathtt{t})$ existen $b_1, \dots, b_r \in L$ tales que $\zeta := \sum_{i=1}^{r} b_i\zeta_i$. Cada σ_j es un L-automorfismo, por lo que $\sigma_j(b_i) = b_i$, luego

$$\Big(\sum_{j=1}^{s} c_j\sigma_j\Big)(\zeta) = \sum_{j=1}^{s} c_j\sigma_j(\zeta) = \sum_{j=1}^{s} c_j\sigma_j\Big(\sum_{i=1}^{r} b_i\zeta_i\Big)$$
$$= \sum_{i=1}^{r} b_i \sum_{j=1}^{s} c_j\sigma_j(\zeta_i) = \sum_{i=1}^{r} b_i \sum_{j=1}^{s} a_{ij}c_j = 0,$$

lo que demuestra que $\sum_{j=1}^{s} c_j\sigma_j = 0$ como pretendíamos. □

Número VII.13 (Ternas pitagóricas) Emplear el Teorema 90 de Hilbert para demostrar que una terna (x, y, z) de números enteros no nulos primos dos a dos cumple $x^2 + y^2 = z^2$ si y sólo si existen $s, m, n \in \mathbb{Z}$ tales que $s \neq 0$ y

$$(sx, sy, sz) = (m^2 - n^2, 2mn, m^2 + n^2).$$

Solución. Las ternas del enunciado cumplen la relación $x^2 + y^2 = z^2$ pues

$$s^2(x^2+y^2) = (m^2-n^2)^2+(2mn)^2 = m^4+n^4-2m^2n^2+4m^2n^2 = (m^2+n^2)^2 = s^2z^2,$$

y basta dividir ambos miembros por s^2.

Recíprocamente, sea $(x, y, z) \in \mathbb{Z}^3$ tal que $x^2 + y^2 = z^2$. Denotamos $i := \sqrt{-1}$. La extensión $\mathbb{Q}(i)|\mathbb{Q}$ tiene grado 2, luego es de Galois, y el grupo $G\big(\mathbb{Q}(i) : \mathbb{Q}\big)$ está formado por la identidad y la restricción $\tau : \mathbb{Q}(i) \to \mathbb{Q}(i)$, $u + iv \mapsto u - iv$ de la conjugación compleja. Así, la norma $\mathsf{N} : \mathbb{Q}(i) \to \mathbb{Q}$ asociada a esta extensión es

$$\mathsf{N} : \mathbb{Q}(i) \to \mathbb{Q},\ \zeta := u + iv \mapsto \zeta \cdot \tau(\zeta) = (u + iv)(u - iv) = u^2 + v^2.$$

Como $x^2 + y^2 = z^2$ y $z \neq 0$, se tiene $(x/z)^2 + (y/z)^2 = 1$, es decir, la norma de $\zeta := (x/z) + i(y/z)$ vale 1. Por el Teorema 90 de Hilbert existe $\alpha \in \mathbb{Q}(i)$ tal que $\zeta := \alpha/\tau(\alpha)$. Sean $m, n, t \in \mathbb{Z}$ tales que $\alpha = (m/t)+i(n/t)$. Así $\tau(\alpha) = (m/t)-i(n/t)$, y por tanto

$$\frac{x}{z} + \frac{yi}{z} = \zeta = \frac{\alpha}{\tau(\alpha)} = \frac{m+in}{m-in} = \frac{(m+in)^2}{m^2+n^2} = \frac{m^2-n^2}{m^2+n^2} + \frac{2mni}{m^2+n^2}.$$

Como $\mathrm{mcd}(x, z) = \mathrm{mcd}(y, z) = 1$ existe $s \in \mathbb{Z} \setminus \{0\}$ que cumple

$$sx = m^2 - n^2, \quad sy = 2mn \quad \& \quad sz = m^2 + n^2.$$

□

Número VII.14 (Forma aditiva del Teorema 90 de Hilbert) (1) Sean $L|K$ una extensión de Galois y $x \in L$. Se llama *traza* de x a

$$\mathsf{T}(x) := \sum_{\sigma \in G(L:K)} \sigma(x).$$

Demostrar que $\mathsf{T}(x) \in K$.

(2) Supongamos que $\mathrm{char}(K) = 0$ y que el grupo de Galois $G(L:K) := \langle \sigma \rangle$ es cíclico. Probar que la traza de un elemento $x \in L$ es nula si y sólo si existe $\alpha \in L$ tal que $x = \alpha - \sigma(\alpha)$.

Solución. (1) Como la extensión $L|K$ es de Galois, K está formado por los elementos de L que quedan fijos bajo la acción de cada automorfismo $\tau \in G = G(L:K)$. Empleando la Proposición I.1.3, vol. I, resulta

$$\tau(\mathsf{T}(x)) = \tau\Big(\sum_{\phi \in G} \phi(x)\Big) = \sum_{\phi \in G} (\phi \cdot \tau)(x) = \sum_{\psi \in G} \psi(x) = \mathsf{T}(x).$$

(2) Denotemos $n := \mathrm{ord}(G)$. Entonces, si $x := \alpha - \sigma(\alpha)$ para algún $\alpha \in L$ la traza de x es nula ya que, por ser $\sigma^n = \sigma_0 = \mathrm{id}_L$,

$$\mathsf{T}(x) = \sum_{j=0}^{n-1} \sigma^j(x) = \sum_{j=0}^{n-1} \sigma^j\big(\alpha - \sigma(\alpha)\big) = \sum_{j=0}^{n-1} \sigma^j(\alpha) - \sum_{j=1}^{n} \sigma^j(\alpha) = \sigma^0(\alpha) - \sigma^n(\alpha) = 0.$$

Recíprocamente, supongamos que $\mathsf{T}(x) = 0$ y, puesto que $\mathrm{char}(K) = 0$, tiene sentido definir

$$\alpha := \frac{1}{n} \sum_{j=0}^{n-2} \Big(\sum_{k=0}^{j} \sigma^k(x) \Big) \in L.$$

Como $\sigma(n) = n$ puesto que $\sigma(1) = 1$, resulta que

$$\sigma(\alpha) = \frac{1}{n} \sum_{j=0}^{n-2} \Big(\sum_{k=0}^{j} \sigma^{k+1}(x) \Big).$$

Restando las expresiones de α y $\sigma(\alpha)$ que acabamos de calcular, y puesto que $\mathsf{T}(x) = 0$, tenemos

$$\begin{aligned} \alpha - \sigma(\alpha) &= \frac{1}{n} \sum_{j=0}^{n-2} \Big(\sum_{k=0}^{j} \sigma^k(x) - \sum_{k=0}^{j} \sigma^{k+1}(x) \Big) = \frac{1}{n} \sum_{j=0}^{n-2} (x - \sigma^{j+1}(x)) \\ &= \frac{(n-1)x}{n} - \frac{1}{n} \sum_{\ell=1}^{n-1} \sigma^\ell(x) = \frac{(n-1)x - (\mathsf{T}(x) - x)}{n} = x. \end{aligned}$$

□

Número VII.15 (Teorema de la base normal) Sean K un cuerpo de característica 0 y $L|K$ una extensión de Galois cuyo grupo de Galois es $G(L:K) := \{\sigma_1, \ldots, \sigma_n\}$.

(1) Probar que existe $u \in L$ tal que la matriz $A := (a_{ij}) \in \mathcal{M}_n(L)$ cuyos coeficientes son $a_{ij} := \sigma_i(\sigma_j^{-1}(u))$ tiene determinante no nulo.

(2) Probar que el conjunto $\mathcal{B} := \{\sigma_j(u) : 1 \leq j \leq n\}$ es una base de L como K-espacio vectorial.

Solución. (1) Por el Teorema del elemento primitivo II.2.2, existe $\theta \in L$ tal que $L = K(\theta)$. Como los K-automorfismos de L quedan determinados por la imagen de θ, los elementos del conjunto $R := \{\sigma_k(\theta) : 1 \leq k \leq n\}$ son distintos dos a dos. En particular, si suponemos que $\sigma_1 := \mathrm{id}$,

$$c := \prod_{k=2}^{n} \big(\theta - \sigma_k(\theta)\big) \neq 0,$$

luego el polinomio $f(\mathtt{t}) := \frac{1}{c}\prod_{k=2}^{n}\big(\mathtt{t} - \sigma_k(\theta)\big) \in L[\mathtt{t}]$ cumple que $f(\theta) = 1$.

Además, para cada par de índices distintos i, j comprendidos entre 1 y n existe otro índice k con $2 \leq k \leq n$ tal que $\sigma_j(\sigma_i^{-1}(\theta)) = \sigma_k(\theta)$, por lo que $f(\sigma_j(\sigma_i^{-1}(\theta))) = 0$. En consecuencia, $f(\sigma_j(\sigma_i^{-1}(\theta))) = \delta_{ij}$, donde δ es la delta de Kronecker.

Para cada par de índices, no necesariamente distintos, $1 \leq i, j \leq n$ consideremos el isomorfismo de anillos

$$\Phi_{ij} : L[\mathtt{t}] \to L[\mathtt{t}],\ \sum_{k=0}^{d} c_k \mathtt{t}^k \mapsto \sum_{k=0}^{d} (\sigma_j^{-1} \cdot \sigma_i)(c_k)\mathtt{t}^k.$$

Nótese que dados $1 \leq i, j \leq n$ la restricción $\Phi_{ij}|_L = \sigma_j^{-1} \cdot \sigma_i$ y $\Phi_{ij}(f)(\theta) = \delta_{ij}$. Esto último es evidente si $i = j$ pues Φ_{ii} es el homomorfismo identidad, y por ello $\Phi_{ii}(f)(\theta) = f(\theta) = 1$. Suponemos ahora que $i \neq j$, por lo que $\sigma_i^{-1} \cdot \sigma_j = \sigma_\ell$ para algún índice $2 \leq \ell \leq n$. Como Φ_{ij} es homomorfismo de anillos y,

$$\Phi_{ij}(\mathtt{t} - \sigma_k(\theta)) = \mathtt{t} - (\sigma_j^{-1} \cdot \sigma_i)(\sigma_k(\theta)) = \mathtt{t} - \sigma_\ell^{-1}(\sigma_k(\theta)),$$

se tiene

$$\Phi_{ij}(f) = \frac{1}{\sigma_\ell^{-1}(c)} \prod_{k=2}^{n} \big(\mathtt{t} - \sigma_\ell^{-1}(\sigma_k(\theta))\big)$$

y, como $2 \leq \ell \leq n$ uno de los factores de grado 1 del polinomio $\Phi_{ij}(f)$ es $\mathtt{t} - \theta$, luego $\Phi_{ij}(f)(\theta) = 0$.

Consideremos la matriz $M(\mathtt{t}) := (m_{ij}(\mathtt{t}))$ de orden n cuyos coeficientes son los polinomios $m_{ij}(\mathtt{t}) := \Phi_{ij}(f)(\mathtt{t}) \in L[\mathtt{t}]$, y el polinomio $g(\mathtt{t}) := \det(M(\mathtt{t})) \in L[\mathtt{t}]$.

Este polinomio no es nulo ya que $M(\theta)$ es la matriz identidad, por lo que $g(\theta) = 1$. En consecuencia g tiene un número finito de raíces en un cierre algebraico de K y, como K es infinito por ser de característica 0, existe $\zeta \in K$ tal que $g(\zeta) \neq 0$.

Como cada σ_k es un K-automorfismo, $(\sigma_j^{-1}\cdot\sigma_i)(\zeta)=\zeta$ para $1\le i,j\le n$, y denotando $\sigma_j^{-1}\cdot\sigma_i:=\sigma_s$ se tiene

$$(\sigma_j^{-1}\cdot\sigma_i)(f(\zeta))=\sigma_s(f(\zeta))=\sigma_s\Big(\frac{1}{c}\prod_{k=2}^{n}\big(\zeta-\sigma_k(\theta)\big)\Big)$$
$$=\frac{1}{\sigma_s(c)}\prod_{k=2}^{n}\big(\zeta-\sigma_s(\sigma_k(\theta))\big)=\Phi_{ij}(f)(\zeta).$$

En consecuencia, $u:=f(\zeta)\in L$ cumple, con las notaciones del enunciado,

$$a_{ij}=\sigma_i(\sigma_j^{-1}(u))=(\sigma_j^{-1}\cdot\sigma_i)(u)=(\sigma_j^{-1}\cdot\sigma_i)(f(\zeta))=\Phi_{ij}(f)(\zeta),$$

es decir, $a_{ij}=m_{ij}(\zeta)$, o lo que es lo mismo, $A=M(\zeta)$, y por tanto

$$\det(A)=\det(M(\zeta))=g(\zeta)\neq 0.$$

(2) Consideremos el elemento $u\in L$ obtenido en el apartado anterior. Como la extensión $L|K$ es de Galois, $[L:K]=\operatorname{ord}\big(G(L:K)\big)=n$, luego para probar que $\mathcal{B}$ es base de L como K-espacio vectorial es suficiente demostrar que sus elementos son K-linealmente independientes. Para utilizar las notaciones del apartado anterior escribimos $\mathcal{B}:=\{\sigma_j^{-1}(u):1\le j\le n\}$, y hemos de probar que si $x_1,\dots,x_n\in K$ satisfacen la igualdad

$$\sum_{j=1}^{n}x_j\sigma_j^{-1}(u)=0,$$

entonces $x_1=0,\dots,x_n=0$. Para $1\le i\le n$ se tiene

$$\sum_{j=1}^{n}x_j\big(\sigma_i(\sigma_j^{-1}(u)\big)=\sigma_i\Big(\sum_{j=1}^{n}x_j\sigma_j^{-1}(u)\Big)=\sigma_i(0)=0. \tag{VII.37}$$

Pero $a_{ij}:=\sigma_i(\sigma_j^{-1}(u))\in L$ y (VII.37) se escribe $\sum_{j=1}^{n}a_{ij}x_j=0$ para $1\le i\le n$. Si denotamos $x:=(x_1,\dots,x_n)\in K^n\subset L^n$, las ecuaciones (VII.37) anteriores se escriben en forma matricial como $Ax^t=0$. Por el Teorema de Rouché, y puesto que $\det(A)\neq 0$, se deduce que cada $x_i=0$, lo que prueba que $\mathcal{B}$ es base. □

Número VII.16 Sean m y n enteros positivos y $M:=\operatorname{mcm}(m,n)$ su mínimo común múltiplo. Supongamos que los polígonos regulares de m y n lados son constructibles con regla y compás. Demostrar que también es constructible con regla y compás el polígono con M lados.

Solución. Si $m=2^r$ y $n=2^s$ para ciertos enteros $r,s\ge 2$, entonces $M=2^{\max\{r,s\}}$ y la constructibilidad del polígono regular de M lados es obvia. Supongamos que $m=2^r$ es potencia de 2 pero n no lo es. Entonces, existen números primos $p_1,\dots,p_k$

distintos dos a dos tales que cada $p_j = 2^{2^{s_j}} + 1$, donde s_j es un entero no negativo, $n = 2^s p_1 \cdots p_k$, y si $t := \text{máx}\{r, s\}$,

$$M = \text{mcm}(m, n) = 2^t p_1 \cdots p_k.$$

Aplicando de nuevo el Corolario VII.2.18 se deduce que el polígono con M lados es constructible. Como los papeles de m y n son intercambiables sólo falta estudiar el caso en que

$$m = 2^r q_1 \cdots q_\ell \quad \& \quad n = 2^s p_1 \cdots p_k,$$

para ciertos enteros no negativos r y s, y números primos $q_i := 2^{2^{r_i}} + 1$ distintos dos a dos y $p_j := 2^{2^{s_j}} + 1$, también distintos dos a dos. Denotamos $t := \text{máx}\{r, s\}$ y podemos suponer que $p_i = q_i$ para $1 \leq i \leq \nu \leq \text{mín}\{k, \ell\}$. Entonces,

$$M = \text{mcm}(m, n) = 2^t q_1 \cdots q_\ell \cdot p_{\nu+1} \cdots p_k,$$

y la constructibilidad del polígono de M lados se deduce, de nuevo, del Corolario VII.2.18. □

Número VII.17 Demostrar que si n es un divisor de $2^{32} - 1$, el polígono regular de n lados es constructible con regla y compás.

Solución. Al factorizar $2^{32} - 1$ como producto de números primos se tiene

$$\begin{aligned} 2^{32} - 1 &= (2^{16} + 1)(2^{16} - 1) = (2^{16} + 1)(2^8 + 1)(2^8 - 1) \\ &= (2^{16} + 1)(2^8 + 1)(2^4 + 1)(2^4 - 1) \\ &= (2^{16} + 1)(2^8 + 1)(2^4 + 1)(2^2 + 1)(2^2 - 1), \end{aligned}$$

aunque la comprobación de la primalidad de $2^{16} + 1 = 65537$ es tediosa. Por tanto, todos los factores primos de n son de la forma $2^{2^r} + 1$, lo que implica, por el Corolario VII.2.18, que el polígono regular de n lados es constructible. □

Número VII.18 ¿Para qué valores del entero positivo n es trisecable con regla y compás el ángulo $2\pi/n$?

Solución. Hay que decidir para qué valores de n el ángulo $2\pi/3n$ es constructible. Por el Corolario VII.2.18, esto equivale a que existan un entero $r \geq 0$ y primos impares $p_1 < \cdots < p_k$ tales que $p_j = 2^{2^{r_j}} + 1$, donde $r_j \geq 0$ es un entero, y $3n = 2^r p_1 \cdots p_k$. Esto implica que $p_1 = 3$, por lo que $n = 2^r p_2 \cdots p_k$ y $5 \leq p_2 < \cdots < p_k$. Éstos son los enteros que cumplen que el ángulo $2\pi/n$ es trisecable con regla y compás. □

Bibliografía

La resolución de ecuaciones polinómicas constituyó el hilo conductor del Álgebra hasta mediados del siglo XIX. En el siglo XVI los matemáticos italianos Ferro y Ferrari obtuvieron fórmulas que expresan mediante radicales las raíces de los polinomios de grado tres y cuatro, respectivamente. Por ello creemos que resulta muy motivadora la lectura del siguiente libro, que presenta un estudio muy detallado de las distintas soluciones de este problema obtenidas por matemáticos españoles. Su lectura detenida pone de manifiesto las limitaciones de los diversos procedimientos si el grado es mayor que cuatro.

(1) R. Moreno, *Andanzas y aventuras de las ecuaciones cúbica y cuártica a su paso por España.* Editorial Complutense. Línea 300, (2011).

Fueron Abel y Galois quienes demostraron la irresolubilidad de algunas ecuaciones polinómicas. En el libro siguiente se expone admirablemente la obra del segundo de ellos.

(2) P. Neumann ed., *The mathematical writings of Évariste Galois.* European Mathematical Society, (2011).

Los resultados de Abel y Galois prueban que existen polinomios de grado 5 no resolubles por radicales cuyos coeficientes son números enteros. Los polinomios de grado 5 están íntimamente relacionados con la geometría del icosaedro, y el texto de Klein que citamos a continuación, cuya lectura no es sencilla, muestra la extraordinaria riqueza matemática que encierra la ecuación quíntica y constituye un ejemplo representativo de la fuerte interrelación entre el álgebra y la geometría.

(3) F. Klein, *Lectures on the Icosahedron and the solution of equations of fifth degree.* Dover, (2003).

El siguiente texto es de carácter mucho más elemental, pero nos parece muy recomendable para quien se inicia en este campo.

(4) J. Bewersdorff, *Galois Theory for beginners. A historical approach.* A.M.S. Student Mathematical Library. vol. **35**, (2006).

Para los interesados en la vida de los matemáticos más insignes y no sólo en su quehacer científico pueden resultar de interés las biografías de los dos personajes claves en este campo, Abel y Galois.

(5) C. Sánchez, T. Noriega, *Abel. El romántico noruego.* Nivola, (2005).

(6) F. Corbalán, *Galois. Revolución y matemáticas.* Nivola, (2006).

Por otro lado, y especialmente dirigida a quienes deseen adquirir una adecuada perspectiva histórica de la teoría de Galois, citamos la obra:

(7) J.P. Tignol, *Galois theory of algebraic equations.* World Scientific, Singapur, (2001).

Más aún, existen varios libros muy bien escritos que tratan la historia del álgebra, y no sólo de la teoría de Galois. Entre ellos nos parecen sobresalientes los siguientes.

(8) I. Bashmakova, G. Smirnova, *The beginnings and evolution of Algebra.* The Dolciani Mathematical Expositions, **23**. The Mathematical Association of America, (2000).

(9) I. Kleiner, *A History of Abstract Algebra.* Birkhäuser, (2007).

Libros que se adaptan al contenido de este texto.

La teoría de Galois ha merecido la atención de innumerables algebristas, por lo que son muchos los textos dedicados a exponerla. Un clásico entre los clásicos fue escrito por Emil Artin, y en él se presenta por vez primera la teoría de Galois como la entendemos actualmente. La editorial Vicens Vives publicó una traducción al castellano en 1970.

(10) E. Artin, *Galois Theory.* Notre Dame Mathematical Lectures **2**, University of Notre Dame Press, (1971).

Otro libro excepcional fue escrito por Ian Stewart en 1973. Su tercera edición, del año 2003, constituye una mejora sustancial del texto original.

(11) I. Stewart, *Galois Theory.* CRC Press, (2003).

Entre los textos en castellano nos permitimos recomendar los siguientes, que conocemos muy bien.

(12) F. Delgado, C. Fuertes, S. Xambó, *Introducción al Álgebra. Anillos, factorización y teoría de cuerpos.* Universidad de Valladolid, (1993).

(13) J.M. Gamboa, J.M. Ruiz, *Anillos y cuerpos conmutativos.* Cuadernos de la UNED, (2002).

Libros que permiten ampliar conocimientos.

Nuestra presentación de la Teoría de Galois ha obviado, deliberadamente, las cuestiones relativas a las extensiones infinitas y las inseparables. En los textos que se citan a continuación se tratan cuidadosamente las dificultades técnicas que ambas generalizaciones suponen, e incluso en el ámbito de las extensiones finitas de cuerpos de característica cero, se presentan resultados de mayor profundidad que los expuestos en nuestro libro.

(14) D.A. Cox, *Galois Theory.* Wiley, (2012).

(15) T.H. Hungerford, *Algebra.* GTM **73**. Springer (1980).

(16) N. Jacobson, *Basic Algebra.* I. Dover, (2009).

(17) P. J. Morandi, *Field and Galois Theory.* GTM **167**. Springer (1996).

Aunque su lectura resulta áspera, es obligatorio citar la última edición del manual de Álgebra de Lang, que en nuestra opinión no mejora la edición de Addison-Wesley de 1965, de la que existe una traducción al castellano editada por Aguilar, pero cubre un material aún más amplio.

(18) S. Lang, *Algebra.* GTM **211**, Springer-Verlag, (2002).

El siguiente es un excelente libro de consulta tanto para el alumno como para el profesor.

(19) D.S. Dummit, R.M. Foote, *Abstract Algebra.* Wiley, (2003).

Libros con ejercicios resueltos.

(20) A. Bigard, *Problèmes d'Algèbre Générale,* Dunod, Paris, (1971).

(21) T.S. Blyth, E.F. Robertson (Editores), *Algebra Through Practice:* vol. 6, Rings, Fields and Modules. A Collection of Problems in Algebra with Solutions. Chapman & Hall, (1985).

(22) F. Delgado, C. Fuertes, S. Xambó, *Introducción al Álgebra. Soluciones de los Problemas.* Universidad de Valladolid, (2000).

(23) J.M. Gamboa, J.M. Ruiz, *Anillos y cuerpos conmutativos.* Cuadernos de la UNED, (2002).

Índice