Capítulo 3

Teoría de Galois

3.1. Extensiones normales y separables

La teoría de Galois trata de representar la estructura de la extensión generada por todas las raíces de un polinomio, por medio de sus simetrías. Para que este proyecto funcione en un contexto general son necesarias dos condiciones. La primera es que realmente podamos inventarnos un sitio donde vivan las raíces de un polinomio (¿dónde están las raíces de $x^2 + 1 \in \mathbb{F}_3[x]$?). La segunda está en los márgenes de los contraejemplos del curso por su naturaleza mucho más técnica, y es que ningún elemento sea raíz múltiple de todos los polinomios que anula. Esto provocaría que algunas simetrías colapsasen y que no representaran fielmente la extensión. Como veremos más adelante, no hay que preocuparse mucho por esta condición, porque la cumplen prácticamente todas las extensiones que podemos imaginar este curso.

La primera condición, a la que dedicaremos casi todos nuestros esfuerzos en esta sección, tiene que ver con los conceptos de cuerpo de descomposición y de extensión normal. En breve probaremos que ambos están estrechamente relacionados y que son en cierto modo equivalentes para extensiones finitas, pero ahora limitémonos a sus definiciones. En ellas y en el resto del capítulo utilizaremos el abuso de notación consistente en hablar de la descomposición de $P \in K[x]$ en $L[x]$ cuando L/K es una extensión. En rigor el polinomio P sólo está en $L[x]$ después de aplicar el monomorfismo de la extensión $j : K \longrightarrow L$ a sus coeficientes. (Quien no entienda este comentario no debe preocuparse porque tampoco detectará el abuso de notación).

Definición: Se dice que una extensión algebraica L/K es *normal* si todo polinomio irreducible $P \in K[x]$ que tiene una raíz en L se descompone en factores lineales en $L[x]$.

Definición: Sea L/K una extensión. Se dice que L es un *cuerpo de descomposición* (o *cuerpo raíz*) de $P \in K[x]$, $\partial P > 1$, si P se descompone en factores lineales en $L[x]$, esto es, $P = k(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)$, y no existe ningún subcuerpo propio de L (conteniendo la imagen de K en L) con esta propiedad.

Observación: Con la notación de la definición anterior, imponiendo $L \supset K$, se tiene que el cuerpo de descomposición de P es $L = K(\alpha_1, \alpha_2, \dots, \alpha_n)$, el cuerpo más pequeño

que contiene a las raíces. Sin embargo no hay que olvidar que fuera de $\mathbb{C}$, donde el teorema fundamental del álgebra acude en nuestro auxilio, no está en absoluto claro que las raíces existan en algún sitio (esto es, que siempre haya un cuerpo de descomposición) ni tampoco que no podamos crear muchos cuerpos de descomposición distintos. En seguida resolveremos estas cuestiones de existencia y unicidad.

Ejemplo. El cuerpo de descomposición de $P = x^2 - 2 \in \mathbb{Q}[x]$ es $\mathbb{Q}(\sqrt{2})$.

Ejemplo. El cuerpo de descomposición de $P = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$ es $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ (nótese que $P = (x^2 - 2)(x^2 - 3)$).

Ejemplo. El cuerpo de descomposición de $P = x^n - 1 \in \mathbb{Q}(\sqrt{2})[x]$ es $\mathbb{Q}(\sqrt{2}, \zeta)$ con $\zeta = e^{2\pi i/n}$.

Como acabamos de señalar, la existencia del cuerpo de descomposición no es evidente porque en sitios suficientemente raros no sabemos hallar las raíces de un polinomio, por ejemplo en el caso antes citado $x^2+1 \in \mathbb{F}_3[x]$. Para resolver este problema nos inventaremos un sitio más raro todavía, un anillo cociente, donde vive algo que se comporta como una raíz. Después bastará darle a la manivela de la inducción para que el resto de las raíces se unan a la fiesta. Realmente todo el artificio fue ya introducido en el primer capítulo.

Lema 3.1.1 *Dado un polinomio no constante $P \in K[x]$, existe una extensión finita, L/K, tal que P tiene una raíz en L.*

Demostración: Podemos suponer que P es irreducible (en otro caso elegiríamos uno de sus factores irreducibles) y que $\partial P > 1$ (si $\partial P = 1$, $L = K$). Sea el anillo $L = K[x]/\langle P\rangle$. Obviamente K está "incluido" en L, o más exactamente, existe un monomorfismo $\phi : K \longrightarrow L$. Además L es de hecho un cuerpo, por la Proposición 1.2.3 en combinación con la 1.3.2. Por último, la finitud de L/K se sigue de la Proposición 2.2.4, porque $L = K(\overline{x})$ con $\overline{x} = x + \langle P\rangle$, y $\overline{x}$ es algebraico al ser $P(\overline{x}) = \overline{P(x)}$ la clase de cero en L. □

Ejemplo. Según el resultado anterior, $P = x^2 + x + 1 \in \mathbb{F}_2[x]$ factoriza en $L = \mathbb{F}_2[x]/\langle P\rangle = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$.

Para que los más escépticos se sientan a gusto, demos a estos cuatro elementos nombre más vulgares, digamos $L = \{0, 1, \alpha, \beta\}$. Entonces las tablas de suma y multiplicación en L son

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

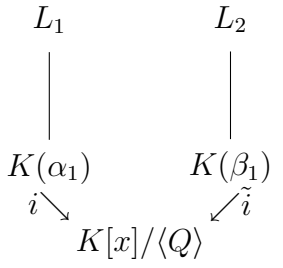
$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Si lo preferimos, podemos empezar desde aquí y definir L como un cuerpo cuyas operaciones tienen las tablas anteriores. Como $\alpha+\beta = \alpha\beta = 1$, se concluye $P = (x-\alpha)(x-\beta)$ en $L[x]$. De hecho L es el cuerpo de descomposición de P, ya que $[L : \mathbb{F}_2] = 2$ (ejercicio) y por tanto no hay subextensiones propias de $L/\mathbb{F}_2$. También podemos comprobar directamente con estas tablas que α y β son raíces de P. Por ejemplo $\alpha^2 + \alpha + 1 = \beta + \alpha + 1 = 1 + 1 = 0$.

Si hubiéramos partido de un polinomio de tercer grado, el lema anterior nos habría llevado a un lugar donde hay una descomposición del tipo $k(x-\gamma)(x^2+\delta x+\epsilon)$. Para conseguir la factorización total en factores lineales, sólo hay que iterar. Si además recordamos la Proposición 2.2.5, veremos que las raíces están exactamente representadas por los anillos cociente, y que el procedimiento lleva a un único resultado salvo los nombres con los que nos apetezca bautizar a las raíces invitadas. En breve:

Proposición 3.1.2 *Para cada $P \in K[x]$ existe un cuerpo de descomposición L de P y además es único salvo isomorfismos que dejan fijo K (en rigor la imagen de K en L).*

Demostración: Para la existencia basta aplicar repetidas veces el Lema 3.1.1 hasta obtener un L en el que P se descomponga en factores lineales: $P = k(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$, entonces $K(\alpha_1,\alpha_2,\dots,\alpha_n)$ será el cuerpo de descomposición de P (para ser totalmente rigurosos deberíamos escribir en lugar de K su imagen en L). Para demostrar la unicidad salvo isomorfismos que dejan fijo K, supongamos que L_1 y L_2 son cuerpos de descomposición de P. Procedemos por inducción en el grado de P. Si gr $P = 1$ es trivial. Si gr $P > 1$, sea Q un factor mónico irreducible de P, entonces $Q = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$ en $L_1[x]$ y $Q = (x-\beta_1)(x-\beta_2)\dots(x-\beta_n)$ en $L_2[x]$. Por la Proposición 2.2.5 se tienen isomorfismos $i : K(\alpha_1) \longrightarrow K[x]/\langle Q\rangle$, $\widetilde{i} : K(\beta_1) \longrightarrow K[x]/\langle Q\rangle$, por tanto $\widetilde{i}^{-1} \circ i : K(\alpha_1) \longrightarrow K(\beta_1)$ es un isomorfismo, que por la construcción de i e $\widetilde{i}$, deja fijo K.



Por definición, L_1 es una extensión de $K(\alpha_1)$ y también L_2 puede considerarse que extiende a $K(\alpha_1)$ por medio del monorfismo $j \circ \widetilde{i}^{-1} \circ i : K(\alpha_1) \hookrightarrow L_2$ donde $j : K(\beta_1) \hookrightarrow L_2$ es la inclusión. Nótese que L_1 y L_2 son obviamente cuerpos de descomposición de P sobre $K(\alpha_1)$ y también lo son de $\widetilde{P} = P/(x-\alpha_1)$ porque $\alpha_1 \in K(\alpha_1)$. La demostración se concluye por la hipótesis de inducción (ya que gr $\widetilde{P} <$ gr P). □

Ejemplo. El cuerpo $\mathbb{F}_3[i]$ donde $i \notin \mathbb{F}_3$ es un símbolo que operamos formalmente como $i^2 = -1$, es el cuerpo de descomposición de x^2+1 sobre $\mathbb{F}_3$.

Si nos creemos que $\mathbb{F}_3[i]$ es un cuerpo bien definido (en principio sólo tiene estructura de anillo), entonces $\mathbb{F}_3[i] = \mathbb{F}_3(i) = \mathbb{F}_3(i,-i)$. Como $x^2+1 = (x-i)(x+i)$ en $(\mathbb{F}_3[i])[x]$, se tiene que es el cuerpo de descomposición (el cuerpo generado por las raíces). La forma de probar que $\mathbb{F}_3[i]$ es un cuerpo es considerar el isomorfismo $\mathbb{F}_3[i] \longrightarrow \mathbb{F}_3[x]/\langle x^2+1\rangle$ donde $i \mapsto \overline{x}$. Como el segundo anillo es un cuerpo (por la Proposición 1.2.3), el primero también lo es. Ambos son cuerpos de descomposición de x^2+1 porque los dos conforman extensiones de grado 2 que contienen a las raíces. En concordancia con la última proposición la única diferencia entre ambos se reduce a un cambio de nombre en las raíces, $\pm i$ por $\pm\overline{x}$.

Nota: Siempre podemos dar a las raíces los nombres que nos apetezca, pero el ejemplo anterior no debe hacernos pensar que podemos imponer junto con esos nombres una estructura algebraica a nuestro arbitrio. Por ejemplo, el cuerpo de descomposición de x^2+1 sobre $\mathbb{F}_2$ no es $\mathbb{F}_2[i]$ con i definido como antes, porque $x^2+1 = (x+1)^2$ en $\mathbb{F}_2[x]$

y por tanto el cuerpo de descomposición es el propio $\mathbb{F}_2$. De hecho $\mathbb{F}_2[i]$ no es un cuerpo si nos empeñamos en que i sea algo distinto de 1 que tenga la propiedad $i^2 = -1$, ya que $(i-1)(i-1) = 0$ implicaría $i = 1$ en un dominio de integridad.

Aparentemente, lo que pedimos a una extensión para que sea normal es mucho más restrictivo que lo que exigimos en la definición de cuerpo de descomposición, ya que una extensión normal debe contener los cuerpos de descomposición de "muchos" polinomios. Pero el siguiente resultado nos da en el caso finito (el único de interés en este curso) las dos definiciones al precio de una:

Proposición 3.1.3 *Una extensión L/K es normal y finita si y sólo si L es el cuerpo de descomposición de un polinomio de $K[x]$.*

Demostración: Distingamos cada una de las implicaciones. Como siempre, comenzamos con lo más fácil:

$\Rightarrow$) Sea $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ y sea $P = P_1 \cdot P_2 \cdot \cdots \cdot P_n$ donde P_j es el polinomio mínimo de α_j sobre K. Como L/K es normal, cada P_i se descompone en factores lineales en $L[x]$ y lo mismo ocurre con P, por tanto L contiene al cuerpo de descomposición de P y como L está generado por la raíces de P, coincide con él.

$\Leftarrow$) Sea L el cuerpo de descomposición de $Q \in K[x]$. Basta demostrar que si α y β son raíces de un polinomio mónico irreducible en $K[x]$, entonces $\alpha \in L \Rightarrow \beta \in L$.

Por la Proposición 2.2.5 (empleada como en la demostración de la proposición anterior) existe un K-isomorfismo $i : K(\alpha) \longrightarrow K(\beta)$. Por otra parte, $L(\alpha)$ es un cuerpo de descomposición de $Q \in K(\alpha)[x]$ y también $L(\beta)$ puede considerarse como otro cuerpo de descomposición teniendo en cuenta el monomorfismo $K(\alpha) \longrightarrow K(\beta) \hookrightarrow L(\beta)$. Así pues, por la proposición anterior, los cuerpos $L(\alpha)$ y $L(\beta)$ son isomorfos como extensiones de $K(\alpha)$. En definitiva, si $\alpha \in L$, se tiene

$$1 = [L(\alpha) : L] = \frac{[L(\alpha) : K(\alpha)][K(\alpha) : K]}{[L : K]} = \frac{[L(\beta) : K(\alpha)][K(\alpha) : K]}{[L : K]} = [L(\beta) : L] = 1,$$

es decir, $\beta \in L$. Por tanto L/K es normal (la finitud es inmediata porque cada raíz de Q está en una extensión de grado menor o igual que ∂Q). $\square$

Ejemplo. La extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ es normal porque $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ es el cuerpo de descomposición de $P = (x^2 - 2)(x^2 - 3)$ sobre $\mathbb{Q}$.

Ejemplo. La extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal porque sólo una de las raíces de $x^3 - 2$ está en $\mathbb{Q}(\sqrt[3]{2})$, las otras son números complejos. Sin embargo la extensión $\mathbb{Q}(\sqrt[3]{2}, \sqrt{7})/\mathbb{Q}(\sqrt[3]{2})$ sí es normal porque $\mathbb{Q}(\sqrt[3]{2}, \sqrt{7})$ es el cuerpo de descomposición de $x^2 - 7$ sobre $\mathbb{Q}(\sqrt[3]{2})$.

Ejemplo. La extensión $\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}$ es normal porque $\mathbb{Q}(e^{2\pi i/n})$ es el cuerpo de descomposición de $x^n - 1$ sobre $\mathbb{Q}$.

Entre los cuerpos de descomposición vamos a señalar un caso especial que seguidamente veremos que es general en el universo de los cuerpos finitos. Históricamente aparecieron por vez primera en uno de los trabajos del propio Galois bajo el epígrafe *Sur la théorie des nombres* [Gal].

Definición: Si $q = p^n$ donde p es primo y $n \in \mathbb{Z}^+$, se denota con $\mathbb{F}_q$ (o con GF_q) y se llama a veces *cuerpo de Galois*, al cuerpo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$.

Ejemplo. $\mathbb{F}_4$ es, salvo isomorfismos, el cuerpo $L = \{0, 1, \alpha, \beta\}$ descrito anteriormente porque $x^4 - x = x(x+1)(x^2+x+1)$.

Ejemplo. $\mathbb{F}_9$ es, salvo isomorfismos, el cuerpo $L = \mathbb{F}_3[i]$, también considerado anteriormente, porque tras la factorización:

$$x^9 - x = x(x-1)(x-2)(x^2+1)\big((x+1)^2+1\big)\big((x-1)^2+1\big)$$

se sigue que todas las raíces están en L.

Parece una gran casualidad estas coincidencias de cuerpos, pero ya deberíamos estar acostumbrados a que en Matemáticas las grandes casualidades suelen ser en realidad teoremas, pequeñas verdades universales veladas a nuestros ojos. La sorpresa es que los cuerpos de descomposición sobre $\mathbb{F}_p$, y de hecho todos los cuerpos finitos, son lo mismo que (isomorfos a) algún $\mathbb{F}_q$. Con este resultado que probaremos a continuación, los $\mathbb{F}_q$ que se ocultaban humildemente bajo su apariencia de caso particular, adquieren un puesto de palco en la teoría de cuerpos. Todavía suben más alto teniendo en cuenta su importancia en las aplicaciones. Por ejemplo parte de la teoría de códigos (sí, la que hace funcionar los discos compactos) vive de los cuerpos finitos y hasta la prueba del último teorema de Fermat requiere entenderlos bien. En este curso, sin embargo, no les daremos una importancia especial prefiriendo centrarnos en ejemplos más familiares y completos que viven dentro del reino de los números complejos (la teoría de Galois es muy fácil en cuerpos finitos). Tal felonía, requiere al menos unas líneas en letra pequeña.

Un *byte* es una lista ordenada de 8 *bits*, es decir, de ocho ceros y unos. Al transmitir un conjunto de *bytes*, un fichero, para tener alguna certeza de que no ha habido errores podemos añadir un *byte de paridad* que no contiene información adicional pero fuerza a que en nuestro conjunto de *bytes* haya un número par de unos en el primer *bit*, y en el segundo, ... y así hasta el octavo.

byte 1	1	0	0	0	1	0	0	1
byte 2	1	1	1	1	1	1	0	0
byte 3	1	0	1	0	1	0	0	1

byte de paridad	1	1	0	1	1	1	0	0
nº total de unos	4	2	2	2	4	2	0	2

Podemos identificar los ceros y unos de los *bits* con los elementos de $\mathbb{F}_2$. En seguida veremos que $\mathbb{F}_{256}/\mathbb{F}_2$ es una extensión de grado 8, por tanto $\mathbb{F}_{256}$ es un espacio vectorial de dimensión 8 sobre $\mathbb{F}_2$ y cada uno de sus elementos corresponde a un vector $(b_1, b_2, \ldots, b_8)$ con $b_i \in \mathbb{F}_2$, esto es, a un *byte*, y la suma en $\mathbb{F}_{256}$ corresponde a la suma coordenada a coordenada módulo 2. Así pues, si el fichero (con su *byte* de paridad) está representado en $\mathbb{F}_{256}$ por $\alpha_1, \alpha_2, \ldots, \alpha_N$, se debe cumplir $\sum \alpha_i = 0$ si no hay errores. Hasta aquí toda esta terminología son ganas de complicar las cosas. Idealmente, si hubiera algún error de transmisión nos gustaría que se reparase automática e inmediatamente, sin tener que transmitir de nuevo el fichero. Con este fin, fijamos de antemano N elementos distintos no nulos, $\beta_1, \ldots, \beta_N \in \mathbb{F}_{256}$ (suponemos $N < 256$) y ponemos ahora dos *bytes* de paridad α_{N-1} y α_N elegidos

de manera que se cumpla $\sum \alpha_i = 0$ y $\sum \beta_i \alpha_i = 0$. Si un solo *byte* α_j se hubiera modificado durante la transmisión pasando a $\alpha_j + \gamma$ entonces lo notaríamos porque el valor de $\sum \alpha_i$ sería $\gamma \neq 0$, mientras que el de $\sum \beta_i \alpha_i$ sería $\beta_j \gamma$. Por tanto $\beta_j = \sum \beta_i \alpha_i / \sum \alpha_i$. Como los β_i son distintos, β_j corresponde a un solo *byte*, al j-ésimo, y podríamos detectar el error y corregirlo (simplemente restando a este *byte* $\gamma = \sum \alpha_i$).

Complicando las cosas se pueden detectar y corregir más posibles errores siempre a costa de añadir algunos *bytes* de sobra. Más información sobre el tema (o, más bien, alguna información sobre el tema) se puede encontrar por ejemplo en [Ak] y [Ga] y por supuesto en el curso de Teoría de Códigos y Criptografía. Como curiosidad, un CD recién sacado de su envoltorio de regalo puede tener medio millón de errores. Tan asombroso o más que la existencia de algoritmos eficientes para eliminarlos es que la tecnología haya sido capaz de hacer que operen en tiempo real, manejando cantidades ingentes de información por segundo.

Teorema 3.1.4 *Sea L un cuerpo finito, entonces es isomorfo a $\mathbb{F}_q$, $q = p^n$, donde p es la característica de L, $n = [L : \mathbb{F}_p]$ y q es el cardinal de L. Además $L/\mathbb{F}_p$ es normal.*

Demostración: Notemos antes de comenzar que la característica de un cuerpo, si no es nula, es un primo, ya que $\mathrm{char}(L) = n_1 n_2 \Rightarrow (1 + 1 + \overset{n_1 \text{ veces}}{\ldots} + 1)(1 + 1 + \overset{n_2 \text{ veces}}{\ldots} + 1) = 0 \Rightarrow 1 + 1 + \overset{n_1 \text{ veces}}{\ldots} + 1 = 0$ ó $1 + 1 + \overset{n_2 \text{ veces}}{\ldots} + 1 = 0$, lo que contradice la minimalidad pedida en la definición de característica.

Por ser L finito, su característica es positiva (el grupo aditivo es de orden finito). Digamos $\mathrm{char}(L) = p$. La función $\overline{n} \mapsto 1 + 1 + \overset{n \text{ veces}}{\ldots} + 1$ induce un monomorfismo de $\mathbb{F}_p$ en L y por tanto $L/\mathbb{F}_p$ es una extensión. Sea $n = [L : \mathbb{F}_p]$. Una vez fijada una base $\{\alpha_1, \ldots, \alpha_n\}$, todo elemento de L se escribe de forma única como $\lambda_1 \alpha_1 + \cdots + \lambda_n \alpha_n$ con $\lambda_j \in \mathbb{F}_p$, por tanto $|L| = p^n = q$. El orden del grupo multiplicativo $L - \{0\}$ es $q - 1$ y consecuentemente, por el teorema de Lagrange, $x^{q-1} - 1 = 0$ para todo $x \in L - \{0\}$. Así pues todos los elementos de L son raíces de $P = x^q - x$. Por otra parte, el número de raíces de un polinomio no puede superar a su grado. Como $\partial P = q = |L|$, se sigue necesariamente que P se descompone en factores lineales en L y que L es su cuerpo de descomposición (en particular normal sobre $\mathbb{F}_p$), por tanto es isomorfo a $\mathbb{F}_q$. □

Observación: Del teorema se sigue que $\mathbb{F}_q$ y todos los cuerpos finitos isomorfos a él tienen $q = p^n$ elementos. Así hay cuerpos con 16, 17 y 19 elementos pero no con 18 o 20.

Ejemplo. El cuerpo de descomposición de $x^3 + 2x + 1 \in \mathbb{F}_5[x]$ es isomorfo a $\mathbb{F}_{125}$.

El polinomio $x^3 + 2x + 1 \in \mathbb{F}_5[x]$ es irreducible (no tiene raíces en $\mathbb{F}_5$). Sea α una raíz en el cuerpo de descomposición, entonces $\mathbb{F}_5(\alpha)$ es un cuerpo finito (ya que $\mathbb{F}_5(\alpha)/\mathbb{F}_5$ es una extensión finita). Por el teorema anterior $\mathbb{F}_5(\alpha)/\mathbb{F}_5$ es normal y por tanto $x^3 + 2x + 1$ se descompone en factores lineales en $\mathbb{F}_5(\alpha)$, que es su cuerpo de descomposición. Como $\mathbb{F}_5(\alpha)$ tiene característica 5 y $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = 3$, según el teorema es isomorfo a $\mathbb{F}_{5^3}$.

Ejemplo. Estudiar si el polinomio $P = x^4 + x + 1$ es irreducible en $\mathbb{F}_4[x]$ y hallar el grado de su cuerpo de descomposición sobre $\mathbb{F}_4$.

El polinomio P no tiene raíces en $\mathbb{F}_2$ ni tampoco es divisible por $x^2 + x + 1$, que es el único polinomio en $\mathbb{F}_2[x]$ de grado dos irreducible, por tanto P es irreducible en $\mathbb{F}_2[x]$ y procediendo como en el ejemplo anterior su cuerpo de descomposición sobre $\mathbb{F}_2$ es isomorfo a $\mathbb{F}_{2^4}$. Como $[\mathbb{F}_{2^4} : \mathbb{F}_{2^2}] = [\mathbb{F}_{2^4} : \mathbb{F}_2]/[\mathbb{F}_{2^2} : \mathbb{F}_2] = 4/2$, el grado buscado es 2. Si P fuera irreducible en $\mathbb{F}_4$ entonces el cuerpo de descomposición de P tendría al menos grado 4 sobre $\mathbb{F}_4$ y por tanto 8 sobre $\mathbb{F}_2$, lo que contradice que sea isomorfo a $\mathbb{F}_{2^4}$.

Pasemos ahora a estudiar la segunda condición técnica a la que nos referimos al comienzo de la sección, relacionada con la existencia de raíces múltiples de polinomios irreducibles. Para ahorrar en papel, tinta y analgésicos, prácticamente aquí nos limitaremos a probar que en casi todas las extensiones que podemos imaginar la condición que solicitamos se cumple. (Para un análisis breve más profundo, véase [Ka] p. 55-59).

El concepto básico está recogido en la siguiente definición. Para no sobrecargar demasiado la terminología nos limitaremos a polinomios irreducibles.

Definición: Se dice que un polinomio irreducible $P \in K[x]$ es *separable* sobre K si no tiene raíces múltiples (en su cuerpo de descomposición). Si L/K es una extensión algebraica, se dice que $\alpha \in L$ es *separable* sobre K si su polinomio mínimo lo es. Finalmente, se dice que la propia extensión L/K es *separable* si todo $\alpha \in L$ lo es sobre K. En caso de que un polinomio, elemento o extensión no sea separable, se dice que es *inseparable*.

Antes de nada, veamos un resultado auxiliar que a primera vista parece implicar que no existen polinomios inseparables.

Lema 3.1.5 *Dado $P = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ irreducible, entonces P es inseparable si y sólo si el polinomio $P' = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1$, llamado* derivada formal *de P, es el polinomio nulo.*

Nota: La denominación tiquismiquis de P' como *derivada formal* en vez de simplemente *derivada* es inofensiva y sólo intenta recordarnos que en muchos cuerpos, por ejemplo en $\mathbb{F}_p$, no tiene sentido el concepto usual de límite ni por tanto la definición usual de derivada. La definición de P' es simplemente formal, aunque comparta las propiedades algebraicas (por ejemplo la fórmula para derivar un producto) con la de toda la vida de Cálculo I.

Demostración: Distinguimos las dos implicaciones:

$\Rightarrow$) Si P es inseparable, existe α en el cuerpo de descomposición tal que $(x-\alpha)^2 | P$ y se tiene $P = (x-\alpha)^2 Q$, y de aquí $P' = 2(x-\alpha)Q + (x-\alpha)^2 Q'$. Por tanto $x - \alpha$ divide a $R = \mathrm{mcd}(P, P') \in K[x]$. Si $P' \neq 0$ entonces R es un polinomio no constante con $\partial R < \partial P$ que divide a P, lo que contradice la irreducibilidad.

$\Leftarrow$) Si P fuera separable $P = k(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ con $\alpha_i \neq \alpha_j$ perteneciendo al cuerpo de descomposición de P sobre K. Entonces $P' = \sum_{i=1}^{n} P_i$ donde $P_i(x) = P(x)/(x-\alpha_i)$. Como $x - \alpha_1 | P_i$ para $2 \leq i \leq n$ y $x - \alpha_1 \not| P_1$ (porque α_1 no coincide con ninguna otra raíz) se tiene que $x - \alpha_1 \not| P'$ lo cual contradice $P' = 0$. $\square$

Una consecuencia inmediata es la imposibilidad de encontrar ejemplos de extensiones inseparables con números normales y corrientes.

Proposición 3.1.6 *Si K es un cuerpo de característica cero, todo polinomio irreducible en $K[x]$ es separable. En particular cualquier extensión algebraica L/K con $K \subset \mathbb{C}$ es separable.*

Demostración: Por el lema anterior, para que $P = a_n x^n + \dots a_1 x + a_0 \in K[x]$ sea inseparable, $ja_j = 0$, $1 \leq j \leq n$. Por estar en un cuerpo de característica cero, $j = 1 + 1 + \overset{j \text{ veces}}{\dots} + 1 \neq 0$, así pues $a_j = 0$ para todo $1 \leq j \leq n$. □

Nuestras sospechas se centran ahora sobre $\mathbb{F}_p$, pero tampoco allí es posible encontrar ejemplos inseparables.

Proposición 3.1.7 *Si K es un cuerpo finito, todo polinomio irreducible en $K[x]$ es separable. En particular cualquier extensión algebraica $L/\mathbb{F}_q$ es separable.*

Demostración: Es fácil ver que si L/M y M/K son extensiones algebraicas, L/K separable implica L/M separable (ejercicio). Así que, después del teorema de clasificación de cuerpos finitos (Teorema 3.1.4), basta considerar el caso $K = \mathbb{F}_p$.

Según el lema, los únicos polinomios inseparables deberán ser de la forma $P = a_{np}x^{np} + \dots + a_{2p}x^{2p} + a_p x^p + a_0$. Por el pequeño teorema de Fermat, $a^p = a$ para todo $a \in \mathbb{F}_p$. Además $(A+B)^p = A^p + B^p$ para $A, B \in \mathbb{F}_p[x]$, ya que los coeficientes binómicos $\binom{p}{k}$ son divisibles por p para $0 < k < p$ (ejercicio). Por tanto

$$P = (a_{np}x^n)^p + \dots + (a_{2p}x^2)^p + (a_p x)^p + a_0^p = \left(a_{np}x^n + \dots + a_{2p}x^2 + a_p x + a_0\right)^p,$$

y se concluye que P no es irreducible. □

La pregunta natural es qué diantres puede ser una extensión no separable, no vaya a ser que estemos introduciendo un nuevo nombre para el conjunto vacío.

Ejemplo. La extensión $\mathbb{F}_2(t)/\mathbb{F}_2(t^2)$ (donde t es una variable) es inseparable, porque el polinomio mínimo de t sobre $\mathbb{F}_2(t^2)$ es $x^2 - t^2 \in \mathbb{F}_2(t^2)[x]$ que se descompone en $\mathbb{F}_2(t)[x]$ como $(x-t)^2$.

Para terminar esta ya larga sección, estableceremos que las extensiones separables, esto es, todas las que aparecerán en este curso excluyendo el ejemplo anterior, tienen una insospechada propiedad que ya anunciamos en el segundo capítulo.

Teorema 3.1.8 (Teorema del elemento primitivo) *Toda extensión separable finita es simple.*

Demostración: Separamos primero el caso en que los cuerpos de la extensión son finitos. Por el Teorema 3.1.4 nos podemos restringir a la extensión $\mathbb{F}_q/\mathbb{F}_p$ (ejercicio). Si $q = p^n$, escojamos un polinomio mónico irreducible $P \in \mathbb{F}_p[x]$ de grado n, tal polinomio existe porque en otro caso cada elemento de $\mathbb{F}_q$ estaría en algún $\mathbb{F}_{p^m}$ con $m|n$ (ejercicio), lo cual es imposible porque $p + p^2 + \dots + p^{n-1} < p^n$. Si α es una raíz de P, $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n$ y según el Teorema 3.1.4 (véase también el ejemplo posterior) se tiene que $\mathbb{F}_p(\alpha)$ es igual (isomorfo) a $\mathbb{F}_q$.

Supongamos ahora que los cuerpos que participan en la extensión tienen infinitos elementos. Todo lo que hay que probar es que toda extensión $K(\alpha, \beta)/K$ con α y β algebraicos sobre K es simple, porque de ahí, iterando, se deduce que cualquier extensión finita $K(\alpha_1, \alpha_2, \dots, \alpha_n)/K$ es simple.

Sean Q y P los polinomios mínimos de α y β respectivamente. Digamos que sus raíces en el cuerpo de descomposición de QP son $\alpha = s_1, s_2 \dots, s_m$ y $\beta = r_1, r_2, \dots, r_l$. Sea $\gamma = k\beta - \alpha$ donde $k \in K$ es no nulo y distinto de todos los elementos de la forma $(s_i - \alpha)/(r_j - \beta)$, $1 < i \leq m$, $1 < j \leq l$, como K es infinito es posible esta elección. Consideremos el polinomio $R \in K[\gamma][x]$ con $R(x) = Q(kx - \gamma)$. Nótese que β es raíz de P y R, y además ninguna de las otras raíces de P lo es de R (porque la elección de k implica $kr_j - \gamma \neq s_i$). Así pues $\mathrm{mcd}(P, R) \in K(\gamma)[x]$ tiene como única raíz a β y por la separabilidad esta raíz es simple en P. Por tanto este máximo común divisor es $x - \beta$. De la pertenencia a $K(\gamma)[x]$ se deduce $\beta \in K(\gamma)$ y de aquí $\alpha = k\beta - \gamma \in K(\gamma)$ concluyéndose $K(\alpha, \beta) = K(\gamma)$. □

3.2. El grupo de Galois

La estética que anima el edificio de las Matemáticas muchas veces no es otra cosa que una arquitectura de las simetrías, y dentro de las estructuras algebraicas, la de grupo es la que más comúnmente se asocia con la idea de simetría. El propio concepto de grupo nació (al tiempo que la teoría de Galois) a partir del estudio de las simetrías de las funciones al intercambiar sus variables.

En muchos contextos la representación a través de un grupo es una manera útil de distinguir o incluso caracterizar objetos matemáticos. Una de las manifestaciones más conocidas de este hecho es el llamado *Erlanger Programm* (véase [Kl]), basado en una conferencia que dio F. Klein en la Universidad de Erlangen en 1872, que postula que las diferentes geometrías se deben definir y clasificar por medio de los grupos de transformaciones que admiten. Como ya hemos anunciado, el objetivo de la teoría de Galois (materializado en la próxima sección) se encuadra también dentro de esquemas similares, siendo caracterizar la estructura de ciertas extensiones por medio de un grupo de simetrías. Antes de entrar en las puras definiciones, dejémonos cautivar por unos ejemplos bobos que pueden arrojar alguna luz y darnos no sólo coraje sino también ganas de continuar.

Pensemos en cualquier identidad involucrando las operaciones elementales (suma, resta, multiplicación y división) dentro del cuerpo de los números complejos. Por ejemplo:

$$-2 = \frac{2+3i}{1+i} \cdot (3-i) - (10+i).$$

Si en todos los sitios cambiamos i por $-i$, la igualdad sigue siendo válida. Más adelante expresaremos esto diciendo que la conjugación está en el grupo de Galois de $\mathbb{C}/\mathbb{R}$, un grupo que engloba todas las posibles simetrías. Podemos representar que el primer miembro es un número real, porque queda invariante por la conjugación.

Si escribimos ahora una identidad en $\mathbb{Q}(\sqrt{2},\sqrt{3})$, por ejemplo:

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

esta vez tenemos dos conjugaciones reales. Todas las formas de elegir los signos en $\sqrt{2} \mapsto \pm\sqrt{2}$ y $\sqrt{3} \mapsto \pm\sqrt{3}$, dan lugar a simetrías (invariancias) de esta identidad o de cualquier otra en $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Podríamos decir que el segundo miembro está en $\mathbb{Q}(\sqrt{2})$ porque es invariante por las simetrías que cambian de signo $\sqrt{3}$.

Por último, analicemos la situación con una identidad en $\mathbb{Q}(\sqrt[3]{2})$. Por ejemplo:

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

No está claro cuál es la conjugación en $\mathbb{Q}(\sqrt[3]{2})$. De hecho probaremos que no hay simetrías dentro de $\mathbb{Q}(\sqrt[3]{2})$ y diremos que el grupo de Galois de $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ es trivial. La razón de este fracaso (una extensión no trivial tienen grupo trivial) es que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal, y lo podemos transformar en un éxito sin más que ampliarla a una extensión normal que la contenga, como $\mathbb{Q}(\sqrt[3]{2},\sqrt{-3})/\mathbb{Q}$, donde vive la simetría $\sqrt[3]{2} \mapsto (-1+\sqrt{-3})\sqrt[3]{2}/2$.

Vayamos a las definiciones que sintetizan estas ideas. Los automorfismos serán los objetos matemáticos que representen las simetrías.

Definición: Dada una extensión L/K, se dice que $\sigma : L \longrightarrow L$ es un *K-automorfismo* si es un automorfismo que deja fijos los elementos de K (en rigor, sus imágenes en L). Al conjunto formado por todos los K-automorfismos se le llama *grupo de Galois* de la extensión y lo representaremos con $\mathcal{G}(L/K)$.

Definición: Dado un subgrupo H de $\mathcal{G}(L/K)$, se dice que $\{x \in L \ : \ \sigma(x) = x, \ \forall \sigma \in H\}$ es el *subcuerpo fijo por H* y lo denotaremos con H'.

Con estas definiciones nos hemos adelantado a la estructura algebraica que tienen estos objetos. Para que sean definiciones coherentes necesitamos el siguiente resultado básico y sencillo que probaremos sólo por romper el hielo.

Proposición 3.2.1 *$\mathcal{G}(L/K)$ es un grupo con la composición de automorfismos, y si H es un subgrupo de $\mathcal{G}(L/K)$, entonces H' es un subcuerpo de L que contiene a K (en rigor a su imagen en L).*

Demostración: La composición es cerrada porque si σ y τ son K-automorfismos, es decir, dejan fijo K, entonces $\sigma \circ \tau$ (que abreviaremos con $\sigma\tau$) también deja fijo K. El resto de las propiedades de grupo son consecuencia de las propiedades de la composición de funciones.

Si $x, y \in H'$, para todo $\sigma \in H'$ se tiene $\sigma(x) = x$ y $\sigma(y) = y$, entonces $\sigma(x+y) = x+y$ y por tanto $x + y \in H'$. Lo mismo se haría con el resto de las operaciones. □

La acción del grupo de Galois preserva el conjunto de raíces de polinomios en el siguiente sentido:

Proposición 3.2.2 *Sea L/K y $P \in K[x]$. Si $\alpha \in L$ es una raíz de P, entonces $\sigma(\alpha)$ con $\sigma \in \mathcal{G}(L/K)$ también lo es.*

Observación: Esto implica que cada $\sigma \in \mathcal{G}(L/K)$ induce una permutación actuando sobre el conjunto $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ de raíces distintas de P en L. (Nótese que $\sigma(\alpha_i) = \sigma(\alpha_j) \ \Rightarrow \ \sigma(\alpha_i - \alpha_j) = 0 \ \Rightarrow \ \alpha_i = \alpha_j$). Lo cual está relacionado con la forma en que apareció el grupo de Galois históricamente como subgrupo de permutaciones [Gal], [Ed], porque en tiempos de Galois no existían los K-automorfismos. También sugiere la naturalidad de las condiciones de normalidad y separabilidad que exigiremos más adelante para que el grupo de Galois represente bien la extensión. Si la extensión no es normal, faltarán raíces de algunos polinomios y nos perderemos algunos automorfismos, y si no es separable la coincidencia entre raíces provocará que los automorfismos se repitan.

Demostración: $P(\alpha) = 0 \Rightarrow \sigma\big(P(\alpha)\big) = 0 \Rightarrow P\big(\sigma(\alpha)\big) = 0$. □

Antes de ahogarnos en un mar de ideas intuitivas sostenidas por un par de definiciones y proposiciones, agarrémonos a la tabla salvadora de algunos ejemplos que concreten lo dicho al comienzo de la sección.

Ejemplo. $\mathcal{G}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}, \mathrm{conj}\} \cong \mathbb{Z}_2$, donde $\mathrm{conj}(z) = \overline{z}$ es la conjugación compleja.

Se tiene $\mathbb{C} = \mathbb{R}(i)$ y como i y $-i$ son las raíces de $x^2 + 1 \in \mathbb{R}[x]$, los únicos posibles automorfismos son $a + ib \mapsto a + ib$ y $a + ib \mapsto a - ib$. El primero es la identidad y el segundo la conjugación. Este último es un $\mathbb{R}$-automorfismo porque deja fijos a los reales, es biyectivo (es su propia inverso) y satisface las propiedades de homomorfismo ($\overline{z + w} = \overline{z} + \overline{w}$, $\overline{zw} = \overline{z}\,\overline{w}$ y $\overline{1} = 1$). Si $H = \mathcal{G}(\mathbb{C}/\mathbb{R})$ se tiene $H' = \mathbb{R}$.

Ejemplo. $\mathcal{G}\big(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\big) = \{\mathrm{Id}, \sigma_1, \sigma_2, \sigma_1\sigma_2\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ donde σ_1 y σ_2 son los $\mathbb{Q}$-automorfismos verificando $\sigma_1(\sqrt{2}) = -\sqrt{2}$, $\sigma_1(\sqrt{3}) = \sqrt{3}$, $\sigma_2(\sqrt{2}) = \sqrt{2}$, $\sigma_2(\sqrt{3}) = -\sqrt{3}$.

Cada elemento de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ se puede escribir de forma única como $x + y\sqrt{2}$ con $x, y \in \mathbb{Q}(\sqrt{3})$. La aplicación $\sigma_1(x + y\sqrt{2}) = x - y\sqrt{2}$ es un $\mathbb{Q}$-automorfismo por la misma razón que lo es la conjugación compleja (es biyectiva, fija $\mathbb{Q}$ y respeta las operaciones). Análogamente, también se puede escribir cada elemento de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ de forma única como $x + y\sqrt{3}$ con $x, y \in \mathbb{Q}(\sqrt{2})$, y se deduce que $\sigma_2(x + y\sqrt{3}) = x - y\sqrt{3}$ es un $\mathbb{Q}$-automorfismo. Esto prueba que $\{\mathrm{Id}, \sigma_1, \sigma_2, \sigma_1\sigma_2\} \subset \mathcal{G}\big(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\big)$. No puede haber más $\mathbb{Q}$-automorfismos en $\mathcal{G}\big(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\big)$ porque según la última proposición aplicada a los polinomios $x^2 - 2$ y $x^2 - 3$, cualquier elemento del grupo de Galois sólo puede modificar el signo de $\sqrt{2}$ y $\sqrt{3}$, que generan la extensión y las cuatro combinaciones de signos quedan cubiertas por los automorfismos ya enumerados.

Al ser $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$ una base de la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$,

$$L = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \ : \ a, b, c, d \in \mathbb{Q}\}$$

y para $H = \{\mathrm{Id}, \sigma_1\sigma_2\}$ se tiene $H' = \{a + d\sqrt{2}\sqrt{3} \ : \ a, d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{6})$. De la misma forma, $\{\mathrm{Id}, \sigma_1\}' = \mathbb{Q}(\sqrt{3})$, $\{\mathrm{Id}, \sigma_2\}' = \mathbb{Q}(\sqrt{2})$ y $\big(\mathcal{G}\big(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\big)\big)' = \mathbb{Q}$.

Ejemplo. $\mathcal{G}\big(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\big) = \{\mathrm{Id}\}$ porque un $\mathbb{Q}$-automorfismo no trivial debería aplicar $\sqrt[3]{2}$ (que genera la extensión) en alguna de las otras dos raíces de $x^3 - 2$, y ninguna de ellas está en $\mathbb{Q}(\sqrt[3]{2})$. Obviamente $\big(\mathcal{G}\big(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\big)\big)' = \{\mathrm{Id}\}' = \mathbb{Q}(\sqrt[3]{2})$.

Hay una sencilla relación entre el grado de los subcuerpos fijos y el orden de los subgrupos que los fijan. Su prueba pasa por un curioso lema auxiliar que trata los automorfismos como si fueran vectores.

Lema 3.2.3 *Sean $\sigma_1, \sigma_2, \ldots, \sigma_r \in \mathcal{G}(L/K)$ automorfismos distintos, entonces el conjunto $\{\sigma_1, \sigma_2, \ldots, \sigma_r\}$ es linealmente independiente sobre L. Es decir, si $\lambda_1, \lambda_2, \ldots, \lambda_r \in L$ no son simultáneamente nulos entonces $\lambda_1\sigma_1 + \lambda_2\sigma_2 + \cdots + \lambda_r\sigma_r$ no es la función idénticamente nula en L.*

Demostración: Procedemos por reducción al absurdo. Sea n el menor número de coeficientes λ_j no nulos que participan en una combinación lineal que produce la función nula. Renombrando los automorfismos podemos suponer que son $\lambda_1, \lambda_2, \ldots, \lambda_n$. Esto es,

$$\lambda_1\sigma_1(\alpha) + \lambda_2\sigma_2(\alpha) + \cdots + \lambda_n\sigma_n(\alpha) = 0 \quad \forall \alpha \in L \tag{3.1}$$

para ciertos $\lambda_j \neq 0$. Como α es arbitrario lo podemos sustituir por $\alpha\beta$ donde $\beta \in L$ se escogerá a continuación, por tanto

$$\lambda_1\sigma_1(\alpha)\sigma_1(\beta) + \lambda_2\sigma_2(\alpha)\sigma_2(\beta) + \cdots + \lambda_n\sigma_n(\alpha)\sigma_n(\beta) = 0 \quad \forall \alpha \in L.$$

Elijamos β tal que $\sigma_1(\beta) \neq \sigma_n(\beta)$, esto es posible porque σ_1 y σ_n son distintos. Multiplicando (3.1) por $\sigma_n(\beta)$ y restándole la igualdad anterior, se tiene

$$\lambda'_1\sigma_1(\alpha) + \lambda'_2\sigma_2(\alpha) + \cdots + \lambda'_{n-1}\sigma_{n-1}(\alpha) = 0 \quad \forall \alpha \in L$$

con $\lambda'_1 \neq 0$, pero esto contradice que hubiéramos tomado la combinación lineal más corta. □

Proposición 3.2.4 *Sea H un subgrupo finito de $\mathcal{G}(L/K)$. Si H' es el subcuerpo fijo por los automorfismos de H, entonces*

$$[L : H'] = |H|. \qquad y \qquad [H' : K] = \frac{[L : K]}{|H|}.$$

Demostración: Obviamente la segunda igualdad se sigue de la primera por la Proposición 2.2.2. Sea $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ una base de L/H', sea $H = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ (por tanto $r = [L : H']$ y $n = |H|$) y sea la matriz $A \in \mathcal{M}_{r\times n}(L)$ cuyas columnas son $\sigma_j(\vec{\alpha})$ donde $\vec{\alpha} \in L^r$ es el vector cuya i-ésima coordenada es α_i y los automorfismos σ_j actúan de la manera obvia coordenada a coordenada. Estas columnas son linealmente independientes por el lema anterior (ya que $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ es una base y $\sum \lambda_j\sigma_j(\vec{\alpha}) = \vec{0}$ implicaría $\sum \lambda_j\sigma_j(x) = 0$ para todo $x \in L$). Queremos demostrar demostrar $r = n$, es decir, que la matriz A es cuadrada. Procedemos por reducción al absurdo.

Si $r < n$ entonces $\mathrm{rg}(A) \leq r$, lo que contradice que las n columnas de A sean linealmente independientes.

Si $r > n$ entonces $\mathrm{rg}(A) = n$ y las r filas de A deben ser linealmente dependientes. Por tanto existe $\vec{x} \in L^r - \{0\}$ con $\sigma_j(\vec{\alpha})\cdot\vec{x} = 0$ para todo j. Si x_r es una coordenada no nula de $\vec{x}$, por el lema anterior se puede elegir t tal que $\sigma_1+\sigma_2+\cdots+\sigma_n$ aplicado a tx_r sea no nulo (ya que no es la aplicación nula). En particular, el vector $\vec{v} = \sigma_1(t\vec{x})+\sigma_2(t\vec{x})+\cdots+\sigma_n(t\vec{x})$ es no nulo. Además $\vec{v} \in (H')^r$ porque $\sigma(\vec{v}) = \vec{v}$ para $\sigma \in H$ (ya que la suma es en todos los elementos de H). Aplicando σ_j^{-1} a $\sigma_j(\vec{\alpha}) \cdot t\vec{x} = 0$, debe cumplirse $\vec{\alpha} \cdot \sigma_j^{-1}(t\vec{x}) = 0$, $1 \leq j \leq n$, esto es, $\vec{\alpha} \cdot \sigma(t\vec{x}) = 0$ para todo $\sigma \in H$. En particular $\vec{\alpha} \cdot \vec{v} = 0$, lo que contradice que las coordenadas de $\vec{\alpha}$ conformen una base de L sobre H'. □

Sólo por el placer de ver funcionar los engranajes de los teoremas, comprobemos la primera igualdad de la proposición anterior en nuestra exigua colección de grupos de Galois.

Ejemplo. Si $H = \mathcal{G}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}, \mathrm{conj}\}$, se tiene $[\mathbb{C} : H'] = [\mathbb{C} : \mathbb{R}] = 2 = |H|$.

Ejemplo. Si $H = \{\mathrm{Id}, \sigma_1\sigma_2\} \subset \mathcal{G}\big(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\big)$, donde se ha usado la notación de un ejemplo anterior, se tiene $H' = \mathbb{Q}(\sqrt{6})$ y $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : H'] = 2 = |H|$.

Ejemplo. Si $H = \mathcal{G}\big(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\big) = \{\mathrm{Id}\}$, se tiene $[\mathbb{Q}(\sqrt[3]{2}) : H'] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 1 = |H|$.

Los pocos ejemplos que hemos visto de grupos de Galois, se resisten a grandes generalizaciones. Vaya por delante que incluso cuando se utilizan ordenadores para calcular grupos de Galois, los grados y las formas de presentar las extensiones están seriamente limitados. Una ambición razonable es no tener que comprobar con todo cuidado que los presumibles K-automorfismos lo son realmente, y disponer de alguna fórmula con la que sepamos cuántos K-automorfismos tenemos que buscar. Todas estas aspiraciones se consiguen bajo hipótesis de finitud, normalidad y separabilidad, gracias a una propiedad de extensión de isomorfismos. Más importante que el resultado en sí son las consecuencias, que prácticamente constituyen la primera mitad del teorema fundamental de la teoría de Galois que enunciaremos en la próxima sección.

Proposición 3.2.5 *Sea L/K normal y finita y sean M_1 y M_2 dos subcuerpos de L conformando extensiones de K. Si $i : M_1 \longrightarrow M_2$ es un isomorfismo que deja fijos los elementos de K (en rigor de su imagen en L), entonces existe $\sigma \in \mathcal{G}(L/K)$ tal que restringido a M_1 coincide con i.*

Demostración: Como $[L : M_1] < \infty$, basta aplicar repetidas veces que si $\alpha \in L$ entonces se puede extender a un K-isomorfismo $\widetilde{i} : M_1(\alpha) \longrightarrow M_2(\beta)$ con cierto $\beta \in L$. El resto de la demostración se dedica a construir $\widetilde{i}$.

Sea P el polinomio mínimo de α sobre K y sea P_1 el polinomio mínimo sobre M_1, obviamente $P_1|P$. Podemos suponer que $\partial P_1 > 1$ (en otro caso tomaríamos $\widetilde{i} = i$). Sea $P_2 = i(P_1)$ (i actúa sobre los coeficientes). P_2 es mónico e irreducible y divide a P, porque $P = P_1 \cdot Q_1 \Rightarrow P = i(P) = i(P_1) \cdot i(Q_1)$. Como L/K es normal, todas las raíces de P, y por tanto también las de P_2, están en L. Sea $\beta \in L$ con $P_2(\beta) = 0$, por la Proposición 2.2.5 se tienen isomorfismos

$$i_1 : M_1(\alpha) \longrightarrow M_1[x]/\langle P_1\rangle, \qquad i_2 : M_2(\beta) \longrightarrow M_2[x]/\langle P_2\rangle.$$

Por otra parte, i induce un isomorfismo $i_3 : M_1[x]/\langle P_1\rangle \longrightarrow M_2[x]/\langle P_2\rangle$, así pues basta tomar $\widetilde{i} = i_2^{-1} \circ i_3 \circ i_1$. Por construcción los elementos de K quedan fijos por $\widetilde{i}$. □

Corolario 3.2.6 *Sea L/K normal y finita. Si P es un polinomio irreducible y $\alpha, \beta \in L$ son raíces de P, entonces existe $\sigma \in \mathcal{G}(L/K)$ con $\sigma(\alpha) = \beta$.*

Demostración: Basta aplicar la proposición tomando $M_1 = K(\alpha)$, $M_2 = K(\beta)$ y el isomorfismo $i : M_1 \longrightarrow M_2$ de la Proposición 2.2.5. □

Corolario 3.2.7 *Si L/K es normal, finita y separable, $|\mathcal{G}(L/K)| = [L : K]$.*

Demostración: Tomando $H = \mathcal{G}(L/K)$ en la Proposición 3.2.4 se sigue $[L : K] \geq [L : H'] = |\mathcal{G}(L/K)|$. Si fuera $[L : K] > |\mathcal{G}(L/K)|$, necesariamente existiría $\alpha \in \big(\mathcal{G}(L/K)\big)' - K$. Al ser la extensión normal y separable, el polinomio mínimo de α sobre K factoriza totalmente en $L[x]$ y tiene raíces distintas en L. Por el corolario anterior existe un elemento de $\mathcal{G}(L/K)$ que no fija a α, que lo envía a otra de las raíces, lo que contradice $\alpha \in \big(\mathcal{G}(L/K)\big)'$. □

Ahora veamos ejemplos y más ejemplos, en multitud tan abigarrada que invadirán la siguiente sección.

Nota: Al hallar grupos de Galois, para asegurar la normalidad, muchas veces se presentan los cuerpos como cuerpos de descomposición de un polinomio. De hecho es común usar la expresión *grupo de Galois de* $P \in K[x]$ para referirse a $\mathcal{G}(L/K)$ con L el cuerpo de descomposición de P sobre K, aunque aquí preferimos evitar esta notación.

Ejemplo. Hallar $\mathcal{G}\big(\mathbb{Q}(\zeta)/\mathbb{Q}\big)$ donde $\zeta = e^{2\pi i/5}$.

Como la extensión es simple y generada por ζ, cada $\sigma \in \mathcal{G}\big(\mathbb{Q}(\zeta)/\mathbb{Q}\big)$ está determinado por el valor en el que aplica ζ. Las raíces del polinomio ciclotómico $x^4+x^3+x^2+x+1$ son ζ, ζ^2, ζ^3 y ζ^4; así pues, $\mathbb{Q}(\zeta)$ es su cuerpo de descomposición y el Corolario 3.2.6 implica que existen $\mathbb{Q}$-automorfismos σ_1, σ_2, σ_3 y σ_4 tales que $\sigma_1(\zeta)=\zeta$, $\sigma_2(\zeta)=\zeta^2$, $\sigma_3(\zeta)=\zeta^3$, $\sigma_4(\zeta)=\zeta^4$. Con lo cual se tiene $\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\} \subset \mathcal{G}\big(\mathbb{Q}(\zeta)/\mathbb{Q}\big)$. Y la igualdad se da por el Corolario 3.2.7 (porque $[\mathbb{Q}(\zeta):\mathbb{Q}]=4$). Nótese que $\sigma_1 =$Id y que σ_2 genera al resto de los automorfismos, ya que

$$\sigma_2^2(\zeta)=\sigma_2(\sigma_2(\zeta))=(\zeta^2)^2=\sigma_4(\zeta) \quad \text{y} \quad \sigma_2^3(\zeta)=\sigma_2(\sigma_2^2(\zeta))=(\zeta^4)^2=\zeta^3=\sigma_3(\zeta).$$

Por consiguiente $\mathcal{G}\big(\mathbb{Q}(\zeta)/\mathbb{Q}\big) \cong \mathbb{Z}_4$.

No es difícil generalizar este ejemplo reemplazando 5 por cualquier primo.

Ejemplo. Si $\zeta = e^{2\pi i/p}$ con p primo, entonces $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \big\{\sigma_1,\sigma_2,\ldots,\sigma_{p-1}\big\}$ donde $\sigma_j : \zeta \mapsto \zeta^j$. Además $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ es isomorfo al grupo (multiplicativo) de unidades de $\mathbb{Z}_p$. (aunque no lo haremos aquí, se puede probar que este grupo es siempre isomorfo a $\mathbb{Z}_{p-1}$).

Como antes, $\mathbb{Q}(\zeta)$ es el cuerpo de descomposición del polinomio ciclotómico $P = x^{p-1}+x^{p-2}+\cdots+1 = (x^p-1)/(x-1)$. Como P es irreducible y tiene a ζ como raíz, $[\mathbb{Q}(\zeta):\mathbb{Q}] = p-1$, por tanto $|\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})| = p-1$. Por otra parte $\sigma_j \in \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$, gracias al Corolario 3.2.6 y se tiene $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \big\{\sigma_1,\sigma_2,\ldots,\sigma_{p-1}\big\}$.

El isomorfismo $\phi : \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) \longrightarrow \mathbb{Z}_p^*$ donde $\mathbb{Z}_p^*$ son las unidades de $\mathbb{Z}_p$, viene dado simplemente por $\phi(\sigma_j) = \overline{j}$. Se reduce a un cálculo comprobar que $\phi(\sigma_i\sigma_j) = \phi(\sigma_i)\phi(\sigma_j)$, y su inversa es simplemente $\overline{j} \mapsto \sigma_j$ para $0 < j < p$.

Ejemplo. En $\mathbb{Q}(\zeta)/\mathbb{Q}$ con $\zeta = e^{2\pi i/7}$ hallar el cuerpo fijo $H' =< \sigma_2 >'$ y su grado sobre $\mathbb{Q}$. (Empleamos la notación anterior, esto es, $\sigma_2 : \zeta \mapsto \zeta^2$).

Al ser $B = \{1,\zeta,\zeta^2,\zeta^3,\zeta^4,\zeta^5\}$ una base de la extensión (Proposición 2.2.4) todo $x \in \mathbb{Q}(\zeta)$ se puede expresar como $x = \sum_{j=0}^{5} \lambda_j\zeta^j$ con $\lambda_j \in \mathbb{Q}$. Entonces la condición $x = \sigma_2(x)$ necesaria y suficiente para que $x \in H'$, es

$$\begin{aligned} x &= \lambda_0+\lambda_1\zeta^2+\lambda_2\zeta^4+\lambda_3\zeta^6+\lambda_4\zeta^8+\lambda_5\zeta^{10} \\ &= \lambda_0+\lambda_4\zeta+\lambda_1\zeta^2+\lambda_5\zeta^3+\lambda_2\zeta^4+\lambda_3\zeta^6 \\ &= (\lambda_0-\lambda_3)+(\lambda_4-\lambda_3)\zeta+(\lambda_1-\lambda_3)\zeta^2+(\lambda_5-\lambda_3)\zeta^3+(\lambda_2-\lambda_3)\zeta^4-\lambda_3\zeta^5 \end{aligned}$$

donde se ha empleado $\zeta^8=\zeta$, $\zeta^{10}=\zeta^3$ y $\zeta^6 = -1-\zeta-\zeta^2-\zeta^3-\zeta^4-\zeta^5$ (recuérdese el polinomio ciclotómico). Igualando coordenadas con respecto a la base B, se tiene:

$$\lambda_0=\lambda_0-\lambda_3, \quad \lambda_1=\lambda_4-\lambda_3, \quad \lambda_2=\lambda_1-\lambda_3, \quad \lambda_3=\lambda_5-\lambda_3, \quad \lambda_4=\lambda_2-\lambda_3, \quad \lambda_5=-\lambda_3.$$

En definitiva, $\lambda_3 = \lambda_5 = 0$, $\lambda_1 = \lambda_4 = \lambda_2$, o escrito de otra forma, $x = a + b(\zeta + \zeta^2 + \zeta^4)$. Esto prueba $H' = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$. El orden de σ_2 es 3, y según la Proposición 3.2.4, el grado de la extensión es $[H' : \mathbb{Q}] = 6/|H| = 2$.

Observación: Una forma más breve de calcular H' en el problema anterior pasa por notar que para cualquier $x \in \mathbb{Q}(\zeta)$ se cumple $u = x + \sigma_2(x) + \sigma_2^2(x) \in H'$ porque $\sigma_2(u) = u$ (utilizamos que σ_2 tiene orden 3). Tomando $x = \zeta$ se obtiene $\zeta + \zeta^2 + \zeta^4 \in H'$. Además $\zeta + \zeta^2 + \zeta^4 \notin \mathbb{Q}$ porque σ_3 no lo deja invariante, y $[H' : \mathbb{Q}] = 2$ implica $H' = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$. Este truco de forzar las simetrías haciendo actuar todos los elementos de un grupo ya apareció en la demostración de la Proposición 3.2.4 y se muestra también en diferentes versiones en áreas alejadas del tema que nos ocupa, por ejemplo es análogo al *método de las imágenes* introducido por Lord Kelvin para resolver algunas ecuaciones en derivadas parciales provinientes de problemas físicos. Históricamente fue Gauss el primero en calcular subcuerpos fijos en $\mathbb{Q}(e^{2\pi i/p})$ de esta forma, antes de que existiera la teoría de Galois y el propio Galois (un lector avezado podría tratar de interpretar en nuestro lenguaje los ejemplos de [Gau] Art. 353, 354). A pesar de que nos permitiría reducir algunos cálculos, no sistematizaremos el método en este curso.

La sencillez del cálculo del grupo de Galois en los tres ejemplos anteriores se debe a que el cuerpo de descomposición del polinomio ciclotómico está generado por una de sus raíces. Todavía podemos encontrar ejemplos sencillos saliéndonos de esta situación.

Ejemplo. Hallar el grupo de Galois del cuerpo de descomposición de $P = x^3 - 2$ sobre $\mathbb{Q}$.

Las raíces de P son $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$, donde $\omega = (-1 + i\sqrt{3})/2$, por tanto el cuerpo de descomposición es $\mathbb{Q}(\omega, \sqrt[3]{2})$. La conjugación compleja es claramente en $\mathbb{Q}$-automorfismo en $\mathbb{C}$, en particular lo es en $\mathbb{Q}(\omega, \sqrt[3]{2})$. Llamémosla τ cuando la consideramos como elemento de $\mathcal{G}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$. Su efecto sobre los generadores de la extensión es $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, $\tau(\omega) = \overline{\omega} = \omega^2$. Por otra parte, el Corolario 3.2.6 asegura que existe $\sigma \in \mathcal{G}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ con $\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$. Además $\sigma(\omega)$ debe ser ω ó $\overline{\omega} = \omega^2$ porque ambas cantidades son raíces de $x^2 + x + 1$. Quizá sustituyendo σ por $\sigma\tau$ siempre podemos suponer por ejemplo $\sigma(\omega) = \omega$. El automorfismo σ tiene orden tres porque

$$\sigma^3(\omega) = \omega \quad \text{y} \quad \sigma^3(\sqrt[3]{2}) = \sigma^2(\omega\sqrt[3]{2}) = \omega\,\sigma^2(\sqrt[3]{2}) = \omega\,\sigma(\omega\sqrt[3]{2}) = \omega^3\sqrt[3]{2} = \sqrt[3]{2}.$$

Los $\mathbb{Q}$-automorfismos Id, σ, σ^2, τ, $\sigma\tau$ y $\sigma^2\tau$ son distintos. Su acción sobre ω y $\sqrt[3]{2}$ se recoge en las siguientes tablas:

	ω	$\sqrt[3]{2}$
Id	ω	$\sqrt[3]{2}$
σ	ω	$\omega\sqrt[3]{2}$
σ^2	ω	$\omega^2\sqrt[3]{2}$

	ω	$\sqrt[3]{2}$
τ	ω^2	$\sqrt[3]{2}$
$\sigma\tau$	ω^2	$\omega\sqrt[3]{2}$
$\sigma^2\tau$	ω^2	$\omega^2\sqrt[3]{2}$

El grupo de Galois tiene orden 6 (Corolario 3.2.7), así pues se debe tener

$$\mathcal{G}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

Este grupo no es abeliano, porque por ejemplo $\sigma\tau(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ y $\tau\sigma(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$.

Si recordamos los tiempos de Álgebra I, tendremos que el único grupo no abeliano de orden 6 es S_3 (el de permutaciones de tres elementos), por tanto $\mathcal{G}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}) \cong S_3$. Una forma de realizar este isomorfismo es asignar a cada elemento del grupo de Galois la permutación que efectúa sobre las raíces $r_1 = \sqrt[3]{2}$, $r_2 = \omega\sqrt[3]{2}$, $r_3 = \omega^2\sqrt[3]{2}$, del polinomio P. Por ejemplo, la acción de σ es $r_1 \mapsto r_2$, $r_2 \mapsto r_3$, $r_3 \mapsto r_1$, lo que corresponde a la permutación $(1, 2, 3)$, mientras que la conjugación τ corresponde a la transposición $(2, 3)$. (Como ya hemos comentado, en su infancia histórica el grupo de Galois era un subgrupo de permutaciones que hoy en día se muestra ataviado con las galas del álgebra como grupo de K-automorfismos).

Veamos un breve ejemplo en el que el cuerpo base no es $\mathbb{Q}$, y otro más completo con un grupo que tenemos que recordar de Álgebra I.

Ejemplo. Hallar el grupo de Galois de $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}(\omega)$ donde, como antes, ω es la raíz cúbica de la unidad $(-1 + i\sqrt{3})/2$.

La extensión es normal de grado 3. Cada automorfismo del grupo de Galois queda evidentemente caracterizado por la imagen de $\sqrt[3]{2}$. Por el Corolario 3.2.6 aplicado a x^3-2, existen, aparte de la identidad, $\mathbb{Q}(\omega)$-automorfismos $\sigma_1 : \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$ y $\sigma_2 : \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}$. Así pues $\mathcal{G}\big(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}(\omega)\big) = \{\mathrm{Id}, \sigma_1, \sigma_2\}$ que es claramente isomorfo a $\mathbb{Z}_3$.

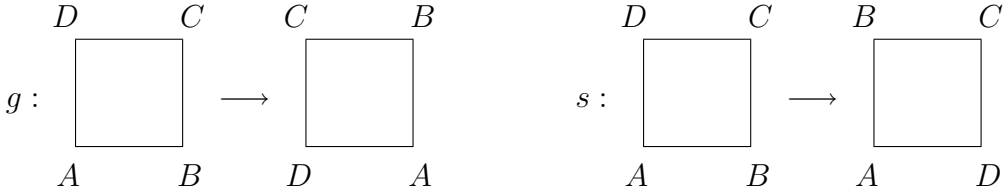
Ejemplo. Hallar el grupo de Galois del cuerpo de descomposición del polinomio $P = x^4 - 2$ sobre $\mathbb{Q}$.

Las raíces de P son $i^k\sqrt[4]{2}$ con $k = 0, 1, 2, 3$, por tanto su cuerpo de descomposición es $L = \mathbb{Q}(\sqrt[4]{2}, i)$. Como antes, tenemos que la conjugación compleja, digamos τ, pertenece al grupo de Galois de $L/\mathbb{Q}$ porque incluso pertenece al de $\mathbb{C}/\mathbb{Q}$. El grado de la extensión es sencillo de calcular porque

$$[L : \mathbb{Q}(\sqrt[4]{2})] = 2 \;\Rightarrow\; [L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 8.$$

Por el Corolario 3.2.6 existe un $\mathbb{Q}$-automorfismo con $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ y, quizá cambiando σ por $\sigma\tau$, podemos suponer que $\sigma(i) = i$. Este automorfismo tiene orden 4 (ejercicio). De aquí se deduce que $\{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$ es un subconjunto de ocho automorfismos distintos y por tanto debe coincidir con $\mathcal{G}(L/\mathbb{Q})$.

Este grupo de Galois no es abeliano. Por ejemplo, $\sigma\tau(\sqrt[4]{2}) = i\sqrt[4]{2}$ mientras que $\tau\sigma(\sqrt[4]{2}) = -i\sqrt[4]{2}$. Podemos identificarlo como un grupo conocido en Álgebra I notando que $\tau\sigma = \sigma^3\tau$ (ejercicio), de donde $\mathcal{G}(L/\mathbb{Q}) = \langle \sigma, \tau \;:\; \sigma^4 = \tau^2 = \mathrm{Id},\ \tau\sigma = \sigma^3\tau \rangle$, lo cual era la presentación de D_8, el grupo diédrico de ocho elementos (también denotado a veces como D_4, lo que causa desafortunadas confusiones). Recuérdese que por definición, D_8 es el grupo de movimientos del plano que dejan fijos un cuadrado, y que está generado por el giro, g, de 90° y la simetría, s, por una de las diagonales



El isomorfismo $\mathcal{G}(L/\mathbb{Q}) \cong D_8$ consiste simplemente en asociar $\sigma \mapsto g$ y $\tau \mapsto s$.

Ejemplo. Hallar el subcuerpo fijo por $H = \langle \sigma^2, \tau \rangle$ en el ejemplo anterior.

Como $\{1, i\}$ y $\{1, \sqrt[4]{2}, \sqrt[4]{2^2}, \sqrt[4]{2^3}\}$ son bases de $L/\mathbb{Q}(\sqrt[4]{2})$ y de $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$, por la Proposición 2.2.2 cada $x \in L$ se escribe de forma única como

$$x = \lambda_0 + \lambda_1 i + \lambda_2 \sqrt[4]{2} + \lambda_3 i \sqrt[4]{2} + \lambda_4 \sqrt[4]{2^2} + \lambda_5 i \sqrt[4]{2^2} + \lambda_6 \sqrt[4]{2^3} + \lambda_7 i \sqrt[4]{2^3}$$

con $\lambda_j \in \mathbb{Q}$. Por una parte, $\tau(x) = x$ implica $\lambda_1 = \lambda_3 = \lambda_5 = \lambda_7 = 0$, y por otra, para x con estos coeficientes, $\sigma^2(x) = x$ implica $\lambda_2 = \lambda_6 = 0$. En definitiva, $H' = \{\lambda_0 + \lambda_4 \sqrt[4]{2^2} : \lambda_2, \lambda_4 \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2})$. Nótese que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [L : \mathbb{Q}]/|H| = 8/4$.

Hasta ahora no ha sido necesaria una extensión efectiva de los automorfismos, porque teníamos la conjugación que de hecho se aplica en algo tan grande como $\mathbb{C}/\mathbb{Q}$. Veamos un ejemplo un poco artificial que incide en que la extensión de automorfismos no es arbitraria.

Ejemplo. Hallar el grupo de Galois del cuerpo de descomposición de $P = x^4 - 2x^2 - 1$ sobre $\mathbb{Q}$.

Resolviendo la ecuación bicuadrada $P = 0$, se tiene que sus raíces son $\pm\sqrt{1+\sqrt{2}}$, $\pm\sqrt{1-\sqrt{2}}$, así que el cuerpo de descomposición es

$$L = \mathbb{Q}\big(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}}\big).$$

Antes de seguir, intentemos simplificar los generadores, para ello nótese que

$$\sqrt{1+\sqrt{2}} \cdot \sqrt{1-\sqrt{2}} = \sqrt{-1} = i,$$

por tanto, definiendo $\alpha = \sqrt{1+\sqrt{2}}$ se tiene que las raíces de P son $\alpha, -\alpha, i/\alpha, -i/\alpha$, y $L = \mathbb{Q}(\alpha, i)$. Obsérvese que α genera una extensión de grado 4 sobre $\mathbb{Q}$ que contiene a $\sqrt{2}$ (porque $\sqrt{2} = \alpha^2 - 1$ y $\alpha \neq a + b\sqrt{2}$). Por tanto $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8$.

Sea $M = \mathbb{Q}(\sqrt{2}, i)$, como $[L : M] = 2$, el polinomio mínimo de α en M es $x^2 - (1+\sqrt{2})$, lo que asegura que hay un elemento $\sigma \in \mathcal{G}(L/M)$ tal que $\sigma(\alpha) = -\alpha$. Evidentemente también $\sigma \in \mathcal{G}(L/\mathbb{Q})$ y se cumple $\sigma(i) = i$ y $\sigma(\sqrt{2}) = \sqrt{2}$. Lo que no esta claro es cómo deben comportarse los automorfismos que sí actúan sobre M, para ello bajamos un nivel y estudiamos primero los elementos de $\mathcal{G}(M/\mathbb{Q})$. Los cuatro automorfismos que debe haber en $\mathcal{G}(M/\mathbb{Q})$ se extenderán a $\mathcal{G}(L/\mathbb{Q})$ y después de componerlos con $\mathrm{Id}, \sigma \in \mathcal{G}(L/M)$ darán lugar a los ocho automorfismos de $\mathcal{G}(L/\mathbb{Q})$. Nótese que este proceso lo podemos llevar a cabo en general siempre que podamos "descomponer" una extensión (finita y separable) en subextensiones normales.

En $\mathbb{Q}(\sqrt{2})$ se tiene la conjugación real $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ que se extiende a un elemento de $\mathcal{G}(M/\mathbb{Q})$. También está la conjugación compleja. Combinándolas de todas las formas posibles se tienen los cuatro $\mathbb{Q}$-automorfismos de $\mathcal{G}(M/\mathbb{Q})$. Escribamos $\mathcal{G}(M/\mathbb{Q}) = \langle \beta_1, \beta_2 \rangle = \{\mathrm{Id}, \beta_1, \beta_2, \beta_1\beta_2\}$ donde $\beta_1(i) = -i$, $\beta_1(\sqrt{2}) = \sqrt{2}$, $\beta_2(i) = i$, $\beta_2(\sqrt{2}) = -\sqrt{2}$,

Por la Proposición 3.2.5, existen $\tau_1, \tau_2 \in \mathcal{G}(L/\mathbb{Q})$ tales que $\tau_1|_M = \beta_1$ y $\tau_2|_M = \beta_2$. Como α está en una extensión de grado 4, su polinomio mínimo sobre $\mathbb{Q}$ es P, así pues se tiene que $\tau_j(\alpha) \in \{\alpha, -\alpha, i/\alpha, -i/\alpha\}$, $j = 1, 2$; es decir, que en principio τ_1 y τ_2 podrían tomar cuatro valores distintos, y componer con σ sólo permite pasar de uno de

los valores a otro. Cuando sucede esto es que hay algunas extensiones de β_1 y β_2 que no son posibles, por ejemplo $\tau_2(\alpha) = \alpha \Rightarrow \tau_2(\alpha^2) = \alpha^2 \Rightarrow \tau_2(\sqrt{2}) = \sqrt{2}$ lo que contradice $\tau_2|_M = \beta_2$. De la misma forma, $\tau_2(\alpha) = -\alpha$, $\tau_1(\alpha) = i/\alpha$, $\tau_1(\alpha) = -i/\alpha$, son imposibles, así pues $\tau_1(\alpha) \in \{\alpha, -\alpha\}$, $\tau_2(\alpha) \in \{i/\alpha, -i/\alpha\}$, y, quizá componiendo con σ, siempre podemos suponer $\tau_1(\alpha) = \alpha$ y $\tau_2(\alpha) = i/\alpha$. El grupo de Galois viene entonces dado por

$$\mathcal{G}(L/\mathbb{Q}) = \{\mathrm{Id}, \tau_1, \tau_2, \tau_1\tau_2, \sigma, \sigma\tau_1, \sigma\tau_2, \sigma\tau_1\tau_2\}.$$

Nótese que no es abeliano: $\tau_1\tau_2(\alpha) = \tau_1(i/\alpha) = -i/\alpha$ y $\tau_2\tau_1(\alpha) = \tau_2(\alpha) = i/\alpha$. Aunque no lo haremos aquí, como antes, se puede comprobar que $\mathcal{G}(L/\mathbb{Q}) \cong D_8$.

Una extensión finita que no sea normal siempre podemos considerarla dentro de una extensión mayor que sí lo sea. Gracias a la Proposición 3.2.5 todos los elementos del grupo de Galois de la primera extensión serán restricciones de los de la segunda. Pero muchas veces no hace falta ir tan lejos.

Ejemplo. Hallar $\mathcal{G}\big(\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})/\mathbb{Q}\big)$.

Por el Lema 3.2.2, cualquier elemento de $\mathcal{G}\big(\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})/\mathbb{Q}\big)$ debe dejar fijo $\sqrt[3]{3}$ porque el resto de las raíces de $x^3 - 2$ son complejas y no pertenecen a $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. Como $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})/\mathbb{Q}(\sqrt[3]{3})$ es normal, por el Corolario 3.2.6 existe un automorfismo σ que pasa $\sqrt{2}$ a $-\sqrt{2}$ y deja fijo $\mathbb{Q}(\sqrt[3]{3})$, y de hecho éste y la identidad son los únicos $\mathbb{Q}(\sqrt[3]{2})$-automorfismos, ya que el grado de la extensión anterior es 2. Por tanto el grupo de Galois buscado es $\{\mathrm{Id}, \sigma\}$.

Para terminar, vamos a estudiar el grupos de Galois de las extensiones más raras con las que hemos trabajado: las de cuerpos finitos. Resulta que la teoría en ellos es ridículamente sencilla. Esencialmente sólo hay un automorfismo y sus potencias.

Definición: Se llama *automorfismo de Frobenius* en $\mathbb{F}_q$ con $q = p^n$ a la aplicación $\phi : \mathbb{F}_q :\longrightarrow \mathbb{F}_q$ definida como $\phi(x) = x^p$.

Proposición 3.2.8 *El automorfismo de Frobenius es realmente un automorfismo y ϕ^n (esto es, ϕ compuesto consigo mismo n veces) deja invariantes a los elementos de $\mathbb{F}_q$ con $q = p^n$ y tiene orden d en $\mathbb{F}_{q'}$ con $q' = p^{nd}$.*

Demostración: Es evidente que $\phi(x)\phi(y) = \phi(xy)$ y $\phi(1) = 1$, mientras que la igualdad $\phi(x + y) = \phi(x) + \phi(y)$ se sigue del binomio de Newton empleando que el número combinatorio $\binom{p}{k}$ es divisible por p, $0 < k < p$. Es un monomorfismo porque $x^p = 0 \Rightarrow x = 0$ (estamos en un dominio de integridad), por tanto $|\mathrm{Im}\ \phi| = |\mathbb{F}_q|$ y se tiene que también es biyectiva.

Por definición los elementos de $\mathbb{F}_q$ satisfacen $x^{p^n} = x$, esto es, $\phi^n(x) = x$. Por otro lado, si ϕ^{nk} fuera la identidad en $\mathbb{F}_{q'}$ para algún $0 < k < d$, entonces todos los elementos de $\mathbb{F}_{q'}$ satisfarían $x^{p^{nk}} = x$ y de aquí se deduciría $\mathbb{F}_{p^{nk}} \supset \mathbb{F}_{q'}$, lo cual contradice $|\mathbb{F}_{p^{nk}}| = p^{nk} < |\mathbb{F}_{q'}| = p^{nd}$. □

Corolario 3.2.9 *Si $q = p^n$ y $q' = p^{nd}$ entonces $\mathcal{G}(\mathbb{F}_{q'}/\mathbb{F}_q) = \langle\phi^n\rangle \cong \mathbb{Z}_d$.*

Demostración: Según la proposición, $\mathbb{Z}_d \cong \langle \phi^n \rangle \subset \mathcal{G}(\mathbb{F}_{q'}/\mathbb{F}_q)$ y la igualdad se sigue, a través del Corolario 3.2.7, de $[\mathbb{F}_{q'} : \mathbb{F}_q] = [\mathbb{F}_{q'} : \mathbb{F}_p]/[\mathbb{F}_q : \mathbb{F}_p] = nd/n = d$. □

Ejemplo. Hallar $\mathcal{G}(L/\mathbb{F}_2)$ y $\mathcal{G}(L/\mathbb{F}_4)$ donde L es el cuerpo de descomposición de $P = x^4 + x + 1$.

Ya habíamos visto anteriormente que P es irreducible en $\mathbb{F}_2[x]$ y que L es (isomorfo a) $\mathbb{F}_{2^4}$. Según el corolario anterior $\mathcal{G}(L/\mathbb{F}_2) = \langle \phi \rangle \cong \mathbb{Z}_4$ y $\mathcal{G}(L/\mathbb{F}_4) = \langle \phi^2 \rangle \cong \mathbb{Z}_2$ con $\phi(x) = x^2$.

Como comprobación, nótese que es fácil verificar que ϕ^4 deja fija a cada raíz α de P en L porque $\phi^4(\alpha) = \alpha^{16} = (\alpha^4)^4 = (-\alpha - 1)^4 = \alpha^4 + 1 = -\alpha - 1 + 1 = \alpha$.

3.3. El teorema fundamental de la teoría de Galois

A continuación vamos a enunciar un teorema de tal calado que justifica su aparición en solitario dentro de esta sección sin más compañía que un leve acuerdo de notación y la ineludible corte de ejemplos que den boato a su majestad. Este teorema establecerá un diccionario que permite traducir problemas de extensiones finitas en otros de grupos finitos. Todavía más, dentro del reino de las extensiones finitas normales y separables, el diccionario será perfecto, sin ambigüedades ni sinónimos. En particular todo funcionará a las mil maravillas en los cuerpos de descomposición de polinomios sobre un subcuerpo de $\mathbb{C}$. Éste es el caso sobre el que trabajaba Galois para atacar el problema de la resolubilidad por radicales. Aunque en su tiempo no existiera ni siquiera la definición de cuerpo, no está de más hacer de la notación un monumento a su nombre.

Definición: Se dice que L/K es una *extensión de Galois* si es normal, finita y separable.

Teorema 3.3.1 (Teorema fundamental de la teoría de Galois) *Sea L/K una extensión de Galois. La aplicación $H \mapsto H'$ define una biyección entre los subgrupos de $\mathcal{G}(L/K)$ y los subcuerpos $M \subset L$ que conforman extensiones de K, cuya inversa es $M \mapsto \mathcal{G}(L/M)$. Además M/K es una extensión normal si y sólo si $\mathcal{G}(L/M) \triangleleft \mathcal{G}(L/K)$. En este caso $\mathcal{G}(M/K) \cong \mathcal{G}(L/K)/\mathcal{G}(L/M)$.*

Nota: Recuérdese que la notación $H \triangleleft G$ significa que H es un subgrupo normal de G, esto es, que para todo $\tau \in G$ se cumple $\tau^{-1} H \tau = H$.

Demostración: Para probar la biyectividad de la aplicación indicada basta *precomponerla* y *poscomponerla* con su posible inversa y verificar que se obtiene la identidad, esto es, hay que verificar las igualdades $\big(\mathcal{G}(L/M)\big)' = M$ y $\mathcal{G}(L/H') = H$.

Por la Proposición 3.2.4 y el Corolario 3.2.7, $[L : \big(\mathcal{G}(L/M)\big)'] = |\mathcal{G}(L/M)| = [L : M]$ y como $\big(\mathcal{G}(L/M)\big)' \supset M$, se deduce la primera igualdad (de hecho ya fue implícitamente probada en la demostración del Corolario 3.2.7). Para la segunda, nótese que por la Proposición 3.2.4 y la primera igualdad, $|\mathcal{G}(L/H')| = [L : \big(\mathcal{G}(L/H')\big)'] = [L : H'] = |H|$, de donde $\mathcal{G}(L/H') = H$, ya que la inclusión $\mathcal{G}(L/H') \supset H$ es trivial.

Supongamos que M/K es normal. Dado $\sigma \in \mathcal{G}(L/K)$, como M es un cuerpo de descomposición (Proposición 3.1.3), la Proposición 3.2.2 implica que σ aplica M en M

y por tanto $\sigma|_M \in \mathcal{G}(M/K)$, donde $\sigma|_M$ es la restricción de σ a M. Esto define un homomorfismo de grupos

$$\begin{array}{rcl} \phi : \mathcal{G}(L/K) & \longrightarrow & \mathcal{G}(M/K) \\ \sigma & \longrightarrow & \sigma|_M \end{array}$$

que es sobreyectivo (por la Proposición 3.2.5 con $M_1 = M_2 = M$) y cuyo núcleo es $\mathcal{G}(L/M)$, por tanto el teorema del homomorfismo (véase el repaso de teoría de grupos del próximo capítulo) implica que $\mathcal{G}(L/M)$ es un grupo normal de $\mathcal{G}(L/K)$ y que $\mathcal{G}(M/K)$ es isomorfo a $\mathcal{G}(L/K)/\mathcal{G}(L/M)$.

Por otra parte, si M/K no es normal, existen $\alpha \in M$ y $\beta \notin M$ raíces de un mismo polinomio irreducible en $K[x]$. Sea $\gamma \neq \beta$ una raíz del polinomio mínimo de β sobre M (existe por la separabilidad). Por el Corolario 3.2.6, existen automorfismos $\tau \in \mathcal{G}(L/K)$ y $\sigma \in \mathcal{G}(L/M)$ tales que $\tau(\alpha) = \beta$ y $\sigma(\beta) = \gamma$. Si fuera $\mathcal{G}(L/M) \lhd \mathcal{G}(L/K)$ entonces $\tau^{-1}\sigma\tau \in \mathcal{G}(L/M)$ y en particular debería dejar invariante a $\alpha \in M$, pero esto contradice $\tau^{-1}\sigma\tau(\alpha) = \tau^{-1}(\gamma) \neq \tau^{-1}(\beta) = \alpha$. □

Un resultado como el anterior raramente nos podrá dejar impávidos una vez que lo comprendemos. Resulta que la estructura fina de los conjuntos de números que podemos construir con sumas, restas, multiplicaciones y divisiones, operaciones ancestrales y naturales, adquiere fiel reflejo en la artificial definición de un grupo, al tiempo que el concepto de subgrupo normal que permanecía agazapado en nuestros apuntes de un curso pasado se revela ahora como representante de todos los números que podemos obtener a partir de las soluciones de ecuaciones algebraicas (cuerpos de descomposición). Es cautivador soñar que los grupos y subgrupos normales ya preexistían en algún mundo de las ideas matemáticas y que fueron descubiertos, como pieza que completa un rompecabezas, más que inventados. Esta tendencia al platonismo es lugar de recreo eventual entre los matemáticos, a pesar de los jarros de agua fría descargados por la realidad, la historia de la Ciencia y los filósofos empiristas seguidores de D. Hume, quien ya recogió la situación en su *Tratado de la Naturaleza Humana*, escribiendo: "A los matemáticos les es habitual pretender que las ideas de que se ocupan son de naturaleza tan refinada y espiritual que no son del dominio de la fantasía, sino que deben ser comprendidas por una visión pura e intelectual de la que sólo las facultades del alma son capaces".

Como hemos anunciado, el resto de la sección estará compuesta de ejemplos. Para abreviar y no alargar más este capítulo, ya desproporcionado, aprovecharemos parte de los ejemplos desarrollados en la sección anterior. Para comenzar, un ejemplo conspicuo en la historia de nuestra ciencia ya que constituye un descubrimiento del joven Gauss a los 19 años que favoreció su decisión de dedicarse a las Matemáticas. En el último capítulo volveremos sobre la teoría general al respecto que plasmó en la última sección de su obra maestra [Gau].

Ejemplo. Existen cuerpos $\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset L_3 = \mathbb{Q}(\cos(2\pi/17))$ satisfaciendo $[L_j : L_{j-1}] = 2$, $j = 1, 2, 3$. Por tanto el polígono regular de 17 lados inscrito en la circunferencia unidad es construible con regla y compás. (Nótese que a partir de $\cos(2\pi/17)$ se puede construir el ángulo de $2\pi/17$ radianes).

Sabemos que $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_{16}\}$ con $\zeta = e^{2\pi i/17}$ y $\sigma_j(\zeta) = \zeta^j$. Tras algunos cálculos, se tiene que este grupo de orden 16 es cíclico generado por ejemplo por $\sigma = \sigma_3$. Los únicos subcuerpos serán $\mathbb{Q} = \langle\sigma\rangle'$, $L_1 = \langle\sigma^2\rangle'$, $L_2 = \langle\sigma^4\rangle'$, $L_3 = \langle\sigma^8\rangle'$ y $\mathbb{Q}(\zeta) = \langle\{\mathrm{Id}\}\rangle'$. Por la Proposición 3.2.4, $[L_j : \mathbb{Q}] = 2^j$. De la relación $x + 1/x = 2\cos(2\pi/17)$ válida para $x = \zeta$ se sigue que $[\mathbb{Q}(\zeta) : \mathbb{Q}(\cos(2\pi/17))] \leq 2$, además $\mathbb{Q}(\zeta) \neq \mathbb{Q}(\cos(2\pi/17))$ porque el segundo cuerpo no contiene números complejos. Así que la única posibilidad es $\mathbb{Q}(\cos(2\pi/17)) = L_3$.

Ejemplo. Hallar todos los subcuerpos de $L = \mathbb{Q}(\zeta)/\mathbb{Q}$ con $\zeta = e^{2\pi i/7}$.

La extensión $L/\mathbb{Q}$ es de Galois (L es el cuerpo de descomposición de $x^7 - 1$ sobre $\mathbb{Q}$) y todo subcuerpo $M \subset L$ conforma una extensión de $\mathbb{Q}$ ($1 \in M \Rightarrow \mathbb{Z} \subset M \Rightarrow \mathbb{Q} \subset M$).

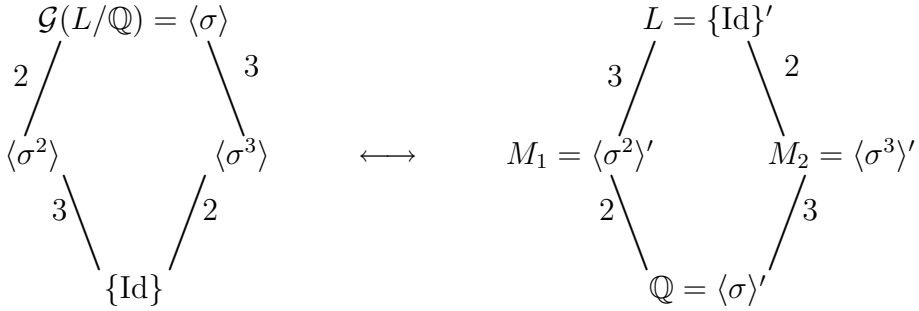
Sabíamos que $\mathcal{G}(L/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_6\}$ con $\sigma_j(\zeta) = \zeta^j$. Es fácil ver con algunos cálculos que $\sigma = \sigma_3$ es generador de este grupo ya que $\sigma^2, \sigma^3 \neq \mathrm{Id}$. Así pues $\mathcal{G}(L/\mathbb{Q}) = \langle\sigma\rangle \cong \mathbb{Z}_6$. Los subgrupos propios son por tanto $\langle\sigma^2\rangle$ y $\langle\sigma^3\rangle$, de órdenes 3 y 2 respectivamente. Los subcuerpos fijos son $M_1 = \langle\sigma^2\rangle'$ y $M_2 = \langle\sigma^3\rangle'$ con $[M_1 : \mathbb{Q}] = 6/3 = 2$ y $[M_2 : \mathbb{Q}] = 6/2 = 3$. En un ejemplo anterior ya habíamos probado que el subcuerpo fijo por σ_2, que coincide con σ^2, es $M_1 = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$. Podemos proceder de la misma forma para hallar M_2. Nótese que $\sigma^3(\zeta) = \zeta^6 = -1 - \zeta - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5$ y por tanto para $x = \sum_{j=0}^{6} \lambda_j \zeta^j \in L$, $\sigma^3(x) = x$ equivale a

$$\begin{aligned} x &= \lambda_0 + \lambda_1\zeta^6 + \lambda_2\zeta^{12} + \lambda_3\zeta^{18} + \lambda_4\zeta^{24} + \lambda_5\zeta^{30} \\ &= \lambda_0 + \lambda_5\zeta^2 + \lambda_4\zeta^3 + \lambda_3\zeta^4 + \lambda_2\zeta^5 + \lambda_1\zeta^6 \\ &= (\lambda_0 - \lambda_1) - \lambda_1\zeta + (\lambda_5 - \lambda_1)\zeta^2 + (\lambda_4 - \lambda_1)\zeta^3 + (\lambda_3 - \lambda_1)\zeta^4 + (\lambda_2 - \lambda_1)\zeta^5 \end{aligned}$$

y de aquí $\lambda_1 = 0$, $\lambda_3 = \lambda_4$, $\lambda_2 = \lambda_5$. Lo cual prueba $M_2 = \mathbb{Q}(\zeta^3 + \zeta^4, \zeta^2 + \zeta^5)$.

Nótese que $2\cos(2\pi/7) = \zeta + \zeta^6 = -1 - (\zeta^3 + \zeta^4) - (\zeta^2 + \zeta^5) \in M_2$ y como $[\mathbb{Q}(\cos(2\pi/7)) : \mathbb{Q}] = 3$ se cumple $M_2 = \mathbb{Q}(\cos(2\pi/7))$. También M_1 se puede simplificar, ya que $[M_1 : \mathbb{Q}] = 2$ implica $M_1 = \mathbb{Q}(\sqrt{q})$ con $q \in \mathbb{Q}$. Con algo de trabajo se puede demostrar que $M_1 = \mathbb{Q}(\sqrt{7})$, aunque no lo haremos aquí.

El teorema fundamental de la teoría de Galois asegura que M_1 y M_2 son los únicos subcuerpos propios (distintos de L y $\mathbb{Q}$) de L. En un esquema se puede visualizar la relación entre el retículo de subgrupos y el de subcuerpos. A través de la aplicación $H \mapsto H'$ el segundo se obtiene a partir del primero de forma invertida. Los números indican índices (cocientes de órdenes de grupos) y grados.



Todos los subgrupos de $\mathcal{G}(L/\mathbb{Q})$ son normales porque es abeliano, por tanto $M_1/\mathbb{Q}$ y $M_2/\mathbb{Q}$ son normales.

Observación: La correspondencia entre índices y grados es consecuencia de la Proposición 3.2.4. Si $N \subset M \subset L$ con $M = H'$ y $N = G'$, entonces el índice de H en G, habitualmente denotado con $[G : H]$, es $|G|/|H| = [L : N]/[L : M] = [M : N]$.

Ejemplo. Hallar todos los subcuerpos de L, el cuerpo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$ e indicar si dan lugar a extensiones normales sobre $\mathbb{Q}$.

Sabíamos que $\mathcal{G}(L/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\} \cong S_3$ donde τ es la conjugación (de orden 2) y $\sigma(\omega) = \omega$, $\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ (de orden 3), $\omega = (-1+i\sqrt{3})/2$. Como $|S_3| = 6$, los órdenes de sus subgrupos propios sólo puede ser dos o tres. Los de orden 2 están generados por un elemento del mismo orden y hay tres de ellos, correspondiendo a cada una de las trasposiciones: $(1, 2)$, $(1, 3)$ y $(2, 3)$. Hay un solo subgrupo de orden tres, $A_3 = \langle(1, 2, 3)\rangle$, generado por un elemento de orden tres. En $\mathcal{G}(L/\mathbb{Q})$ tenemos los elementos de orden dos τ, $\sigma\tau$ y $\sigma^2\tau$, y el de orden tres σ. Por el teorema fundamental de la teoría de Galois los subcuerpos propios son, por consiguiente, $M_1 = \langle\sigma\rangle'$, $M_2 = \langle\tau\rangle'$, $M_3 = \langle\tau\sigma\rangle'$, y $M_4 = \langle\tau\sigma^2\rangle'$. Como $A_3 \lhd S_3$, pero una transposición no genera un subgrupo normal (ejercicio), se tiene que $M_1/\mathbb{Q}$ es una extensión normal mientras que $M_2/\mathbb{Q}$, $M_3/\mathbb{Q}$ y $M_4/\mathbb{Q}$ no lo son. Para calcularlos, escribamos cada $x \in L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ en función de una base de $L/\mathbb{Q}$, $x = \lambda_0 + \lambda_1\omega + \lambda_2\sqrt[3]{2} + \lambda_3\omega\sqrt[3]{2} + \lambda_4\sqrt[3]{2^2} + \lambda_5\omega\sqrt[3]{2^2}$. Por definición, $x \in M_1$ si y sólo si $x = \sigma(x)$, que empleando $\omega^2 = -\omega - 1$ se puede escribir como

$$x = \lambda_0 + \lambda_1\omega - \lambda_3\sqrt[3]{2} + (\lambda_2 - \lambda_3)\omega\sqrt[3]{2} + (\lambda_5 - \lambda_4)\sqrt[3]{2^2} - \lambda_4\omega\sqrt[3]{2^2}.$$

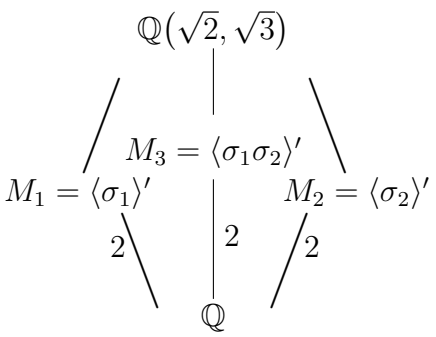
Al igualar coeficientes se obtiene $\lambda_2 = \lambda_3 = \lambda_4 = \lambda_5 = 0$, lo que implica $M_1 = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$. Los otros cuerpos fijos se hallan de igual manera. Por ejemplo, al imponer $x = \tau(x)$ se tiene

$$x = (\lambda_0 - \lambda_1) - \lambda_1\omega + (\lambda_2 - \lambda_3)\sqrt[3]{2} - \lambda_3\omega\sqrt[3]{2} + (\lambda_4 - \lambda_5)\sqrt[3]{2^2} - \lambda_5\omega\sqrt[3]{2^2}.$$

Así que $\lambda_1 = \lambda_3 = \lambda_5 = 0$ y $M_2 = \mathbb{Q}(\sqrt[3]{2})$. Igualmente, $M_3 = \mathbb{Q}(\omega\sqrt[3]{2})$ y $M_4 = \mathbb{Q}(\omega^2\sqrt[3]{2})$.

Ejemplo. Hallar los subcuerpos de L, el cuerpo de descomposición de $P = x^4 - 5x^2 + 6$ sobre $\mathbb{Q}$.

Gracias a la factorización $P = (x^2 - 2)(x^2 - 3)$, se sigue $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Ya habíamos calculado su grupo de Galois, $\mathcal{G}(L/\mathbb{Q}) = \{\mathrm{Id}, \sigma_1, \sigma_2, \sigma_1\sigma_2\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ donde $\sigma_1(\sqrt{2}) = -\sqrt{2}$, $\sigma_1(\sqrt{3}) = \sqrt{3}$, $\sigma_2(\sqrt{2}) = \sqrt{2}$, $\sigma_2(\sqrt{3}) = -\sqrt{3}$. Como $\mathbb{Z}_2 \times \mathbb{Z}_2$ sólo tiene tres subgrupos propios, $\langle(\overline{0}, \overline{1})\rangle$, $\langle(\overline{1}, \overline{0})\rangle$, $\langle(\overline{1}, \overline{1})\rangle$, el teorema fundamental de la teoría de Galois asegura que L sólo tiene tres subcuerpos propios que vienen dados por $M_1 = \langle\sigma_1\rangle'$, $M_2 = \langle\sigma_2\rangle'$, $M_3 = \langle\sigma_1\sigma_2\rangle'$. Ya habíamos comprobado que estos subcuerpos fijos son $M_1 = \mathbb{Q}(\sqrt{3})$, $M_2 = \mathbb{Q}(\sqrt{2})$ y $M_3 = \mathbb{Q}(\sqrt{6})$. De nuevo, como $\mathbb{Z}_2 \times \mathbb{Z}_2$ es un grupo abeliano todos sus subgrupos son normales y de antemano podríamos saber que las extensiones correspondientes son normales.



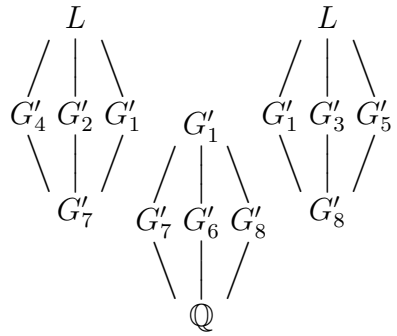
Ejemplo. Calcular cuántos subcuerpos tiene $L = \mathbb{Q}(\sqrt[4]{2}, i)$.

La extensión $L/\mathbb{Q}$ es de Galois porque L es el cuerpo de descomposición de $x^4 - 2$ sobre $\mathbb{Q}$. Según un ejemplo de la sección anterior, $\mathcal{G}(L/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$ con τ la conjugación compleja y $\sigma(i) = i$, $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$. Por el teorema fundamental de la teoría de Galois el número de subcuerpos coincide con el de subgrupos de $\mathcal{G}(L/\mathbb{Q})$. Aparte de los subgrupos triviales $\{\mathrm{Id}\}$ y $\mathcal{G}(L/\mathbb{Q})$, el resto sólo puede tener orden dos o cuatro. Los subgrupos de orden dos son los generados por un elemento de orden dos, y los subgrupos de orden cuatro o bien están generados por un elemento de orden cuatro (si es que son isomorfos a $\mathbb{Z}_4$) o por dos de orden dos que conmutan (si es que son isomorfos a $\mathbb{Z}_2 \times \mathbb{Z}_2$). Podemos revisar todas las posibilidades empleando la siguiente tabla que expresa la accción de los elementos de $\mathcal{G}(L/\mathbb{Q})$ sobre i y $\sqrt[4]{2}$, los generadores de la extensión.

	i	$\sqrt[4]{2}$	orden
Id	i	$\sqrt[4]{2}$	1
σ	i	$i\sqrt[4]{2}$	4
σ^2	i	$-\sqrt[4]{2}$	2
σ^3	i	$-i\sqrt[4]{2}$	4

	i	$\sqrt[4]{2}$	orden
τ	$-i$	$\sqrt[4]{2}$	2
$\sigma\tau$	$-i$	$i\sqrt[4]{2}$	2
$\sigma^2\tau$	$-i$	$-\sqrt[4]{2}$	2
$\sigma^3\tau$	$-i$	$-i\sqrt[4]{2}$	2

De aquí se deduce que los subgrupos de orden dos son $G_1 = \langle\sigma^2\rangle$, $G_2 = \langle\tau\rangle$, $G_3 = \langle\sigma\tau\rangle$, $G_4 = \langle\sigma^2\tau\rangle$, $G_5 = \langle\sigma^3\tau\rangle$, y los de orden cuatro son $G_6 = \langle\sigma\rangle$, $G_7 = \langle\sigma^2, \tau\rangle$, $G_8 = \langle\sigma^2, \sigma\tau\rangle$.



En total hay, por tanto, diez subcuerpos de L: todos los G'_j y los subgrupos triviales L y $\mathbb{Q}$.

Hemos representado el retículo de subcuerpos en tres esquemas por razonas tipográficas (debemos unir el de en medio a los de los lados pegando los cuerpos idénticos). Los subcuerpos a la altura inmediatamente posterior a $\mathbb{Q}$ dan lugar a extensiones de grado dos, y los siguientes, a extensiones de grado cuatro. No todas las extensiones son normales, de hecho, aunque no lo comprobaremos aquí, exactamente $G'_2/\mathbb{Q}$, $G'_3/\mathbb{Q}$, $G'_4/\mathbb{Q}$ y $G'_5/\mathbb{Q}$ no son normales y el resto de los subcuerpos fijos dan lugar a extensiones normales sobre $\mathbb{Q}$.

Ejemplo. Hallar todos los subcuerpos $\mathbb{Q}(\sqrt{2}) \subsetneq M \subsetneq \mathbb{Q}(\sqrt[4]{2}, i)$.

Con la notación del ejemplo previo, ya habíamos visto en la sección anterior que $\mathbb{Q}(\sqrt{2}) = G'_7$. Por tanto debe ser $M = H'$ con H un subgrupo propio de G_7. Las únicas posibilidades son $M = G'_1$, $M = G'_2$ y $M = G'_4$. Escribamos cada $x \in M$ como

$$x = \lambda_0 + \lambda_1 i + \lambda_2\sqrt[4]{2} + \lambda_3 i\sqrt[4]{2} + \lambda_4\sqrt[4]{2^2} + \lambda_5 i\sqrt[4]{2^2} + \lambda_6\sqrt[4]{2^3} + \lambda_7 i\sqrt[4]{2^3} \qquad \text{con} \quad \lambda_j \in \mathbb{Q}.$$

En el primer caso $\sigma^2(x) = x$ lleva a $\lambda_2 = \lambda_3 = \lambda_6 = \lambda_7 = 0$, de donde $M = \mathbb{Q}(\sqrt{2}, i)$. En el segundo caso $\tau(x) = x$ conduce claramente a $M = \mathbb{Q}(\sqrt[4]{2})$. Finalmente, $\sigma^2\tau(x) = x$ implica $\lambda_1 = \lambda_2 = \lambda_3 = \lambda_6 = 0$ y $M = \mathbb{Q}(i\sqrt[4]{2})$.

Podemos trabajar con extensiones que no sean de Galois si es posible extenderlas a otras que lo sean.

Ejemplo. Hallar todos los subcuerpos de $\mathbb{Q}(\sqrt[4]{2})$.

Como $\mathbb{Q}(\sqrt[4]{2}) \subset L = \mathbb{Q}(\sqrt[4]{2}, i)$, los subcuerpos de $\mathbb{Q}(\sqrt[4]{2})$ lo serán también de L. Además $\mathbb{Q}(\sqrt[4]{2}) = G_2'$ implica que corresponderán a subgrupos de $\mathcal{G}(L/\mathbb{Q})$ que contengan a G_2. Según nuestro estudio, las únicas posibilidades son G_7, $\mathcal{G}(L/\mathbb{Q})$ y el propio G_2. En definitiva, los únicos subcuerpos son $G_7' = \mathbb{Q}(\sqrt{2})$, $\big(\mathcal{G}(L/\mathbb{Q})\big)' = \mathbb{Q}$ y $\mathbb{Q}(\sqrt[4]{2})$.

Demos paso ahora a un ejemplo bastante más complicado en el que calcular el grupo de Galois, e incluso el grado de la extensión, lleva a aplicar el teorema fundamental de la teoría de Galois.

Ejemplo. Hallar $\mathcal{G}(\mathbb{Q}(\zeta, \sqrt[3]{3})/\mathbb{Q})$ con $\zeta = e^{2\pi i/13}$.

No está claro si la extensión es normal. Tenemos la inclusión $\mathbb{Q}(\zeta, \sqrt[3]{3}) \subset L = \mathbb{Q}(\zeta, \sqrt[3]{3}, \omega)$ con $L/\mathbb{Q}$ normal, $\omega = (-1 + i\sqrt{3})/2$. En $\mathcal{G}(L/\mathbb{Q})$, de acuerdo con el Corolario 3.2.6, cualquier $\mathbb{Q}$-automorfismo aplica $\sqrt[3]{3}$ en $\sqrt[3]{3}$, $\omega\sqrt[3]{3}$ o $\omega^2\sqrt[3]{3}$. A continuación probaremos que $\omega\sqrt[3]{3}, \omega^2\sqrt[3]{3} \notin \mathbb{Q}(\zeta, \sqrt[3]{3})$, de donde se concluye que todos los automorfismos de $\mathcal{G}(\mathbb{Q}(\zeta, \sqrt[3]{3})/\mathbb{Q})$ fijan $\sqrt[3]{3}$. Por tanto sus automorfismos serán los extendidos desde $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$, es decir, $\mathcal{G}(\mathbb{Q}(\zeta, \sqrt[3]{3})/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_{12}\}$ con $\sigma_j(\zeta) = \zeta^j$ y $\sigma_j(\sqrt[3]{3}) = \sqrt[3]{3}$.

Resta por tanto demostrar que $\omega\sqrt[3]{3}, \omega^2\sqrt[3]{3} \notin \mathbb{Q}(\zeta, \sqrt[3]{3})$, lo cual equivale a $\omega \notin \mathbb{Q}(\zeta, \sqrt[3]{3})$. No puede ser $\sqrt[3]{3} \in \mathbb{Q}(\zeta)$ porque al ser $\mathbb{Q}(\zeta)/\mathbb{Q}$ normal se tendría la inclusión $\mathbb{Q}(\sqrt[3]{3}, \omega\sqrt[3]{3}, \omega^2\sqrt[3]{3}) \subset \mathbb{Q}(\zeta)$ lo que lleva a una contradicción porque el grupo de Galois (sobre $\mathbb{Q}$) del primer cuerpo no es abeliano y el segundo sí. Por consiguiente $[\mathbb{Q}(\zeta, \sqrt[3]{3}) : \mathbb{Q}(\zeta)] = 3$ lo que implica que $\omega \notin \mathbb{Q}(\zeta, \sqrt[3]{3}) - \mathbb{Q}(\zeta)$ ya que ω está en una extensión de grado a lo más dos sobre $\mathbb{Q}(\zeta)$. Con algunos cálculos (ejercicio) se prueba que el único subcuerpo de $\mathbb{Q}(\zeta)$ de grado dos sobre $\mathbb{Q}$ es $\mathbb{Q}(\zeta + \zeta^3 + \zeta^4 + \zeta^9 + \zeta^{10} + \zeta^{12})$. Este subcuerpo es de números reales ya que $\zeta^k + \zeta^{13-k} = 2\cos(2\pi k/13)$, por tanto no puede coincidir con $\mathbb{Q}(\omega)$.

En extensiones de cuerpos finitos todo es muy fácil, porque el grupo de Galois es siempre cíclico y hay un subgrupo de cada orden que divida al del grupo. Cada uno de ellos corresponderá a un subcuerpo isomorfo a algún $\mathbb{F}_q$. Sin embargo siempre podemos complicar un poco las cosas pidiendo una representación particular de los subcuerpos.

Ejemplo. Sea α una raíz de $x^4 + x + 1 \in \mathbb{F}_2[x]$ en su cuerpo de descomposición. Describir los subcuerpos $\mathbb{F}_2 \subsetneq M \subsetneq \mathbb{F}_2(\alpha)$ como $M = \mathbb{F}_2(\beta)$ para algún $\beta \in \mathbb{F}_2(\alpha)$

Como x^4+x+1 es irreducible, $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 4$, $\mathbb{F}_2(\alpha)$ es isomorfo a $\mathbb{F}_{2^4}$ y el grupo de Galois es $\mathcal{G}(\mathbb{F}_2(\alpha)/\mathbb{F}_2) = \langle\phi\rangle \cong \mathbb{Z}_4$ donde ϕ es el automorfismo de Frobenius $\phi(x) = x^2$. El único subgrupo propio es $\langle\phi^2\rangle$ y por tanto $M = \langle\phi^2\rangle'$. Cualquier $x \in \mathbb{F}_2(\alpha)$ se escribe como $x = \lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \lambda_3\alpha^3$ con $\lambda_j \in \mathbb{F}_2$. En $\mathbb{F}_2(\alpha)$, $(a+b)^4 = a^4 + b^4$ (porque tiene característica dos, ejercicio) y empleando $\alpha^4 + \alpha + 1 = 0$ se tiene que $x = \phi^2(x)$ equivale a

$$\begin{aligned} x &= \lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \lambda_3\alpha^3 = \lambda_0 + \lambda_1(\alpha+1) + \lambda_2(\alpha+1)^2 + \lambda_3(\alpha+1)^3 \\ &= (\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3) + (\lambda_1 + \lambda_3)\alpha + (\lambda_2 + \lambda_3)\alpha^2 + \lambda_3\alpha^3 \end{aligned}$$

de donde $\lambda_3 = 0$ y $\lambda_1 = \lambda_2$. Por tanto $M = \mathbb{F}_2(\alpha + \alpha^2)$.

Ejercicios del Capítulo 3

LEYENDA: ♡ fácil, ♢ difícil, ♢♢ muy difícil, ∘ opcional.

Sección 3.1

1. Hallar el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $x^6 - 8$, y calcular el grado de la extensión correspondiente.

2. Hallar el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $x^4 + 5x^2 + 5$ y calcular su grado.

3. Probar que $P = x^4 - 2x^3 - x^2 - 2x - 2$ y $Q = x^5 - 3x^3 + x^2 - 3$ tienen el mismo cuerpo de descomposición sobre $\mathbb{Q}$. *Indicación*: Nótese que i es raíz del primero y que $\sqrt{3}$ es raíz del segundo.

4. Sean cuerpos $K \subset M \subset L$ y sea $P \in K[x]$ no constante. Si L es cuerpo de descomposición de P sobre K, probar que L es cuerpo de descomposición de P sobre M.

5. Si L es el cuerpo de descomposición de $P \in K[x]$, demostrar que $[L : K] \big| (\partial P)!$. *Indicación*: Procédase por inducción en el grado del polinomio, distinguiendo dos casos al aplicar la hipótesis de inducción dependiendo de la irreducibilidad de P. Recuérdese que $r!s!$ divide a $(r + s)!$ por la fórmula para los números combinatorios.

6. Sea L/K una extensión de grado 4. Demostrar que si L es el cuerpo de descomposición de un polinomio irreducible de la forma $x^4 + ax^2 + b \in K[x]$, existe un cuerpo intermedio $K \subset E \subset L$ tal que $[E : K] = 2$.

7. Si $K \subset M \subset L$, demostrar que L/K normal $\Rightarrow$ L/M normal, pero L/K normal $\not\Rightarrow$ M/K normal, y L/M, M/K normales $\not\Rightarrow$ L/K normal.

8. Estudiar si las extensiones $\mathbb{Q}(\sqrt[3]{-2}, \sqrt{-2})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt[3]{-3}, \sqrt{-3})/\mathbb{Q}$, son normales.

9. Probar que $P = x^6 + x^3 + 1$ es irreducible en $\mathbb{Q}[x]$ y utilizarlo para demostrar que la extensión $\mathbb{Q}(e^{2\pi i/9})/\mathbb{Q}$, es normal y de grado 6.

10. Demostrar que toda extensión de grado dos es normal.

11. Dar un ejemplo de una extensión normal que no sea finita.

12. Estudiar si $\mathbb{Q}(x)/\mathbb{Q}(x^3)$ es normal.

13. Dar un ejemplo de una extensión normal de grado 3.

♢**14.** Dar un ejemplo de extensión normal de grado 3 sobre $\mathbb{Q}$. *Indicación*: Buscar un polinomio cuyas raíces sean $\cos(2\pi/7)$, $\cos(4\pi/7)$ y $\cos(6\pi/7)$.

15. Demostrar que dada una extensión finita M/K siempre existe un L, $L \supset M \supset K$ tal que L/K es normal y finita. A un cuerpo con estas características y $[L : K]$ mínimo

se le llama *clausura normal* (o cierre normal) de M/K. Probar que sólo hay una clausura normal salvo isomorfismos y hallar la de $\mathbb{Q}(\sqrt[5]{5})/\mathbb{Q}$.

16. Demostrar que $K_1 = \mathbb{F}_2[x]/\langle x^3+x+1\rangle$ y $K_2 = \mathbb{F}_2[x]/\langle x^3+x^2+1\rangle$ son cuerpos de descomposición de $x^8 - x \in \mathbb{F}_2[x]$. Concluir que K_1 y K_2 son isomorfos.

17. Probar que $\mathbb{F}_8$ es el cuerpo de descomposición de $x^3+x^2+1 \in \mathbb{F}_2[x]$ y que $\mathbb{F}_8/\mathbb{F}_2$ es simple.

18. ¿Cuál es el grupo aditivo de $\mathbb{F}_8$?

19. Si $P \in \mathbb{F}_p[x]$ es irreducible y gr $P = n$, ¿es su cuerpo de descomposición isomorfo a $\mathbb{F}_{p^n}$?

20. Estudiar si $\mathbb{F}_{64}$ es una extensión de $\mathbb{F}_{16}$ y de $\mathbb{F}_8$ y en su caso hallar el grado.

21. Sea $P = x^q - x$ con $q = p^n$. Demostrar que cualquier polinomio irreducible en $\mathbb{F}_p[x]$ de grado n divide a P.

22. Probar que todos los factores irreducibles de $x^q - x \in \mathbb{F}_p[x]$ con $q = p^n$, son de grado menor o igual que n.

23. Demostrar que si α es una raíz de $x^3 - 2$ en $\mathbb{F}_{7^3}$, entonces -1, α y $-1+\alpha$ tienen orden (multiplicativo) 2, 9 y 19 respectivamente en el grupo multiplicativo de $\mathbb{F}_{7^3}$. Galois utilizó este hecho para deducir que una raíz de $x^3 - x + 1 \in \mathbb{F}_7[x]$ genera este grupo multiplicativo. Tratar de reconstruir su argumento. *Indicación*: $7^3 - 1 = 2 \cdot 9 \cdot 19$ y en un grupo abeliano $|\langle g\rangle| = n$, $|\langle h\rangle| = m \Rightarrow |\langle gh\rangle| = \text{mcm}(n, m)$.

♢**24.** Probar que el grupo multiplicativo de un cuerpo finito es cíclico. *Indicación*: Estudiar el número de raíces de $x^n - 1$.

∘**25.** Se dice que un cuerpo de característica p es un *cuerpo perfecto* si el morfismo de Frobenius $x \mapsto x^p$ es un isomorfismo. Probar que si K es perfecto todo polinomio irreducible en $K[x]$ es separable. *Indicación*: Tratar de ajustar la prueba vista en el caso $K = \mathbb{F}_p$.

26. ¿Cuántas raíces distintas tiene $x^{12} + 2x^6 + 1 \in \mathbb{F}_3[x]$ en su cuerpo de descomposición?

♢**27.** Sea K un cuerpo de característica $p > 0$ y supongamos que $P = x^p - x - a$ es irreducible en $K[x]$. Probar que si $\alpha \in L \supset K$ es raíz de P entonces $K(\alpha)/K$ es normal.

28. Sea K un cuerpo de característica $p \neq 0$, y sea $f(x) = x^p - a \in K[x]$. Demostrar que $f(x)$ es irreducible sobre K, o que descompone como producto de factores de grado 1 sobre K.

29. Si $K \subset M \subset L$ con L/K finita, demostrar que L/K separable$\Rightarrow$ L/M separable, pero M/K separable $\not\Rightarrow$ L/K separable.

30. Hallar una extensión separable y normal que no sea finita.

31. Dar un ejemplo de una extensión de grado 3 no separable.

32. Sea K un cuerpo de característica $p \neq 0$. Probar que $x^{p^n} - x$ no tiene raíces repetidas.

33. Sea L/K una extensión algebraica con K un cuerpo de característica $p > 0$. Demostrar que si $\alpha \in L$ es separable sobre K y $\alpha^n \in K$ con n una potencia de la característica, entonces $\alpha \in K$.

34. Sea L/K una extensión algebraica con K un cuerpo de característica $p > 0$. Probar que $\alpha \in L$ es separable sobre K si y sólo si $K(\alpha) = K(\alpha^p)$.

35. Sabiendo que el cuerpo de descomposición de un polinomio sin raíces múltiples da lugar siempre a una extensión separable (lo cual es el contenido de un ejercicio de la próxima sección), probar que los elementos separables sobre un cuerpo siempre forman un cuerpo.

♢♢**36.** Sea L/K finita, a partir de la conclusión del ejercicio anterior, probar que si L/M y M/K son separables, L/K también lo es. *Indicación*: Comenzar probando que para todo $\alpha \in L$ existe n igual a una potencia de $\mathrm{char}(K)$ tal que α^n es separable.

37. ¿Es cierto el recíproco del teorema del elemento primitivo?

♢♢**38.** Demostrar que si $K \subset L$ y $[L : K] < \infty$, la extensión L/K no es simple si y sólo si existen infinitos cuerpos intermedios $K \subset M \subset L$. *Indicación*: Si $L = K(\alpha)$, probar que M debe estar generado sobre K por los coeficientes de algún factor del polinomio mínimo de α.

Sección 3.2

♡**39.** Si $L = K(a_1, \ldots, a_n)$ y σ es un K-automorfismo de L tal que $\sigma(a_i) = a_i$ para todo i, probar que σ es la identidad.

40. Sea L un cuerpo. Demostrar que cualquier automorfismo es un K-automorfismo donde K es la intersección de todos los subcuerpos de L (el llamado *subcuerpo primo*).

41. Demostrar que los conjuntos:

$$A = \{\lambda_1 + \lambda_2\sqrt{7} \ : \ \lambda_1, \lambda_2 \in \mathbb{Q}\} \quad \text{y} \quad B = \left\{\lambda_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \ : \ \lambda_1, \lambda_2 \in \mathbb{Q}\right\}$$

son espacios vectoriales sobre $\mathbb{Q}$ isomorfos, pero no son cuerpos isomorfos. *Indicación*: Sólo en uno de ellos la ecuación $x^2 + 1 = 0$ tiene solución.

42. ¿Cuáles son los automorfismos de $\mathbb{Q}$? ¿y los $\mathbb{R}$-homomorfismos (homomorfismos que dejan fijo $\mathbb{R}$) de $\mathbb{C}$ en $\mathbb{C}$?

43. Este ejercicio determina $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$.

i) Probar que cada $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ lleva cuadrados a cuadrados y reales positivos a reales positivos. Concluir que $a < b \Rightarrow \sigma(a) < \sigma(b)$.

ii) Probar que $|a - b| < 1/m \ \Rightarrow \ |\sigma(a) - \sigma(b)| < 1/m$. Concluir que σ es una aplicación continua de $\mathbb{R}$.

iii) Comprobar que una aplicación continua de $\mathbb{R}$ que es la identidad sobre $\mathbb{Q}$ debe ser la identidad en todo $\mathbb{R}$, y por tanto $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \{\mathrm{Id}\}$.

44. Probar con todo rigor que en $\mathbb{Q}(\sqrt{2},\sqrt{3})$ la aplicación $\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$ con $a,b,c,d \in \mathbb{Q}$ es un $\mathbb{Q}$-automorfismo.

45. Hallar el grupo de Galois del cuerpo de descomposición de x^4+x^2-6 sobre $\mathbb{Q}$.

46. Encontrar el grupo de Galois de una extensión normal de $\mathbb{Q}$ de grado mínimo conteniendo a $\sqrt{2}+\sqrt[3]{2}$.

47. Calcular el grupo de Galois de la extensión $\mathbb{Q}(\sqrt{2},\sqrt{5})/\mathbb{Q}$.

48. Hallar el grupo de Galois del polinomio x^4-9 sobre $\mathbb{Q}$.

49. Hallar el grupo de Galois del polinomio x^4+9 sobre $\mathbb{Q}$.

50. Calcular $\mathcal{G}(L/K)$ donde $K = \mathbb{Q}(e^{2\pi i/5})$ y L es el cuerpo de descomposición de $P = x^5-7$ sobre K.

51. Sea $K \subset \mathbb{C}$ el cuerpo de descomposición de $x^2-x+1 \in \mathbb{Q}[x]$ y L el de x^3-2. Hallar $\mathcal{G}(L/K)$.

52. Hallar el grupo de Galois del cuerpo de descomposición de $x^3-5 \in \mathbb{Q}[x]$.

53. Recuérdese que el cuerpo de descomposición, L, de $P = x^2+x+1 \in \mathbb{F}_2[x]$ es un cuerpo de cuatro elementos. Hallar sus automorfismos y sus $\mathbb{F}_2$-automorfismos.

54. Sea $P \in K[x]$ irreducible de grado tres con $\mathrm{char}(K) = 0$, y sea L su cuerpo de descomposición. Demostrar que o bien $[L:K] = 3$ o bien $[L:K] = 6$.

55. Hallar $\mathcal{G}\big(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})\big)$, $\mathcal{G}\big(\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}(\sqrt{6})\big)$, $\mathcal{G}\big(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}\big)$.

56. Hallar $\mathcal{G}\big(\mathbb{Q}(\sqrt{3}+\sqrt[4]{3})/\mathbb{Q}(\sqrt{3})\big)$.

57. Hallar $\mathcal{G}\big(\mathbb{Q}(\sqrt{5}+\sqrt{7})/\mathbb{Q}\big)$.

58. Sea $P = x^4-3x^2+4 \in \mathbb{Q}[x]$. Calcular el grupo de Galois de su cuerpo de descomposición sobre $\mathbb{Q}$.

59. Sea $\alpha = \sqrt{2}+i$ y sea P el polinomio mínimo de α sobre $\mathbb{Q}$. Hallar el grupo de Galois del cuerpo de descomposición de P sobre $\mathbb{Q}$.

60. Calcular $\mathcal{G}(\mathbb{Q}(x,y)/\mathbb{Q}(x+y,xy))$ y $\mathcal{G}(\mathbb{Q}(x,y,z)/\mathbb{Q}(x+y+z,xy+xz+yz,xyz))$ donde $\mathbb{Q}(x,y)$ y $\mathbb{Q}(x,y,z)$ denotan los cuerpos de funciones racionales en dos y tres variables respectivamente. *Indicación*: En el primer caso, x e y son raíces del polinomio $X^2-(x+y)X+xy \in \mathbb{Q}(x+y,xy)[X]$.

♢**61.** Calcular $\mathcal{G}(\mathbb{Q}(x)/\mathbb{Q})$.

62. Hallar un grupo sencillo que sea isomorfo a $\mathcal{G}\big(\mathbb{Q}(e^{2\pi i/13})/\mathbb{Q}\big)$.

♡**63.** ¿Por qué $\mathcal{G}(L/H') \supset H$ es trivial?

64. Probar que si $L = \mathbb{Q}(\cos\frac{2\pi}{17})$, $\mathcal{G}(L/\mathbb{Q}) = \{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6, \sigma^7\} \cong \mathbb{Z}_8$ donde $\sigma\big(2\cos(2\pi/17)\big) = \sigma\big(\zeta + \zeta^{-1}\big) = \zeta^3 + \zeta^{-3}$ con $\zeta = e^{2\pi i/17}$. Demostrar que $\cos(2\pi k/17) \in L$ y que $\sigma(\cos(2\pi k/17)) = \cos(6\pi k/17)$. Si $H = \{\mathrm{Id}, \sigma^4\}$, probar que $H' = \mathbb{Q}(x_1, x_2)$ donde $x_1 = \cos\frac{2\pi}{17} + \cos\frac{26\pi}{17}$ y $x_2 = \cos\frac{2\pi}{17} \cdot \cos\frac{26\pi}{17}$.

65. Encontrar todos los elementos de $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ con $\zeta = e^{2\pi i/7}$ que dejan fijo a $\zeta + \zeta^2 + 3\zeta^3 + \zeta^4 + 3\zeta^5 + 3\zeta^6$.

66. Hallar $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta + \zeta^3 + \zeta^9))$ con $\zeta = e^{2\pi i/13}$.

67. Sean L_1 y L_2 los cuerpos de descomposición de dos polinomios P_1 y P_2 sobre $\mathbb{Q}$. Demostrar que si $L_1 \cap L_2 = \mathbb{Q}$, entonces $\mathcal{G}(L_1/\mathbb{Q}) \times \mathcal{G}(L_2/\mathbb{Q}) \cong \mathcal{G}(L/\mathbb{Q})$ donde L es el cuerpo de descomposición de P_1P_2.

68. Hallar una extensión cuyo grupo de Galois sea isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

69. Si H y N son subgrupos de $\mathcal{G}(L/K)$ cuyos subcuerpos fijos son $H' = L_1$ y $N' = L_2$, indicar qué subcuerpo es $\langle \sigma, \tau \,:\, \sigma \in H,\ \tau \in N\rangle'$.

70. Si $L = \mathbb{Q}(x, y, z)$ y $K = \mathbb{Q}(x + y + z, xy + xz + yz, xyz)$, probar que $\mathbb{Q}\big((x - y)(x - z)(y - z)\big) = \langle\sigma\rangle'$ con σ un elemento de orden 3 de $\mathcal{G}(L/K)$.

♢**71.** Sea L el cuerpo de descomposición de un polinomio sin raíces múltiples. Digamos $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ con $P = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) \in K[x]$, $\alpha_i \neq \alpha_j$. Sea $L_j = K(\alpha_1, \alpha_2, \ldots, \alpha_j)$ y $L_0 = K$. Probar que cada monomorfismo $L_j \longrightarrow L$ se extiende a $[L_{j+1} : L_j]$ monomorfismos $L_{j+1} \longrightarrow L$. Deducir de ello que $|\mathcal{G}(L/K)| = [L : K]$. Concluir finalmente que todos los elementos de L son separables sobre K.

72. Hallar $\mathcal{G}(\mathbb{Q}(x)/\mathbb{Q}(x^n))$, $\mathcal{G}(\mathbb{C}(x)/\mathbb{C}(x^n))$ y $\mathcal{G}(K(x)/K(x^{15}))$ con $K = \mathbb{Q}(e^{2\pi i/3})$, calculando en cada caso los cuerpos que quedan fijos por todos los automorfismos.

73. Hallar $\mathcal{G}(\mathbb{F}_2(x)/\mathbb{F}_2(x^2))$.

74. Consideremos $\zeta = e^{2\pi i/5}$ y sea σ el $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\zeta)$ dado por $\sigma(\zeta) = \zeta^4$. Demostrar que el cuerpo fijo de σ es $\mathbb{Q}(\sqrt{5})$. *Indicación*: Elevar al cuadrado $\frac{1}{2} + \zeta^2 + \zeta^3$.

75. Sea $L = \mathbb{F}_2[x]/\langle x^4 + x^3 + 1\rangle$ y $K = \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$. Hallar $\mathcal{G}(L/K)$ y comprobar que el orden del morfismo de Frobenius en L es 4.

♡**76.** Si σ tiene orden 4 y $\tau \neq \sigma^2$ tiene orden 2, ¿por qué sabemos que los automorfismos en $\{\mathrm{Id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$ son distintos?

77. Sea L el cuerpo de descomposición en $\mathbb{C}$ del polinomio $x^4 + 1$ sobre $\mathbb{Q}$. Encontrar los automorfismos de L con cuerpos fijos $\mathbb{Q}(\sqrt{-2})$ y $\mathbb{Q}(\sqrt{2})$.

78. Sea σ un elemento de $\mathcal{G}(L/K)$ de orden $2n$. Demostrar que para cualquier $\alpha \in L$, $\alpha + \sigma^2(\alpha) + \sigma^4(\alpha) + \cdots + \sigma^{2n-2}(\alpha) \in \langle\sigma^2\rangle'$.

Sección 3.3

79. Sea $L = \mathbb{Q}(\zeta)$ donde $\zeta = e^{2\pi i/11}$. Demostrar que L es una extensión normal de $\mathbb{Q}$ y determinar su grupo de Galois. Encontrar todos los cuerpos intermedios de la

extensión $L/\mathbb{Q}$ y los subgrupos de $\mathcal{G}(L/\mathbb{Q})$ que les corresponden indicando cuáles dan lugar a extensiones normales de $\mathbb{Q}$.

80. Si L/K es una extensión de Galois con grupo de Galois cíclico, probar que dos cuerpos intermedios M_1, M_2 (conteniendo a K) satisfacen $M_1 \subset M_2$ si y sólo si $[L : M_1]$ es un múltiplo de $[L : M_2]$.

81. Sean $K \subset M \subset L$ con L/K de Galois. Probar que $M = K(a)$ con $a \in M$ si y sólo si los únicos elementos de $\mathcal{G}(L/K)$ que fijan a están en $\mathcal{G}(L/M)$. Emplear este resultado para dar una nueva prueba de $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Demostrar de igual manera que $\mathbb{Q}(\sqrt[3]{17}, \sqrt{17}) = \mathbb{Q}(\sqrt[3]{17} + \sqrt{17})$.

♡**82.** Si $K \subset M \subset L$ y L/K es de Galois, ¿deben ser necesariamente L/M y M/K de Galois?

83. Si en una extensión de Galois L/K, con $\mathrm{char}(K) \neq 2$, el grupo de Galois es $\mathbb{Z}_2 \times \mathbb{Z}_2$, demostrar que $L = K(\alpha, \beta)$ con $\alpha^2, \beta^2 \in K$.

84. Sea $\alpha = \sqrt{2} + i$ y sea P el polinomio mínimo de α sobre $\mathbb{Q}$. Hallar todos los subcuerpos de su cuerpo de descomposición sobre $\mathbb{Q}$.

♡**85.** Demostrar que si L es un cuerpo de descomposición de un polinomio sobre $\mathbb{Q}$ y $\mathcal{G}(L/\mathbb{Q})$ es abeliano, entonces $M/\mathbb{Q}$ es normal para todo subcuerpo M, $\mathbb{Q} \subset M \subset L$.

86. Supongamos que $f(x) \in \mathbb{Q}[x]$ es irreducible con $\partial f = 4$ y su cuerpo de descomposición sobre $\mathbb{Q}$ tiene grupo de Galois A_4. Sea θ una raíz de $f(x)$ y sea $L = \mathbb{Q}(\theta)$. Probar que L es una extensión de grado 4 de $\mathbb{Q}$ que no tiene subcuerpos propios. ¿Hay alguna extensión de Galois de $\mathbb{Q}$ de grado cuatro sin subcuerpos propios?

87. Probar que si el grupo de Galois del cuerpo de descomposición de una cúbica sobre $\mathbb{Q}$ es $\mathbb{Z}_3$, entonces todas las raíces de la cúbica son reales.

88. Hallar el grupo de Galois del cuerpo de descomposición de $P = (x^2 - 3)(x^2 + 3)$ sobre $\mathbb{Q}$, calculando los subcuerpos intermedios.

89. Calcular cuántos subcuerpos tiene el cuerpo de descomposición de $P = x^5 + 3x^3 - 3x^2 - 9$ sobre $\mathbb{Q}$.

90. Calcular cuántos subcuerpos tiene el cuerpo de descomposición de $P = x^7 + 4x^5 - x^2 - 4$ sobre $\mathbb{Q}$.

91. Hallar todos los subcuerpos del cuerpo de descomposición sobre $\mathbb{Q}$ de $P = x^4 + 1$.

92. Hallar todos los subcuerpos propios del cuerpo de descomposición de $P = x^4 - 2$ sobre $\mathbb{Q}$.

93. Calcular cuántos subcuerpos tiene $\mathbb{Q}\big(\cos(2\pi/13)\big)$.

94. Estudiar qué automorfismos de $\mathcal{G}\big(\mathbb{Q}(e^{2\pi i/7})/\mathbb{Q}\big)$ dejan invariante $i\,\mathrm{sen}(2\pi/7)$ y utilizar el resultado para hallar $[\mathbb{Q}\big(i\,\mathrm{sen}(2\pi/7)\big) : \mathbb{Q}]$ y $[\mathbb{Q}(e^{2\pi i/7}) : \mathbb{Q}\big(i\,\mathrm{sen}(2\pi/7)\big)]$.

♡**95.** Sabiendo que $L/\mathbb{Q}$ es normal y $[L : \mathbb{Q}] = p$, hallar un grupo isomorfo a $\mathcal{G}(L/\mathbb{Q})$.

96. Si $\mathcal{G}(L/K) \cong \mathbb{Z}_{pq}$ (donde p y q son primos distintos) con L/K normal, finita y separable, ¿cuántos subcuerpos, M, hay con $K \subset M \subset L$?

97. Si $\mathcal{G}(L/\mathbb{Q}) \cong \mathbb{Z}_{p^2q}$ (donde p y q son primos distintos) con $L/\mathbb{Q}$ de Galois, probar que L tiene subcuerpos L_1, L_2, L_3 tales que $[L_1 : \mathbb{Q}] = p$, $[L_2 : \mathbb{Q}] = p^2$ y $[L_3 : \mathbb{Q}] = q$.

98. Sea K un cuerpo de característica cero, y sea E el cuerpo de descomposición de algún polinomio sobre K. Si $\mathcal{G}(E/K)$ es isomorfo a A_4, probar que E no tiene ningún subcuerpo L tal que $[E : L] = 2$.

99. Sea α una raíz de $x^4 + x^3 + 1 \in \mathbb{F}_2[x]$. Hallar β en función de α de tal forma que $\mathbb{F}_2 \subsetneqq \mathbb{F}(\beta) \subsetneqq \mathbb{F}_2(\alpha)$ y dar un polinomio en $\mathbb{F}_2[x]$ cuyo cuerpo de descomposición sea $\mathbb{F}_2(\beta)$.

100. Demostrar que si $\mathbb{Q} \subset M \subset \mathbb{Q}(e^{2\pi i/k})$, entonces $\mathcal{G}(M/\mathbb{Q})$ es abeliano. (Nota: El recíproco, para $M/\mathbb{Q}$ de Galois, es un profundo resultado llamado *teorema de Kronecker-Weber*).

101. Para cada n par hallar un polinomio $P \in \mathbb{Q}[x]$ con $\partial P = n$ y raíces distintas no racionales, tal que el grupo de Galois de su cuerpo de descomposición sea isomorfo a $\mathbb{Z}_2$.

102. Hallar una extensión normal de $\mathbb{Q}$ cuyo grupo de Galois sea $\mathbb{Z}_9$. *Indicación*: $9 = (19 - 1)/2$.

103. Sea L/K una extensión de Galois y sean M_1/K y M_2/K subextensiones de Galois. Demostrar que si M_3 es el menor subcuerpo de L que contiene a M_1 y M_2, entonces $\mathcal{G}(M_3/M_1)$ es isomorfo a $\mathcal{G}(M_2/(M_1 \cap M_2))$.

104. Sea $p = 2q + 1$ con p y q primos, hallar cuántos subcuerpos tiene $\mathbb{Q}(e^{2\pi i/p})$.

105. Sea L un cuerpo y sea G un subgrupo finito del grupo de automorfismos $\phi : L \longrightarrow L$. Sea $K = \{a \in L \ : \ \phi(a) = a, \ \forall \ \phi \in G\}$. *i*) Probar que K es un subcuerpo de L con $[L : K] = |G|$. *ii*) Probar que si L/K es simple, es de Galois. $\diamondsuit$*iii*) Probar incondicionalmente que L/K es de Galois.

106. Demostrar que $\sqrt[3]{n} \in \mathbb{Q}(e^{2\pi i/p})$ con $n \in \mathbb{Z}$ y p primo si y sólo si n es un cubo perfecto.

$\diamondsuit\diamondsuit$**107.** Sea p un primo con $p - 1$ divisible por 4. Demostrar que $\sqrt{n} \in \mathbb{Q}(e^{2\pi i/p})$ con $n \in \mathbb{Z}$ si y sólo si n o n/p son cuadrados perfectos. *Indicación*: Probar que $\sum_{n=1}^{p} e^{2\pi i n^2/p}$ genera la única subextensión de grado 2 de $\mathbb{Q}(e^{2\pi i/p})$.

108. Sea $L = \mathbb{F}_3(\sqrt[3]{x}, \sqrt[3]{y})$ y $K = \mathbb{F}_3(x, y)$. Demostrar que L/K es normal y finita, pero existen infinitos subcuerpos intermedios $K \subset M \subset L$. ¿Por qué esto no contradice el teorema fundamental de la teoría de Galois?

$\circ$**109.** Galois enunció el siguiente lema sin demostración *"Sea una ecuación cualquiera sin raíces iguales, digamos $a, b, c, \ldots$ Siempre se puede formar una función V de las raíces tal que los valores que se obtienen permutando dichas raíces de todas las formas posibles son todos desiguales. Por ejemplo se puede tomar $V = Aa + Bb + Cc + \ldots$,*

siendo $A, B, C, \ldots$ *números enteros* [no nulos] *convenientemente elegidos"*. Y después dedujo otro lema: *"La función tomada anteriormente tienen la propiedad de que todas las raíces de la ecuación propuesta se expresan racionalmente en función de* V*"*. En notación moderna esto es $a, b, c, \cdots \in K(V)$ donde K es el cuerpo generado por los coeficientes de la ecuación. Probar estos resultados (para $K \subset \mathbb{C}$). *Indicación*: El primero se cumple para números complejos arbitrarios. Para el segundo, Galois aplicó el teorema de los polinomios simétricos al producto de factores $(Ax + Bb + Cc + \cdots - V)$ permutando de todas las formas posibles $b, c, \ldots$ pero sin cambiar V.

Apéndice del Capítulo 3

Conoce a tus héroes

(Más información en: `http://turnbull.mcs.st-and.ac.uk/history/`)

Apellido: Galois
Nombre: Evariste
Nacimiento: 1811 Bourg La Reine
Defunción: 1832 París

E. Galois vivió durante los tumultuosos años de la restauración monárquica en Francia después de Napoleón. A pesar de su brevísima vida, el importante estudio que realizó sobre la resolución de ecuaciones algebraicas por medio de grupos de permutaciones ha brindado a las Matemáticas una de sus partes más bellas, conocida hoy de forma genérica en su honor como *teoría de Galois*. Sus trabajos no recibieron la merecida atención en su tiempo, y no alcanzaron difusión entre la comunidad matemática hasta más de una década tras su muerte. Esto, combinado con la juventud de Galois, su intensa actividad revolucionaria y su fallecimiento en un duelo, ha transformado a veces su biografía en una leyenda no siempre fiel a la realidad [Rot].

Bla, bla, bla

- *Sea una ecuación tal con congruencias, $F(x) = 0$, y p el módulo. Supongamos, para simplificar, que la congruencia no admite ningún factor conmensurable, esto es, que no existen funciones $\phi(x)$, $\psi(x)$, $\chi(x)$ tales que $\phi(x)\psi(x) = F(x) + p\chi(x)$. En ese caso, la congruencia no admitirá ninguna raíz entera, ni ninguna raíz inconmensurable de grado inferior. Consideremos las raíces de esta congruencia como una especie de símbolos imaginarios, ya que no se ajustan a discusiones con números enteros, símbolos cuyo empleo en los cálculos será tan útil como el del imaginario $\sqrt{-1}$ en el análisis ordinario.* E. Galois 1830.

- Teorema: *Sea una ecuación dada y a, b, c, ... sus m raíces. Hay un grupo de permutaciones de las letras a, b, c, ... que goza de las propiedades siguientes:* i) *Toda función de las raíces invariante por las sustituciones del grupo es racionalmente conocida;* ii) *Recíprocamente, toda función de las raíces determinable racionalmente es invariante por las sustituciones.* E. Galois 1831.

- *Hemos hecho grandes esfuerzos para comprender las pruebas de Galois. Su razonamiento no está ni suficientemente claro ni desarrollado para permitirnos juzgar su corrección, y no podemos hacernos una idea de él. El autor anuncia que la proposición que constituye el objetivo de esta memoria forma parte de una teoría general susceptible de muchas aplicaciones.* S.D. Poisson 1831.

- *Pide a Jacobi o a Gauss públicamente que den su opinión, no acerca de la certeza, sino de la importancia de estos teoremas. Más adelante habrá gente, espero, que encontrará provechoso descifrar todo este lío.* E. Galois 1832 (de su carta a A. Chevalier, el día antes del duelo que causó su muerte).

¿Qué hay que saberse?

Esencialmente, manejar extensiones normales, conocer el concepto de separabilidad, calcular grupos de Galois de extensiones suficientemente sencillas y, por supuesto, hay que saberse perfectamente el teorema fundamental de la teoría de Galois y cómo se aplica en diferentes ejemplos.

(PQR) Preguntón, quejoso y respondón

P- La teoría de Galois, ¿es realmente de Galois?

R- En tiempos de Galois no habían sido definidos los automorfismos, ni las extensiones de cuerpos, ni sus grados, y los grupos eran sólo de permutaciones; de modo que no podemos esperar encontrar en los trabajos de Galois algo similar a lo que contienen los libros de hoy en día titulados "Teoría de Galois".

Q- Entonces el nombre es inadecuado.

R- No, porque la idea de que la estructura del cuerpo de descomposición queda fielmente reflejado en un grupo y la utilización de ello para dar una solución final al problema de resolubilidad por radicales, son suyas.

P- El cálculo del grupo de Galois parece algo combinatorio que se reduce a comprobar unas cuantas posibilidades, ¿no es así?

R- Sólo cuando tenemos extensiones de Galois presentadas de forma muy simple. Si nos enfrentásemos al cuerpo de descomposición de $x^5 - 6x + 3$ no sabríamos cómo empezar.

P- Tendríamos que hallar explícitamente las raíces.

R- Una consecuencia de la teoría de Galois es que tal cosa es imposible con las operaciones algebraicas habituales.

Q- Entonces no hay ningún método general para hallar $\mathcal{G}(L/\mathbb{Q})$ con $L/\mathbb{Q}$ de Galois.

R- En realidad sí, pero requeriría tantas operaciones que es impracticable.

Q- Pero si en general no podemos hallar el grupo de Galois, la teoría de Galois no sirve para nada.

R- Nos dice que es lo mismo estudiar subcuerpos que subgrupos, lo cual es un descubrimiento matemático de primer orden, independientemente de lo difíciles que sean los cálculos.

P- ¿Y es posible obtener cualquier grupo finito como grupo de Galois del cuerpo de descomposición de un polinomio en $\mathbb{Q}[x]$?

R- Se cree que sí, pero nadie ha conseguido demostrarlo hasta ahora.