Álgebra III

Versión 3.0. Cursos 22/23, 23/24, 24/25 y 25/26. [1]

José Gómez Torrecillas
Departamento de Álgebra
Universidad de Granada

[1] actualización: 19 de febrero de 2026

Índice general

Capítulo 1

Extensiones de cuerpos y raíces de polinomios

Comenzaremos introduciendo las nociones fundamentales que necesitaremos para el desarrollo de esta asignatura. Para los conceptos no definidos en lo que sigue, nos remitimos a **[2]**. La bibliografía contiene también aquellos textos sobre Teoría de Galois, de entre la multitud que existen, utilizados en la preparación de estos apuntes. El desarrollo de las clases no tiene porqué coincidir literalmente con lo expuesto aquí, aunque estas notas son el documento básico relacionado con los contenidos del curso. Se recomienda, por tanto, a los estudiantes que tomen sus propias notas en clase.

1.1. Extensiones de cuerpos y elementos algebraicos

Comencemos recordando que un *cuerpo* es un anillo conmutativo K tal que su grupo de unidades es $K \setminus \{0\}$. Observemos que estamos suponiendo implícitamente que un cuerpo nunca es el anillo trivial $\{0\}$.

DEFINICIÓN 1.1. Sea F un subanillo de un cuerpo K que es, a su vez, un cuerpo. Diremos que F es un *subcuerpo* de K. Se dice también que $F \leq K$ es una *extensión* de cuerpos.

Dada cualquier extensión de cuerpos $F \leq K$, la propia multiplicación de K proporciona una estructura de F–espacio vectorial sobre K. Explícitamente, consideramos sobre K, con su suma, la acción de un escalar $\lambda \in F$ sobre un vector $\alpha \in K$ como el producto $\lambda\alpha$ realizado en K. Que estas operaciones dotan a K de una estructura de F–espacio vectorial se sigue inmediatamente de los axiomas de anillo que satisface K.

DEFINICIÓN 1.2. La dimensión de K como F–espacio vectorial se llama *grado* de K sobre F. Se suele usar la notación

$$[K : F] = \dim_F K.$$

La extensión se llama *finita* si $[K : F] < \infty$.

EJEMPLO 1.3. Se tiene que $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$. La segunda igualdad se deduce de que $\mathbb{R}$ no tiene cardinal numerable.

Dado cualquier conjunto no vacío Λ de subcuerpos de K, se comprueba fácilmente que la intersección $\bigcap_{F \in \Lambda} F$ es un subcuerpo de K.

DEFINICIÓN 1.4. Dado un subconjunto S de K, la intersección de todos los subcuerpos de K que contienen a S se llama *subcuerpo de* K *generado por* S. Se trata del menor subcuerpo de K que contiene a S. Si $S = \emptyset$, el conjunto vacío, obtenemos el menor subcuerpo de K, que se llama *subcuerpo primo* de K.

La característica de un anillo A se denotará por $\mathrm{car}(A)$. Recordemos que la característica de un anillo A es el número natural n tal que $\mathrm{Ker}\chi = n\mathbb{Z}$, para $\chi : \mathbb{Z} \to A$ el único homomorfismo de anillos que existe.

PROPOSICIÓN 1.5. *Dado un cuerpo* K*, su subcuerpo primo es isomorfo a* $\mathbb{Z}_p$ *si* $car(K) = p > 0$ *, y es isomorfo a* $\mathbb{Q}$ *si* $car(K) = 0$*.*

DEMOSTRACIÓN. Tomemos el único homomorfismo de anillos $\chi : \mathbb{Z} \to K$, determinado por la condición $\chi(1) = 1$. Se tiene que $Im\chi$ es el menor subanillo de K. Por tanto, $Im\chi$ está contenido en el subcuerpo primo P de K. Sabemos que $Ker\chi = p\mathbb{Z}$, donde $p = car(K)$.

Si $p > 0$, entonces tenemos un isomorfismo de anillos $\mathbb{Z}/p\mathbb{Z} \cong Im\chi$. Como $Im\chi$ está contenido en un cuerpo, ha de ser un dominio de integridad, luego p es un número primo. Así que $Im\chi$ es un subcuerpo de K isomorfo a $\mathbb{Z}_p$. Como $Im\chi \subseteq P$, deducimos que $Im\chi = P$.

Si $p = 0$, entonces $Im\chi \cong \mathbb{Z}$. Por tanto, el cuerpo de fracciones Q de $Im\chi$ es isomorfo a $\mathbb{Q}$. Por otra parte, como $Im\chi \subseteq P$, podemos calcular Q dentro de P. Así, $Q = P$, resultando que P es isomorfo a $\mathbb{Q}$. □

EJERCICIO 1. Demostrar que el cardinal de un cuerpo finito es de la forma p^n, donde p es un entero primo y n es un entero positivo. ¿Qué interpretación tienen p y n?

DEFINICIÓN 1.6. Sea $F \leq K$ una extensión de cuerpos y $S \subseteq K$ un mero subconjunto. Denotaremos por $F(S)$ el menor subcuerpo de K que contiene a $F \cup S$. Diremos que $F(S)$ está *generado sobre* F *por* S y que S es un *conjunto de generadores*. Cuando $S = \{\alpha_1, \ldots, \alpha_t\}$, usaremos la notación abreviada

$$F(\alpha_1, \ldots, \alpha_t) = F(\{\alpha_1, \ldots, \alpha_t\}).$$

Si $K = F(\alpha_1, \ldots, \alpha_t)$, diremos que $F \leq K$ es una extensión *finitamente generada*.

Para un anillo conmutativo A, denotaremos por $A[X]$ al anillo de polinomios en la indeterminada X con coeficientes en A. Para $f \in A[X]$, el subconjunto de $A[X]$ definido por

$$\langle f \rangle = \{gf : g \in A[X]\}$$

es un ideal de $A[X]$ llamado *ideal principal generado por* f. Recordemos que, si A es un cuerpo, entonces todo ideal de $A[X]$ es principal.

DEFINICIÓN 1.7. Para $f \in K[X]$ y una extensión de cuerpos $K \leq E$ tal que f se descompone como producto de polinomios lineales[1] en $E[X]$, y $E = K(\alpha_1, \ldots, \alpha_t)$ para $\alpha_1, \ldots, \alpha_t \in E$ las raíces de f, diremos que E es un *cuerpo de escisión o descomposición* de f. Este cuerpo depende del cuerpo K donde consideramos los coeficientes de f. A veces se enfatiza este hecho hablando del cuerpo de descomposición de f *sobre* K. Observemos que hemos usado el artículo indeterminado «un». Más tarde, daremos una noción más general de cuerpo de descomposición y una formulación de su existencia y unicidad.

OBSERVACIÓN 1.8. Si $f \in \mathbb{Q}[X]$, la existencia de un cuerpo de descomposición para f se deduce fácilmente del Teorema Fundamental del Álgebra[2]: basta con tomar todas las raíces complejas $\alpha_1, \ldots, \alpha_t \in \mathbb{C}$ de f y el subcuerpo $\mathbb{Q}(\alpha_1, \ldots, \alpha_t)$ de $\mathbb{C}$ es un cuerpo de descomposición de f.

EJEMPLO 1.9. Un cuerpo de descomposición de $f = X^2 - 2 \in \mathbb{Q}[X]$ es

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

[1] Por «lineales», entendemos de grado 1.

[2] Ver Sección 3.3 para una demostración en el contexto de este curso, que no necesita variable compleja.

EJERCICIO 2. Dada una extensión de cuerpos $F \leq K$ y subconjuntos $S, T \subseteq K$, razonar que $F(S \cup T) = F(S)(T)$.

EJEMPLO 1.10. Tomemos $f = X^3 - 2 \in \mathbb{Q}[X]$. Las raíces complejas de f son $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$, donde $\omega = e^{i2\pi/3} \in \mathbb{C}$. Un cuerpo de descomposición de f es $\mathbb{Q}(\sqrt[3]{2}, \omega)$.

EJEMPLO 1.11. El polinomio $f = X^n - 1 \in \mathbb{Q}[X]$, para $n \geq 1$, tiene todas sus raíces complejas simples, ya que ninguna es común con la única raíz de $f' = nX^{n-1}$. Estas son las llamadas raíces n–ésimas complejas de la unidad. Forman un grupo cíclico bajo el producto; un generador de dicho grupo es $e^{i2\pi/n} = \cos 2\pi/n + i \sin 2\pi/n$. Los generadores de este grupo se llaman *raíces n–ésimas primitivas complejas de la unidad*. Si ω es una cualquiera de ellas, entonces un cuerpo de descomposición de $X^n - 1$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\omega)$.

Los números complejos que aparecen en los ejemplos anteriores son algebraicos sobre $\mathbb{Q}$, en el sentido de la siguiente definición.

DEFINICIÓN 1.12. Sea $F \leq K$ una extensión de cuerpos. Diremos que un elemento $\alpha \in K$ es *algebraico sobre* F si es raíz de algún polinomio no constante de $F[X]$. En caso contrario, diremos que α es *trascendente* sobre F.

La siguiente proposición enuncia varios hechos fundamentales para el desarrollo posterior.

PROPOSICIÓN 1.13. *Sea $F \leq K$ una extensión de cuerpos y $\alpha \in K$ algebraico sobre F. Existe un único polinomio mónico irreducible $f \in F[X]$ tal que $f(\alpha) = 0$. Además, se tiene un isomorfismo de cuerpos*[3] *$F(\alpha) \cong F[X]/\langle f \rangle$ y que $\{1, \alpha, \ldots, \alpha^{\deg f - 1}\}$ es una base de $F(\alpha)$ como F–espacio vectorial. Por tanto, $[F(\alpha) : F] = \deg f$.*

DEMOSTRACIÓN. La aplicación $e_\alpha : F[X] \to K$ definida por $e_\alpha(g) = g(\alpha)$, para $g \in F[X]$, es un homomorfismo de anillos. Su núcleo es, por tanto, un ideal de $F[X]$, que es no nulo ya que α es algebraico sobre F. Sea $f \in F[X]$ el generador mónico de $\operatorname{Ker} e_\alpha$ que sabemos es el polinomio mónico de grado mínimo contenido en $\operatorname{Ker} e_\alpha$. Veamos que f es, precisamente, el descrito en el enunciado. Que f es irreducible se deduce del primer teorema del isomorfismo, ya que éste da un isomorfismo de anillos

$$\frac{F[X]}{\langle f \rangle} \cong \operatorname{Im} e_\alpha, \qquad (g + \langle f \rangle \mapsto g(\alpha)). \tag{1.1}$$

En efecto, puesto que $\operatorname{Im} e_\alpha$ es un subanillo del cuerpo K, deducimos que es un dominio de integridad, por lo que $F[X]/\langle f \rangle$ lo es también. Dado que $F[X]$ es un dominio de ideales principales, deducimos que f es irreducible y que $F[X]/\langle f \rangle$ es un cuerpo (ver, por ejemplo, [**2**, Teorema 3.45]).

Si h es irreducible y mónico y $h(\alpha) = 0$, entonces $\langle h \rangle \subseteq \langle f \rangle$ y, como el primero de estos ideales es maximal, deducimos que $f = h$, puesto que ambos polinomios son generadores mónicos del mismo ideal de $F[X]$.

Observemos que $\operatorname{Im} e_\alpha \subseteq F(\alpha)$. Puesto que $\operatorname{Im} e_\alpha$ es un cuerpo y contiene a α, deducimos que $\operatorname{Im} e_\alpha = F(\alpha)$. Por último, observemos que una base como F–espacio vectorial de $F[X]/\langle f \rangle$ es

$$\{X^i + \langle f \rangle : i < \deg f\}.$$

[3] Un isomorfismo de cuerpos es un isomorfismo de anillos entre dos cuerpos

El isomorfismo (1.1), que también es F–lineal, lleva esta base en la consignada en el enunciado. □

DEFINICIÓN 1.14. El polinomio f cuya existencia se prueba en la Proposición 1.13 se llama *polinomio mínimo (o polinomio irreducible) de α sobre F*, que denotaremos por $\mathrm{Irr}(\alpha, F)$. Al grado de $\mathrm{Irr}(\alpha, F)$ lo llamaremos también *grado de α sobre F*.

OBSERVACIÓN 1.15. Se sigue de la demostración del la Proposición 1.13 que el polinomio irreducible de un elemento algebraico α sobre F es el polinomio mónico de grado mínimo entre los de $F[X]$ que tienen a α como raíz. Además, cualquier otro polinomio en $F[X]$ que tenga a α como raíz, ha de ser un múltiplo de $\mathrm{Irr}(\alpha, F)$.

EJERCICIO 3. Calcular $\mathrm{Irr}(\omega, \mathbb{Q}(\sqrt[3]{2}))$, para $\omega = e^{i2\pi/3}$.

EJERCICIO 4. Sea p un número primo y $\omega \neq 1$ una raíz p–ésima compleja de la unidad. Calcular $\mathrm{Irr}(\omega, \mathbb{Q})$.

1.2. Extensiones finitas y extensiones algebraicas

Comenzamos con una herramienta básica para trabajar con extensiones finitas.

LEMA 1.16 (De la torre). *Sean $F \leq K \leq L$ extensiones de cuerpos. Entonces $F \leq L$ es finita si, y sólo si, $F \leq K$ y $K \leq L$ son finitas. En tal caso,*

$$[L : F] = [L : K][K : F].$$

DEMOSTRACIÓN. Supongamos que $F \leq L$ es finita. Claramente, K es un F–subespacio vectorial de L, así que $[K : F] \leq [L : F]$ y $F \leq K$ resulta finita. Por otra parte, cualquier sistema de generadores finito de L como F–espacio vectorial también lo es como K–espacio vectorial, luego $K \leq L$ es finita.

Supongamos ahora que $[L : K] = n$, $[K : F] = m$ son finitas, y tomemos bases $\{u_1, \ldots, u_n\}$ de L sobre K y $\{v_1, \ldots, v_m\}$ de K sobre F. Una comprobación rutinaria demuestra que $\{u_i v_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ es una base de L como F–espacio vectorial. □

OBSERVACIÓN 1.17. El nombre que hemos puesto al Lema 1.16, y que nos será útil para agilizar su mención, proviene de que, cuando se tienen varias extensiones de cuerpos de la forma $F_1 \leq \cdots \leq F_n$, se suele decir que tenemos una *torre de cuerpos*.

EJEMPLO 1.18. Observemos que tenemos las extensiones de cuerpos

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{Q}(\sqrt[3]{2}, \omega),$$

para ω una raíz compleja cúbica primitiva de la unidad. Como $\sqrt[3]{2}$ es raíz de $X^3 - 2$ y este polinomio es irreducible en $\mathbb{Q}[X]$, tenemos que se trata del polinomio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}$. Por la Proposición 1.13, una $\mathbb{Q}$–base de $\mathbb{Q}(\sqrt[3]{2})$ es $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. Por otra parte, ω es raíz del polinomio $X^2 + X + 1$, que es irreducible sobre $\mathbb{Q}(\sqrt[3]{2})$, ya que sus raíces, $\omega, \overline{\omega}$, no son números reales y, por tanto, no están en ese subcuerpo. El Lema de la torrre implica que

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6.$$

De hecho, una $\mathbb{Q}$–base de $\mathbb{Q}(\sqrt[3]{2}, \omega)$ es

$$\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \omega\sqrt[3]{2}, \omega\sqrt[3]{4}\}.$$

EJEMPLO 1.19. Vamos a usar lo aprendido hasta ahora para calcular $\mathrm{Irr}(\sqrt{5}+\sqrt{-2},\mathbb{Q})$. Llamamos $\alpha = \sqrt{5}+\sqrt{-2}$. Vamos a calcular el grado del anterior polinomio, para lo que observamos que $\mathbb{Q}(\alpha) \leq \mathbb{Q}(\sqrt{5},\sqrt{-2})$, y queremos demostrar que estos cuerpos son iguales.

Puesto que $\alpha - \sqrt{-2} = \sqrt{5}$, elevando al cuadrado, obtenemos que

$$\alpha^2 - 2\sqrt{-2}\alpha - 2 = 5,$$

de donde

$$\sqrt{-2} = \frac{\alpha^2 - 7}{2\alpha}. \tag{1.2}$$

De modo que $\sqrt{-2} \in \mathbb{Q}(\alpha)$. Procediendo de manera análoga, obtenemos que

$$\sqrt{5} = \frac{\alpha^2 + 7}{2\alpha} \in \mathbb{Q}(\alpha).$$

Deducimos, pues, que $\mathbb{Q}(\sqrt{5},\sqrt{-2}) = \mathbb{Q}(\alpha)$. Usando el Lema 1.16 y la Proposición 1.13, obtenamos

$$\deg(\mathrm{Irr}(\alpha,\mathbb{Q})) = [\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\sqrt{5},\sqrt{-2}):\mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}):\mathbb{Q}] = 2\times 2 = 4.$$

Razonemos los valores asignados a la derecha: $[\mathbb{Q}(\sqrt{5}):\mathbb{Q}] = 2$, puesto que $\sqrt{5}$ es raíz del polinomio $X^2 - 5 \in \mathbb{Q}[X]$, que es irreducible por el criterio de Eisenstein, así que $\mathrm{Irr}(\sqrt{5},\mathbb{Q}) = X^2 - 5$. Por otra parte, $\sqrt{-2}$ es raíz del polinomio $X^2 + 2 \in \mathbb{Q}(\sqrt{5})[X]$, que es irreducible ya que sus raíces no son reales y no pueden pertenecer al subcuerpo $\mathbb{Q}(\sqrt{5})$ de $\mathbb{R}$. Por tanto, $\mathrm{Irr}(\sqrt{-2},\mathbb{Q}(\sqrt{5})) = X^2 + 2$, lo que implica que $[\mathbb{Q}(\sqrt{5},\sqrt{-2}):\mathbb{Q}(\sqrt{5})] = 2$.

Para concluir, elevando en (1.2) al cuadrado y operando, obtenemos que α es raíz del polinomio $f(X) = X^4 - 6X^2 + 49 \in \mathbb{Q}[X]$. Por tanto, $f(X)$ es un múltiplo de $\mathrm{Irr}(\alpha,\mathbb{Q})$ y, como ambos tienen grado 4, deducimos que $\mathrm{Irr}(\alpha,\mathbb{Q}) = f(X)$.

PROPOSICIÓN 1.20. *Dada una extensión de cuerpos $F \leq K$ y $\alpha \in K$, se tiene que α es algebraico sobre F si, y sólo si, existe una sub-extensión $F \leq L \leq K$ tal que $F \leq L$ es finita y $\alpha \in L$.*

DEMOSTRACIÓN. Si α es algebraico sobre F, tomamos $L = F(\alpha)$ y aplicamos la Proposición 1.13.

Recíprocamente, sea L como en el enunciado. Como $F(\alpha) \leq L$, deducimos del Lema 1.16 que $F(\alpha)$ es un F–espacio vectorial de dimensión finita. Por tanto, existe un natural $n \geq 1$ tal que α^n depende linealmente sobre F de $1,\alpha,\ldots,\alpha^{n-1}$. Los coeficientes en F que expresan α^n como combinación lineal de la potencias inferiores de α dan un polinomio no nulo en $F[X]$ que tiene por raíz a α. □

DEFINICIÓN 1.21. Una extensión $F \leq K$ se dice *algebraica* si todo elemento de K es algebraico sobre F.

Las extensiones finitas son algebraicas; es más, se tiene el siguiente resultado.

TEOREMA 1.22. *Una extensión $F \leq K$ es finita si, y sólo si, es algebraica y finitamente generada.*

DEMOSTRACIÓN. Si $F \leq K$ es finita y $\alpha \in K$ entonces, por la Proposición 1.20, α es algebraico sobre F. Así que la extensión es algebraica. Además, $K = F(u_1,\ldots,u_t)$ para cualquier F–base $\{u_1,\ldots,u_t\}$ de K.

Recíprocamente, supongamos que $K = F(\alpha_1, \ldots, \alpha_n)$ y que es algebraica. Entonces cada α_i es algebraico sobre F. Tenemos la sucesión de extensiones finitas $F \leq F(\alpha_1) \leq F(\alpha_1, \alpha_2) \leq \cdots \leq F(\alpha_1, \ldots, \alpha_n) = K$. Aplicando reiteradamente el Lema de la torre, obtenemos que $F \leq K$ es finita. □

OBSERVACIÓN 1.23. La demostración del Teorema 1.22 muestra que, si $K = F(\alpha_1, \ldots, \alpha_n)$ para $\alpha_1, \ldots, \alpha_n$ algebraicos sobre F, entonces la extensión $F \leq K$ es finita.

COROLARIO 1.24. *Dada una extensión $F \leq K$, el conjunto Λ de los elementos de K que son algebraicos sobre F es un subcuerpo de K. Obviamente, la extensión $F \leq \Lambda$ es algebraica.*

DEMOSTRACIÓN. Si $\alpha, \beta \in K$ son algebraicos sobre F, entonces $\alpha + \beta, \alpha\beta \in F(\alpha, \beta)$. Como la extensión $F \leq F(\alpha, \beta)$ es finita, según se observa en 1.23, deducimos del Teorema 1.22 que es algebraica, así que $\alpha + \beta, \alpha\beta$ son algebraicos sobre F. Luego Λ es un subanillo de K. Por último, si $\alpha \neq 0$, entonces $\alpha^{-1} \in F(\alpha)$, por lo que resulta ser algebraico sobre F. Así que Λ es un subcuerpo de K. □

DEFINICIÓN 1.25. El subcuerpo Λ de K descrito en el Corolario 1.24 se llama *clausura algebraica de F en K*.

EJEMPLO 1.26. La clausura algebraica $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ en $\mathbb{C}$ se llama *cuerpo de los números algebraicos*. Nótese que la extensión $\mathbb{Q} \leq \overline{\mathbb{Q}}$ es algebraica pero no finita, ya que contiene elementos cualquier grado, por ejemplo, $\sqrt[n]{2}$ para cualquier natural $n \geq 2$.

EJERCICIO 5. Calcular $\mathrm{Irr}(\sqrt{2} + i, \mathbb{Q})$.

EJERCICIO 6. Calcular $\mathrm{Irr}(\sqrt{2} + i\sqrt{3}, \mathbb{Q})$.

EJERCICIO 7. Calcular un cuerpo de descomposición de $X^4 + 16 \in \mathbb{Q}[X]$ y su grado sobre $\mathbb{Q}$.

EJERCICIO 8. Calcular $\mathrm{Irr}(\sqrt{2} + \sqrt[3]{2}, \mathbb{Q})$.

EJERCICIO 9. Calcular $f(X) = \mathrm{Irr}(1 + \sqrt[3]{2}, \mathbb{Q})$. Calcular las raíces complejas de $f(X)$ y un cuerpo de descomposición suyo.

1.3. Construcciones con regla y compás, I

En lo que sigue, consideraremos algunas construcciones geométricas en el plano afín euclidiano que veremos están relacionadas con ciertas extensiones de cuerpos.

Para un conjunto $\mathcal{S}$ de puntos del plano, con, al menos, dos puntos, consideremos Γ el conjunto cuyos elementos son las rectas determinadas por pares de puntos de $\mathcal{S}$ junto con las circunferencias con centros en $\mathcal{S}$ y radio determinado por este centro y cualquier otro punto de $\mathcal{S}$. Llamemos $\mathcal{S}^c$ a los puntos obtenidos al intersecarse todo par de elementos de Γ. Es claro que $\mathcal{S} \subseteq \mathcal{S}^c$.

DEFINICIÓN 1.27. Dado un conjunto de puntos $\mathcal{S}$ del plano euclidiano, definimos recursivamente la sucesión de subconjuntos $\mathcal{S}_n$ del plano como sigue: $\mathcal{S}_0 = \mathcal{S}$, $\mathcal{S}_{n+1} = \mathcal{S}_n^c$, para $n \in \mathbb{N}$. El conjunto de los *puntos construibles* (con regla y compás) a partir de $\mathcal{S}$ es

$$C(\mathcal{S}) = \bigcup_{n \in \mathbb{N}} \mathcal{S}_n \tag{1.3}$$

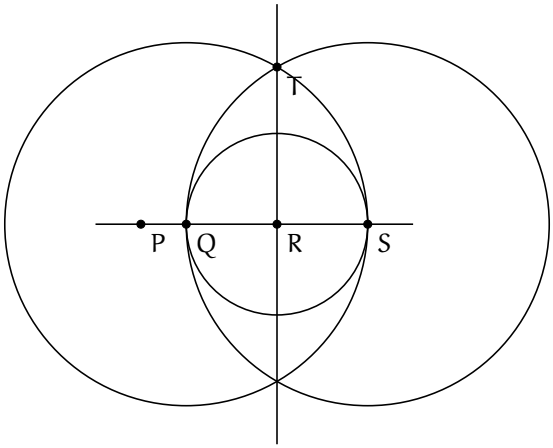


FIGURA 1. Recta perpendicular, caso 1

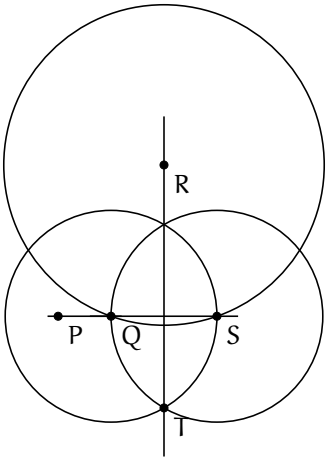


FIGURA 2. Recta perpendicular, caso 2

LEMA 1.28. *Dados tres puntos* P, Q, R *del plano, con* P, Q *distintos, se puede construir con regla y compás a partir de ellos un punto* T *tal que la rectas* PQ *y* RT *son perpendiculares.*

DEMOSTRACIÓN. Distinguimos dos casos, según R esté en la recta PQ o no.

Para el primer caso (ver Figura 1), trazamos la recta PQ y la circunferencia con centro R que pasa por Q. En caso de ser $R = Q$, usaríamos la misma construcción con P en el papel de Q. Esta circunferencia corta a la recta PQ en otro punto S. Ahora, trazamos dos circunferencias, una con centro Q pasando por S y otra con centro S y conteniendo al punto Q. Tomemos un punto T de intersección de ambas, que será, claro, equidistante de Q y S. Así, el triángulo QST es equilátero. Lo que implica que la recta RT es perpendicular a la recta PQ.

Para el segundo caso, se sigue un procedimiento similar, ilustrado por la Figura 2.

□

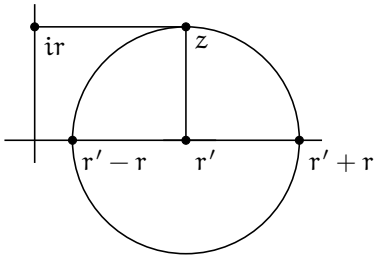


FIGURA 3. Suma de números reales

EJERCICIO 10. Construir, a partir de tres puntos no colineales, usando regla y compás, el cuarto punto que completa un paralelogramo.

EJERCICIO 11. Dados dos puntos que determinan una recta r y un punto A no contenido en ella, construir, usando regla y compás, el simétrico de A con respecto de r.

Seguidamente, vamos a ver los puntos construibles como números complejos. Para ello, elijamos dos puntos en $\mathcal{S}$. Podemos tomar un sistema de referencia para el cual las coordenadas de estos puntos son $(0,0)$ y $(1,0)$. Además, cada punto del plano con coordenadas (x,y) puede verse como el número complejo $x+iy$. De esta forma, el conjunto $C(\mathcal{S})$ de los puntos construibles a partir de $\mathcal{S}$ es un subconjunto de $\mathbb{C}$. Con esta perspectiva, lo que estamos suponiendo es que $\mathcal{S}$ contiene a los números 0 y 1.

LEMA 1.29. *Dado $z = x+iy \in \mathbb{C}$ se tiene que $z \in C(\mathcal{S})$ si, y sólo si, $x, y \in C(\mathcal{S})$.*

DEMOSTRACIÓN. Observemos que $i \in C(\mathcal{S})$, ya que podemos trazar la recta que pasa por 0 perpendicular a la recta real determinada por $0,1$ y obtener i como intersección de esta recta con la circunferencia de centro 0 que pasa por 1. Con argumentos similares, es fácil deducir que si $r \in \mathbb{R}$, entonces $r \in C(\mathcal{S})$ si, y sólo si, $ri \in C(\mathcal{S})$.

Bien, si $x+iy \in C(\mathcal{S})$, entonces obtenemos x, iy como proyecciones ortogonales sobre el eje real y el eje imaginario. Por tanto, $x, y \in C(\mathcal{S})$. Recíprocamente, si $x, y \in C(\mathcal{S})$, entonces podemos obtener $x+iy$ como la intersección de la recta perpendicular al eje imaginario que pasa por iy y la perpendicular al eje real que pasa por x. □

PROPOSICIÓN 1.30. *El conjunto $C(\mathcal{S})$ es un subcuerpo de $\mathbb{C}$. Además, si $z \in C(\mathcal{S})$, entonces $\overline{z} \in C(\mathcal{S})$.*

DEMOSTRACIÓN. En virtud del Lema 1.29, y de la expresión de las operaciones suma, producto e inversión de números complejos en función de sus componentes real e imaginaria, basta, para la primera afirmación, que demostremos que $C(\mathcal{S}) \cap \mathbb{R}$ es un subcuerpo de $\mathbb{R}$.

Vayamos con la suma y el producto: dados $r, r' \in C(\mathcal{S}) \cap \mathbb{R}$, podemos suponer que los dos son positivos, ya que, en otro caso, sabemos que tomar opuestos es un proceso construible. Bien, tenemos que $z = r' + ir \in C(\mathcal{S})$. Los puntos de corte de la circunferencia con centro r' que pasa por z con el eje real son los números $r'-r, r'+r$ (ver Figura 3).

Para el producto rr', supongamos que $r, r' > 0$, ya que el resto de los casos se deduce de éste teniendo en cuenta, de nuevo, que si $x \in C(\mathcal{S}) \cap \mathbb{R}$, entonces $-x \in C(\mathcal{S}) \cap \mathbb{R}$. Bien, trazamos la recta paralela a la determinada por $1, ir$ que pasa por r' y tomamos iy su corte con el eje imaginario. Los

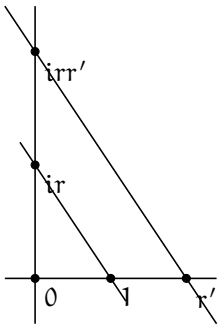


FIGURA 4. Producto de números reales

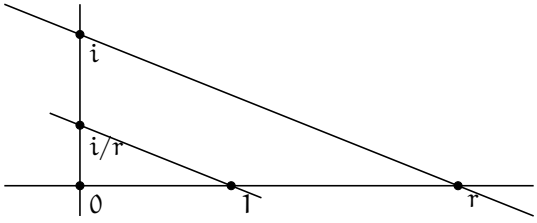


FIGURA 5. Inversión de números reales

triángulos de vértices $0, 1, ir$ y $0, r', iy$ son semejantes, lo que implica que $y = rr'$ y, por tanto, $rr' \in C(\mathcal{S})$ (ver Figura 4).

Por último, para ver que el inverso de un número real no nulo r puede construirse con regla y compás, trazamos la recta paralela a la determinada por r, i que pasa por 1. Su corte, de nuevo por semejanza de triángulos, con el eje imaginario es $r^{-1}i$, lo que prueba que $r^{-1} \in C(\mathcal{S})$ (ver Figura 5).

La segunda afirmación se deduce del hecho de que tomar el conjugado de un número complejo consiste en tomar el opuesto de su parte imaginaria. □

LEMA 1.31. *Si* $z \in C(S)$, *entonces* $\sqrt{z} \in C(S)$.

DEMOSTRACIÓN. Demostremos primero que, si $r \in C(\mathcal{S})$ es real y positivo, entonces $\sqrt{r} \in C(\mathcal{S})$. Para ello (ver Figura 6), construimos la circunferencia con centro $m = (1 + r)/2$ que pasa por 0. Trazamos la recta perpendicular al eje real que pasa por 1 y la intersectamos con la citada circunferencia en un punto $w = 1 + xi$ para cierto $x \in C(\mathcal{S})$ positivo. Resulta que los triángulos $0, 1, w$ y $1, w, 1 + r$ son semejantes, lo que implica que $x/1 = r/x$, de donde $x^2 = r$.

De esta forma, escribiendo cualquier número complejo en forma polar, vemos que la extracción de una raíz cuadrada suya se reduce a la extracción de la de su módulo, que acabamos de ver que es un proceso construible, y la de un número de módulo 1. Tomemos, pues, $z = e^{i\theta} \in C(\mathcal{S})$. El número $z + 1 \in C(\mathcal{S})$ es entonces de la forma $re^{i\theta/2}$ para $r = |z + 1|$ (usar la regla del paralelogramo para sumar z y 1). Cortando la recta que une 0 y $z + 1$ con la circunferencia obtenemos $s = e^{i\theta/2} \in C(\mathcal{S})$, que es una raíz cuadrada de z (ver Figura 7).

□

EJERCICIO 12. Sea F un subcuerpo de $\mathbb{R}$. Los puntos $(x, y) \in F \times F$ se llaman F–puntos del plano. Una F–recta es aquella determinada por dos

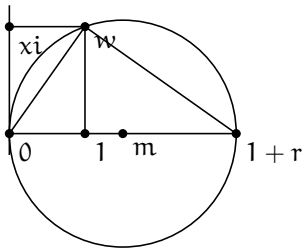


FIGURA 6. Extracción de raíces cuadradas de números reales positivos

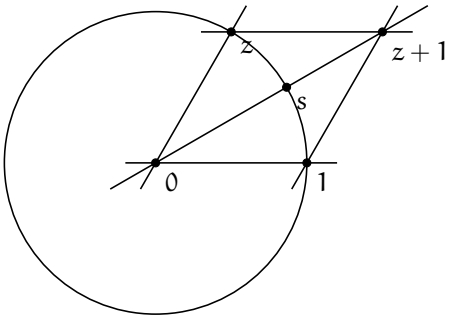


FIGURA 7. Construcción de la raíz cuadrada $s = \sqrt{z}$, con $|z| = 1$.

F–puntos. Demostrar que la intersección de dos F–rectas, de ser no vacía, es un F–punto.

EJERCICIO 13. Con la notación del Ejercicio 12. Una F–circunferencia es aquella que tiene como centro un F–punto y pasa por otro F–punto. Demostrar que la intersección de una F–recta y una F–circunferencia, de ser no vacía, consiste en uno o dos $F(\sqrt{c})$–puntos para cierto $c \in F$ positivo. Deducir que dos F–circunferencias se intersecan, de hacerlo, en $F(\sqrt{c})$–puntos, para $c \in F$ positivo adecuado.

TEOREMA 1.32. *El menor subcuerpo de* $\mathbb{C}$ *cerrado para conjugación y extracción de raíces cuadradas que contiene a* $\mathcal{S}$ *es* $C(\mathcal{S})$.

DEMOSTRACIÓN. Ya sabemos que $C(\mathcal{S})$ es un subcuerpo de $\mathbb{C}$ que contiene a $\mathcal{S}$ y es cerrado por conjugación y raíces cuadradas. Tomemos otro subcuerpo C' con las mismas propiedades, y demostremos que $C(\mathcal{S}) \subseteq C'$. En vista de (1.3), basta con que demostremos que $\mathcal{S}_n \subseteq C'$ para todo $n \in \mathbb{N}$. Obviamente, $\mathcal{S}_0 = \mathcal{S} \subseteq C'$. Supongamos $\mathcal{S}_n \subseteq C'$ para algún $n \in \mathbb{N}$, para razonar por inducción. Dado $z \in \mathcal{S}_{n+1}$, tenemos que $z \in X \cap Y$ para X, Y rectas o circunferencias trazadas a partir de puntos de $\mathcal{S}_n$ y, por tanto, de puntos de C'. Como C' es cerrado por conjugación, estos puntos tienen coordenadas en $F = C' \cap \mathbb{R}$, así que son F-puntos. Por tanto, X, Y son F–rectas o F–circunferencias, lo que implica que las componentes de z pertenecen a $F(\sqrt{c})$ para algún $c \in F$. Así, $z \in C'$, ya que este último es un subcuerpo cerrado para raíces cuadradas. □

DEFINICIÓN 1.33. Sea $F \leq K$ una extensión de cuerpos. Diremos que K una *torre por raíces cuadradas sobre* F si $K = F(u_1, \ldots, u_t)$ donde $u_1^2 \in F$ y $u_{i+1}^2 \in F(u_1, \ldots, u_i)$ para cada $i = 1, \ldots, t-1$.

Para un subconjunto $\mathcal{S}$ de $\mathbb{C}$, definimos $\overline{\mathcal{S}} = \{\overline{z} : z \in \mathcal{S}\}$.

TEOREMA 1.34. *Sea $\mathcal{S} \subseteq \mathbb{C}$ y $F = \mathbb{Q}(\mathcal{S} \cup \overline{\mathcal{S}})$. Denotemos por $\mathcal{T}$ el conjunto de todas las torres por raíces cuadradas sobre F contenidas en $\mathbb{C}$. Entonces*

$$C(\mathcal{S}) = \bigcup_{K \in \mathcal{T}} K.$$

DEMOSTRACIÓN. Sea $L = \bigcup_{K \in \mathcal{T}} K$. Observemos que L es un subcuerpo de $\mathbb{C}$: si $\alpha, \beta \in L$, no nulos, entonces existen sendas torres por raíces cuadradas K y E sobre F tales que $\alpha \in K$, $\beta \in E$. Ahora es fácil comprobar que el menor subcuerpo M de $\mathbb{C}$ que contiene a K y a E es también una torre por raíces cuadradas sobre F. Obviamente, $\alpha - \beta, \alpha\beta^{-1} \in M \leq L$, lo que prueba que L es un subcuerpo de $\mathbb{C}$.

Puesto que $F \leq C(\mathcal{S})$, se deduce del Lema 1.31 que $L \leq C(\mathcal{S})$. Además, si z pertenece a una torre $F(u_1, \ldots, u_t) \in \mathcal{T}$, entonces $\overline{z} \in F(\overline{u_1}, \ldots, \overline{u_t})$, ya que F es cerrado por conjugación. Como $F(\overline{u_1}, \ldots, \overline{u_t})$ es otra torre por raíces cuadradas sobre F, deducimos que L es cerrado por conjugación. Obviamente, L es también cerrado por raíces cuadradas, lo que implica, por el Teorema 1.32, que $C(\mathcal{S}) \leq L$. Por tanto, $L = C(\mathcal{S})$. □

COROLARIO 1.35. *El cuerpo $C(\mathcal{S})$ es una extensión algebraica de F. De hecho, todo número en $C(\mathcal{S})$ tiene como grado sobre F una potencia de 2.*

DEMOSTRACIÓN. Si $\alpha \in C(\mathcal{S})$ entonces, por el Teorema 1.34, existe una torre por raíces cuadradas K sobre F tal que $\alpha \in K$. Como $F(\alpha) \leq K$, deducimos del Lema de la Torre que la extensión $F \leq F(\alpha)$ es finita y $[F(\alpha) : F]$ es un divisor de $[K : F]$. Puesto que este último número es una potencia de 2, deducimos que así lo es el grado de α sobre F. □

DEFINICIÓN 1.36. Un número complejo z se dice *construible* si lo es a partir de $\{0, 1\}$.

COROLARIO 1.37. *Todo número construible es algebraico con grado sobre $\mathbb{Q}$ una potencia de 2.*

OBSERVACIÓN 1.38. Veremos más adelante que la afirmación recíproca a la del Corolario 1.37 no es cierta. Concretamente, hay números de grado 4 sobre $\mathbb{Q}$ que no son construibles (ver Ejemplo 4.21).

EJEMPLO 1.39. Consideremos la circunferencia de radio 1 centrada en 0. Si el lado ℓ de un cuadrado de área igual a la del círculo delimitado por la circunferencia fuera construible, entonces $\ell^2 = \pi$. Eso implica que π es construible y, por el Corolario 1.37, algebraico. Lo que contradice el Teorema de Lindemann-Weierstrass.

EJEMPLO 1.40. Un ángulo de 60^o está determinado por los segmentos del plano complejo con extremos $0, 1$ y $0, e^{i\pi/3} = \cos \pi/3 + i \sin \pi/3$. Vamos a analizar si este ángulo se puede trisecar con regla y compás. Esto es equivalente a construir el número complejo $e^{i\pi/9} = \cos \pi/9 + i \sin \pi/9$ a partir de $e^{i\pi/3} = 1/2 + i\sqrt{3}/2$. Como éste es un número construible, en caso de que la respuesta fuese positiva, tendríamos que $\cos \pi/9$ sería construible. De acuerdo con el Corolario 1.37, esto implicaría que el grado de $\cos \pi/9$ sobre $\mathbb{Q}$ sería una potencia de 2. Calculemos este grado encontrando el polinomio mínimo de $\cos \pi/9$ sobre $\mathbb{Q}$.

De la relación general $\cos 3\alpha = 4 \cos^3 \alpha - 3 \cos \alpha$, evaluada en $\alpha = \pi/9$, obtenemos que

$$\frac{1}{2} = 4 \cos^3 \pi/9 - 3 \cos \pi/9.$$

Deducimos que $\cos \pi/9$ es raíz del polinomio $f = 8X^3 - 6X - 1$. Este polinomio de grado 3 será irreducible sobre $\mathbb{Q}$ si, y sólo si, no tiene raíces en $\mathbb{Q}$. Si r es una raíz racional de f, entonces $2r$ es raíz racional de $X^3 - 3X - 1$. Pero las únicas dos posibles raíces racionales (± 1) de este último polinomio no lo son, así que $2r$ no puede ser raíz suya y, por tanto, r no puede existir como raíz racional de f. Luego $f \in \mathbb{Q}[X]$ es irreducible, y así lo es $f/8$. Por la Proposición 1.13, $f/8$ es el polinomio mínimo de $\cos \pi/9$ sobre $\mathbb{Q}$ de donde este número tiene grado 3 sobre $\mathbb{Q}$. Por tanto, no es construible y deducimos que el ángulo de 20^o no se puede construir con regla y compás a partir del ángulo de 60^o y, de hecho, no es construible.

1.4. Ejercicios

EJERCICIO 14. Sea $F \leq K$ una extensión de cuerpos y $\alpha \in K$ de grado 2 sobre F. Demostrar que $F(\alpha)$ es un cuerpo de descomposición de $\mathrm{Irr}(\alpha, F)$.

EJERCICIO 15. Sea $F \leq K$ una extensión de cuerpos de grado 2. Mostrar que, si la característica de F es distinta de dos, existe $\beta \in K$ tal que $\beta^2 \in F$ y $K = F(\beta)$.

EJERCICIO 16. Calcular $\mathrm{Irr}(\omega, \mathbb{Q}(\sqrt[3]{2}))$, para $\omega = e^{i2\pi/3}$.

EJERCICIO 17. Razonar cuáles de los siguientes números complejos son algebraicos sobre $\mathbb{Q}$, suponiendo conocido que e y π son trascendentes:

$$\sqrt[5]{4}, (1 + \sqrt[5]{4})(1 - \sqrt[5]{16})^{-1}, \pi^2, e^2 - i, i\sqrt{i} + \sqrt{2}, \sqrt{1 - \sqrt[3]{2}}, \sqrt{\pi}, \sqrt{2}(\sqrt[3]{2} + \sqrt[5]{2})^{-1}.$$

EJERCICIO 18. Sea $F \leq K$ una extensión de cuerpos, $\alpha \in K$ y n natural no nulo. Demostrar que α es algebraico sobre F si, y sólo si, α^n es algebraico sobre F.

EJERCICIO 19. Sea $F \leq K$ una extensión de cuerpos, $\alpha \in K$ y $\beta = 1 + \alpha^2 + \alpha^5$. Demostrar que α es algebraico sobre F si, y sólo si, β es algebraico sobre F.

EJERCICIO 20. Calcular $\mathrm{Irr}(\alpha, \mathbb{Q})$ para los siguientes valores de α:

$$3 + \sqrt{2}, \sqrt{3} - \sqrt[4]{3}, \sqrt[3]{2} + \sqrt[3]{4}, \sqrt{\frac{3 + \sqrt{5}}{2}}.$$

EJERCICIO 21. Calcular $[E : \mathbb{Q}]$ y una base de E sobre $\mathbb{Q}$ en los siguientes casos:

$$E = \mathbb{Q}(\sqrt{6}, i), E = \mathbb{Q}(\sqrt[3]{5}, \sqrt{-2}), E = \mathbb{Q}(\sqrt{18}, \sqrt[4]{2}).$$

EJERCICIO 22. Sea $\alpha \in \mathbb{C}$ una raíz del polinomio $X^3 + 3X + 1$. Describir una base de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$ y calcular las coordenadas racionales con respecto de la misma de $(1 + \alpha)(1 + \alpha + \alpha^2)^{-1}$.

EJERCICIO 23. Sea $\eta = e^{i2\pi/5} \in \mathbb{C}$. Calcular $\mathrm{Irr}(\eta + \overline{\eta}, \mathbb{Q})$. Deducir que η es construible con regla y compás[4].

EJERCICIO 24. Dar una expresión para la raíz cuadrada de un número complejo $z = a + ib$ que sólo involucre operaciones suma, resta, multiplicación, división y extracción de raíces cuadradas, éstas de números reales positivos, a partir de la parte real a y la parte imaginaria b.

[4]Más tarde caracterizaremos aquellos polígonos regulares construibles con regla y compás

Capítulo 2

Homomorfismos y construcción de cuerpos

Nuestro próximo objetivo es construir cuerpos donde los polinomios con coeficientes sobre un cuerpo dado tengan raíces, más allá del caso de polinomios con coeficientes en un subcuerpo de $\mathbb{C}$. En particular, todos los cuerpos finitos serán construidos y su clasificación desentrañada. A cada extensión de cuerpos le asignaremos su grupo de automorfismos, que será descrito para cuerpos finitos. Además, mostraremos cómo cada cuerpo puede ser extendido a un cuerpo que «cotiene» a todas sus extensiones finitas. Se trata de su clausura algebraica.

2.1. Homomorfismos de cuerpos. Cuerpos de descomposición

Para consultar la noción de anillo y homomorfismo de anillos remitimos a [**2**]. Vamos a estudiar qué propiedades y utilidad tienen estos homomorfismos en el caso de que los anillos involucrados sean cuerpos. Comencemos por una observación sencilla.

LEMA 2.1. *Sea* $\sigma : F \to A$ *un homomorfismo de anillos, para* F *cuerpo y* A *un anillo no trivial. Entonces* $\mathrm{Im}\sigma$ *es un subanillo de* A *isomorfo a* F *como anillo. Como consecuencia, si* A *es también un cuerpo, entonces* $\mathrm{Im}\sigma$ *es un subcuerpo de* A *isomorfo a* F*.*

DEMOSTRACIÓN. Calculemos el núcleo $\mathrm{Ker}\sigma$. Sabemos que se trata de un ideal de F. Como $\sigma \neq 0$, ya que $\sigma(1) = 1 \neq 0$, la única posibilidad es que $\mathrm{Ker}\sigma = \{0\}$. Así, pues, f es un homomorfismo inyectivo de anillos, por lo que $F \cong \mathrm{Im}\sigma$, como anillos. □

OBSERVACIÓN 2.2. Los homomorfismos de anillos entre cuerpos se suelen llamar homomorfismos de cuerpos, ya que, automáticamente, preservan inversos multiplicativos. En consecuencia, los isomorfismos de anillos entre cuerpos se llamarán isomorfismos de cuerpos.

OBSERVACIÓN 2.3. Dado un homomorfismo de cuerpos $\sigma : F \to K$, el Lema 2.1 indica que F es isomorfo, vía σ, al subcuerpo $\sigma(F) = \mathrm{Im}\sigma$ de K. Observemos que la estructura de $\sigma(F)$–espacio vectorial de K puede entenderse, también, como una estructura de F–espacio vectorial mediante la definición $ab := \sigma(a)b$, para $a \in F$, $b \in K$.

Sea $f \in F[X]$ un polinomio con coeficientes en un cuerpo F, y escribamos

$$f = \sum_i f_i X^i, \quad (f_i \in F).$$

Dado un homomorfismo de cuerpos $\sigma : F \to K$, consideramos el polinomio

$$f^\sigma = \sum_i \sigma(f_i) X^i \in K[X].$$

Se deduce de la propiedad universal del anillo de polinomios ([**2**, Teorema 3.5]) que la aplicación $F[X] \to K[X]$ definida por la asignación $f \mapsto f^\sigma$ es un homomorfismo de anillos.

EJEMPLO 2.4. Supongamos un polinomio no constante $f \in F[X]$ y $p \in F[X]$ un factor irreducible de f. Tenemos entonces el cuerpo $F[X]/\langle p\rangle$. La aplicación $\sigma : F \to F[X]/\langle p\rangle$ definida por $\sigma(a) = a + \langle p\rangle$, para $a \in F$, es un homomorfismo de cuerpos. Resulta que $\alpha = X + \langle p\rangle$ es una raíz de f^σ. En efecto, escribiendo $f = \sum_i f_i X^i$, tenemos

$$f^\sigma(\alpha) = \sum_i \sigma(f_i)(X + \langle p\rangle)^i = \sum_i (f_i + \langle p\rangle)(X^i + \langle p\rangle) = f + \langle p\rangle = 0 + \langle p\rangle,$$

ya que $f \in \langle p\rangle$. Observemos que $F[X]/\langle p\rangle = \sigma(F)(\alpha)$.

Extraigamos una consecuencia obvia del Ejemplo 2.4, enunciándola como lema, para su uso posterior.

LEMA 2.5. *Sea $f \in F[X]$ no constante y $p \in F[X]$ un factor irreducible de f. Existen un homomorfismo de cuerpos $\sigma : F \to K$ y $\alpha \in K$ tal que $p^\sigma(\alpha) = 0$ y $\sigma(F)(\alpha) = K$.*

PROPOSICIÓN 2.6. *Sea $F[X]$ el anillo de polinomios en la indeterminada X con coeficientes en un cuerpo F, y $f \in F[X]$ un polinomio de grado $n \geq 1$. Entonces existe un homomorfismo de cuerpos $\sigma : F \to E$ tal que E es un cuerpo de descomposición de f^σ.*

DEMOSTRACIÓN. Primero, observemos que podemos suponer que f es mónico. Vamos a demostrar que existe un homomorfismo de cuerpos $\sigma : F \to L$ tal que f^σ se descompone como producto de factores lineales en $L[X]$.

Mirando una descomposición de f como producto de irreducibles, podemos escribir $f = gh$, donde $g \in F[X]$ es producto de polinomios lineales[1] y $h \in F[X]$ no tiene raíces en F. Razonamos por inducción sobre $\deg h$. Si este número es 0 es porque f es un producto de polinomios lineales en $F[X]$; tomamos $L = F$ y $\sigma = \mathrm{id}_F$.

Vayamos al caso propio, que ocurre cuando h tiene algún divisor irreducible p de grado mayor que 1. Por el Lema 2.5, existe un homomorfismo de cuerpos $\tau : F \to K$ tal que p^τ tiene una raíz $\alpha \in K$ que, obviamente, es también raíz de h^τ. Si escribimos $g = (X-\alpha_1)\dots(X-\alpha_t)$, para $\alpha_1, \dots, \alpha_t \in F$, y extraemos los factores lineales a h^τ, tenemos que

$$f^\tau = g^\tau h^\tau = (X - \tau(\alpha_1))\dots(X - \tau(\alpha_t))(X - \beta_1)\cdots(X - \beta_s)k$$

para ciertos $\beta_1, \dots, \beta_s \in K$ (entre los que está incluido α), $k \in K[X]$ sin raíces en K y de grado menor que el de h^τ. Por hipótesis de inducción, existe un homomorfismo de cuerpos $\rho : K \to L$ tal que $(f^\tau)^\rho$ se descompone completamente como producto de factores lineales en $L[X]$. Tomando la composición $\sigma = \rho\tau : F \to L$, f^σ se descompone como producto de polinomios lineales en $L[X]$.

Ahora, tomando el subcuerpo E de L generado por $\sigma(F)$ y las raíces de f^σ, obtenemos un cuerpo de descomposición de este polinomio. Finalmente, basta con considerar la corestricción $\sigma : F \to E$. □

Extendemos la definición de cuerpo de descomposición que habíamos dado inicialmente con objeto de recoger la situación más general descrita por la anterior proposición.

DEFINICIÓN 2.7. Sea $f \in F[X]$. Un cuerpo de descomposición de f es un homomorfismo de cuerpos $\sigma : F \to E$ tal que E es cuerpo de descomposición de f^σ.

[1] es decir, de grado 1.

EJEMPLO 2.8. Tomamos $f = X^2 + X + 1 \in \mathbb{Z}_2[X]$. Un cuerpo de descomposición de f es $\mathbb{Z}_2[X]/\langle f\rangle$. Observemos que este cuerpo tiene cuatro elementos, y se suele denotar por $\mathbb{F}_4$. Usando la notación $\mathbb{F}_2 = \mathbb{Z}_2$, tenemos que $\mathbb{F}_4 = \mathbb{F}_2(a)$, donde $a \in \mathbb{F}_4$ satisface la ecuación $a^2 + a + 1 = 0$. Deducimos que $\mathbb{F}_4 = \{0, 1, a, a+1\} = \{0, 1, a, a^2\}$. La factorización en $\mathbb{F}_4[X]$ de f es $f = (X + a)(X + a^2)$.

EJEMPLO 2.9. Describamos un cuerpo de descomposición de $f = X^3 + X + 1 \in \mathbb{F}_2[X]$. Notemos que f es irreducible. Construimos, siguiendo el método del Ejemplo 2.4, una extensión $L = \mathbb{F}_2(a)$ para $a \in L$ que satisface la igualdad $a^3 + a + 1 = 0$. Este cuerpo tiene 8 elementos, que se pueden escribir como $L = \{0, 1, a, a^2, a^3, a^4, a^5, a^6\}$. De hecho, se tienen las igualdades

$$a^3 = a + 1, a^4 = a^2 + a, a^5 = a^2 + a + 1, a^6 = a^2 + 1, a^7 = 1.$$

Por construcción, a es una raíz de f. Realizando una división con resto, obtenemos $f = (X + a)g$, donde $g = X^2 + aX + a^6$. Como $g(a^2) = 0$, realizado una segunda división euclidiana, obtenemos la factorización

$$f = (X + a)(X + a^2)(X + a^4).$$

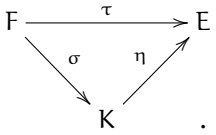
Por tanto, L es un cuerpo de descomposición de f. Más adelante, daremos alguna información general sobre los cuerpos de descomposición de polinomios con coeficientes en cuerpos finitos.

Vamos a abordar el problema de la unicidad del cuerpo de descomposición de un polinomio.

LEMA 2.10. *Sea $\sigma : F \to K$ un homomorfismo de cuerpos y $p \in F[X]$ irreducible. Si $\alpha \in K$ es una raíz de p^σ, entonces se tiene un isomorfismo de cuerpos $\sigma_\alpha : F[X]/\langle p\rangle \to \sigma(F)(\alpha)$ definido por $\sigma_\alpha(g + \langle p\rangle) = g^\sigma(\alpha)$.*

DEMOSTRACIÓN. Consideremos el homomorfismo de anillos $\overline{\sigma} : F[X] \to K$ dado por $\overline{\sigma}(g) = g^\sigma(\alpha)$. Tenemos que $\mathrm{Im}\overline{\sigma} = \sigma(F)(\alpha)$, en tanto que $\mathrm{Ker}\overline{\sigma} = \langle p\rangle$, ya que $p \in \mathrm{Ker}\overline{\sigma}$ es irreducible. Ahora, aplicamos el Teorema del Isomorfismo de anillos para obtener σ_α. □

DEFINICIÓN 2.11. Sean $\tau : F \to E$ y $\sigma : F \to K$ homomorfismos de cuerpos. Diremos que un homomorfismo de cuerpos $\eta : K \to E$ es una *σ–extensión de τ* si $\tau = \eta\sigma$. Denotamos al conjunto de estas σ-extensiones por $\mathrm{Ex}(\tau, \sigma)$. Esta situación puede representarse por el diagrama



Si $F \leq K$ es una extensión de cuerpos y $\sigma : F \to K$ es la inclusión, entonces nos referiremos a los elementos de $\mathrm{Ex}(\tau, \sigma)$ como *extensiones* de τ.

La siguiente proposición será una herramienta fundamental.

PROPOSICIÓN 2.12 (Extensión de homomorfismos). *Sean $\tau : F \to E$ y $\sigma : F \to K$ homomorfismos de cuerpos, $p \in F[X]$ un polinomio irreducible y $\alpha \in K$ una raíz de p^σ. Sea $\mathcal{R} \subseteq E$ el conjunto de todas las raíces de p^τ en E. Si $K = \sigma(F)(\alpha)$, entonces se tiene una aplicación biyectiva*

$$\mathrm{Ex}(\tau, \sigma) \to \mathcal{R}, \quad (\eta \mapsto \eta(\alpha)).$$

DEMOSTRACIÓN. Sea $\eta \in \mathrm{Ex}(\tau, \sigma)$. Tenemos que comprobar que $\eta(\alpha)$ es una raíz de p^τ. En efecto,

$$p^\tau(\eta(\alpha)) = p^{\eta\sigma}(\eta(\alpha)) = \eta(p^\sigma(\alpha)) = \eta(0) = 0.$$

Comprobemos que la aplicación del enunciado es sobreyectiva: dada una raíz $\beta \in E$ de p^τ, tenemos el isomorfismo $\tau_\beta : F[X]/\langle p\rangle \to \tau(F)(\beta)$ dado por el Lema 2.10. El mismo lema da el isomorfismo $\sigma_\alpha : F[X]/\langle p\rangle \to \sigma(F)(\alpha) = K$. Definimos $\eta : K \to E$ como la composición $\tau_\beta \sigma_\alpha^{-1}$ seguida por la inclusión $\tau_\beta(F)(\beta) \subseteq E$. Tenemos que $\eta \in \mathrm{Ex}(\tau, \sigma)$ y, además,

$$\eta(\alpha) = \tau_\beta(X + \langle p\rangle) = \beta. \tag{2.1}$$

Observemos que, de lo demostrado hasta ahora, deducimos que $\mathrm{Ex}(\tau, \sigma)$ es no vacío si, y sólo si, $\mathcal{R}$ es no vacío.

Por último, veamos que la aplicación del enunciado es biyectiva. Sean $\eta, \eta' \in \mathrm{Ex}(\tau, \sigma)$ tales que $\eta(\alpha) = \eta'(\alpha)$. Un elemento cualquiera de $K = \sigma(F)(\alpha)$ es una suma finita $\sum_i \sigma(a_i)\alpha^i$, para ciertos $a_i \in F$. Tenemos que

$$\begin{aligned}\eta\Big(\sum_i \sigma(a_i)\alpha^i\Big) &= \sum_i \eta(\sigma(a_i))\eta(\alpha)^i \\ &= \sum_i \tau(a_i)\eta'(\alpha)^i = \sum_i \eta'(\sigma(a_i))\eta'(\alpha)^i = \eta'\Big(\sum_i \sigma(a_i)\alpha^i\Big).\end{aligned}$$

Luego $\eta = \eta'$. □

OBSERVACIÓN 2.13. Obsérvese que la Proposición 2.12 no excluye, como queda patente en su demostración, el caso en que $\mathrm{Ex}(\tau, \sigma) = \emptyset$, que se da, justamente, cuando p^τ no tiene raíces en E.

LEMA 2.14. *Sean homomorfismos de cuerpos $\tau : F \to L$, $\sigma_1 : F \to E_1$, $\sigma_2 : E_1 \to E_2$. Entonces se tiene una unión disjunta*

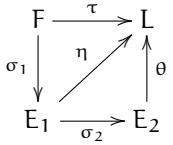
$$\mathrm{Ex}(\tau, \sigma_2\sigma_1) = \bigcup_{\eta \in \mathrm{Ex}(\tau, \sigma_1)} \mathrm{Ex}(\eta, \sigma_2).$$

DEMOSTRACIÓN. Si tomo $\theta \in \mathrm{Ex}(\eta, \sigma_2)$ para $\eta \in \mathrm{Ex}(\tau, \sigma_1)$, tenemos que $\theta\sigma_2\sigma_1 = \eta\sigma_1 = \tau$, luego $\mathrm{Ex}(\eta, \sigma_2) \subseteq \mathrm{Ex}(\tau, \sigma_2\sigma_1)$.

Por otra parte, si $\theta \in \mathrm{Ex}(\tau, \sigma_2\sigma_1)$, tomando $\eta = \theta\sigma_2$ tenemos que $\eta\sigma_1 = \tau$, luego $\eta \in \mathrm{Ex}(\tau, \sigma_1)$. Obviamente, $\theta \in \mathrm{Ex}(\eta, \sigma_2)$. Así que

$$\mathrm{Ex}(\tau, \sigma_2\sigma_1) = \bigcup_{\eta \in \mathrm{Ex}(\tau, \sigma_1)} \mathrm{Ex}(\eta, \sigma_2).$$

Como, claramente, $\mathrm{Ex}(\eta, \sigma_2) \cap \mathrm{Ex}(\eta', \sigma_2) = \emptyset$ para $\eta \neq \eta'$, obtenemos que la unión es disjunta. El siguiente diagrama ilustra la prueba recién hecha.



□

Dado un conjunto finito A, denotaremos su cardinal por $\#A$.

PROPOSICIÓN 2.15. *Sean $\tau : F \to E$, $\sigma : F \to K$ homomorfismos de cuerpos tales que $[K : \sigma(F)]$ es finita. Entonces $\#\mathrm{Ex}(\tau, \sigma) \leq [K : \sigma(F)]$.*

DEMOSTRACIÓN. Haremos inducción sobre $n = [K : \sigma(F)]$. Si $n = 1$, entonces σ es un isomorfismo y $\eta = \tau\sigma^{-1} \in Ex(\tau, \sigma)$. De hecho, es el único elemento de $Ex(\tau, \sigma)$ en este caso.

Si $n > 1$, existe $\alpha \in K$ tal que $[\sigma(F)(\alpha) : \sigma(F)] > 1$. Por el Lema de la Torre, $[K : \sigma(F)(\alpha)] < n$.

Denotemos por $\iota : \sigma(F)(\alpha) \to K$ la inclusión, lo que da $\sigma = \iota\sigma'$ para $\sigma' : F \to \sigma(F)(\alpha)$ la adecuada correstricción de σ. La situación viene ilustrada por el diagrama

$$\begin{array}{ccc} F & \xrightarrow{\tau} & E \\ {\scriptstyle\sigma'}\downarrow & \nearrow_{\sigma} & \\ \sigma(F)(\alpha) & \xrightarrow[\iota]{} & K \end{array}$$

Por el Lema 2.14, tenemos la unión disjunta

$$Ex(\tau, \sigma) = \bigcup_{\eta \in Ex(\tau, \sigma')} Ex(\eta, \iota),$$

de donde

$$\#Ex(\tau, \sigma) = \sum_{\eta \in Ex(\tau, \sigma')} \#Ex(\eta, \iota).$$

Para cada $\eta \in Ex(\tau, \sigma')$ tenemos, por hipótesis de inducción, que $\#Ex(\eta, \iota) \leq [K : \sigma(F)(\alpha)]$, de donde

$$\#Ex(\tau, \sigma) \leq \#Ex(\tau, \sigma')[K : \sigma(F)(\alpha)].$$

Tomemos $p \in F[X]$ tal que $p^\sigma = Irr(\alpha, \sigma(F))$. Según la Proposición 2.12, $\#Ex(\tau, \sigma')$ es igual al número de raíces de p^τ en E. Así,

$$\#Ex(\tau, \sigma) \leq \deg(p^\tau)[K : \sigma(F)(\alpha)] = [\sigma(F)(\alpha) : F][K : \sigma(F)(\alpha)] = [K : \sigma(F)].$$

□

PROPOSICIÓN 2.16. *Sean $\tau : F \to E$, $\sigma : F \to K$ homomorfismos de cuerpos tales que $\sigma : F \to K$ da un cuerpo de descomposición de un polinomio no constante $f \in F[X]$ y f^τ se descompone como producto de polinomios lineales en $E[X]$. Entonces $Ex(\tau, \sigma)$ es no vacío. Además, $\#Ex(\tau, \sigma) = [K : \sigma(F)]$ si f^σ tiene $\deg f$ raíces distintas.*

DEMOSTRACIÓN. Razonamos por inducción sobre $n = [K : \sigma(F)]$. Para $n = 1$, σ es un isomorfismo y $Ex(\tau, \sigma) = \{\tau\sigma^{-1}\}$. Como $[K : \sigma(F)] = 1$, vemos que el enunciado es correcto en este caso.

Supongamos, pues, que $n > 1$, lo que garantiza que f tiene un factor irreducible $p \in F[X]$ de grado mayor que 1. Tomamos un raíz $\alpha \in K$ de p^σ y deducimos, como en la prueba de la Proposición 2.15, que $[K : \sigma(F)(\alpha)] < n$. Denotemos por $\iota : \sigma(F)(\alpha) \to K$ la inclusión, lo que da $\sigma = \iota\sigma'$ para $\sigma' : F \to \sigma(F)(\alpha)$ la adecuada correstricción de σ. De nuevo, como en la Proposición 2.15, deducimos que

$$\#Ex(\tau, \sigma) = \sum_{\eta \in Ex(\tau, \sigma')} \#Ex(\eta, \iota). \tag{2.2}$$

De la Proposición 2.12 deducimos que $Ex(\tau, \sigma')$ tiene tantos elementos como raíces de p^τ haya en E. Pero p^τ es un factor de f^τ, luego se factoriza como producto de polinomios de grado 1 en $E[X]$. En particular, el conjunto $\mathcal{R}$ de raíces p^τ en E es no vacío, y así ha de serlo $Ex(\tau, \sigma')$. Por hipótesis de inducción, $Ex(\eta, \iota)$ es no vacío para cada $\eta \in Ex(\tau, \sigma')$ con lo que concluimos que $Ex(\tau, \sigma)$ es no vacío.

Por otra parte, si f^σ tiene $\deg f$ raíces distintas, entonces p^σ tiene $\deg p$ raíces distintas. Por tanto,

$$\#\mathrm{Ex}(\tau,\sigma') = \#\mathcal{R} = \deg p^\sigma = [\sigma(F)(\alpha) : \sigma(F)].$$

Por hipótesis de inducción, para cada $\eta \in \mathrm{Ex}(\tau,\sigma')$, tenemos que $\#\mathrm{Ex}(\eta,\iota) = [K : \sigma(F)(\alpha)]$ lo que, en vista de (2.2), implica que

$$\#\mathrm{Ex}(\tau,\sigma) = [K : \sigma(F)(\alpha)][\sigma(F)(\alpha) : \sigma(F)] = [K : \sigma(F)].$$

□

EJERCICIO 25. Demostrar que, si P es el subcuerpo primo de un cuerpo K, entonces el único homomorfismo de cuerpos $P \to K$ es la inclusión.

EJEMPLO 2.17. Consideremos $K = \mathbb{Q}(\sqrt[3]{2},\omega)$, para ω una raíz cúbica primitiva de la unidad compleja. Sabemos que K es cuerpo de descomposición de $X^3-2 \in \mathbb{Q}[X]$. Vamos a describir, con la ayuda de la Proposición 2.16, y de su demostración, todos los homomorfismos de cuerpos de K a $\mathbb{C}$. Para ello, denotemos por $\sigma : \mathbb{Q} \to K$ y $\tau : \mathbb{Q} \to \mathbb{C}$ a las correspondientes inclusiones. Si $\eta : K \to \mathbb{C}$ es cualquier homomorfismo de cuerpos, entonces $\eta\tau : \mathbb{Q} \to \mathbb{C}$ ha de ser la inclusión (ver Ejercicio 25). Esto es, lo que queremos calcular es $\mathrm{Ex}(\tau,\sigma)$. Según la Proposición 2.16, aplicada a $f = X^3-2$, el cardinal de este conjunto es $[K : \mathbb{Q}] = 6$. Para calcularlos, procedemos como se describe a continuación.

Según la Proposición 2.12, puesto que las raíces en $\mathbb{C}$ de f son

$$\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\},$$

hay tres homomorfismos de cuerpos $\eta_j : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$, con $j = 0,1,2$, determinados por $\eta_j(\sqrt[3]{2}) = \omega^j\sqrt[3]{2}$. Para cada $\eta_j : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ tenemos, por la Proposición 2.12 aplicada a $X^2+X+1 \in \mathbb{Q}(\sqrt[3]{2})[X]$, que es irreducible, las extensiones $\eta_{jk} : \mathbb{Q}(\sqrt[3]{2},\omega) \to \mathbb{C}$, para $k = 1,2$ de cada η_j, determinadas por $\eta_{jk}(\omega) = \omega^k$. En resumen, los 6 homomorfismos de cuerpos buscados son $\eta_{jk} : K \to \mathbb{C}$, determinados por

$$\eta_{jk} : \begin{cases} \sqrt[3]{2} \mapsto \omega^j\sqrt[3]{2} \\ \omega \mapsto \omega^k, \end{cases}$$

para $j = 0,1,2; k = 1,2$.

Para comprobar si entiendes esta descripción, calcula $\eta_{jk}(\omega\sqrt[3]{2})$.

Para concluir el ejemplo, observemos que la anterior discusión es aplicable si tomamos, en lugar de $\mathbb{C}$, cualquier subcuerpo suyo E que contenga a K.

EJERCICIO 26. Sean $\tau : F \to E$ y $\rho : E \to E$ homomorfismos de cuerpos. Demostrar que ρ es $\tau(F)$–lineal si, y sólo si, $\rho\tau = \tau$.

TEOREMA 2.18 (Unicidad del cuerpo de descomposición). *Sean $\tau : F \to E$ y $\tau' : F \to E'$ cuerpos de descomposición de un polinomio no constante $f \in F[X]$. Entonces existe un isomorfismo de cuerpos $\eta : E \to E'$ tal que $\eta\tau = \tau'$.*

DEMOSTRACIÓN. En virtud de la Proposición 2.16, existen $\eta : E \to E'$ tal que $\eta\tau = \tau'$ y $\eta' : E' \to E$ tal que $\eta'\tau' = \tau$. Entonces $\eta\eta'\tau' = \tau'$. Esto implica que $\eta\eta'$ es $\tau'(F)$–lineal. Como E' es de dimensión finita sobre $\tau'(F)$ y $\eta\eta'$ es inyectiva, se sigue que es biyectiva. Por tanto, η ha de ser sobreyectiva. Al ser un homomorfismo de cuerpos, es inyectiva, luego η es un isomorfismo de cuerpos. □

EJERCICIO 27. Sea $\sigma : F \to E$ un homomorfismo de cuerpos tal que la extensión $\sigma(F) \leq E$ es finita. Demostrar que existe un polinomio $f \in F[X]$ y un homomorfismo de cuerpos $\tau : E \to K$ tal que $\tau\sigma : F \to K$ es cuerpo de descomposición de f.

2.2. Clasificación de los cuerpos finitos

Vamos a discutir un caso particular de cuerpo de descomposición que nos dará información relevante sobre los cuerpos finitos. Un hecho fundamental para ello es el siguiente.

PROPOSICIÓN 2.19. *Sea F un cuerpo finito de característica p y cardinal $q = p^n$. Entonces F es cuerpo de descomposición de $X^q - X \in \mathbb{F}_p[X]$. Así, cada cuerpo finito es de esta forma.*

DEMOSTRACIÓN. Llamemos $f = X^q - X$. Observemos que $F^\times = F \setminus \{0\}$ es un grupo multiplicativo de cardinal $q - 1$. Por el Teorema de Lagrange, cada $\alpha \in F^\times$ tiene por orden un divisor de $q - 1$ y, así, $\alpha^{q-1} - 1 = 0$. Por tanto, todo elemento de F es raíz de f y F es cuerpo de descomposición de f. □

Vamos con la clasificación de los cuerpos finitos. Necesitamos el hecho descrito en el siguiente ejercicio.

EJERCICIO 28. Sea F es un cuerpo de característica positiva p. Demostrar que, si $a, b \in F$, entonces $(a - b)^q = a^q - b^q$ para todo $q = p^n$ con n natural no nulo.

TEOREMA 2.20. *Para cada número primo p, y cada natural $n \geq 1$, existe un único, salvo isomorfismos, cuerpo de cardinal $q = p^n$. No hay más cuerpos finitos que éstos.*

DEMOSTRACIÓN. Para $q = p^n$, con p primo, tomamos F un cuerpo de descomposición del polinomio $f = X^q - X \in \mathbb{F}_p[X]$. Sea S el conjunto de las raíces de f en F. Comprobemos que S es un subcuerpo de F. En efecto, $1 \in S$, obviamente. Ahora, si $a, b \in S$, entonces $(a - b)^q = a^q - b^q = a - b$, y $(ab)^q = a^q b^q = ab$, luego $a - b, ab \in S$. Por último, $(a^{-1})^q = a^{-q} = (a^q)^{-1} = a^{-1}$. Como F es cuerpo de descomposición de f, tenemos que $S = F$. Dado que[2] $f' = -1$, no hay raíces comunes entre f y f'. Por tanto, todas las raíces de f son distintas [**2**, Proposición 4.45], así que $S = F$ tiene q elementos.

Si E es cualquier otro cuerpo con q elementos, tenemos, por la Proposición 2.19, que E es cuerpo de descomposición de f. El Teorema 2.18 garantiza que E es isomorfo a F. □

Usaremos la notación $\mathbb{F}_q$ para referirnos «al» cuerpo finito con q elementos. Estos cuerpos se llaman también *cuerpos de Galois*.

2.3. El grupo de automorfismos de una extensión

Dado un cuerpo K, denotaremos por $\mathrm{Aut}(K)$ al conjunto de todos los automorfismos de cuerpos $\sigma : K \to K$. Este conjunto es un grupo cuyo producto es la composición. Si $F \leq K$ es una extensión de cuerpos, entonces tenemos el subgrupo

$$\mathrm{Aut}_F(K) = \{\sigma \in \mathrm{Aut}(K) : \sigma \text{ es } F - \text{lineal}\},$$

que llamaremos grupo de automorfismos de la extensión.

[2] f' denota la derivada formal de f.

EJERCICIO 29. Demostrar que, si P denota el subcuerpo primo de K, entonces $\mathrm{Aut}_P(K) = \mathrm{Aut}(K)$.

OBSERVACIÓN 2.21. Sea $F \leq K$ una extensión finita de cuerpos e $\iota : F \to K$ el homomorfismo inclusión. Se sigue del Ejercicio 26 que $\mathrm{Aut}_F(K) = \mathrm{Ex}(\iota, \iota)$, para $\iota : F \to K$ la inclusión.

PROPOSICIÓN 2.22. *Supongamos una extensión $F \leq K$ tal que K es cuerpo de descomposición de un polinomio $f \in F[X]$. Entonces $\#\mathrm{Aut}_F(K) \leq [K : F]$. Si todas las raíces de f en K son simples, entonces $\#\mathrm{Aut}_F(K) = [K : F]$.*

DEMOSTRACIÓN. Aplicar la Proposición 2.16 a $\mathrm{Ex}(\iota, \iota)$, teniendo en cuenta la Observación 2.21. □

EJEMPLO 2.23. Del Ejemplo 2.17 deducimos que $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega))$ tiene seis elementos, que son los automorfismos determinados por las condiciones

$$\eta_{jk}(\sqrt[3]{2}) = \omega^j \sqrt[3]{2}, \quad \eta_{jk}(\omega) = \omega^k, \qquad (j = 0, 1, 2; k = 1, 2).$$

Vamos a obtener información sobre el grupo de automorfismos de un cuerpo finito.

TEOREMA 2.24. *Sea $\mathbb{F}_q$ un cuerpo finito, para $q = p^n$ con p primo. Entonces $\mathrm{Aut}(\mathbb{F}_q)$ es un grupo cíclico de orden n.*

DEMOSTRACIÓN. Como, de acuerdo con la Proposición 2.19, $\mathbb{F}_q$ es cuerpo de descomposición de $X^q - X \in \mathbb{F}_p[X]$, deducimos de la Proposición 2.16 que $\#\mathrm{Aut}(\mathbb{F}_q) = [\mathbb{F}_q : \mathbb{F}_p] = n$. Vamos a dar un elemento de orden n, que, necesariamente, será generador del grupo. Definimos la aplicación

$$\tau : \mathbb{F}_q \to \mathbb{F}_q, \qquad (x \mapsto x^p). \tag{2.3}$$

Usando que la característica es p, es fácil ver que τ es un automorfismo de cuerpos. Veamos que su orden es n. Si m es no nulo y tal que $\tau^m = \mathrm{id}$, entonces, tomado un generador a del grupo cíclico (ver Ejercicio 30) $\mathbb{F}_q^\times$, tenemos que $a = \tau^m(a) = a^{p^m}$. Como a tiene orden multiplicativo $p^n - 1$, se sigue que $m \geq n$. □

DEFINICIÓN 2.25. El generador τ de $\mathrm{Aut}(\mathbb{F}_q)$ definido según (2.3) se llama *automorfismo de Frobenius* del cuerpo $\mathbb{F}_q$.

2.4. Clausura algebraica

Por economía del lenguaje, diremos que un homomorfismo de cuerpos $\sigma : F \to K$ es finito si K es de dimensión finita como F–espacio vectorial, equivalentemente, la extensión $\sigma(F) \leq K$ es finita. Diremos que $\sigma : F \to K$ es algebraico si la extensión $\sigma(F) \leq K$ es algebraica. A veces se usan las expresiones extensión finita o algebraica al referirse al propio homomorfismo σ.

El problema que vamos a abordar en esta sección es si, dadas dos extensiones finitas de un cuerpo, existe una extensión del mismo que las «contenga» a ambas. Una solución puede formularse como la siguiente proposición.

PROPOSICIÓN 2.26. *Dados homomorfismos finitos* $\sigma_1 : F \to L_1, \sigma_2 : F \to L_2$, *existen homomorfismos finitos* τ, τ_1 *y* τ_2 *que hacen conmutar el siguiente diagrama,*

(2.4)
$$\begin{array}{ccc} F & \xrightarrow{\sigma_1} & L_1 \\ {\scriptstyle\sigma_2}\downarrow & \searrow^{\tau} & \downarrow{\scriptstyle\tau_1} \\ L_2 & \xrightarrow[\tau_2]{} & E \end{array} ,$$

esto es, $\tau_1\sigma_1 = \tau = \tau_2\sigma_2$. *Además,* $\tau : F \to E$ *se puede tomar como un cuerpo de descomposición de un polinomio de* $F[X]$.

DEMOSTRACIÓN. Vamos a construir un polinomio $f_i \in F[X]$, para cada $i = 1, 2$, tal que existe un homomorfismo de cuerpos $\lambda_i : L_i \to K_i$ de manera que $\lambda_i\sigma_i : F \to K_i$ es cuerpo de descomposición de f_i. Por economía en la notación, razonamos para $i = 1$. Puesto que $\sigma_1(F) \leq L_1$ es finita, tenemos que $L_1 = \sigma_1(F)(\alpha_1, \ldots, \alpha_t)$, para $\alpha_1, \ldots, \alpha_t$ algebraicos sobre $\sigma_1(F)$. Tomamos $g_j = \mathrm{Irr}(\alpha_j, \sigma_1(F))$ para $j = 1, \ldots, t$, y $f_1 \in F[X]$ tal que $f_1^{\sigma_1} = g_1 \ldots g_t$.

Por la Proposición 2.6, existe un cuerpo de descomposición $\tau : F \to E$ de $f_1 f_2$. Por la Proposición 2.16, existen homomorfismos $\eta_i : K_i \to E$ tales que $\eta_i\lambda_i\sigma_i = \tau$. Es decir, el diagrama

$$\begin{array}{ccccc} F & \xrightarrow{\sigma_1} & L_1 & \xrightarrow{\lambda_1} & K_1 \\ {\scriptstyle\sigma_2}\downarrow & \searrow^{\tau} & & & \\ L_2 & & & & {\scriptstyle\eta_1}\downarrow \\ {\scriptstyle\lambda_2}\downarrow & & & & \\ K_2 & & \xrightarrow[\eta_2]{} & & E \end{array}$$

es conmutativo. Tomando $\tau_i = \eta_i\lambda_i$ para $i = 1, 2$, obtenemos el diagrama conmutativo (2.4). □

La resolución del problema planteado antes de enunciar la Proposición 2.26 a partir de ésta es como sigue. El cuerpo E contiene el subcuerpo $\tau(F)$, que es isomorfo a F. Además, los subcuerpos $\tau_1(L_1), \tau_2(L_2)$ de E contienen a $\tau(F)$ y son isomorfos, respectivamente, a L_1 y L_2.

La Proposición 2.26 puede extenderse sin dificultad a una cantidad finita $\sigma_i : F \to L_i$, para $i = 1, \ldots, n$ de homomorfismos finitos. De su enunciado, obtendríamos un homomorfismo finito $\tau : F \to E$ donde yacen todas las extensiones finitas $\tau(F) \leq \tau(L_i) \leq E$, para $i = 1, \ldots, n$. Para los propósitos de este curso, esto es suficiente. No obstante, la pregunta de si existe una extensión algebraica de un cuerpo F que «contenga» a todas sus extensiones finitas tiene una respuesta afirmativa, siempre que admitamos inducción transfinita (Lema de Zorn). La clave está en la noción de clausura algebraica, que definimos a continuación.

DEFINICIÓN 2.27. Sea F un cuerpo. Diremos que un homomorfismo de cuerpos algebraico $\sigma : F \to C$ es una *clausura algebraica* de F si todo homomorfismo finito $\tau : C \to E$ es un isomorfismo.

PROPOSICIÓN 2.28. *Las siguientes condiciones son equivalentes para un homomorfismo algebraico de cuerpos* $\sigma : F \to C$.

1. $\sigma : F \to C$ *es una clausura algebraica de* F;
2. *todo polinomio no constante en* $C[X]$ *tiene una raíz en* C.

DEMOSTRACIÓN. Supongamos que $\sigma : F \to C$ es una clausura algebraica de F y tomemos un polinomio no constante $f \in C[X]$. Tomo $\tau : C \to K$ un cuerpo de descomposición de f, que es un homomorfismo finito. Por tanto, es un isomorfismo. Si $\alpha \in K$ una raíz de f^τ, entonces $\tau^{-1}(\alpha) \in C$ es una raíz de f.

Recíprocamente, supongamos que todo polinomio no constante en $C[X]$ tiene una raíz en C y que $\tau : C \to E$ es un homomorfismo finito. Tomo $x \in E$ y $f \in C[X]$ tal que $f^\tau = \mathrm{Irr}(x, \tau(C))$. Usando que cada polinomio no constante en $C[X]$ tiene una raíz, obtenemos una factorización $f = \Pi_{i=0}^{n}(X - c_i)$, con $c_1, \ldots, c_n \in C$. Obtenemos, pues, que $f^\tau = \Pi_{i=0}^{n}(X - \tau(c_i))$. Dado que x es una raíz de f^τ, se tiene que $x = \tau(c_i)$ para algún c_i. Hemos demostrado que τ es sobreyectivo y, por ser homomorfismo de cuerpos, biyectivo. □

DEFINICIÓN 2.29. Un cuerpo C se dice *algebraicamente cerrado* si todo polinomio no constante de $C[X]$ tiene una raíz en C. La Proposición 2.28 se puede, pues, reformular diciendo que una clausura algebraica de F es un homomorfismo algebraico $\sigma : F \to C$ tal que C es algebraicamente cerrado.

Nuestro próximo objetivo es demostrar que las clausuras algebraicas existen. Para exponer una demostración, necesitamos hacer ciertas precisiones e introducir alguna nomenclatura.

Un cuerpo K está dotado de dos operaciones, suma y producto. Ambas operaciones pueden formularse como una aplicación $e : K \times K \to K \times K$ definida por $e(x, y) = (x + y, xy)$. Esta aplicación satisface ciertas condiciones que reflejan fielmente aquéllas que fueron requeridas a la suma y el producto. Nos referiremos a un tal e como la *aplicación estructura* de K. Si L es otro cuerpo con aplicación estructura $f : L \times L \to L \times L$ y $\sigma : K \to L$ es una aplicación, entonces σ es homomorfismo de cuerpos si, y sólo si, el diagrama

$$\begin{array}{ccc} K \times K & \xrightarrow{e} & K \times K \\ \downarrow{\scriptstyle \sigma\times\sigma} & & \downarrow{\scriptstyle \sigma\times\sigma} \\ L \times L & \xrightarrow{f} & L \times L \end{array}$$

es conmutativo y $\sigma(1) = 1$.

Dado el cuerpo K y una biyección $\chi : K \to X$ con cualquier otro conjunto X, la aplicación $s : X \to X$ definida por $s = (\chi \times \chi)e(\chi^{-1} \times \chi^{-1})$ hace conmutar el diagrama

$$\begin{array}{ccc} K \times K & \xrightarrow{e} & K \times K \\ \downarrow{\scriptstyle \chi\times\chi} & & \downarrow{\scriptstyle \chi\times\chi} \\ X \times X & \xrightarrow{s} & X \times X \end{array},$$

de modo que X se convierte en un cuerpo cuyo uno es $\chi(1)$. Además, χ deviene un isomorfismo de cuerpos. Diremos que hemos *trasladado* a X la estructura de cuerpo de K mediante χ.

LEMA 2.30. *Si $\sigma : F \to E$ es un homomorfismo algebraico y F es infinito, entonces E tiene el mismo cardinal que F. Si F es finito, el cardinal de E es numerable.*

DEMOSTRACIÓN. Comparemos primero los cardinales de F y del anillo de polinomios $F[X]$. Éste se puede poner como $F[X] = \cup_{n\in\mathbb{N}} P_n$, donde P_n es el F–espacio vectorial de los polinomios de grado menor o igual que n. Como F–espacio vectorial, cada P_n es isomorfo al producto cartesiano F^{n+1}.

Deducimos que, si $\#F$ es finito, entonces $\#P_n$ es finito. Si $\#F$ es infinito, entonces $\#F = \#P_n$ para todo n. Por tanto, $\#F[X]$ es numerable si $\#F$ es finito, y $\#F[X] = \#F$ cuando $\#F$ es infinito. Esta última afirmación usa el hecho de que una unión numerable de conjuntos infinitos del mismo cardinal da un conjunto con igual cardinal.

La observación clave ahora es que, puesto que σ es algebraico, E es unión de conjuntos de raíces de polinomios f^σ con $f \in F[X]$. Como cada uno de estos conjuntos es finito, el cardinal de E resulta ser el mismo que el de $F[X]$. □

TEOREMA 2.31. *Existe una clausura algebraica de cada cuerpo* F.

DEMOSTRACIÓN. Tomemos un conjunto U de cardinal no numerable estrictamente mayor que el de F. Elegimos un subconjunto F_1 de U y una biyección $\sigma : F \to F_1$. Trasladamos la estructura de cuerpo de F a F_1 mediante σ.

Definamos Γ el conjunto parcialmente ordenado cuyos elementos son los pares (K, e), donde K un subconjunto de U que es un cuerpo con aplicación estructura e y que es una extensión algebraica de F_1. La relación de orden $\preceq$ en Γ viene dada declarando que $(K, e) \preceq (L, f)$ si K es un subcuerpo de L. Obviamente, Γ es no vacío, ya que contiene a F_1. Además, dado cualquier subconjunto totalmente ordenado $\mathcal{C}$ de Γ, la unión

$$M = \bigcup_{(C,c)\in\mathcal{C}} C$$

de subconjuntos de U tiene una única estructura de cuerpo que contiene a cada C como subcuerpo. De hecho, dados $x, y \in M$, puesto que $\mathcal{C}$ es un subconjunto totalmente ordenado de Γ, existe $(C, c) \in \mathcal{C}$ tal que $x, y \in C$. La suma y el producto de x, y en M se definen entonces como las correspondientes operaciones en C. Una comprobación rutinaria muestra que esta suma y producto no dependen del elemento (C, c) de $\mathcal{C}$ escogido. Los axiomas de cuerpo para estas operaciones definidas sobre M se comprueban fácilmente tras observar que cualquier conjunto finito de elementos de M, por ejemplo de tres elementos, está incluido en algún C de la cadena. El cero y el uno de M son los de F_1. De hecho, M es una extensión algebraica de de F_1. Esto se deduce fácilmente del hecho de que todas las extensiones $F_1 \leq C$ con $(C, c) \in \mathcal{C}$ lo son.

En definitiva, llamando m a la aplicación estructura de M, hemos encontrado $(M, m) \in \Gamma$ que es cota superior de todos los elementos de $\mathcal{C}$. Podemos aplicar el Lema de Zorn que nos da un elemento maximal $(\overline{F}, t)$ de Γ. Vamos a demostrar que el cuerpo $\overline{F}$ es una clausura algebraica de F.

En primer lugar, tomamos el isomorfismo $\sigma : F \to F_1$ seguido de la inclusión $F_1 \leq \overline{F}$ para obtener un homomorfismo de cuerpos, que denotamos también por $\sigma : F \to \overline{F}$. Como $(\overline{F}, t) \in \mathcal{C}$, tenemos que σ es algebraico.

Tomemos ahora cualquier homomorfismo finito de cuerpos $\tau : \overline{F} \to E$. Puesto que E es un $\overline{F}$–espacio vectorial de dimensión finita, por el Lema 2.30, tanto el cardinal de E como el de $\overline{F}$ son estrictamente menores que el de U. Existe, así, una biyección $b : E \setminus \tau(\overline{F}) \to X$ para algún subconjunto X de U disjunto con $\overline{F}$.

El siguiente paso es dotar a $\overline{F} \cup X$ de estructura de cuerpo. Para ello, vamos a trasladar la de E mediante una biyección $\chi : E \to \overline{F} \cup X$. Dicha

biyección viene dada, para $y \in E$, por

$$\chi(y) = \begin{cases} \tau^{-1}(y) & \text{si } y \in \tau(\overline{F}) \\ b(y) & \text{si } y \notin \tau(\overline{F}) \end{cases}$$

Tenemos, pues, que $\overline{F} \cup X$ es un cuerpo isomorfo a E con aplicación estructura s que hace conmutar el diagrama

$$\begin{array}{ccc} E \times E & \xrightarrow{e} & E \times E \\ \downarrow{\scriptstyle \chi\times\chi} & & \downarrow{\scriptstyle \chi\times\chi} \\ (\overline{F} \cup X) \times (\overline{F} \cup X) & \xrightarrow{s} & (\overline{F} \cup X) \times (\overline{F} \cup X), \end{array}$$

donde e es la aplicación estructura del cuerpo E. Tenemos, pues, el diagrama conmutativo

$$\begin{array}{ccc} \overline{F} \times \overline{F} & \xrightarrow{t} & \overline{F} \times \overline{F} \\ \downarrow{\scriptstyle \tau\times\tau} & & \downarrow{\scriptstyle \tau\times\tau} \\ E \times E & \xrightarrow{e} & E \times E \\ \downarrow{\scriptstyle \chi\times\chi} & & \downarrow{\scriptstyle \chi\times\chi} \\ (\overline{F} \cup X) \times (\overline{F} \cup X) & \xrightarrow{s} & (\overline{F} \cup X) \times (\overline{F} \cup X) \end{array}$$

Pero la composición $\chi\tau$ no es sino la inclusión $\overline{F} \subseteq \overline{F} \cup X$, que, en vista del diagrama anterior, es un homomorfismo de cuerpos. Esto es, tenemos la extensión de cuerpos $\overline{F} \leq \overline{F} \cup X$, que es finita puesto que la estructura de $\overline{F}$–espacio vectorial de $\overline{F} \cup X$ viene de trasladar la de $\tau(\overline{F})$–espacio vectorial de E.

Si X es no vacío, entonces tenemos que $(\overline{F} \cup X, s) \in \Gamma$ es estrictamente mayor que el elemento maximal $(\overline{F}, t)$. Por tanto, X es vacío y τ es un isomorfismo. □

Vamos a discutir finalmente la unicidad de la clausura algebraica de un cuerpo.

PROPOSICIÓN 2.32. *Sea $\tau : F \to E$ un homomorfismo algebraico y $\sigma : F \to C$ una clausura algebraica de F. Entonces existe un homomorfismo de cuerpos $\eta : E \to C$ tal que $\eta\tau = \sigma$.*

DEMOSTRACIÓN. Vamos a construir una demostración aplicando el Lema de Zorn al conjunto Λ de todos los pares (L, λ), donde L es una extensión $\tau(F) \leq L \leq E$ y $\lambda : L \to C$ es un homomorfismo de cuerpos tal que $\lambda\tau = \sigma$. El orden parcial que consideramos en Λ es $(L, \lambda) \preceq (K, \kappa)$ si $L \subseteq K$ y $\kappa_{|L} = \lambda$. Es fácil comprobar que cada subconjunto totalmente ordenado de Λ tiene una cota superior en Λ. Por el Lema de Zorn, Λ tiene algún elemento maximal (M, η). La demostración concluye comprobando que $M = E$.

Dado $a \in E$, tomamos $f = \mathrm{Irr}(a, M) \in M[X]$. Por la Proposición 2.28, C contiene una raíz de f^η. La Proposición 2.12 garantiza la existencia de un homomorfismo de cuerpos $\mu : M(a) \to C$ tal que $\mu_{|M} = \eta$. Esto es, $(M, \eta) \preceq (M(a), \mu)$. Como (M, η) es maximal en Λ, deducimos que $M(a) = M$, luego $a \in M$. Esto prueba que $E = M$. □

TEOREMA 2.33. *Si $\tau : F \to E$ y $\sigma : F \to C$ son clausuras algebraicas de un cuerpo F, entonces existe un isomorfismo de cuerpos $\eta : E \to C$ tal que $\eta\tau = \sigma$.*

DEMOSTRACIÓN. Por la Proposición 2.32, existe un homomorfismo de cuerpos $\eta : E \to C$ tal que $\eta\tau = \sigma$. La demostración se completa mostrando que η es sobreyectivo. Dado $c \in C$, la extensión $\eta(E) \leq \eta(E)(c)$ es finita porque c es algebraico sobre $\tau(F)$ y, por ende, sobre $\eta(E)$. El homomorrfismo η compuesto con la inclusión $\eta(E) \leq \eta(E)(c)$ resulta ser finito. Como $\tau : F \to E$ es una clausura algebraica, dicho homomorfimo es un isomorfismo, lo cual sólo es posible si $\eta(E) = \eta(E)(c)$, esto es, $c \in \eta(E)$. Por tanto, η es sobreyectivo. □

2.5. Ejercicios

EJERCICIO 30. Demostrar que, si F es un cuerpo, entonces cualquier subgrupo finito de $F^\times$ es cíclico. Deducimos que, en particular, $\mathbb{F}_q^\times$ es un grupo cíclico de orden $q-1$. (Pista: usar la descomposición cíclica de un grupo finito abeliano).

EJERCICIO 31. Pongamos $\mathbb{F}_4 = \mathbb{F}_2(a)$ con $a^2+a+1 = 0$. Comprobar que $\mathbb{F}_{16}$ puede presentarse como $\mathbb{F}_{16} = \mathbb{F}_2(b)$ donde $b^4 + b + 1 = 0$. Determinar todos los homomorfismos de cuerpos $\mathbb{F}_4 \to \mathbb{F}_{16}$ en función de a y b.

EJERCICIO 32. Demostrar los anillos $\mathbb{Z}[i]/\langle 3\rangle$ y $\mathbb{F}_3[X]/\langle X^2 + X + 2\rangle$ son isomorfos, sin necesidad de dar un isomorfismo concreto. ¿Serías capaz de darlo? ¿Y de calcularlos todos?

EJERCICIO 33. Realizar las siguientes tareas:

1. Probar que $\sqrt{3} \in \mathbb{Q}(\sqrt{1+2\sqrt{3}})$.
2. Calcular $\mathrm{Irr}(\sqrt{1+2\sqrt{3}}, \mathbb{Q}(\sqrt{3}))$.
3. Describir todos los homomorfismos de cuerpos de $\mathbb{Q}(\sqrt{1+2\sqrt{3}})$ en $\mathbb{C}$.
4. Calcular $\mathrm{Irr}(\sqrt{1+2\sqrt{3}}, \mathbb{Q})$ y sus raíces en $\mathbb{C}$.

EJERCICIO 34. ¿Son los cuerpos $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{3})$ isomorfos?.

EJERCICIO 35. Demostrar que si $\lambda : F \to E$ es un homomorfismo algebraico de cuerpos, entonces las clausuras algebraicas de F y E son isomorfas.

Capítulo 3

Extensiones de Galois

En este capítulo veremos los fundamentos de la Teoría de Galois de extensiones finitas de cuerpos. Indagaremos en las propiedades de los cuerpos de descomposición de los polinomios separables, que darán la noción de extensión de Galois finita. La Conexión de Galois parametrizará todas las subextensiones de una extensión de Galois en términos del grupo de automorfismos de la extensión (llamado grupo de Galois). Como aplicación, demostraremos el Teorema Fundamental del Álgebra, que dice que el cuerpo de los números complejos es algebraicamente cerrado.

3.1. Extensiones de Galois

Comencemos consignando una consecuencia de lo visto en el capítulo anterior.

PROPOSICIÓN 3.1. *Si* $F \leq K$ *es finita, entonces* $\#\mathrm{Aut}_F(K) \leq [K : F]$.

DEMOSTRACIÓN. Llamemos $\iota : F \to K$ a la inclusión. Como, en virtud de la Observación 2.21, $\mathrm{Aut}_F(K) = \mathrm{Ex}(\iota, \iota)$, la desigualdad se sigue de la Proposición 2.15. □

Así, cada extensión finita de cuerpos da lugar a un grupo finito. Vamos a describir un proceso en sentido contrario.

Dado un subgrupo $G \subseteq \mathrm{Aut}(K)$, definimos el subconjunto

$$K^G = \{a \in K : \sigma(a) = a, \text{ para todo } \sigma \in G\},$$

que es un subcuerpo de K llamado *subcuerpo fijo bajo* G.

PROPOSICIÓN 3.2 (Artin). *Si* G *es un subgrupo finito de* $\mathrm{Aut}(K)$, *entonces* $[K : K^G] \leq \#G$.

DEMOSTRACIÓN. Pongamos $n = \#G$ y

$$G = \{\sigma_1, \ldots, \sigma_n\}.$$

Tomemos $\alpha_1, \ldots, \alpha_m \in K$ con $m > n$. Queremos demostrar que tales elementos son K^G–linealmente dependientes.

Consideremos la matriz $A = (\sigma_j(\alpha_i))$ de tamaño $m \times n$ con coeficientes en K. Como $n < m$, el rango de A es menor que m, así que existe algún vector no nulo $v = (v_1, \ldots, v_m) \in K^m$ tal que $vA = 0$. Podemos tomar v con el número de componentes no nulas mínimo. Además, podemos suponer[1] que se tiene que $0 \neq v_l \in K^G$ para algún índice l.

Supongamos que $v_{l'} \neq \sigma_k(v_{l'})$ para alguna pareja de índices l', k. Escribamos

$$\sigma_k(v) = (\sigma_k(v_1), \ldots, \sigma_k(v_m)).$$

[1] Por ejemplo, podemos obtener un tal v con $v_l = 1$ para alguna componente de v.

La igualdad $vA = 0$ es equivalente a

$$\sum_i v_i \sigma_j(\alpha_i) = 0, \qquad j = 1, \dots, n. \tag{3.1}$$

Si aplicamos σ_k a la anterior igualdad, obtenemos que

$$\sum_i \sigma_k(v_i)\sigma_k\sigma_j(\alpha_i) = 0, \qquad j = 1, \dots, n.$$

Como $G = \{\sigma_k\sigma_1, \dots, \sigma_k\sigma_n\}$, resulta que $\sigma_k(v)A = 0$. Así,

$$(v - \sigma_k(v))A = 0.$$

Pero $v - \sigma_k(v) \neq 0$ y este vector tiene, al menos, una componente nula más que v (concretamente, la l-ésima). Esta contradicción nos muestra que $v_{l'} \in K^G$ para todo l'. Lo que, tomando en (3.1) la igualdad correspondiente al automorfismo identidad, da la relación de dependencia lineal sobre K^G

$$v_1\alpha_1 + \cdots + v_m\alpha_m = 0.$$

□

Queremos ahora ver cómo se comporta la correspondencia descrita entre extensiones finitas y grupos finitos.

LEMA 3.3. *Para un cuerpo K, son ciertas las siguientes afirmaciones.*

1. *Si $H \subseteq G$ son subgrupos de $\mathrm{Aut}(K)$, entonces $K^H \geq K^G$.*
2. *Si $F \leq E$ son subcuerpos de K, entonces $\mathrm{Aut}_F(K) \supseteq \mathrm{Aut}_E(K)$.*
3. *Si G es subgrupo de $\mathrm{Aut}(K)$, entonces $G \subseteq \mathrm{Aut}_{K^G}(K)$.*
4. *Si F es subcuerpo de K, entonces $F \leq F^{\mathrm{Aut}_F(K)}$.*

DEMOSTRACIÓN. Comprobaciones rutinarias. □

TEOREMA 3.4. *Si G es un subgrupo finito de $\mathrm{Aut}(K)$, entonces $[K : K^G] = \#G$ y $G = \mathrm{Aut}_{K^G}(K)$.*

DEMOSTRACIÓN. Sabemos, por el Lema 3.3, que $G \subseteq \mathrm{Aut}_{K^G}(K)$. Aplicando las proposiciones 3.2 y 3.1, obtenemos

$$\#G \leq \#\mathrm{Aut}_{K^G}(K) \leq [K : K^G] \leq \#G,$$

luego $G = \mathrm{Aut}_{K^G}(K)$. □

El siguiente ejemplo puede ser un buen entrenamiento para lo que sigue.

EJEMPLO 3.5. Tomemos $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$, el cuerpo de descomposición de $X^3 - 2 \in \mathbb{Q}[X]$ cuyo grupo de automorfismos describimos en 2.23. Usaremos dicha descripción (y notación) para calcular los subgrupos de $\mathrm{Aut}(K)$. En este caso, en vista del Teorema de Lagrange, todos los subgrupos propios son cíclicos, ya que tienen orden primo, así que basta con calcular el orden de los elementos del grupo $\mathrm{Aut}(K)$. De esta manera, obtendremos que los subgrupos son

$$\mathrm{Aut}(K),\ \langle\eta_{11}\rangle = \langle\eta_{21}\rangle,\ \langle\eta_{02}\rangle,\ \langle\eta_{12}\rangle,\ \langle\eta_{22}\rangle,\ \langle\mathrm{id}\rangle.$$

El segundo de ellos tiene orden 3, mientras que los tres siguientes tienen cardinal 2. Calculemos los subcuerpos fijos de K por cada uno de estos subgrupos.

Obviamente, $K^{\langle\mathrm{id}\rangle} = K$. En lo que concierne a $K^{\mathrm{Aut}(K)}$ tenemos que, por el Teorema 3.4, $[K : K^{\mathrm{Aut}(K)}] = \#\mathrm{Aut}(K) = 6$, luego la única salida es $K^{\mathrm{Aut}(K)} = \mathbb{Q}$.

Vayamos con los subgrupos propios. Respecto a $K^{\langle \eta_{11} \rangle}$, observemos que $\eta_{11}(\omega) = \omega$, luego $\omega \in K^{\langle \eta_{11} \rangle}$. De esta forma, $\mathbb{Q}(\omega) \leq K^{\langle \eta_{11} \rangle}$. Por otra parte, $[K : \mathbb{Q}(\omega)] = 3$ y, por el Teorema 3.4, $[K : K^{\langle \eta_{11} \rangle}] = \#\langle \eta_{11} \rangle = 3$. En vista del Lema de la torre, hemos de admitir que $K^{\langle \eta_{11} \rangle} = \mathbb{Q}(\omega)$.

Razonamientos paralelos a éste permiten calcular el resto de subcuerpos invariantes de K, obteniendo la siguiente lista, que incluye sólo los casos propios:

$$K^{\langle \eta_{11} \rangle} = \mathbb{Q}(\omega),\ K^{\langle \eta_{02} \rangle} = \mathbb{Q}(\sqrt[3]{2}),\ K^{\langle \eta_{12} \rangle} = \mathbb{Q}(\omega^2 \sqrt[3]{2}),\ K^{\langle \eta_{22} \rangle} = \mathbb{Q}(\omega \sqrt[3]{2}). \tag{3.2}$$

Más adelante, veremos que todos los subcuerpos de K son fijos por subgrupos de $\mathrm{Aut}(K)$, por lo que la anterior es una descripción completa de los subcuerpos de K.

EJERCICIO 36. Demostrar que $\omega + \sqrt[3]{2}$ no pertenece a ninguno de los cuerpos de la lista (3.2).

Seguidamente, vamos a exponer algunos conceptos y hechos constitutivos de las que llamaremos extensiones de Galois.

DEFINICIÓN 3.6. Un polinomio no constante $f \in F[X]$ se dice *separable* si todas sus raíces en un cuerpo de descomposición suyo son simples, es decir, tiene $\deg f$ raíces distintas ahí.

OBSERVACIÓN 3.7. Veamos que $f \in F[X]$ es separable si, y sólo si, f es coprimo con su polinomio derivado f'. Denotemos por $d \in F[X]$ el máximo común divisor de f y f'. Si $d = 1$, entonces, por la identidad de Bezout, f y f' no tienen ninguna raíz común en el cuerpo de descomposición E de f. Por [**2**, Proposición 4.45], f no tiene raíces múltiples. Si d es no constante, tomo una raíz suya en E, que es también raíz de f', ya que d es un divisor tanto de f como de f'. Por tanto, f y f' tienen alguna raíz común en E y, de nuevo por [**2**, Proposición 4.45], f tiene raíces múltiples en E.

EJEMPLO 3.8. Si F es de característica 0, entonces todo polinomio irreducible $f \in F[X]$ es separable. Esto es porque $f' \neq 0$ y tiene grado menor que el de f y, por ser f irreducible, deducimos que $\mathrm{mcd}(f, f') = 1$.

EJEMPLO 3.9. El polinomio $X^q - X \in \mathbb{F}_p[X]$ para $q = p^n$ es separable.

EJEMPLO 3.10. Sea $\mathbb{F}_p(t)$ el cuerpo de fracciones del anillo de polinomios $\mathbb{F}_p[t]$. Entonces el polinomio irreducible[2] $f = X^p - t \in \mathbb{F}_p(t)[X]$ no es separable, ya que $f' = 0$.

DEFINICIÓN 3.11. Una extensión algebraica $F \leq K$ es *separable* si el polinomio $\mathrm{Irr}(\alpha, F)$ es separable para todo $\alpha \in K$.

EJEMPLO 3.12. Toda extensión algebraica de cuerpos de característica cero es separable.

DEFINICIÓN 3.13. Una extensión algebraica $F \leq K$ es *normal* si $\mathrm{Irr}(\alpha, F)$ se descompone como producto de polinomios lineales en $K[X]$ para todo $\alpha \in K$.

EJEMPLO 3.14. La extensión $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ no es normal (aunque es separable).

El siguiente teorema es la piedra angular de la Teoría de Galois.

[2] Aplicar el criterio de Eisenstein

TEOREMA 3.15. *Para una extensión de cuerpos* $F \leq K$*, las siguientes afirmaciones son equivalentes.*

(I) K *es cuerpo de descomposición de un polinomio separable* $f \in F[X]$*;*
(II) $F \leq K$ *es finita y* $F = K^{Aut_F(K)}$*;*
(III) $F = K^G$ *para un subgrupo finito* G *de* $Aut(K)$*;*
(IV) $F \leq K$ *es finita, normal y separable.*

DEMOSTRACIÓN. (I) $\Rightarrow$ (II). Sea $f \in F[X]$ separable tal que K es cuerpo de descomposición de f. Sabemos que $F \leq K$ es finita. Tenemos que $F' = K^{Aut_F(K)} \geq F$. Aplicando el Teorema 3.4 para $G = Aut_F(K)$, obtenemos que $Aut_F(K) = Aut_{F'}(K)$. Como K es también cuerpo de descomposición de $f \in F'[X]$, la Proposición 2.22 nos da que

$$[K : F] = \#Aut_F(K) = \#Aut_{F'}(K) = [K : F'],$$

de donde $F' = F$.

(II) $\Rightarrow$ (III). Tomamos $G = Aut_F(K)$ que es finito por la Proposición 3.1.

(III) $\Rightarrow$ (IV). Por la Proposición 3.2, $F \leq K$ es finita. Sea $\alpha \in K$, y $h = Irr(\alpha, F)$. Tomamos $\{\alpha_1, \ldots, \alpha_t\}$ la órbita de α bajo la acción de G sobre K, y definamos un polinomio $g \in K[X]$ por

$$g = \prod_{i=1}^{t}(X - \alpha_i) = \sum_{j=0}^{t} a_j X^j.$$

Para cada $\sigma \in G$, tenemos que

$$\sum_{j=1}^{t} \sigma(a_j)X^j = g^\sigma = \prod_{i=1}^{t}(X - \alpha_i)^\sigma = \prod_{i=1}^{t}(X - \sigma(\alpha_i)) = g,$$

ya que σ permuta los elementos $\alpha_1, \ldots, \alpha_t$. Por tanto, $a_i \in K^G = F$ para todo $i = 1, \ldots, t$. Esto es, $g \in F[X]$. Como $g(\alpha) = 0$, deducimos que h divide a g en $F[X]$. Ahora, aplicando cada $\sigma \in G$ a la igualdad $h(\alpha) = 0$, obtenemos que todos los elementos $\alpha_1, \ldots, \alpha_t$, que son distintos por constituir una órbita de la acción de G sobre K, son raíces de h. Por tanto, h tiene en mismo grado mayor o igual que el de g. Esto sólo es posible si $h = g$. Así, h se factoriza en $K[X]$ como producto de polinomios lineales distintos.

(IV) $\Rightarrow$ (I). Como $F \leq K$ es finita, podemos escribir $K = F(\alpha_1, \ldots, \alpha_n)$, para $\alpha_1, \ldots, \alpha_n \in K$ algebraicos sobre F. Consideremos $f \in F[X]$ el producto de los polinomios $f_i = Irr(\alpha_i, F)$, eliminando repeticiones. Como cada f_i se factoriza como producto de factores lineales distintos en $K[X]$, por ser $F \leq K$ separable, obtenemos que K es cuerpo de descomposición de f. Como $F \leq K$ es separable, todas las raíces de cada f_i son simples. Además, por ser f_i y f_j polinomios irreducibles distintos para $i \neq j$, cada uno de estos pares son coprimos, por lo que no tienen raíces comunes. Concluimos que f es separable. □

OBSERVACIÓN 3.16. En la demostración del Teorema 3.15, hemos visto que, si $F = K^G$ para G un subgrupo finito de $Aut(K)$, entonces $Irr(\alpha, F) = \prod_i (X - \alpha_i)$, donde $\{\alpha_1, \ldots, \alpha_t\}$ es la órbita de α bajo la acción de G. Estos elementos son los llamados *conjugados de* α bajo G.

DEFINICIÓN 3.17. Si $F \leq K$ satisface las condiciones equivalentes del Teorema 3.15, entonces diremos que es una *extensión de Galois*, al grupo $Aut_F(K)$ se le llama *Grupo de Galois* de la extensión.

COROLARIO 3.18. *Si la característica de* F *es cero y* K *es cuerpo de descomposición de cualquier* $f \in F[X]$*, entonces* $F \leq K$ *es Galois.*

DEMOSTRACIÓN. Tomamos la descomposición $f = p_1^{e_1} \cdots p_r^{e_r}$, para $p_i \in F[X]$ irreducibles distintos. Entonces K es cuerpo de descomposición de $g = p_1 \cdots p_r$, que es un polinomio separable. □

COROLARIO 3.19. *Si $F \leq K$ es una extensión de Galois y E es un subcuerpo de K tal que $F \leq E \leq K$, entonces $E \leq K$ es de Galois.*

DEMOSTRACIÓN. Por el Teorema 3.15, K es cuerpo de descomposición de un polinomio separable $f \in F[X]$. Viendo $f \in E[X]$, obtenemos que K sigue siendo cuerpo de descomposición de f. Por tanto, $E \leq K$ es de Galois. □

TEOREMA 3.20. *Toda extensión de cuerpos finitos es de Galois con grupo de Galois cíclico.*

DEMOSTRACIÓN. Sea $F \leq K$ una extensión de cuerpos finitos. Denotemos por p a su característica. De acuerdo con la Proposición 2.19, K es cuerpo de descomposición un polinomio $X^q - X \in \mathbb{F}_p[X]$. Como la derivada formal del mismo es -1, dicho polinomio es separable. Así, la extensión $\mathbb{F}_p \leq K$ es de Galois. El Corolario 3.19 nos da que $F \leq K$ es de Galois.

El Teorema 2.24 muestra aue $\mathrm{Aut}(K)$ es cíclico. Puesto que $\mathrm{Aut}_F(K)$ es un subgrupo suyo, ha de ser también cíclico. □

EJEMPLO 3.21. Consideremos la extensión $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{5}, i\sqrt{5}) = E$. Si se tratara de una extensión de Galois, entonces todas las raíces de $\mathrm{Irr}(\sqrt[3]{5}, \mathbb{Q}) = X^3 - 5$ han de estar en E. Así, $\sqrt[3]{5}e^{i2\pi/3} \in E$, de donde $e^{i2\pi/3} \in E$. Puesto que $e^{i2\pi/3} = -1/2 + i\sqrt{3}/2$, deducimos que $i\sqrt{3} \in E$. Pero, entonces, $\mathbb{Q}(i\sqrt{5}, i\sqrt{3}) \leq E$. Queremos ver que esta inclusión lleva a una contradicción.

Puesto que $[E : \mathbb{Q}] = 6$, ya que $i\sqrt{5} \notin \mathbb{Q}(\sqrt[3]{5})$, deducimos que $[\mathbb{Q}(i\sqrt{5}, i\sqrt{3}) : \mathbb{Q}]$ es un divisor de 6. La contradicción consiste en que $[\mathbb{Q}(i\sqrt{5}, i\sqrt{3}) : \mathbb{Q}] = 4$. Comprobemos, pues, esta igualdad. Para lo que basta ver que $i\sqrt{3} \notin \mathbb{Q}(i\sqrt{5})$. Escribimos $i\sqrt{3} = a + bi\sqrt{5}$ con $a, b \in \mathbb{Q}$, entonces $a = 0$, obtenemos que b es raíz de $5X^2 - 3$, imposible, ya que ese polinomio es irreducible en $\mathbb{Q}[X]$ por el criterio de Eisenstein.

La conclusión de nuestros razonamientos es que $\mathbb{Q} \leq E$ no es una extensión de Galois.

EJERCICIO 37. Calcular $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{5}, i\sqrt{5}))$.

3.2. Teorema fundamental de la Teoría de Galois

Dada una extensión de cuerpos de nuestro interés $F \leq K$, a los subcuerpos E de K tales que $F \leq E \leq K$ se les llama *subextensiones de* $F \leq K$. Denotamos a este conjunto por $\mathrm{Subex}(F \leq K)$, y lo consideramos ordenado por inclusión.

Recordemos que, si H es un subgrupo de un grupo G, el índice de H en G, denotado por $(G : H)$, es el número de clases laterales de G con respecto de H. Las clases laterales pueden tomarse a izquierda o a derecha, el índice no cambia. El conjunto de los subgrupos de G, ordenado por inclusión, será denotado como $\mathrm{Subgr}(G)$.

TEOREMA 3.22. *Sea $F \leq K$ una extensión de Galois con grupo de Galois $G = \mathrm{Aut}_F(K)$. La aplicación*

$$\mathrm{Subgr}(G) \to \mathrm{Subex}(F \leq K), \qquad (H \mapsto K^H)$$

es un anti-isomorfismo de conjuntos ordenados con aplicación inversa

$$\mathrm{Subex}(F \leq K) \to \mathrm{Subgr}(G), \qquad (E \mapsto \mathrm{Aut}_E(K)).$$

Además, para subgrupos $H_1 \subseteq H_2$ *de* G*, y subextensiones* $F \leq E_2 \leq E_1 \leq K$ *correspondientes según la anterior biyección, se tiene*

$$(H_2 : H_1) = [E_1 : E_2].$$

DEMOSTRACIÓN. Observemos primero que G es finito, en virtud del Teorema 3.15.

Dado $H \in Subgr(G)$, el Teorema 3.4 asegura que $Aut_{K^H}(K) = H$. Por otra parte, dado $E \in Subex(F \leq K)$, tenemos que $E = K^{Aut_E(K)}$, ya que $E \leq K$ es de Galois de acuerdo con el Corolario 3.19. Esto demuestra que las aplicaciones del enunciado son biyectivas e inversas entre sí. En virtud del Lema 3.3, resultan anti-isomorfismos de conjuntos ordenados.

Dados ahora $H_1 \subseteq H_2$ subgrupos de G, las subextensiones correspondientes son $E_1 = K^{H_1}$, $E_2 = K^{H_2}$. Por el Teorema 3.4, $[K : E_i] = \#H_i$, para $i = 1, 2$. Así,

$$\#H_2 = [K : E_2] = [K : E_1][E_1 : E_2] = \#H_1[E_1 : E_2].$$

De donde $[E_1 : E_2] = (H_2 : H_1)$. □

DEFINICIÓN 3.23. A la biyección establecida en el Teorema 3.22 la llamaremos *conexión de Galois* para la extensión de Galois $F \leq K$.

EJEMPLO 3.24. El el Ejercicio 3.5 fueron descritos los subcuerpos de $\mathbb{Q}(\sqrt[3]{2}, \omega)$ fijos bajo cada uno de los subgrupos de $Aut(\mathbb{Q}(\sqrt[3]{2}, \omega))$, para ω una raíz cúbica primitiva de la unidad compleja. Ahora sabemos, puesto que la extensión $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}, \omega)$ es de Galois, que esos son todos los subcuerpos del citado cuerpo.

EJEMPLO 3.25. Vamos a describir los subcuerpos de $\mathbb{F}_q$, para $q = p^n$. Sabemos, por el Corolario 3.20 y el Teorema 2.24, que la extensión $\mathbb{F}_p \leq \mathbb{F}_q$ es de Galois y que $G = Aut(\mathbb{F}_q) = Aut_{\mathbb{F}_p}(\mathbb{F}_q)$ es cíclico de orden n generado por el automorfismo de Frobenius τ. Por tanto, los subgrupos de G son de la forma $\langle \tau^d \rangle$ para d un divisor de n. Según el Teorema 3.22, los subcuerpos de $\mathbb{F}_q$ son, exactamente, los subcuerpos fijos para estos subgrupos. Así, para cada divisor d de n tenemos el subcuerpo fijo $\mathbb{F}_q^{\langle \tau^d \rangle}$ y $[\mathbb{F}_q^{\langle \tau^d \rangle} : \mathbb{F}_p] = (G : \langle \tau^d \rangle) = d$. Por tanto, para cada divisor d de n existe un único subcuerpo de $\mathbb{F}_q$ que tiene p^d elementos, y éstos son todos los subcuerpos de $\mathbb{F}_q$.

EJERCICIO 38. Supongamos que hemos expresado

$$\mathbb{F}_{16} = \{0, a, a^2, \cdots, a^{15}\}.$$

Describir explícitamente, usando potencias de a, todos los subcuerpos de $\mathbb{F}_{16}$.

Vamos ahora a caracterizar qué subextensiones de una extensión de Galois están ligadas, por la correspondencia de Galois, con subgrupos normales del grupo de Galois.

LEMA 3.26. *Sea* $F \leq K$ *una extensión de Galois con grupo de Galois* G*,* H *un subgrupo de* G *y* E *una subextensión de* $F \leq K$*. Si* H *y* E *están en correspondencia por la conexión de Galois, y* $\sigma \in G$*, entonces* $\sigma H \sigma^{-1}$ *y* $\sigma(E)$ *lo están también.*

DEMOSTRACIÓN. A partir de $E = K^H$ hemos de mostrar que $K^{\sigma H \sigma^{-1}} = \sigma(K^H)$. En efecto, dado $\alpha \in K$, tenemos que

$$\begin{aligned}\alpha \in K^{\sigma H \sigma^{-1}} &\Leftrightarrow \sigma\tau\sigma^{-1}(\alpha) = \alpha,\ \forall \tau \in H \\ &\Leftrightarrow \tau\sigma^{-1}(\alpha) = \sigma^{-1}(\alpha),\ \forall \tau \in H \Leftrightarrow \sigma^{-1}(\alpha) \in K^H \Leftrightarrow \alpha \in \sigma(K^H).\end{aligned}$$

□

TEOREMA 3.27. *Sea $F \leq K$ una extensión de Galois con grupo de Galois G. Tomemos H un subgrupo de G y E una subextensión de $F \leq K$ correspondientes bajo la conexión de Galois. Entonces H es normal en G si, y sólo si, $F \leq E$ es de Galois. En tal caso, $\mathrm{Aut}_F(E)$ es isomorfo a G/H.*

DEMOSTRACIÓN. Si H es normal, entonces, según el Lema 3.26, $\sigma(E) = E$ para todo $\sigma \in G$. Por tanto, tenemos un homomorfismo de grupos $r : G \to \mathrm{Aut}_F(E)$ dado por $r(\sigma) = \sigma_{|E}$. Su núcleo es $\mathrm{Aut}_E(K) = H$. Ahora,

$$[E : F] = (G : H) = \#\mathrm{Im} r \leq \#\mathrm{Aut}_F(E) \leq [E : F].$$

Por tanto, r es sobreyectivo y tenemos definido un isomorfismo de grupos $G/H \cong \mathrm{Aut}_F(E)$. Pero, además, dado $\alpha \in E^{\mathrm{Aut}_F(E)}$, entonces, para todo $\sigma \in G$, se tiene que $\alpha = r(\sigma)(\alpha) = \sigma(\alpha)$, luego $\alpha \in K^G = F$. De modo que $F = E^{\mathrm{Aut}_F(E)}$ y $F \leq E$ es de Galois por el Teorema 3.15.

Supongamos ahora que $F \leq E$ es Galois. Así, $E = F(\alpha_1, \ldots, \alpha_n)$ para un polinomio separable $f \in F[X]$ con $f = \prod_{i=1}^n (X - \alpha_i)$. Dado $\sigma \in G$, tenemos

$$f = f^\sigma = \prod_{i=1}^n (X - \sigma(\alpha_i)).$$

Luego $\sigma(\alpha_i) = \alpha_j \in E$, para cada i. Por tanto, $\sigma(E) = E$. Del Lema 3.26 deducimos que $K^H = E = \sigma(E) = K^{\sigma H \sigma^{-1}}$. Por la conexión de Galois, $H = \sigma H \sigma^{-1}$ y H es normal en G. □

EJEMPLO 3.28. Consideremos la cuártica $f = X^4 - 2X^2 - 2 \in \mathbb{Q}[X]$. Para calcular las raíces complejas de f, pensemos que, si s es una de ellas, entonces s^2 es raíz de $X^2 - 2X - 2$. Resolviendo la ecuación cuadrática correspondiente, vemos que las raíces de f son $\alpha, -\alpha, \beta, -\beta$, donde

$$\alpha = \sqrt{\sqrt{3} + 1}, \quad \beta = i\sqrt{\sqrt{3} - 1}.$$

Observemos que $\alpha\beta = i\sqrt{2}$. Por tanto, el cuerpo de descomposición de f es

$$K = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \alpha\beta) = \mathbb{Q}(\sqrt{\sqrt{3} + 1}, i\sqrt{2}).$$

Como f es irreducible en virtud del criterio de Eisenstein, $\mathrm{Irr}(\alpha, \mathbb{Q}) = f$, por lo que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Ahora, $i\sqrt{2}$ es raíz de $X^2 + 2$, polinomio cuadrático que es irreducible sobre $\mathbb{Q}(\alpha)$, al no tener raíces ahí. El Lema de la torre permite así deducir que

$$[K : \mathbb{Q}] = 8.$$

Puesto que K es cuerpo de descomposición de un polinomio en característica cero, la extensión $\mathbb{Q} \leq K$ es de Galois (Corolario 3.18), de donde

$$\#\mathrm{Aut}_{\mathbb{Q}}(K) = 8.$$

Calculemos estos ocho automorfismos usando la Proposición 2.12. Así, los homomorfismos de cuerpos de $\mathbb{Q}(\alpha)$ a K están determinados por

$$\eta_0 : \alpha \mapsto \alpha, \quad \eta_1 : \alpha \mapsto -\alpha, \quad \eta_2 : \alpha \mapsto \beta, \quad \eta_3 : \alpha \mapsto -\beta,$$

puesto que $f \in \mathbb{Q}[X]$ es irreducible.

Cada uno de ellos se extiende a dos automorfismos de K, correspondientes a sendas raíces del polinomio irreducible $X^2+2 \in \mathbb{Q}(\alpha)$, descritos por

$$\eta_{jk} : \begin{cases} \alpha \mapsto \eta_j(\alpha) \\ \alpha\beta \mapsto (-1)^k \alpha\beta, \end{cases}$$

para $j = 0,1,2,3; k = 0,1$.

La extensión cuadrática $\mathbb{Q}(i\sqrt{2})$, a la luz del Teorema 3.27, por ser de Galois, determina el subgrupo normal de $\mathrm{Aut}_{\mathbb{Q}}(K)$ dado por

$$\mathrm{Aut}_{\mathbb{Q}(i\sqrt{2})} = \{\eta_{j0} : j = 0,1,2,3\}.$$

La siguiente tabla recoge el orden de todos los elementos de $\mathrm{Aut}_{\mathbb{Q}}(K)$.

η_{00}	η_{10}	η_{20}	η_{30}	η_{01}	η_{11}	η_{21}	η_{31}
1	2	2	2	2	2	4	4

A modo de ilustración, calculamos el orden de η_{20}, llevando pautas similares el resto:

$$\eta_{20}^2(\alpha) = \eta_{20}(\beta) = \eta_{20}(\alpha\beta/\alpha) = \eta_{20}(\alpha\beta)/\eta_{20}(\alpha) = \alpha\beta/\beta = \alpha.$$

Como $\eta_{20}^2(\alpha\beta) = \alpha\beta$, deducimos que $\eta_{20}^2 = \eta_{00}$, lo que muestra que el orden de η_{20} es 2.

Del conocimiento del orden de cada elemento del grupo de 8 elementos $\mathrm{Aut}_{\mathbb{Q}}(K)$ colegimos que es isomorfo a D_4, ya que éste es el único de dicho cardinal con 5 elementos de orden 2. Sabemos que este grupo tiene tres subgrupos de orden 4, que se corresponderán por la conexión de Galois con las tres extensiones de grado 2 de $\mathbb{Q}$ contenidas en K. Aparte de la ya descrita $\mathbb{Q}(i\sqrt{2})$, tenemos las siguientes dos: $\mathbb{Q}(\sqrt{3})$ y $\mathbb{Q}(i\sqrt{6})$. La primera, como ya hemos observado, se corresponde con el grupo $\langle \eta_{10}, \eta_{20} \rangle$, isomorfo al grupo de Klein. Podemos escribir esta relación como

$$K^{\langle \eta_{10}, \eta_{20} \rangle} = \mathbb{Q}(i\sqrt{2}).$$

Observemos que $\sqrt{3} = \alpha^2 - 1$, lo que muestra que este número queda fijo por los automorfismos $\eta_{00}, \eta_{10}, \eta_{01}, \eta_{11}$. Como, en vista siempre de la conexión de Galois, el subgrupo correspondiente a la extensión cuadrática $\mathbb{Q} \leq \mathbb{Q}(\sqrt{3})$ ha de tener 4 elementos, deducimos que los automorfismos listados forman dicho subgrupo. Puesto que todos tienen orden un divisor de 2, se trata de un grupo ismorfo al de Klein, así que generado por cualesquier par de sus elementos de orden 2. En definitiva, podemos escribir

$$K^{\langle \eta_{10}, \eta_{01} \rangle} = \mathbb{Q}(\sqrt{3}).$$

El tercer subgrupo de orden 4 ha de ser el cíclico, con generador η_{21}. Observemos que

$$\eta_{21}(\sqrt{3}) = \eta_{21}(\alpha^2 - 1) = \eta_{21}(\alpha)^2 - 1 = \beta^2 - 1 = -\sqrt{3}.$$

Por tanto,

$$\eta_{21}(i\sqrt{6}) = \eta_{21}(i\sqrt{2})\eta_{21}(\sqrt{3}) = (-i\sqrt{2})(-\sqrt{3}) = i\sqrt{6},$$

lo que muestra no sólo que $\mathbb{Q}(i\sqrt{6})$ es un subcuerpo distinto de los dos extensiones cuadráticas $\mathbb{Q}(i\sqrt{2})$ y $\mathbb{Q}(\sqrt{3})$ sino que, además,

$$K^{\langle \eta_{21} \rangle} = \mathbb{Q}(i\sqrt{6}).$$

Las subextensiones de grado 4 están en correspondencia con los subgrupos de orden 2, así que hay, exactamente, 5. Como α y β son números de grado 4 sobre $\mathbb{Q}$, tenemos que dos de ellas son $\mathbb{Q}(\alpha)$ y $\mathbb{Q}(\beta)$. Como

$\eta_{01}(\alpha) = \alpha$, tenemos que $\alpha \in K^{\langle \eta_{01} \rangle}$. La conexión de Galois me dice que la segunda extensión de $\mathbb{Q}$ es de grado 4, así que deducimos que

$$K^{\langle \eta_{01} \rangle} = \mathbb{Q}(\alpha).$$

Por otra parte,

$$\eta_{11}(\beta) = \eta_{11}(\alpha\beta/\alpha) = -\alpha\beta/(-\alpha) = \beta,$$

lo que implica, por un argumento similar, que

$$K^{\langle \eta_{11} \rangle} = \mathbb{Q}(\beta).$$

La extensión $\mathbb{Q} \leq \mathbb{Q}(i\sqrt{2}, \sqrt{3})$ es la menor que contiene a $K^{\langle \eta_{10}, \eta_{20} \rangle}$ y a $K^{\langle \eta_{10}, \eta_{01} \rangle}$, de modo que, bajo la conexión de Galois, ha de corresponder al mayor subgrupo contenido en $\langle \eta_{10}, \eta_{20} \rangle$ y $\langle \eta_{10}, \eta_{01} \rangle$, esto es, la intersección de ambos. Tenemos, pues,

$$K^{\langle \eta_{10} \rangle} = \mathbb{Q}(i\sqrt{2}, \sqrt{3}).$$

Nos faltan dos extensiones de grado 4, correspondientes a los subgrupos $\langle \eta_{20} \rangle$ y $\langle \eta_{30} \rangle$.

Observemos que

$$\eta_{20}(\alpha + \beta) = \beta + \eta_{20}(\alpha\beta/\alpha) = \beta + \alpha\beta/\beta = \beta + \alpha.$$

Por tanto, $\mathbb{Q}(\alpha+\beta) \leq K^{\langle \eta_{20} \rangle}$. Por la Conexión de Galois, $\langle \eta_{20} \rangle \subseteq \mathrm{Aut}_{\mathbb{Q}(\alpha+\beta)}(K)$. Por tanto, $\mathrm{Aut}_{\mathbb{Q}(\alpha+\beta)}(K)$ puede adoptar tres valores: $\mathrm{Aut}(K), \langle \eta_{10}, \eta_{20} \rangle$ o $\langle \eta_{20} \rangle$. La primera opción queda excluida porque $\alpha + \beta \notin \mathbb{Q}$. Observemos que

$$\eta_{10}(\alpha + \beta) = -\alpha + \eta_{10}(\frac{\alpha\beta}{\alpha}) = -\alpha - \beta \neq \alpha + \beta,$$

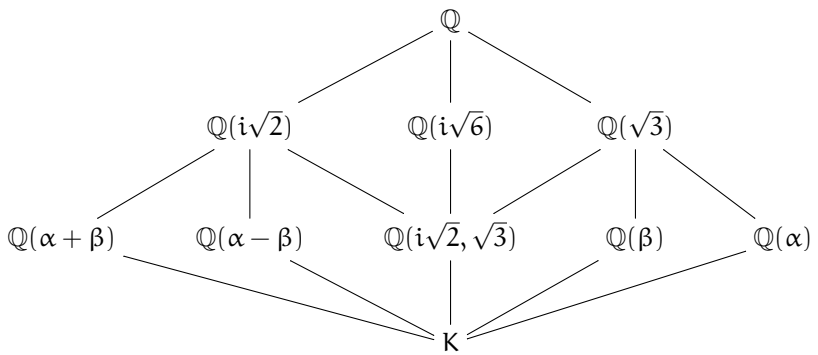
lo que excluye la segunda opción. La única salida que deja la conexión de Galois es que

$$K^{\langle \eta_{20} \rangle} = \mathbb{Q}(\alpha + \beta).$$

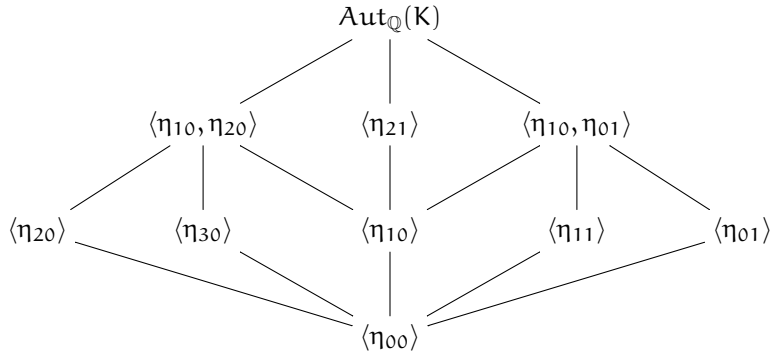
Una línea argumental análoga deja que

$$K^{\langle \eta_{30} \rangle} = \mathbb{Q}(\alpha - \beta).$$

En definitiva, los subcuerpos de K, organizados en un diagrama de Hasse, son



quienes, bajo la conexión de Galois, se corresponden con los subgrupos de $\mathrm{Aut}_{\mathbb{Q}}(K)$.



EJERCICIO 39. Sea $F \leq K$ una extensión de Galois de grado 3^n. Demostrar que, para cada $1 \leq i \leq n$, existe una subextensión $F \leq E \leq K$ tal que $[E : F] = 3^i$.

EJERCICIO 40. Supongamos que tenemos cuerpos $F \leq E \leq K$ tales que $F \leq E$ y $E \leq K$ son extensiones de Galois. ¿Es necesariamente $F \leq K$ de Galois?.

3.3. El Teorema Fundamental del Álgebra

Vamos a dar una demostración del Teorema Fundamental del Álgebra que sólo se apoya, desde el punto de vista del Análisis Matemático, en dos hechos básicos. De una parte, que cada polinomio de grado impar con coeficientes reales tiene alguna raíz real. Esto es una consecuencia del Teorema del Bolzano. De otra, que cada número real positivo tiene una raíz cuadrada. Lo que es consecuencia del Axioma del Supremo.

La conjugación compleja es un automorfismo $\mathbb{R}$–lineal del cuerpo $\mathbb{C}$ y, de hecho, es el generador del grupo $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$, cuyo orden es dos, ya que $\mathbb{C}$ es cuerpo de descomposición de $X^2 + 1 \in \mathbb{R}[X]$.

Para $f \in \mathbb{C}[X]$, por $\overline{f}$ denotaremos, en esta sección, el polinomio obtenido de aplicar el automorfismo conjugación a sus coeficientes.

TEOREMA 3.29 (Fundamental del Álgebra). *Si $f \in \mathbb{C}[X]$ es no constante, entonces f tiene todas sus raíces en $\mathbb{C}$. Es decir, el cuerpo de los números complejos es algebraicamente cerrado.*

DEMOSTRACIÓN. Observemos que $g = f\overline{f} \in \mathbb{R}[X]$ es no constante. Ahora, $(X^2 + 1)g \in \mathbb{R}[X]$ tiene un cuerpo de descomposición K que contiene a $\mathbb{C}$. Nuestro objetivo es probar que $K = \mathbb{C}$, con lo que, en particular, f tendrá todas sus raíces en $\mathbb{C}$.

Como $\mathbb{C}$ es una subextensión de la extensión de Galois $\mathbb{R} \leq K$, tenemos, por el Lema de la torre, que el orden de $G = \mathrm{Aut}_{\mathbb{R}}(K)$ es un múltiplo de 2. Podemos, por tanto, tomar un 2–subgrupo de Sylow H de G.

Por la conexión de Galois, $[K^H : \mathbb{R}] = (G : H)$, luego es impar. Dado $\alpha \in K^H$, $\mathrm{Irr}(\alpha, \mathbb{R})$ tiene grado $[\mathbb{R}(\alpha) : \mathbb{R}]$, luego impar. Por tanto, $\mathrm{Irr}(\alpha, \mathbb{R})$ ha de tener una raíz en $\mathbb{R}$, por lo que ha de ser de grado 1. Así, $\alpha \in \mathbb{R}$ y deducimos que $K^H = \mathbb{R}$. La conexión de Galois da ahora que $H = G$, por lo que G es un 2–grupo.

Deducimos que $\mathrm{Aut}_{\mathbb{C}}(K)$ es un 2–grupo. Si fuese no trivial, podríamos tomar un subgrupo suyo N de índice 2. Entonces, por el Teorema 3.22, la extensión $\mathbb{C} \leq K^N$ es de grado 2. Por tanto, $K^N = \mathbb{C}(\beta)$, para $\beta \in K^N$ tal que

$\mathrm{Irr}(\beta, \mathbb{C})$ tiene grado 2. Pero entonces $\mathrm{Irr}(\beta, \mathbb{C})$ es un polinomio de grado 2 con coeficientes complejos, por lo que tiene raíces en $\mathbb{C}$, ya que todo número complejo tiene raíces cuadradas complejas. Por tanto, no puede ser irreducible, y tenemos una contradicción.

La conclusión es que $\mathrm{Aut}_{\mathbb{C}}(K)$ es trivial y, por tanto, $K = \mathbb{C}$. De donde todas las raíces de g y, por ende, de f, están en $\mathbb{C}$. □

COROLARIO 3.30. *Si* $f \in \mathbb{R}[X]$ *es irreducible, entonces* f *tiene grado menor o igual que* 2.

DEMOSTRACIÓN. Sea $f \in \mathbb{R}[X]$ irreducible de grado mayor que 1. Tomemos una raíz suya $\alpha \in \mathbb{C}$. Entonces $\overline{\alpha}$ es raíz de f y, por tanto, $(X-\alpha)(X-\overline{\alpha})$ divide a f en $\mathbb{C}[X]$. Pero este polinomio tiene coeficientes reales, así que ha de ser asociado a f. □

EJERCICIO 41. Sea $\overline{\mathbb{Q}}$ la clausura algebraica de $\mathbb{Q}$ en $\mathbb{C}$. Razonar que todo polinomio no contante $f \in \overline{\mathbb{Q}}[X]$ tiene todas sus raíces en $\overline{\mathbb{Q}}$.

Capítulo 4

Teoría de Galois de ecuaciones

En este capítulo, veremos el grupo de Galois de un polinomio separable como subgrupo del grupo de permutaciones de sus raíces. Completaremos la discusión sobre puntos construibles con regla y compás. Como tema central, expondremos los resultados clásicos sobre resolución por radicales de ecuaciones. Daremos una pincelada final sobre resolución de ecuaciones en cuerpos finitos.

4.1. Grupo de Galois de un polinomio

Definamos el *discriminante* de un polinomio mónico $f \in F[X]$ de grado n con raíces[1] $\alpha_1, \ldots, \alpha_n$ en un cuerpo de descomposición K como

$$\mathrm{Disc}(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \in K.$$

Si f no es mónico, su discriminante se define como cierto elemento no nulo de F multiplicado por la anterior expresión, que no nos interesa aquí. Supondremos implícitamente que todos nuestros polinomios son mónicos, ya que, en lo que concierne a raíces, podemos reducirnos a este caso fácilmente. Es claro que f es separable si, y sólo si, $\mathrm{Disc}(f) \neq 0$.

Una raíz cuadrada del discriminante está dada por

$$\Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j),$$

elemento de K determinado salvo signo (dependiendo de cómo ordenemos las raíces de f).

DEFINICIÓN 4.1. Para f separable, el grupo $\mathrm{Aut}_F(K)$ es llamado *grupo de Galois* de f y, por la unicidad del cuerpo de descomposición, es único salvo isomorfismos.

Sea $\mathrm{Sim}(\alpha_1, \ldots, \alpha_n)$ el grupo de permutaciones del conjunto de raíces $\{\alpha_1, \ldots, \alpha_n\}$ de un polinomio separable f. Tenemos un homomorfismo de grupos

$$\mathrm{Aut}_F(K) \longrightarrow \mathrm{Sim}(\alpha_1, \ldots, \alpha_n),$$

puesto que cada $\sigma \in \mathrm{Aut}_F(K)$ permuta las raíces[2] de f. Dicho homomorfismo es inyectivo, porque cada automorfismo del grupo de Galois está determinado por su valor sobre las raíces de f, que generan K sobre F, así que podemos identificar el grupo $\mathrm{Aut}_F(K)$ como un subgrupo del grupo de permutaciones S_n.

Si $\sigma \in \mathrm{Aut}_F(K)$, se tiene que

$$\sigma(\Delta(f)) = \mathrm{sign}(\sigma)\Delta(f), \qquad \sigma(\mathrm{Disc}(f)) = \mathrm{Disc}(f), \tag{4.1}$$

[1] Cada raíz aparece tantas veces como indique su multiplicidad

[2] Esto es porque si α es una raíz de f, entonces $\sigma(\alpha)$ es también raíz de f para todo σ del grupo de Galois.

donde $\mathrm{sign}(\sigma)$ denota la signatura de σ visto como permutación de las raíces.

PROPOSICIÓN 4.2. *Para un polinomio separable $f \in F[X]$ con grupo de Galois $G = \mathrm{Aut}_F(K)$, se tiene que $\mathrm{Disc}(f) \in F$. Además, el subcuerpo fijo, bajo la conexión de Galois, de K para $G \cap A_n$ es $F(\Delta(f))$. Por tanto, $\Delta(f) \in F$ si, y sólo si, $G \subseteq A_n$.*

DEMOSTRACIÓN. Se sigue de (4.1) que $\mathrm{Disc}(f) \in K^G = F$. También se deduce de (4.1) que $\Delta(f) \in K^{G\cap A_n}$. Así, $F(\Delta(f)) \leq K^{G\cap A_n}$. Como

$$[K^{G\cap A_n} : F] = (G : G \cap A_n) \leq (S_n : A_n) = 2,$$

deducimos que sólo se pueden dar dos casos: $F(\Delta(f)) = F$ o bien $F(\Delta(f)) = K^{G\cap A_n}$. El primer caso ocurre, en vista de la Conexión de Galois, exactamente cuando $G \subseteq A_n$. □

EJEMPLO 4.3. Dado un polinomio

$$f = X^n + \sum_{i=0}^{n-1} a_i X^i,$$

no necesariamente separable, con raíces $\alpha_1, \ldots, \alpha_n$, donde cada una aparece tantas veces como indique su multiplicidad, calculando el producto $f = \prod_{i=1}^{n}(X-\alpha_i)$ e igualando coeficientes de igual grado, se obtienen las llamadas *relaciones de Cardano-Vieta* (ver Ejercicio 42) que, potencialmente, permiten calcular el discriminante de f a partir de sus coeficientes. Por ejemplo, para $n = 2$ se obtiene

$$a_0 = \alpha_1\alpha_2, a_1 = -(\alpha_1 + \alpha_2),$$

relaciones a partir de las cuales se obtiene que $\mathrm{Disc}(f) = a_1^2 - 4a_0$.

Para $n = 3$ se obtienen las relaciones

$$a_0 = -\alpha_1\alpha_2\alpha_3,\ a_1 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3,\ a_2 = -(\alpha_1 + \alpha_2 + \alpha_3).$$

A partir de ellas, se calcula una expresión para $\mathrm{Disc}(f)$, que no merece la pena registrar aquí. Quizás el caso particular de la cúbica reducida $f = X^3 + pX + q$ pueda interesar para los ejemplos. Sale

$$\mathrm{Disc}(f) = -4p^3 - 27q^2. \tag{4.2}$$

PROPOSICIÓN 4.4. *Sea $f \in F[X]$ un polinomio separable con grupo de Galois G. Entonces f es irreducible si, y sólo si, G actúa transitivamente sobre sus raíces. En tal caso, $\deg f$ divide a $\#G$.*

DEMOSTRACIÓN. Sea K un cuerpo de descomposición de f. Supongamos f irreducible y sean $\alpha, \beta \in K$ raíces de f. La Proposición 2.12 da una extensión $\tau : F(\alpha) \to K$ de la inclusión $F \leq F(\alpha)$ tal que $\tau(\alpha) = \beta$. Ahora, la Proposición 2.16 da la existencia de una extensión $\eta : K \to K$ de τ. Obviamente, $\eta(\alpha) = \tau(\alpha) = \beta$ y $\eta \in \mathrm{Aut}_F(K) = G$. Por tanto, G actúa transitivamente sobre las raíces de f.

Recíprocamente, sea g un factor irreducible de f. Si $\alpha \in K$ es una raíz de g, entonces $\sigma(\alpha)$ es una raíz de g para todo $\sigma \in G$. Como G actúa transitivamente sobre las raíces de f, tenemos que toda raíz de f lo es de g, lo que implica que $g = f$.

Por último, si α es una raíz de f, entonces

$$\#G = [K : F] = [K : F(\alpha)][F(\alpha) : F] = [K : F(\alpha)] \deg f.$$

□

EJEMPLO 4.5. Tomemos $f \in F[X]$ separable e irreducible de grado 2. Sabemos que el cuerpo de descomposición K de f tiene grado 2 sobre F, así que el grupo de Galois de f es cíclico de orden 2.

EJEMPLO 4.6. Para $f \in F[X]$ separable e irreducible de grado 3 sabemos que su grupo de Galois G es un subgrupo transitivo[3] de S_3. Si $\mathrm{Disc}(f)$ es un cuadrado en F, entonces $G \subseteq A_3$, luego ha de darse la igualdad. Si $\mathrm{Disc}(f)$ no es un cuadrado en F, entonces G es un subgrupo transitivo de S_3 distinto de A_3. Luego $G = S_3$.

EJEMPLO 4.7. Ahora, supongamos que $f \in F[X]$ es separable e irreducible de grado 4. Su grupo de Galois G es un subgrupo transitivo de S_4. Sean $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ las raíces de f en su cuerpo de descomposición K y definamos

$$\begin{aligned} \beta_1 &= \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ \beta_2 &= \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ \beta_3 &= \alpha_1\alpha_4 + \alpha_2\alpha_3. \end{aligned}$$

Consideremos el polinomio

$$g = (X - \beta_1)(X - \beta_2)(X - \beta_3).$$

Como cada $\sigma \in G$ permuta[4] los elementos β_i, resulta que $g^\sigma = g$ y, por tanto, los coeficientes de g están en $K^G = F$. Este polinomio es lo que se llama *una resolvente cúbica* de f. Si

$$f = X^4 + bX^3 + cX^2 + dX + e,$$

entonces, tras algunos cálculos, se obtiene que

$$g = X^3 - cX^2 + (bd - 4e)X - b^2e + 4ce - d^2.$$

Por otra parte, es fácil comprobar que los elementos $\beta_1, \beta_2, \beta_3$ son distintos. Por ejemplo,

$$\beta_2 - \beta_1 = \alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_2 - \alpha_3\alpha_4 = (\alpha_2 - \alpha_3)(\alpha_4 - \alpha_1).$$

De hecho, si calculamos las otras diferencias $\beta_3 - \beta_1$ y $\beta_3 - \beta_2$, veremos que $\mathrm{Disc}(f) = \mathrm{Disc}(g)$. Tenemos que g es separable y $E = F(\beta_1, \beta_2, \beta_3)$ es su cuerpo de descomposición. Por el Teorema 3.27, $F \leq E$ es de Galois y $N = \mathrm{Aut}_E(K)$ es un subgrupo normal de G. Además, $\mathrm{Aut}_F(E)$ es isomorfo a G/N.

Vamos a identificar quién es N. Para ello, consideremos el homomorfismo de grupos

$$s : \mathrm{Sim}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \to \mathrm{Sim}(\beta_1, \beta_2, \beta_3)$$

dado por $s(\sigma)(\alpha_i\alpha_j + \alpha_k\alpha_l) = \alpha_{\sigma(i)}\alpha_{\sigma(j)} + \alpha_{\sigma(k)}\alpha_{\sigma(l)}$. Este homomorfismo es sobreyectivo, ya que es fácil ver que en su imagen está cualquier trasposición. Su núcleo, que tiene cardinal cuatro por el Teorema de Lagrange, contiene claramente a

$$V = \{(1), (12)(34), (13)(24), (14)(23)\},$$

luego ha de ser justo este subgrupo.

Observemos que, puesto que $F \leq E$ es de Galois, se tiene, como en la demostración del Teorema 3.27, que $\sigma(E) = E$ para cada $\sigma \in G$. Como allí, denotemos por $r : G \to \mathrm{Aut}_F(E)$ la aplicación que lleva cada $\sigma \in G$ en su

[3] Es decir, que actúa transitivamente sobre los elementos que permuta.

[4] Basta con descoponer σ, visto como permutación, como producto de trasposiciones y comprobar que cada una de éstas permuta los elementos citados.

restricción a E. Tenemos el diagrama conmutativo de homomorfismos de grupos con filas exactas[5]

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \xrightarrow{r} & \mathrm{Aut}_F(E) & \longrightarrow & 1\,, \\ & & & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & V & \longrightarrow & \mathrm{Sim}(\alpha_1,\alpha_2,\alpha_3,\alpha_4) & \xrightarrow{s} & \mathrm{Sim}(\beta_1,\beta_2,\beta_3) & \longrightarrow & 1 \end{array}$$

donde las flechas verticales representan los homomorfismos inyectivos de grupos que llevan cada automorfismo en la correspondiente permutación de las raíces de f y g, respectivamente. Se sigue de aquí que $N = G \cap V$.

EJEMPLO 4.8. Tomemos $f = X^4 - 2 \in \mathbb{Q}[X]$, que es irreducible por el criterio de Eisenstein. Por otra parte, es fácil comprobar que, si K es su cuerpo de descomposición, entonces $[K : \mathbb{Q}] = 8$. Por tanto, su grupo de Galois ha de ser de orden 8. Visto como subgrupo transitivo de S_4, la única opción es que sea isomorfo a D_4.

EJEMPLO 4.9. Consideremos la cuártica $f = X^4 + X + 1 \in \mathbb{Q}[X]$. Reduciendo módulo 2, vemos que es un polinomio irreducible en $\mathbb{Z}[X]$ y, por ser primitivo, en $\mathbb{Q}[X]$. De manera que su grupo de Galois G, visto como permutaciones de sus raíces, es un subgrupo transitivo de S_4, como establece la Proposición 4.4. Su resolvente cúbica es $g = X^3 - 4X - 1$, por lo que

$$\mathrm{Disc}(f) = \mathrm{Disc}(g) = 229.$$

Este número es primo, de donde $X^2 - 229 \in \mathbb{Q}[X]$ es irreducible y, así, $\sqrt{229} \notin \mathbb{Q}$. Por tanto, G no está contenido en A_4. Como G es un subgrupo transitivo de S_4, tiene que ser alguno de los subgrupos de S_4 isomorfos a C_4, D_4 o el propio S_4. Ahora bien, g es una cúbica irreducible, ya que no tiene raíces en $\mathbb{Q}$. Por tanto, su grupo de Galois tiene orden un múltiplo de 3. Si E es su cuerpo de descomposición, entonces, en virtud del Teorema 3.27, $N = \mathrm{Aut}_E(K)$ es un subgrupo normal de G y $G/N \cong \mathrm{Aut}(E)$. Como, por la Proposición 4.4, este último tiene cardinal un múltiplo de 3, la única posibilidad es que $G = S_4$.

EJERCICIO 42 (Identidades de Cardano-Vieta). Sea $f \in F[X]$ un polinomio mónico de grado n con raíces $\alpha_1, \ldots, \alpha_n$ en un cuerpo de descomposición suyo (no suponemos que f sea separable, así que entre las raíces puede haber repeticiones). Definamos

$$s_k = \sum_{1 \le i_1 < \cdots < i_k \le n} \alpha_{i_1} \cdots \alpha_{i_k}.$$

para $k = 1, \ldots, n$. Demostrar que

$$f = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n.$$

EJERCICIO 43. Sea $f \in F[X]$ un polinomio separable e irreducible de grado primo p. Demostrar que el grupo de Galois de f sobre el cuerpo F contiene un ciclo de orden p. (Pista: usar el Teorema de Cauchy de existencia de p–subgrupos).

EJERCICIO 44. Sea $f \in \mathbb{Q}[X]$ irreducible de grado primo p. Demostrar que, si f tiene exactamente dos raíces complejas no reales, entonces el grupo de Galois de f sobre $\mathbb{Q}$ es isomorfo a S_p. (Pista: usar el Ejercicio 43).

[5] Esto es una manera rápida de decir que r y s son sobreyectivos, N es el núcleo de r y V es el núcleo de s, además de que las dos composiciones posibles de G a $\mathrm{Sim}(\beta_1,\beta_2,\beta_3)$ dan el mismo homomorfismo.

EJERCICIO 45. Demostrar que el grupo de Galois de $f = X^5 - 4X - 1 \in \mathbb{Q}[X]$ es isomorfo a S_5.

EJERCICIO 46. Sea $f \in \mathbb{R}[X]$ un polinomio de grado 3. Discutir el número de raíces reales de f en función del signo de su discriminante.

4.2. Extensiones ciclotómicas

Comencemos con la siguiente observación: dado $f = X^n - 1 \in F[X]$ el conjunto de sus raíces en cualquier extensión K de F es un subgrupo de $K^\times = K\backslash\{0\}$, llamado grupo de raíces n–ésimas de la unidad en K. Sabemos, por el Ejercicio 30, que se trata de un grupo cíclico cuyo orden ha de ser un divisor de n. Si f es separable y K contiene al cuerpo de descomposición de f, entonces se trata de un grupo cíclico de orden n. Sus generadores se llaman raíces n–ésimas primitivas de la unidad sobre F. En lo que sigue, **suponemos que** $X^n - 1$ **es separable**, es decir, que la característica de F es cero o, de ser positiva, no es un divisor de n.

DEFINICIÓN 4.10. El cuerpo de descomposición de $X^n - 1 \in F[X]$ se llama n–ésima extensión ciclotómica de F.

Es claro que, si ζ es una raíz n–ésima primitiva de la unidad sobre F, entonces la n–ésima extensión ciclotómica de F es $F(\zeta)$.

EJEMPLO 4.11. Las raíces n–ésimas de la unidad sobre $\mathbb{Q}$ son los números complejos $\{e^{i2k\pi/n} : k = 0, 1, \ldots, n-1\}$, y la n–ésima extensión ciclotómica de $\mathbb{Q}$ es $\mathbb{Q}(e^{i2\pi/n})$. Obviamente, podemos tomar cualquier otra raíz n–ésima primitiva de la unidad como generador.

Dado $n \geq 2$ natural, denotamos por $U(\mathbb{Z}_n)$ el grupo de unidades del anillo $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, que sabemos es abeliano de orden $\varphi(n)$ (función de Euler aplicada a n). Si ζ es una raíz n–ésima primitiva de la unidad sobre F, describiremos el conjunto de todas las raíces n–ésimas de la unidad como

$$\{\zeta^k : k \in \mathbb{Z}_n\},$$

lo que es un pequeño pero muy práctico abuso de notación. Las raíces primitivas son, así,

$$\{\zeta^k : k \in U(\mathbb{Z}_n)\}.$$

PROPOSICIÓN 4.12. *Sea G el grupo de Galois de la n–ésima extensión ciclotómica de F. Entonces G es isomorfo a un subgrupo de $U(\mathbb{Z}_n)$. Además, G es isomorfo a $U(\mathbb{Z}_n)$ si, y sólo si, G actúa transitivamente sobre las raíces n–ésimas primitivas de la unidad sobre F.*

DEMOSTRACIÓN. Tomemos ζ una raíz n–ésima primitiva de la unidad. Dado $\sigma \in G = \mathrm{Aut}_F(F(\zeta))$, es fácil ver que $\sigma(\zeta)$ es otra raíz n–ésima primitiva de la unidad. Por tanto, $\sigma(\zeta) = \zeta^k$ para algún $k \in U(\mathbb{Z}_n)$. Este k es único, como consecuencia de ser ζ raíz primitiva, así que tenemos definida una aplicación $G \to U(\mathbb{Z}_n)$. Ahora, si $\tau \in G$ y $\tau(\zeta) = \zeta^l$, entonces

$$(\tau\sigma)(\zeta) = \tau(\zeta^k) = \tau(\zeta)^k = (\zeta^l)^k = \zeta^{kl}.$$

Por tanto, tenemos un homomorfismo de grupos $G \to U(\mathbb{Z}_n)$. Además, es inyectivo, ya que $\sigma \in G$ está determinado por su valor sobre ζ. Deducimos que G es isomorfo a un subgrupo de $U(\mathbb{Z}_n)$. El homomorfismo de grupos dado es sobreyectivo si, y sólo si, G actúa transitivamente sobre las raíces n–ésimas primitivas de la unidad sobre F. □

DEFINICIÓN 4.13. Definimos el n–ésimo polinomio ciclotómico como

$$\Phi_n = \prod_{k \in U(\mathbb{Z}_n)} (X - \zeta^k). \tag{4.3}$$

PROPOSICIÓN 4.14. *Se tiene que* $X^n - 1 = \prod_{d|n} \Phi_d$.

DEMOSTRACIÓN. Si denotamos por R_n a conjunto de todas las raíces n–ésimas de la unidad, entonces $X^n - 1 = \prod_{\alpha \in R_n} (X - \alpha)$. Por otra parte, denotemos por P_m al conjunto de las raíces m–ésimas primitivas de la unidad. Se tiene una partición $R_n = \bigcup_{d|n} P_d$, de donde se deduce (4.3). □

PROPOSICIÓN 4.15. *Los polinomios ciclotómicos tienen sus coeficientes en el subcuerpo primo. Además, en el caso de característica cero, los coeficientes son enteros.*

DEMOSTRACIÓN. A partir de la expresión (4.3), hacemos inducción sobre n. Obviamente, $\Phi_1 = X - 1$. Para $n > 1$, tenemos que

$$X^n - 1 = \Phi_n \prod_{\substack{d|n \\ d \neq n}} \Phi_d.$$

Por hipótesis de inducción, el factor de la derecha tiene coeficientes en el subcuerpo primo. La división euclidiana de polinomios muestra que Φ_n también los tiene.

En el caso de característica 0, razonemos de nuevo por inducción sobre n, que $\Phi_n \in \mathbb{Z}[X]$. El caso $n = 1$ es obvio, así que supongamos que $n > 0$. Como $\Phi_n \in \mathbb{Q}[X]$, tenemos que existe a, entero positivo, tal que $f = a\Phi_n \in \mathbb{Z}[X]$ es primitivo. Usando la hipótesis de inducción y el Lema de Gauss, tenemos que $a(X^n - 1) = f \prod_{\substack{d|n \\ d \neq n}} \Phi_d$ tiene coeficientes enteros y es primitivo. Por tanto, $a = 1$ y $\Phi_n = f \in \mathbb{Z}[X]$. □

EJEMPLO 4.16. En característica 0, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$. Calculemos Φ_6. Sabemos que

$$X^6 - 1 = \Phi_1 \Phi_2 \Phi_3 \Phi_6.$$

Realizando varias divisiones euclidianas, obtenemos que $\Phi_6 = X^2 - X + 1$. También podemos calcular las raíces sextas primitivas de la unidad compleja y usar directamente la definición de Φ_6.

EJERCICIO 47. Calcular, en característica 0, Φ_8.

TEOREMA 4.17. *Cada polinomio ciclotómico* $\Phi_n \in \mathbb{Z}[X]$ *es irreducible.*

DEMOSTRACIÓN. Supongamos $f \in \mathbb{Z}[X]$ un factor irreducible de Φ_n, y tomemos cualquier raíz compleja ζ de f. Vamos a demostrar que, si p es un primo que no divide a n, entonces ζ^p también es raíz de f.

Razonemos por reducción al absurdo: Si ζ^p no es raíz de f, entonces ζ^p ha de ser raíz de $g \in \mathbb{Z}[X]$ para $\Phi_n = fg$. Pero podemos ver esto como que ζ es raíz de $g(X^p) \in \mathbb{Z}[X]$. Luego $f(X)$ y $h(X) = g(X^p)$ tienen una raíz común en la n–ésima extensión ciclotómica de $\mathbb{Q}$. Esto sólo es posible, por la identidad de Bezout, si f es un divisor de h en $\mathbb{Q}[X]$. Pero f es primitivo, por lo que ha se ser un divisor de h en $\mathbb{Z}[X]$ (ver [**2**, Lema 4.25]).

Reduciendo módulo p, tenemos que $\overline{\Phi_n} = \overline{f}\overline{g}$. Por otra parte, $\overline{h} = \overline{g(X^p)} = \overline{g(X)}^p$, puesto que, en $\mathbb{F}_p$, se tiene $a^p = a$. Como $\overline{f}$ divide a $\overline{h} = \overline{g}^p$, deducimos que $\overline{f}$ y $\overline{g}$ han de tener un factor común en $\mathbb{F}_p[X]$. Por lo que

$X^n - \overline{1} \in \mathbb{F}_p[X]$ ha de tener, en su cuerpo de descomposición, una raíz múltiple. Pero eso no es posible, ya que, al ser p coprimo con n, el polinomio $X^n - \overline{1}$ es separable sobre $\mathbb{F}_p$.

Para concluir la demostración, tomemos cualquier raíz ζ de f. Puesto que f es un divisor de Φ_n, tenemos que ζ es una raíz primitiva n–ésima de la unidad. Usando reiteradamente el hecho probado anteriormente, vemos que ζ^k es raíz de f para cualquier exponente k coprimo con n. Esto es, toda raíz n–ésima primitiva de la unidad lo es de f. Por tanto, $f = \Phi_n$.

□

COROLARIO 4.18. *El grupo de Galois sobre $\mathbb{Q}$ de la n–ésima extensión ciclotómica es isomorfo a $U(\mathbb{Z}_n)$. Por tanto, su grado sobre $\mathbb{Q}$ es $\varphi(n)$.*

DEMOSTRACIÓN. De acuerdo con el Teorema 4.17, el polinomio irreducible de una raíz n–ésima primitiva de la unidad ζ sobre $\mathbb{Q}$ es ϕ_n, cuyo grado es $\varphi(n)$. Por tanto,

$$\#\mathrm{Aut}(\mathbb{Q}(\zeta)) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \phi_n = \varphi(n).$$

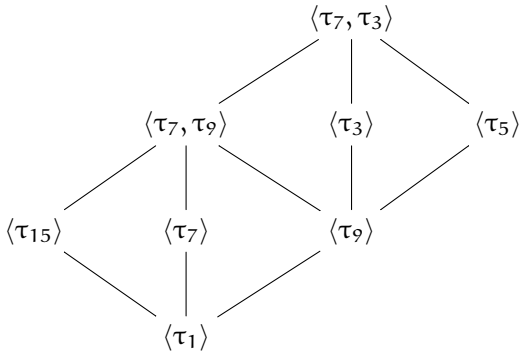
Deducimos de la Proposición 4.12 que $\mathrm{Aut}(\mathbb{Q}(\zeta))$ es isomorfo a $U(\mathbb{Z}_n)$. □

EJEMPLO 4.19. Consideremos $\zeta \in \mathbb{C}$ una raíz decimosexta primitiva de la unidad. Tenemos que la decimosexta extensión ciclotómica de $\mathbb{Q}$ es $K = \mathbb{Q}(\zeta)$. Vamos a calcular los subcuerpos de K. Por el Corolario 4.18,

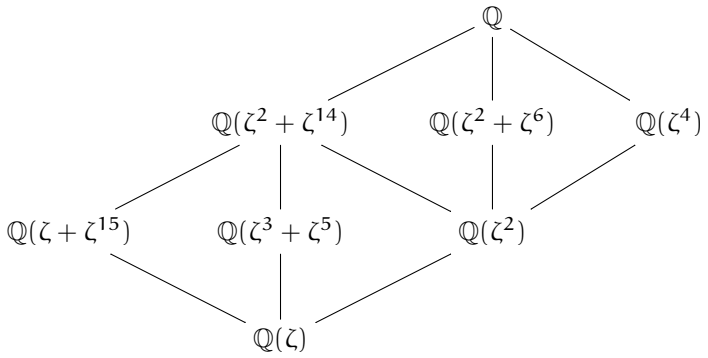
$$\mathrm{Aut}(K) = \{\tau_j : j \in U(\mathbb{Z}_{16})\},$$

donde $\tau_j(\zeta) = \zeta^j$.

Resulta que $\mathrm{Aut}(K) = \langle \tau_7, \tau_3 \rangle$ y, a partir de aquí, el conjunto ordenado de los de subgrupos de $\mathrm{Aut}(K)$ es



El conjunto ordenado de subcuerpos de K se obtiene, por la conexión de Galois, calculando los subcuerpos fijos por cada uno de estos subgrupos. Resulta



4.3. Construcciones con regla y compás, II

Complementamos el Teorema 1.34 sobre números complejos construibles con el siguiente resultado, que nos permitirá tratar el problema clásico de la construcción con regla y compás de un polígono regular. Dado un conjunto S de números complejos, consideramos el subcuerpo $F = \mathbb{Q}(S \cup \overline{S})$ de $\mathbb{C}$. Suponemos que $\{0, 1\} \subseteq S$.

TEOREMA 4.20. *Un número complejo z es construible a partir de S si, y sólo si, existe una extensión de Galois $F \leq K$ tal que $z \in K$ y $[K : F]$ es una potencia de 2.*

DEMOSTRACIÓN. Supongamos que z es construible a partir de S. De acuerdo con el Teorema 1.34, existe una torre de subcuerpos de $\mathbb{C}$

$$F = F_0 \leq F_1 \leq \cdots \leq F_s,$$

tales que $F_{i+1} = F_i(\alpha_{i+1})$ con $\alpha_{i+1}^2 \in F_i$ para $i = 0, \ldots, s-1$, y $z \in F_s$. Vamos a demostrar, razonando por inducción sobre s, que existe una extensión de Galois $F \leq K$ cuyo grado es una potencia de 2 y tal que $F_s \leq K$.

Si $s = 0$, tomamos $K = F$.

Supongamos, pues, que $s > 0$. Por hipótesis de inducción, existe una extensión de Galois $F \leq E$ cuyo grado es una potencia de 2 y tal que $F_{s-1} \leq E$. Llamemos $a_s = \alpha_s^2 \in F_{s-1}$. Pongamos

$$\mathrm{Aut}_F(E) = \{\sigma_0, \ldots, \sigma_t\},$$

y definamos $f = \prod_{j=0}^{t}(X^2 - \sigma_j(a_s))$, que es, claramente, invariante por la acción de $\mathrm{Aut}_F(E)$. Así, $f \in F[X]$.

Como $F \leq E$ es de Galois, E es cuerpo de descomposición de algún $g \in F[X]$. Tomemos K cuerpo de descomposición de $fg \in F[X]$, de manera que $F \leq K$ es de Galois. Además, si $\alpha_{s+j} \in K$ es raíz de $X^2 - \sigma_j(a_s)$ para $j = 0, \ldots, t$, tenemos que $K = E(\alpha_s, \alpha_{s+1}, \ldots, \alpha_t)$. Por el Lema de la torre, $[K : E]$ es una potencia de 2 y, así, lo es $[K : F]$. Como $F_s = F_{s-1}(\alpha_s) \leq E(\alpha_s)$, vemos completa la inducción.

Recíprocamente, dada una extensión de Galois $F \leq K$ cuyo grado es una potencia de 2 tal que $z \in K$, tenemos que $\mathrm{Aut}_F(K)$ es un 2–grupo. Sabemos que, entonces, $\mathrm{Aut}_F(K)$ es resoluble y tiene una serie de composición

$$\mathrm{Aut}_F(K) = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{\mathrm{id}\},$$

todos cuyos factores de composición tienen orden 2. La torre de extensiones de Galois correspondiente

$$F = K_0 \leq K_1 \leq \cdots \leq K_n = K, \tag{4.4}$$

es tal que $[K_{i+1} : K_i] = 2$ para todo $i = 0, \ldots, n-1$. Así, $K_{i+1} = K_i(\beta_i)$, para β_i raíz de un polinomio cuadrático $X^2 + b_i X + c_i \in K_i[X]$. Puesto que $\beta_i = \left(-b_i \pm \sqrt{b_i^2 - 4c_i}\right)/2$, tenemos que $K_{i+1} = K_i(\alpha_i)$ para $\alpha_i = \sqrt{b_i^2 - 4c_i}$. Así que la torre (4.4) es por raíces cuadradas y, de acuerdo con el Teorema 1.34, z es construible a partir de S. □

Recordemos que un número complejo es construible si lo es a partir de $\{0, 1\}$, es decir, usando coordenadas, a partir de dos puntos distintos dados.

EJEMPLO 4.21. Tomemos $\alpha \in \mathbb{C}$ una raíz de $f = X^4 + X + 1 \in \mathbb{Q}[X]$. Según vimos en el Ejemplo 4.9, f un polinomio irreducible cuyo grupo de Galois es isomorfo a S_4. En particular, $\mathrm{Irr}(\alpha, \mathbb{Q}) = f$ y α es un número de grado 4

sobre $\mathbb{Q}$. Ahora, si α fuese costruible, entonces existiría una extensión de Galois K de $\mathbb{Q}$ que contendría a α y de grado una potencia de 2. Pero K ha de contener entonces a todas las raíces de f y, por tanto, a su cuerpo de descomposición. La conexión de Galois impide que esto pueda ser así, ya que el grado de dicho cuerpo de descomposición sobre $\mathbb{Q}$ es el cardinal de S_4 que, obviamente, no es una potencia de 2. De modo que este número α no es construible.

COROLARIO 4.22. *Un polígono regular de n lados es construible si, y sólo si, $\varphi(n)$ es una potencia de 2.*

DEMOSTRACIÓN. La idea clave es que el polígono del enunciado será construible si, y sólo si, lo es la raíz n–ésima primitiva de la unidad $e^{i2\pi/n}$. Según el Teorema 4.20, éste es el caso precisamente cuando $e^{i2\pi/n} \in K$, para una extensión de Galois K de grado una potencia de 2 sobre $\mathbb{Q}$. Así, si $e^{i2\pi/n}$ es construible, entonces $\mathbb{Q}(e^{i2\pi/n})$ es un subcuerpo de un cuerpo K como el descrito, por lo que su grado es un divisor de una potencia de 2. Pero este grado es $\varphi(n)$, por el Corolario 4.18. Recíprocamente, el mismo corolario da que puedo tomar $K = \mathbb{Q}(e^{i2\pi/n})$, que es de Galois, y aplicar el Teorema 4.20. □

EJEMPLO 4.23. Si p es un número primo, el Corolario 4.22 muestra que un polígono regular de p lados es construible si, y sólo si, el primo p es de la forma $p = 1 + 2^k$. Esto muestra que, aparte del polígono degenerado de dos lados, el trángulo y el pentágono regulares son construibles. No obstante, el heptágono regular no lo es y, para encontrar otro polígono regular construible con un número primo de lados, hay que subir hasta $p = 17$.

OBSERVACIÓN 4.24. Los números primos p para los que $\varphi(p)$ es una potencia de 2 se llaman *primos de Fermat*. En este momento, se conocen sólo cinco: $p = 1 + 2^{2^m}, m = 0, 1, 2, 3, 4$. No se sabe si el conjunto de los primos de Fermat es finito.

EJERCICIO 48. Demostrar que un polígono regular de n lados es construible si, y sólo si, n es producto de una potencia de 2 y primos de Fermat distintos entre sí.

4.4. Extensiones cíclicas

Vamos a estudiar el cuerpo de descomposición y el grupo de Galois de polinomios separables del tipo $X^n - a$.

TEOREMA 4.25. *Supongamos que $X^n - a \in F[X]$ es separable y sea K su cuerpo de descomposición. Entonces K contiene una raíz n–ésima primitiva de la unidad ζ y $K = F(\zeta, r)$, para cualquier raíz $r \in K$ de $X^n - a$. Además, el grupo de Galois de la extensión $F(\zeta) \leq K$ es cíclico con orden un divisor de n.*

DEMOSTRACIÓN. Puesto que en el caso $a = 0$ todas las afirmaciones son obvias, discutamos qué ocurre para $a \neq 0$. Como $f = X^n - a$ es separable, el conjunto R de sus raíces en K tiene cardinal n. Por otra parte, dadas $r, s \in R$, se tiene que $r^{-1}s$ es una raíz n–ésima de la unidad que pertenece a K. De esta forma, fijada $r \in R$, el subconjunto $\{r^{-1}s : s \in R\}$ de K consiste en n raíces n–ésimas distintas de la unidad. Así, son todas las posibles, y,

en particular, K contiene una raíz primitiva n–ésima de la unidad ζ. Observemos que, de esta forma, las raíces de $X^n - a$ son $r, \zeta r, \dots, \zeta^{n-1} r \in K$. Por tanto, $K = F(\zeta, r)$.

Dado $\sigma \in \mathrm{Aut}_{F(\zeta)}(K)$, tenemos que $\sigma(r) = r\zeta^j$ para algún $j \in \mathbb{Z}_n$. Como ζ es raíz primitiva, resulta que σ determina de manera única j, luego podemos escribir $j = j(\sigma)$ y tenemos definida una aplicación $j : \mathrm{Aut}_{F(\zeta)} \to \mathbb{Z}_n$. Comprobemos que se trata de un homomorfismo de grupos: $j(\tau\sigma)$ está determinado, para $\tau, \sigma \in \mathrm{Aut}_{F(\zeta)}(K)$, por la condición

$$\tau\sigma(r) = r\zeta^{j(\tau\sigma)}.$$

Pero

$$\tau\sigma(r) = \tau(\sigma(r)) = \tau(r\zeta^{j(\sigma)}) = \tau(r)\zeta^{j(\sigma)} = r\zeta^{j(\tau)}\zeta^{j(\sigma)} = r\zeta^{j(\tau)+j(\sigma)}.$$

Por último, j es inyectivo, ya que si σ es tal que $j(\sigma) = 0$, entonces $\sigma(r\zeta^k) = \sigma(r)\zeta^k = r\zeta^k$ para todo $k \in \mathbb{Z}_n$.

Hemos obtenido, pues, que $\mathrm{Aut}_{F(\zeta)}(K)$ es isomorfo a un subgrupo de $\mathbb{Z}_n$ y, por tanto, cíclico con orden un divisor de n. □

Tenemos la siguiente consecuencia de la demostración del Teorema 4.25.

COROLARIO 4.26. $X^n - a$ *es irreducible sobre* $F(\zeta)$ *si, y sólo si,* $[K : F(\zeta)] = n$.

DEMOSTRACIÓN. Observemos que $K = F(\zeta)(r)$ y que el grado de $\mathrm{Irr}(r, F(\zeta))$ es $[K : F(\zeta)]$. □

DEFINICIÓN 4.27. Una extensión $F \leq K$ se dirá *cíclica* si es de Galois con grupo de Galois cíclico.

EJEMPLO 4.28. Si $X^n - a \in F[X]$ es separable con cuerpo de descomposición K y F contiene una raíz primitiva n–ésima de la unidad, entonces $F \leq K$ es cíclica, en virtud del Teorema 4.25.

EJEMPLO 4.29. Toda extensión de cuerpos finitos es cíclica (ver el Teorema 3.20).

Nuestro siguiente objetivo es ver cómo las extensiones cíclicas son, bajo ciertas hipótesis, cuerpos de descomposición de polinomios de la forma $X^n - a$.

LEMA 4.30 (de independencia de Dedekind). *Sean* $\sigma_1, \dots, \sigma_n : F \to E$ *homomorfismos de cuerpos distintos. Si* $\lambda_1, \dots, \lambda_n \in E$ *satisfacen que* $\lambda_1\sigma_1(x) + \cdots + \lambda_n\sigma_n(x) = 0$ *para todo* $x \in F$*, entonces* $\lambda_1 = \cdots = \lambda_n = 0$.

DEMOSTRACIÓN. El enunciado es trivialmente cierto para $n = 1$, así que supongamos que $n > 1$. Razonemos por reducción al absurdo. Suponemos así que existen $\lambda_1, \cdots, \lambda_n \in E$ no todos nulos tales que

$$\lambda_1\sigma_1(x) + \cdots + \lambda_n\sigma_n(x) = 0, \qquad \forall x \in F. \tag{4.5}$$

Tomamos, de entre todas las listas $\lambda_1, \dots, \lambda_n$ satisfaciendo (4.5), una con número de elementos no nulos mínimo. Reordenando, podemos suponer que $\lambda_1, \cdots, \lambda_m$ son los elementos no nulos de dicha lista. Es claro que $m \geq 2$.

Puesto que los homomorfismos σ_i son distintos, existe $y \in F$ tal que $\sigma_1(y) - \sigma_m(y) \neq 0$. Por otra parte,

$$\lambda_1\sigma_1(yx) + \cdots + \lambda_m\sigma_m(yx) = 0. \tag{4.6}$$

Ya que cada σ_i es multiplicativo, restando (4.6) de (4.5) multiplicada por $\sigma_m(y)$, obtenemos que

$$\lambda_1(\sigma_1(y) - \sigma_m(y))\sigma_1(x) + \cdots + \lambda_{m-1}(\sigma_{m-1}(y) - \sigma_m(y))\sigma_{m-1}(x) = 0,$$

para todo $x \in F$, violando la minimalidad de m. □

TEOREMA 4.31. *Sea $F \leq K$ una extensión cíclica tal que $n = [K : F]$ no es múltiplo de la característica de F. Si F contiene una raíz n–ésima primitiva de la unidad, entonces K es el cuerpo de descomposición de un polinomio irreducible de la forma $X^n - a \in F[X]$. Además, si $\alpha \in K$ es una raíz de $X^n - a$, entonces $K = F(\alpha)$.*

DEMOSTRACIÓN. Sea σ un generador del grupo de Galois $\mathrm{Aut}_F(K)$ y $\zeta \in F$ una raíz n–ésima primitiva de la unidad. El Lema 4.30 asegura que existe $r \in K$ tal que

$$\beta = r + \zeta\sigma(r) + \cdots + \zeta^{n-1}\sigma^{n-1}(r) \neq 0$$

Observemos que $\zeta\sigma(\beta) = \beta$, ya que σ tiene orden n. De aquí, $\beta^n = \zeta^n\sigma(\beta)^n = \sigma(\beta^n)$, de donde $a = \beta^n \in F$. Los elementos $\beta, \zeta\beta, \ldots, \zeta^{n-1}\beta$ son raíces distintas de $X^n - a$, por lo que

$$X^n - a = (X - \beta)(X - \zeta\beta)\cdots(X - \zeta^{n-1}\beta).$$

Por tanto, $F(\beta)$ es cuerpo de descomposición de $X^n - a$. Dado que $\sigma^k(\beta) = \zeta^{-k}\beta$, deducimos que $\mathrm{id}, \sigma, \ldots, \sigma^{n-1}$ son F–automorfismos (distintos) de $F(\beta)$. La Proposición 3.1 implica así que $n \leq [F(\beta) : F]$, lo que no puede ser cierto salvo que $F(\beta) = K$. De ahí, K es el cuerpo de descomposición de $X^n - a$. Además, la igualdad $[F(\beta) : F] = n$ implica que $\mathrm{Irr}(\beta, F)$ tiene grado n, luego $\mathrm{Irr}(\beta, F) = X^n - a$.

La última afirmación es clara, ya que $\alpha = \zeta^k\beta$ para algún k. □

PROPOSICIÓN 4.32. *El grupo de Galois de un polinomio separable de la forma $X^n - a \in F[X]$ es resoluble.*

DEMOSTRACIÓN. Tenemos la torre de cuerpos $F \leq F(\zeta) \leq K$ para K cuerpo de descomposición de $X^n - a$ y $\zeta \in K$ raíz n–ésima primitiva de la unidad. La extensión $F \leq F(\zeta)$ es de Galois y su grupo de Galois es conmutativo por la Proposición 4.12. Además, sabemos por el Teorema 3.27 que el mismo es isomorfo a $\mathrm{Aut}_F(K)/\mathrm{Aut}_{F(\zeta)}(K)$. Tenemos así la serie normal

$$\{\mathrm{id}_K\} \subseteq \mathrm{Aut}_{F(\zeta)}(K) \subseteq \mathrm{Aut}_F(K)$$

con factores abelianos, en vista del Teorema 4.17. Así, $\mathrm{Aut}_F(K)$ es resoluble. □

EJEMPLO 4.33. Tomemos K el cuerpo de descomposición de $X^8 - 3 \in \mathbb{Q}[X]$. Sabemos que $K = \mathbb{Q}(\sqrt[8]{3}, \zeta)$, donde $\zeta \in \mathbb{C}$ es una raíz octava primitiva de la unidad. Por ejemplo, podemos tomar

$$\zeta = e^{i\pi/4} = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}.$$

Observemos que $\sqrt{2} = \zeta + \overline{\zeta} \in \mathbb{Q}(\zeta)$. De aquí, $i = \zeta\sqrt{2} - 1 \in \mathbb{Q}(\zeta)$. Todo lo cual implica que $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{2}, i)$. Deducimos así que $K = \mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$. Por tanto,

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i) : \mathbb{Q}(\sqrt[8]{3}, \sqrt{2})][\mathbb{Q}(\sqrt[8]{3}, \sqrt{2}) : \mathbb{Q}(\sqrt[8]{3})][\mathbb{Q}(\sqrt[8]{3}) : \mathbb{Q}].$$

Calculemos los grados que aparecen a la derecha de la anterior igualdad. Puesto que $X^8 - 3 \in \mathbb{Q}[X]$ es irreducible por el criterio de Eisenstein,

deducimos que $[\mathbb{Q}(\sqrt[8]{3}) : \mathbb{Q}] = 8$. Ya que $i \notin \mathbb{Q}(\sqrt[8]{3}, \sqrt{2})$ y es raíz de $X^2 + 1$, tenemos que $[\mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i) : \mathbb{Q}(\sqrt[8]{3}, \sqrt{2})] = 2$. Deducimos, pues, que

$$[K : \mathbb{Q}] = 16[\mathbb{Q}(\sqrt[8]{3}, \sqrt{2}) : \mathbb{Q}(\sqrt[8]{3})].$$

Por tanto, el valor de $[K : \mathbb{Q}] = 32$ si $\sqrt{2} \notin \mathbb{Q}(\sqrt[8]{3})$. Vamos a demostrar esto último.

Observemos que, como consecuencia del Lema de la torre, cada extensión consecutiva en la torre de cuerpos

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{3}) \leq \mathbb{Q}(\sqrt[4]{3}) \leq \mathbb{Q}(\sqrt[8]{3})$$

tiene grado 2.

Demostremos primero que $\sqrt{2} \notin \mathbb{Q}(\sqrt[4]{3})$. En caso contrario, y, puesto que $\{1, \sqrt[4]{3}\}$ es una $\mathbb{Q}(\sqrt{3})$–base de $\mathbb{Q}(\sqrt[4]{3})$, tendríamos $a, b \in \mathbb{Q}(\sqrt{3})$ tales que $\sqrt{2} = a + b\sqrt[4]{3}$. Elevando al cuadrado, obtenemos

$$2 = a^2 + 2ab\sqrt[4]{3} + b^2\sqrt{3}.$$

Igualando coordenadas con respecto de la base citada, obtenemos que $2ab = 0$, por lo que $a = 0$ o bien $b = 0$. En el primer caso, $2 = b^2\sqrt{3}$. Escribiendo $b = x + y\sqrt{3}$ con $x, y \in \mathbb{Q}$, de donde

$$2 = (x^2 + 2xy\sqrt{3} + 3y^2)\sqrt{3} = (x^2 + 3y^2)\sqrt{3} + 6xy,$$

lo que implicaría que $\sqrt{3} \in \mathbb{Q}$, cosa que sabemos no es cierta ya que $X^2 - 3 \in \mathbb{Q}[X]$ es irreducible. Por tanto, $b = 0$, lo que da $2 = a^2$, con lo que $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$, cosa que sabemos no es cierta por un argumento sencillo. Así que llegamos a una contradicción, luego $\sqrt{2} \notin \mathbb{Q}(\sqrt[4]{3})$.

Vamos a mostrar por fin que $\sqrt{2} \notin \mathbb{Q}(\sqrt[8]{3})$. En otro caso, tendríamos que $\sqrt{2} = c + d\sqrt[8]{3}$ con $c, d \in \mathbb{Q}(\sqrt[4]{3})$ y $d \neq 0$. Razonando como antes, obtenemos que

$$2 = c^2 + 2cd\sqrt[8]{3} + d^2\sqrt[4]{3},$$

de donde, por $\mathbb{Q}(\sqrt[4]{3})$–independencia lineal de $\{1, \sqrt[8]{3}\}$, $c = 0$. Obtenemos así que $2 = d^2\sqrt[4]{3}$. Escribiendo $d = z + t\sqrt[4]{3}$, con $z, t \in \mathbb{Q}(\sqrt{3}$ y sustituyendo, obtenemos

$$2 = (z^2 + 2zt\sqrt[4]{3} + t^2\sqrt{3})\sqrt[4]{3} = (z^2 + t^2\sqrt{3})\sqrt[4]{3} + 2zt\sqrt{3}$$

de donde, como antes, $z^2 + t^2\sqrt{3} = 0$. Pero esto es sólo posible si $z = t = 0$, es decir, $d = 0$; contradicción.

Una solución alternativa viene de razonar que $f = X^8 - 3 \in \mathbb{Q}(\sqrt{2})[X]$ es irreducible y usar otra torre de cuerpos. Gracias a que $\mathbb{Q}(\sqrt{2})$ es el cuerpo de fracciones del DFU $\mathbb{Z}[\sqrt{2}]$, basta con demostrar que $f \in \mathbb{Z}[\sqrt{2}][X]$ es irreducible. Esto se deduce del criterio de Eisenstein si comprobamos que $3 \in \mathbb{Z}[\sqrt{2}]$ es irreducible. Dada cualquier factorización $3 = rs$, con $r, s \in \mathbb{Z}[\sqrt{2}]$, tomando normas, deducimos que $9 = N(r)N(s)$. Si r, s no son unidades, entonces[6] $N(r) = N(s) = 3$. Escribamos $r = a + b\sqrt{2}$, con $a, b \in \mathbb{Z}$. Tenemos que $3 = a^2 - 2b^2$. Reduciendo módulo 3, tenemos la igualdad $0 = a^2 + b^2$ en $\mathbb{Z}_3$. Pero esto no es posible salvo que tanto a como b sean múltiplos de 3. Aunque, en tal caso, r es múltiplo de 3 y su norma no puede ser 3. Deducimos, pues, que 3 es irreducible en $\mathbb{Z}[\sqrt{2}]$.

Demostrado que $X^8 - 3$ es irreducible en $\mathbb{Q}(\sqrt{2})[X]$, concluimos que

$$[\mathbb{Q}(\sqrt[8]{3}, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[8]{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 8 \times 2 = 16.$$

De donde se concluye que $[K : \mathbb{Q}] = 32$.

[6] ambos valores podrían ser -3, lo que no cambia el argumento posterior

EJERCICIO 49. Supongamos que el polinomio $f = X^n - a \in F[X]$ es separable, con $a \neq 0$, y sea K su cuerpo de descomposición. Denotemos por $\zeta \in K$ una raíz primitiva n–ésima de la unidad, y $\sqrt[n]{a} \in K$ una raíz de f. Dado $\sigma \in Aut_F(K)$, denotemos por $j(\sigma), k(\sigma) \in \mathbb{Z}_n$ determinados por las condiciones $\sigma(\sqrt[n]{a}) = \zeta^{j(\sigma)}\sqrt[n]{a}, \sigma(\zeta) = \zeta^{k(\sigma)}$. Demostrar que la aplicación

$$Aut_F(K) \to GL_2(\mathbb{Z}_n), \qquad (\sigma \mapsto \begin{pmatrix} 1 & 0 \\ j(\sigma) & k(\sigma) \end{pmatrix}).$$

es un homomorfismo inyectivo de grupos. Deducir que $\#Aut_F(K)$ es un divisor de $n\varphi(n)$. En el caso $F = \mathbb{Q}$, deducir que $\#Aut(K) = n\varphi(n)$ si, y sólo si, $X^n - a \in \mathbb{Q}(\zeta)[X]$ es irreducible.

EJERCICIO 50. Sea $K = \mathbb{Q}(\sqrt[4]{5}, i)$.

1. Razonar que K es una extensión de Galois de $\mathbb{Q}$ y calcular el cardinal de su grupo de Galois.
2. Describir los elementos del grupo $Aut(K)$.
3. Calcular todos los subcuerpos de K que tienen grado 4 sobre $\mathbb{Q}$.
4. Calcular todos los subcuerpos de K.

4.5. Ecuaciones resolubles por radicales

En esta sección, trabajaremos con cuerpos de **característica 0**. Comencemos definiendo algunos conceptos que serán útiles para el desarrollo de esta parte.

DEFINICIÓN 4.34. Una extensión de cuerpos $F \leq E$ se llamará *una extensión por radicales* si existe una torre de cuerpos

$$F = E_0 \leq E_1 \leq \cdots \leq E_t = E$$

tal que $E_j = E_{j-1}(\alpha_j)$ para $\alpha_j \in E_j$ raíz de un polinomio $X^{n_j} - a_j \in E_{j-1}[X]$ para $j = 1, \ldots, t$.

DEFINICIÓN 4.35. Sea $f \in F[X]$. Diremos que f es *resoluble por radicales* si existe una extensión por radicales $F \leq E$ que contiene al cuerpo de descomposición de f.

Para estudiar los polinomios (o ecuaciones) resolubles por radicales, necesitaremos algunos conceptos más.

DEFINICIÓN 4.36. Diremos que una extensión $F \leq K$ es *radical* si K es cuerpo de descomposición de un polinomio separable de la forma $X^n - a \in F[X]$. La extensión se llamará *radical iterada* si es de Galois y existe una torre de cuerpos

$$F = K_0 \leq K_1 \leq \cdots \leq K_t = K$$

tal que cada $K_{i-1} \leq K_i$, para $i = 1, \ldots, t$, es radical.

OBSERVACIÓN 4.37. Es fácil razonar que toda extensión radical iterada es una extensión por radicales.

PROPOSICIÓN 4.38. *Sea $F \leq E$ una extensión de Galois. Supongamos una extensión $E \leq E(\alpha)$, para α una raíz de $X^n - a \in E[X]$, con $a \neq 0$. Existe una extensión radical iterada $E \leq K$ tal que $E(\alpha) \leq K$ y $F \leq K$ es de Galois.*

DEMOSTRACIÓN. Consideremos el polinomio

$$f = \prod_{\sigma \in Aut_F(E)} (X^n - \sigma(a)).$$

Puesto que, para cada $\sigma \in Aut_F(E)$, se tiene que $f^\sigma = f$, sus coeficientes están en $E^{Aut_F(E)} = F$. Por otra parte, E es cuerpo de descomposición de un polinomio $g \in F[X]$. Definamos K como el cuerpo de descomposición del polinomio $fg \in F[X]$. Ya que estamos en característica cero, $F \leq K$ es de Galois. Obviamente, $\alpha \in K$, así que $E(\alpha) \leq K$. Como K contiene todas las raíces de $X^n - a$, ha de contener, por el Teorema 4.25, una raíz primitiva n–ésima de la unidad ζ, y el cuerpo de descomposición de $X^n - a$ es $E(\alpha, \zeta)$.

Numeremos $Aut_F(E) = \{\sigma_1, \ldots, \sigma_s\}$ con $\sigma_1 = id_E$. Para cada $i = 1, \ldots, s$, tomamos una raíz $\alpha_i \in K$ de $X^n - \sigma_i(a)$ con $\alpha_1 = \alpha$. Tenemos entonces la torre de cuerpos

$$E = K_{-1} \leq K_0 \leq \cdots \leq K_s = K,$$

dada por $K_0 = E(\zeta), K_i = K_{i-1}(\alpha_i)$ para $i = 1, \ldots, s$. Así, K_0 es cuerpo de descomposición de $X^n - 1 \in E[X]$ y, según el Teorema 4.25, K_i es cuerpo de descomposición de $X^n - \sigma_i(a) \in K_{i-1}[X]$ para $i = 1, \ldots, s$. Conclusión: la extensión $E \leq K$ es radical iterada. □

PROPOSICIÓN 4.39. *Si $F \leq E$ es una extensión por radicales, entonces existe una extensión radical iterada $F \leq K$ tal que $E \leq K$.*

DEMOSTRACIÓN. Sea una torre de cuerpos

$$F = E_0 \leq E_1 \leq \cdots \leq E_t = E$$

tal que $E_j = E_{j-1}(\alpha_j)$, donde $\alpha_j \in E_j$ raíz de un polinomio $X^{n_1} - a_j \in E_{j-1}[X]$, para $j = 1, \ldots, t$. Nuestra demostración procede por inducción sobre $t \geq 0$. La afirmación es trivial para $t = 0$, así que vayamos al paso inductivo para $t > 0$. Por hipótesis de inducción, tenemos una extensión radical iterada

$$F = K_0 \leq K_1 \leq \cdots \leq K_r$$

tal que $E_{t-1} \leq K_r$. Tomemos una F–extensión común de K_r y E_t, dentro de la cual podemos considerar el subcuerpo $K_r(\alpha_t)$. Obviamente, $E_t \leq K_r(\alpha_t)$. Por la Proposición 4.38 existe una extensión radical iterada $K_r \leq K$ tal que $K_r(\alpha_t) \leq K$ y $F \leq K$ es de Galois. Por tanto, existe una torre de extensiones radicales

$$K_r \leq K_{r+1} \leq \cdots \leq K_s = K.$$

De modo que en la torre

$$F = K_0 \leq K_1 \leq \cdots \leq K_r \leq K_{r+1} \leq \cdots \leq K_s = K$$

cada extensión es radical y $F \leq K$ es de Galois. Así, $F \leq K$ es una extensión radical iterada. □

LEMA 4.40. *Si $F \leq K$ es una extensión radical iterada, entonces $Aut_F(K)$ es un grupo resoluble.*

DEMOSTRACIÓN. Tomemos una torre de cuerpos

$$F = K_0 \leq K_1 \leq \cdots \leq K_t = K$$

tal que cada $K_{i-1} \leq K_i$, para $i = 1, \ldots, t$, es radical. Por hipótesis, $F \leq K$ de de Galois, así que, por la Conexión de Galois tenemos una cadena de subgrupos

$$Aut_F(K) = Aut_{K_0}(K) \supseteq Aut_{K_1}(K) \supseteq \cdots \supseteq Aut_{K_{t-1}}(K) \supseteq Aut_{K_t}(K) = \{id_K\}.$$

Ahora bien, $Aut_{K_i}(K)$ es normal en $Aut_{K_{i-1}}(K)$ para cada $i = 1, \ldots, t$, ya que $K_{i-1} \leq K_i$ es de Galois, por el Teorema 3.27. Por último, el mismo teorema nos dice que

$$Aut_{K_{i-1}}(K)/Aut_{K_i}(K) \cong Aut_{K_{i-1}}(K_i),$$

y éste último grupo es resoluble por la Proposición 4.32. Por tanto, $Aut_F(K)$ es resoluble. □

EJERCICIO 51. Sea $f \in F[X]$ y L un cuerpo de descomposición de f sobre F. Demostrar que, para cualquier extensión $F \leq E$, si K es cuerpo de descomposición de f sobre E, entonces $Aut_E(K)$ es isomorfo a un subgrupo de $Aut_F(L)$.

TEOREMA 4.41. *Un polinomio $f \in F[X]$ es resoluble por radicales si, y sólo si, su grupo de Galois es resoluble.*

DEMOSTRACIÓN. Sea L un cuerpo de descomposición de f. Si f es resoluble por radicales, tenemos una torre de cuerpos $F \leq L \leq E$ tal que E es una extensión por radicales de F. La Proposición 4.39 proporciona una extensión radical iterada $F \leq K$ tal que $E \leq K$. Obviamente, $L \leq K$ y, por otra parte, $F \leq L$ es de Galois. Por el Teorema 3.27, $Aut_L(K)$ es un subgrupo normal de $Aut_F(K)$ y $Aut_F(L) \cong Aut_F(K)/Aut_L(K)$. Según el Lema 4.40, $Aut_F(K)$ es resoluble, luego así lo es también $Aut_F(L)$.

Recíprocamente, supongamos que $Aut_F(L)$ es resoluble y pongamos $n = [L : F]$. Consideramos la extensión $K = L(\zeta)$, para ζ una raíz n–ésima primitiva de la unidad. La extensión $F \leq K$ es de Galois, puesto que K es cuerpo de descomposición de $(X^n - 1)f \in F[X]$.

Como, de acuerdo con el Ejercicio 51, $Aut_{F(\zeta)}(K)$ es isomorfo a un subgrupo de $Aut_F(L)$, tenemos que $Aut_{F(\zeta)}(K)$ es resoluble y que $\#Aut_{F(\zeta)}(K)$ divide a $n = \#Aut_F(L)$. Tomemos una serie de composición

$$Aut_{F(\zeta)}(K) = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_{t-1} \supseteq G_t = \{id_K\}. \tag{4.7}$$

Cada factor de composición G_{i-1}/G_i es cíclico de orden primo p_i. Observemos que p_i es un divisor de n. Aplicando la conexión de Galois a (4.7) obtenemos una torre de cuerpos

$$F(\zeta) = K^{G_0} \leq K^{G_1} \leq \cdots \leq K^{G_{t-1}} \leq K^{G_t} = K. \tag{4.8}$$

Cada K^{G_i} contiene una raíz p_i–ésima primitiva de la unidad y el grupo de Galois de la extensión es isomorfo a G_{i-1}/G_i, luego cíclico. En virtud del Teorema 4.31, cada extensión $K^{G_{i-1}} \leq K^{G_i}$ es radical y, a la vista de (4.8), $F(\zeta) \leq K$ es una extensión radical iterada. Finalmente, $F \leq K$ es extensión radical iterada y, así, por radicales. Como $L \leq K$, deducimos que f es resoluble por radicales. □

OBSERVACIÓN 4.42. Un ejemplo de quíntica no resoluble por radicales sobre $\mathbb{Q}$ es la que aparece en el Ejercicio 45.

4.6. La ecuación general de grado n

Sea $F[X_1, \ldots, X_n]$ el anillo de polinomios en las indeterminadas $X_1, \ldots, X_n$ con coeficientes en un cuerpo F y denotemos por $E = F(X_1, \ldots, X_n)$ su cuerpo de fracciones. Dada una permutación $\sigma \in S_n$, ésta da un automorfismo F–lineal de anillos $\overline{\sigma} : F[X_1, \ldots, X_n] \to F[X_1, \ldots, X_n]$ determinado por $\overline{\sigma}(X_i) = X_{\sigma(i)}$, para $i = 1, \ldots, n$. Que proporciona un único automorfismo F–lineal de cuerpos de E, que denotamos también por $\overline{\sigma}$. La aplicación que lleva σ a $\overline{\sigma}$ es un homomorfismo inyectivo de grupos de S_n a $Aut_F(E)$. Denotemos por G su imagen.

DEFINICIÓN 4.43. El cuerpo E^G se llama *cuerpo de las funciones racionales simétricas* en $X_1, \ldots, X_n$ con coeficientes en F.

PROPOSICIÓN 4.44. *Para cada* $k = 1, \dots, n$*, escribamos*

$$s_k = \sum_{1 \le i_1 < \cdots < i_k \le n} X_{i_1} \cdots X_{i_k}.$$

Entonces

$$E^G = F(s_1, \dots, s_n).$$

DEMOSTRACIÓN. Tomemos el polinomio

$$f = (X - X_1) \cdots (X - X_n) \in E[X].$$

Para cada $\overline{\sigma} \in G$, es claro que $f^{\overline{\sigma}} = f$, así que sus coeficientes están en E^G. Por otra parte, las identidades de Cardano-Vieta (ver Ejercicio 42), dan

$$f = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n. \tag{4.9}$$

Así, $s_k \in E^G$ para $k = 1, \dots, n$ y deducimos que $F(s_1, \dots, s_n) \le E^G$.

Observemos que E es cuerpo de descomposición de f sobre $F(s_1, \dots, s_n)$. Como f es separable, tenemos que $F(s_1, \dots, s_n) \le E$ es de Galois, gracias al Teorema 3.15. Además, $G \subseteq \mathrm{Aut}_{F(s_1,\dots,s_n)}(E)$. Pero, si $\tau : E \to E$ es un automorfismo $F(s_1, \dots, s_n)$–lineal, entonces, para cada $i = 1, \dots, n$, tenemos

$$0 = \tau(0) = \tau(f(X_i)) = f(\tau(X_i)),$$

luego τ permuta raíces de f, así que $\tau \in G$. Obtenemos que G es el grupo de Galois de la extensión $F(s_1, \dots, s_n) \le E$, de donde, por la Conexión de Galois, $E^G = F(s_1, \dots, s_n)$. □

Abordemos ahora la solubilidad de la ecuación general de grado n. Por tal, entendemos la de un polinomio

$$g = X^n - \lambda_1 X^{n-1} + \cdots + (-1)^n \lambda_n \in F(\lambda_1, \dots, \lambda_n)[X], \tag{4.10}$$

donde $\lambda_1, \dots, \lambda_n$ son indeterminadas y $F(\lambda_1, \dots, \lambda_n)$ es el cuerpo de fracciones del anillo de polinomios $F[\lambda_1, \dots, \lambda_n]$. Los cambios de signo que aparecen en (4.10) son para facilitar la exposición y, obviamente, no suponen restricción sobre la generalidad de g.

LEMA 4.45. *Sea* $h \in F[\lambda_1, \dots, \lambda_n]$ *no nulo. Entonces* $h(s_1, \dots, s_n) \neq 0$.

DEMOSTRACIÓN. Observemos que, definiendo $s_0 = 1$ y $s_n(X_1, \dots, X_{n-1}) = 0$, tenemos la relación

$$s_k(X_1, \dots, X_n) = s_k(X_1, \dots, X_{n-1}) + s_{k-1}(X_1, \dots, X_{n-1}) X_n, \quad (k = 1, \dots, n),$$

de donde

$$s_k(X_1, \dots, X_{n-1}, 0) = s_k(X_1, \dots, X_{n-1}), \quad (k = 1, \dots, n). \tag{4.11}$$

Demostremos el lema razonando por inducción sobre n.

Para $n = 1$, puesto que $s_1(X_1) = X_1$, tenemos que $h(s_1) = h(X_1)$ y la aserción es trivial

Supongamos $n > 1$ y, razonando por reducción al absurdo, que existe $h \neq 0$ tal que $h(s_1, \dots, s_n) = 0$. Tomemos $h = h_0 + h_1 \lambda_n + \cdots + h_m \lambda_n^m$ de grado mínimo m en λ_n con esta propiedad, donde $h_0, \dots, h_{n-1} \in F[\lambda_1, \dots, \lambda_{n-1}]$.

Tenemos que

$$0 = h_0(s_1, \dots, s_{n-1}) + h_1(s_1, \dots, s_{n-1}) s_n + \cdots + h_m(s_1, \dots, s_{n-1}) s_n^m.$$

Evaluando ahora en $X_n = 0$, obtenemos, puesto que $s_n(X_1, \dots, X_n) = X_1 \cdots X_n$, que

$$0 = h_0(s_1(X_1, \dots, X_{n-1}, 0), \dots, s_{n-1}(X_1, \dots, X_{n-1}, 0)).$$

Según (4.11), hemos obtenido que

$$0 = h_0(s_1(X_1, \dots, X_{n-1}), \dots, s_{n-1}(X_1, \dots, X_{n-1})).$$

Por hipótesis de inducción, tenemos que $h_0(\lambda_1, \dots, \lambda_{n-1}) = 0$. Por tanto,

$$h = (h_1 + h_2\lambda_n + \cdots + h_m\lambda_n^{m-1})\lambda_n.$$

Evaluando en $(s_1, \dots, s_n)$, nos queda que

$$0 = (h_1(s_1, \dots, s_{n-1}) + h_2(s_1, \dots, s_{n-1})s_n + \cdots + h_m(s_1, \dots, s_{n-1})s_n^{m-1})s_n.$$

Como $s_n \neq 0$, el primer factor del segundo miembro ha de ser cero, por lo que el polinomio no nulo de grado $m-1$

$$h_1 + h_2\lambda_n + \cdots + h_m\lambda_n^{m-1}$$

se anula en $(s_1, \dots, s_n)$, en contradicción con el carácter minimal del grado m. □

PROPOSICIÓN 4.46. *El polinomio* g *en* (4.10) *es irreducible, separable y su grupo de Galois es isomorfo a* S_n*.*

DEMOSTRACIÓN. Consideremos, con la notación de la Proposición 4.44, el homomorfismo F–lineal de anillos $\epsilon : F[\lambda_1, \dots, \lambda_n] \to F(s_1, \dots, s_n)$ determinado por las condiciones $\epsilon(\lambda_k) = s_k$, para $k = 1, \dots, n$, que existe por la propiedad universal del anillo de polinomios. Como $F(s_1, \dots, s_n)$ es un cuerpo, dicho homomorfismo, que es inyectivo por el Lema 4.45, se extiende de manera única, por la propiedad universal del cuerpo de fracciones, a un homomorfismo de cuerpos, que denotamos igual, $\epsilon : F(\lambda_1, \dots, \lambda_n) \to F(s_1, \dots, s_n)$. Dicho homomorfismo es, obviamente, sobreyectivo y, por tanto, es un isomorfismo F–lineal de cuerpos. Además, $g^\epsilon = f$, en la notación de (4.9). Como $E = F(X_1, \dots, X_n)$ es cuerpo de descomposición de f sobre $E^G = F(s_1, \dots, s_n)$, se sigue que $\epsilon : F(\lambda_1, \dots, \lambda_n) \to E$ da un cuerpo de descomposición de g sobre $F(\lambda_1, \dots, \lambda_n)$. Así, el grupo de Galois de g sobre $F(\lambda_1, \dots, \lambda_n)$ es (isomorfo a) G y, por ende, a S_n. Como f es separable, lo es g y como, obviamente, S_n actúa transitivamente sobre las raíces de f, así lo hace sobre las de g. Deducimos de la Proposición 4.4 que g es irreducible. □

OBSERVACIÓN 4.47. El polinomio $g = X^n - \lambda_1 X^{n-1} + \cdots + (-1)^n\lambda_n \in F[\lambda_1, \dots, \lambda_n][X]$ es también irreducible. Esto se deduce de la Proposición 4.46 junto con [**2**, Proposición 4.24, Teorema 4.26].

TEOREMA 4.48 (Abel-Ruffini). *Si* F *es de característica* 0*, entonces el polinomio* g *dado en* (4.10) *no es resoluble por radicales sobre* $F(\lambda_1, \dots, \lambda_n)$ *para* $n \geq 5$*.*

DEMOSTRACIÓN. Por la Proposición 4.46, el grupo de Galois de g sobre $F(\lambda_1, \dots, \lambda_n)$ es isomorfo a S_n, que no es resoluble para $n \geq 5$. Por el Teorema 4.41, f no es resoluble por radicales sobre $F(\lambda_1, \dots, \lambda_n)$. □

4.7. Resolución de las ecuaciones de grado hasta 4

Las ecuaciones de grado hasta 4 son resolubles por radicales en característica cero, gracias al Teorema 4.41. En realidad, lo son para casi todas las características. Vamos a dar procedimientos clásicos para tal resolución para los diferentes grados.

4.7.1. Ecuación cuadrática. Supongamos $f = X^2 + bX + c \in F[X]$. Si la característica de F es distinta de dos, tenemos

$$f = (X + b/2)^2 + c - b^2/4.$$

Por tanto, las raíces de f en una extensión adecuada de F son

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

4.7.2. Ecuación cúbica. Vamos a usar el llamado método de Cardano. Partimos de

$$f = X^3 + bX^2 + cX + d \in F[X],$$

y suponemos que la característica de F no es 2 ni 3. Definimos

$$g(X) = f(X - b/3) = X^3 + pX + q,$$

para $p, q \in F$ adecuados, que se ajustan igualando coeficientes del mismo grado. Obviamente, si calculamos las raíces de la *cúbica reducida* g, obtendremos fácilmente las de f.

Sean $\alpha_1, \alpha_2, \alpha_3 \in K$ las raíces de g en una extensión $F \leq K$ que, además, tomamos conteniendo una raíz cúbica primitiva de la unidad ω. Definimos

$$\begin{aligned} \beta &= \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \\ \gamma &= \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3. \end{aligned}$$

Sumando y teniendo en cuenta que $\alpha_1 + \alpha_2 + \alpha_3 = 0$, derivamos que

$$\beta + \gamma = 3\alpha_1.$$

Por otra parte,

$$\begin{aligned} \beta\gamma &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_2\alpha_3 - \alpha_1\alpha_3 \\ &= (\alpha_1 + \alpha_2 + \alpha_3)^2 - 3(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3) = -3p. \end{aligned}$$

Tomando

$$u = \beta/3, v = \gamma/3,$$

tenemos que $\alpha_1 = u + v$, de donde

$$0 = (u + v)^3 + p(u + v) + q = u^3 + v^3 + (3uv + p)(u + v) + q = u^3 + v^3 + q,$$

ya que $3uv = -p$. Tenemos así que

$$\begin{aligned} u^3 + v^3 &= -q \\ u^3v^3 &= -p^3/27. \end{aligned}$$

Por tanto, u^3, v^3 son raíces del polinomio cuadrático

$$h(Z) = (Z - u^3)(Z - v^3) = Z^2 + qZ - \frac{p^3}{27}.$$

Calculando las raíces de h, y las raíces cúbicas de éstas, tenemos seis candidatas a u, v. La condición $3uv = -p$ proporciona las parejas que hacen que $u + v$ sean las raíces de g.

EJEMPLO 4.49. Consideremos $f = X^3 - 6X^2 - 9X + 2 \in \mathbb{Q}[X]$. La cúbica reducida es

$$g(X) = f(X + 2) = X^3 - 21X - 32.$$

Escribiendo, según la exposición anterior, las raíces de g como $\alpha = u + v$, tenemos $uv = 7$. Así, u^3, v^3 son las raíces del polinomio

$$h(Z) = Z^2 - 32Z + 343.$$

Estas raíces son $16 \pm i\sqrt{87}$. Pongamos $u^3 = 16 + i\sqrt{87}, v^3 = 16 - i\sqrt{87}$. Fijando valores para las raíces cúbicas complejas involucradas, los posibles valores de u, v se pueden expresar como

$$u_k = e^{ik2\pi/3}\sqrt[3]{16 + i\sqrt{87}}, \qquad (k = 0, 1, 2).$$

$$v_k = e^{ik2\pi/3}\sqrt[3]{16 - i\sqrt{87}}, \qquad (k = 0, 1, 2).$$

Tenemos que $v_0u_0 = v_1u_2 = v_2u_1 = 7$. Las raíces de g son, así,

$$\begin{array}{rcl} u_0 + v_0 & = & \sqrt[3]{16 + i\sqrt{87}} + \sqrt[3]{16 - i\sqrt{87}} \\ u_1 + v_2 & = & e^{i2\pi/3}\sqrt[3]{16 + i\sqrt{87}} + e^{i4\pi/3}\sqrt[3]{16 - i\sqrt{87}} \\ u_2 + v_1 & = & e^{i4\pi/3}\sqrt[3]{16 + i\sqrt{87}} + e^{i2\pi/3}\sqrt[3]{16 - i\sqrt{87}}. \end{array}$$

Finalmente, las de f resultan:

$$\begin{array}{rcl} u_0 + v_0 + 2 & = & \sqrt[3]{16 + i\sqrt{87}} + \sqrt[3]{16 - i\sqrt{87}} + 2 \\ u_1 + v_2 + 2 & = & e^{i2\pi/3}\sqrt[3]{16 + i\sqrt{87}} + e^{i4\pi/3}\sqrt[3]{16 - i\sqrt{87}} + 2 \\ u_2 + v_1 + 2 & = & e^{i4\pi/3}\sqrt[3]{16 + i\sqrt{87}} + e^{i2\pi/3}\sqrt[3]{16 - i\sqrt{87}} + 2. \end{array}$$

4.7.3. Resolución de la cuártica. Aquí vamos a usar el método de Lagrange. Tomemos $f \in F[X]$ de grado 4 para F un cuerpo de característica distinta de $2, 3$. Pongamos

$$f = X^4 + bX^3 + cX^2 + dX + e,$$

entonces

$$g = f(X - b/4) = X^4 + pX^2 + qX + r,$$

para ciertos $p, q, r \in F$ que se calculan a partir de $b, c, d, e \in F$. Vamos a obtener una ecuación cúbica auxiliar cuya resolución llevará a la de la ecuación $g = 0$. Para ello, tomamos las raíces $\beta_1, \beta_2, \beta_3, \beta_4$ de g en un cuerpo de descomposición suyo. Definimos

$$\begin{array}{rcl} \rho_1 & = & -(\beta_1 + \beta_2)(\beta_3 + \beta_4) \\ \rho_2 & = & -(\beta_1 + \beta_3)(\beta_2 + \beta_4) \\ \rho_3 & = & -(\beta_1 + \beta_4)(\beta_2 + \beta_3). \end{array} \tag{4.12}$$

El polinomio

$$h(Y) = (Y - \rho_1)(Y - \rho_2)(Y - \rho_3),$$

tiene coeficientes en F porque es invariante por el grupo de Galois de g visto como grupo de permutaciones. Aunque esta afirmación requiere en principio que las raíces de g sean simples, la conclusión es correcta en general, ya que, de las relaciones de Cardano-Vieta para g deducimos, aparte de la igualdad

$$\beta_1 + \beta_2 + \beta_3 + \beta_4 = 0, \tag{4.13}$$

y tras unos cálculos, que

$$\begin{array}{rcl} \rho_1 + \rho_2 + \rho_3 & = & -2p \\ \rho_1\rho_2 + \rho_1\rho_3 + \rho_2\rho_3 & = & p^2 - 4r \\ \rho_1\rho_2\rho_3 & = & q^2. \end{array}$$

Por tanto,

$$h(Y) = Y^3 + 2pY^2 + (p^2 - 4r)Y - q^2, \tag{4.14}$$

polinomio que es *una resolvente cúbica* de g. Supuesta resuelta, conocemos ρ_1, ρ_2, ρ_3. Deducimos de (4.12) y (4.13) que

$$\begin{array}{llll} \beta_1+\beta_2 = \sqrt{\rho_1}, & \beta_3+\beta_4 = -\sqrt{\rho_1} \\ \beta_1+\beta_3 = \sqrt{\rho_2}, & \beta_2+\beta_4 = -\sqrt{\rho_2} \\ \beta_1+\beta_4 = \sqrt{\rho_3}, & \beta_2+\beta_3 = -\sqrt{\rho_3} \end{array} \tag{4.15}$$

La determinación de las tres raíces cuadradas, que pueden encontrarse en una extensión adecuada de K, ha de hacerse de modo que

$$\sqrt{\rho_1}\sqrt{\rho_2}\sqrt{\rho_3} = -q,$$

lo que se deduce como sigue:

$$\begin{aligned} \sqrt{\rho_1}\sqrt{\rho_2}\sqrt{\rho_3} &= (\beta_1+\beta_2)(\beta_1+\beta_3)(\beta_1+\beta_4) \\ &= \beta_1^3+\beta_1^2\beta_2+\beta_1^2\beta_3+\beta_1^2\beta_4 \\ &+ \beta_1\beta_2\beta_3+\beta_1\beta_3\beta_4+\beta_1\beta_2\beta_4+\beta_2\beta_3\beta_4 \\ &= \beta_1^2(\beta_1+\beta_2+\beta_3+\beta_4)-q \\ &= -q, \end{aligned}$$

donde hemos usado (4.13) y, de nuevo, las identidades de Cardano-Vieta.

Por último, sumando de tres en tres ecuaciones adecuadas de (4.15), obtenemos

$$\begin{aligned} \beta_1 &= \tfrac{1}{2}(\sqrt{\rho_1}+\sqrt{\rho_2}+\sqrt{\rho_3}) \\ \beta_2 &= \tfrac{1}{2}(\sqrt{\rho_1}-\sqrt{\rho_2}-\sqrt{\rho_3}) \\ \beta_3 &= \tfrac{1}{2}(-\sqrt{\rho_1}+\sqrt{\rho_2}-\sqrt{\rho_3}) \\ \beta_4 &= \tfrac{1}{2}(-\sqrt{\rho_1}-\sqrt{\rho_2}+\sqrt{\rho_3}). \end{aligned}$$

EJERCICIO 52. Demostrar que el discriminante de una resolvente cúbica, de entre las definidas durante este curso, de una cuártica coincide con el de ésta.

4.8. Ecuaciones sobre cuerpos finitos

Recordemos de la sección 2.2 que un cuerpo finito tiene $q = p^k$ elementos, para p su característica, que dos cuerpos finitos con el mismo cardinal son isomorfos, y que, para cada cardinal como el mencionado, existe un cuerpo finito de ese tamaño. Sabemos, también, que cualquier extensión de cuerpos finitos es de Galois (Teorema 3.20).

TEOREMA 4.50. *Sea $\mathbb{F}_q \leq \mathbb{F}_{q^n}$ una extensión de cuerpos finitos. Entonces $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ es un grupo cíclico de orden n generado por ϕ, definido por*

$$\phi(\alpha) = \alpha^q, \qquad (\alpha \in \mathbb{F}_{q^n}).$$

Además, $\mathbb{F}_{q^n}$ es cuerpo de descomposición sobre $\mathbb{F}_q$ de $X^{q^n}-X$.

DEMOSTRACIÓN. Como $q = p^k$ tenemos, por el Corolario 3.20, la torre de extensiones de Galois $\mathbb{F}_p \leq \mathbb{F}_{p^k} \leq \mathbb{F}_{p^{kn}}$. Sabemos, por el Teorema 2.24, que $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^{kn}}) = \langle\tau\rangle$, donde τ es el automorfismo de Frobenius de $\mathbb{F}_{p^{kn}}$. Como $[\mathbb{F}_{p^{kn}} : \mathbb{F}_{p^k}] = n$, el grupo $\mathrm{Aut}_{\mathbb{F}_{p^k}}(\mathbb{F}_{p^{kn}})$ es un subgrupo de orden n de $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^{kn}})$, y, por tanto, $\mathrm{Aut}_{\mathbb{F}_{p^k}}(\mathbb{F}_{p^{kn}}) = \langle\tau^k\rangle$. Tomando $\phi = \tau^k$ obtenemos la primera parte del enunciado. La segunda afirmación es consecuencia directa de que, por la Proposición 2.19, $\mathbb{F}_{q^n}$ es cuerpo de descomposición sobre $\mathbb{F}_p$ de $X^{q^n}-X$. □

DEFINICIÓN 4.51. El automorfismo ϕ del enunciado del Teorema 4.50 se llama *automorfismo de Frobenius* de la extensión $\mathbb{F}_q \leq \mathbb{F}_{q^n}$.

TEOREMA 4.52. *Si $f \in \mathbb{F}_q[X]$ es un polinomio irreducible de grado n, entonces su cuerpo de descomposición es $\mathbb{F}_{q^n}$. Además, dada una raíz $\alpha \in \mathbb{F}_{q^n}$ de f, el resto de sus raíces son $\alpha^q, \ldots, \alpha^{q^{n-1}}$.*

DEMOSTRACIÓN. Como f es irreducible de grado n, ha de tener una raíz en una extensión de $\mathbb{F}_q$ de grado n, por ejemplo $\mathbb{F}_q[X]/\langle f\rangle$, que es un cuerpo finito con q^n elementos. Como, según el Teorema 3.20, la extensión $\mathbb{F}_q \leq \mathbb{F}_{q^n}$ es de Galois y f es irreducible, resulta que f es separable y todas sus raíces están en $\mathbb{F}_{q^n}$ y son distintas, en virtud del Teorema 3.15. Deducimos que $\mathbb{F}_{q^n}$ es cuerpo de descomposición de f. Por otra parte, el automorfismo de Frobenius ϕ de la extensión $\mathbb{F}_q \leq \mathbb{F}_{q^n}$ permuta transitivamente estas raíces, por la Proposición 4.4. La descripción de todas ellas se sigue de aquí. □

TEOREMA 4.53. *Un polinomio irreducible $f \in \mathbb{F}_q[X]$ de grado n divide a $X^{q^m} - X$ si, y sólo si, n divide a m. Como consecuencia, $X^{q^m} - X$ es el producto de todos los polinomios mónicos irreducibles de $\mathbb{F}_q[X]$ cuyo grado es un divisor de m.*

DEMOSTRACIÓN. Supongamos que f divide a $X^{q^m} - X$. Tomando los respectivos cuerpos de descomposición, y teniendo en cuenta el Teorema 4.52, obtenemos que $\mathbb{F}_{q^n}$ es un subcuerpo de $\mathbb{F}_{q^m}$. Pero esto implica que n es un divisor de m.

Recíprocamente, supongamos que n divide a m. Entonces $\mathbb{F}_{q^n} \leq \mathbb{F}_{q^m}$. Por el Teorema 4.52, las raíces de f están en $\mathbb{F}_{q^m}$. Pero cada una de ellas es raíz de $X^{q^m} - X$, puesto que todos los elementos de $\mathbb{F}_{q^m}$ son raíces de dicho polinomio. Por tanto, f divide a $X^{q^m} - X$.

Como el polinomio $X^{q^m} - X \in \mathbb{F}_q[X]$ es separable, es producto de polinomios irreducibles mónicos distintos. Según lo descrito en la equivalencia recién demostrada, éstos han de ser todos los polinomios mónicos irreducibles cuyo grado es un divisor de m.

□

EJEMPLO 4.54. De acuerdo con el Teorema 4.53, tenemos la factorización en $\mathbb{F}_2[X]$

$$X^{16}+X = X(X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1). \tag{4.16}$$

Para obtenerla, puede considerarse que hay dos polinomios irreducibles de grado 1 en $\mathbb{F}_2[X]$ y uno de grado 2. Ajustando grados, y de acuerdo con el teorema, $X^{16} + X$ ha de tener, exactamente, tres factores irreducibles de grado 4, que podemos buscar fácilmente de entre los que no tienen raíces en $\mathbb{F}_2$ y no son múltiplos de $X^2 + X + 1$.

De acuerdo con el Teorema 4.52, puedo presentar $\mathbb{F}_{16} = \mathbb{F}_2(a)$, con $a^4 + a + 1 = 0$. Este cuerpo, al ser extensión de Galois de $\mathbb{F}_2$, ha de contener también a todas las raíces de $X^4 + X^3 + 1 \in \mathbb{F}_2[X]$, que vamos a expresar en función de a. Para ello, calculemos el orden de a en el grupo multiplicativo $\mathbb{F}_{16}^\times$, que sabemos es cíclico de orden 15. Así, el orden mencionado ha de ser un divisor de 15. No es 1 ni 3, puesto que $\{1, a, a^2, a^3\}$ es una $\mathbb{F}_2$–base de $\mathbb{F}_{16}$. Veamos si tiene orden 5.

$$a^5 = aa^4 = a(a+1) = a^2 + a \neq 1,$$

ya que $\{1, a, a^2\}$ es $\mathbb{F}_2$–linealmente independiente. Por tanto, a tiene orden 15, y ha de ser un generador de $\mathbb{F}_{16}$. Esto es lo que se llama, en el contexto de cuerpos finitos, un elemento primitivo del cuerpo finito $\mathbb{F}_{16}$.

Las raíces de $f = X^4+X^3+1$ son distintas de las de X^4+X+1, así que, de acuerdo con el Teorema 4.52, son distintas de a, a^2, a^4, a^8. A falta de otro método, y como criterio heurístico de búsqueda, probaremos si las raíces de f están entre los otros elementos primitivos, a saber, $a^7, a^{11}, a^{13}, a^{14}$. De hecho, si una de ellos lo es, el Teorema 4.52 garantiza que lo son el resto. Bien,

$$(a^7)^4 + (a^7)^3 + 1 = a^{28} + a^{21} + 1 = a^{13} + a^6 + 1 = a(a^4)^3 + a^2a^4 + 1$$
$$= a(a+1)^3 + a^2(a+1) + 1 = a^4 + a^3 + a^2 + a + a^3 + a^2 + 1 = a + 1 + a + 1 = 0.$$

Observemos, por último, que, como los elementos de $\mathbb{F}_{16}$ son, precisamente, las raíces de $X^{16} + X$, la factorización (4.16) indica que las raíces de $X^4 + X^3 + X^2 + X + 1$ han de ser a^3, a^6, a^{12}, a^9. Observemos que ninguna de ellas genera el grupo multiplicativo $\mathbb{F}_{16}^\times$. De modo que nuestra suposición heurística no estaba exenta de riesgo...

Capítulo 5

Algunos ejercicios

5.1. Ejercicios propuestos

EJERCICIO 53. Sea F un cuerpo de descomposición de $f = X^3 + X + 1 \in \mathbb{F}_2[X]$ y $\alpha \in F$ una raíz de f. Razonar que $F = \mathbb{F}_2(\alpha)$. Resolver, en F, las siguientes ecuaciones, expresando las soluciones en función de α:

$$x^3 + x + 1 = 0; \quad x^3 + x^2 + 1 = 0; \quad x^2 + x + 1 = 0.$$

EJERCICIO 54. Sea K un cuerpo de descomposición de $f = X^3 + X + 1 \in \mathbb{F}_4[X]$ y $\alpha \in K$ una raíz de f. Razonar que $K = \mathbb{F}_4(\alpha)$. Resolver, en K, las siguientes ecuaciones, expresando las soluciones en función de α:

$$x^3 + x + 1 = 0; \quad x^3 + x^2 + 1 = 0; \quad x^2 + x + 1 = 0.$$

Construir, si es posible, una base de K sobre $\mathbb{F}_2$ usando α y una solución de la tercera ecuación.

EJERCICIO 55. Calcular el número de polinomios irreducibles de grado 6 en $\mathbb{F}_2[X]$. (Nota: hay una fórmula general, si la encuentras en la web, no la uses, no se trata de eso).

EJERCICIO 56. Calcular los grupos de Galois sobre $\mathbb{Q}$ de los polinomios $f = (X^2 + X + 1)(X^2 - 3)$ y $g = (X^2 + X + 1)(X^2 + 3)$.

EJERCICIO 57. Calcular el cardinal del grupo de Galois sobre $\mathbb{Q}$ del polinomio $f = (X^3 + X + 1)(X^2 + 1)$.

EJERCICIO 58. Tomemos $f = (X^3 - 2)(X^2 - 3) \in \mathbb{Q}[X]$ y K el cuerpo de descomposición sobre $\mathbb{Q}$ de f.

1. Decidir razonadamente si $i + \sqrt{3} \in K$.
2. Calcular razonadamente $[K : \mathbb{Q}]$.
3. Describir los elementos del grupo $\mathrm{Aut}(K)$.
4. Describir los elementos de $\mathrm{Aut}_{\mathbb{Q}(i+\sqrt{3})}(K)$ y decidir si es un subgrupo normal de $\mathrm{Aut}(K)$.

EJERCICIO 59. Sea $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$ y α cualquier raíz real de f. Demostrar que el cuerpo de descomposición de f sobre $\mathbb{Q}$ es $\mathbb{Q}(\alpha)$.

EJERCICIO 60. Sea K el cuerpo de descomposición del polinomio $f = (X^2 + 3)(X^3 - 3) \in \mathbb{Q}[X]$. Calcular todos los subcuerpos de K. Demostrar que $\mathbb{Q}(\sqrt[3]{3} + i\sqrt{3}) = K$.

EJERCICIO 61. Sea F un cuerpo de descomposición de $f = X^6 + X + 1 \in \mathbb{F}_2[X]$ y $\alpha \in F$ una raíz de f.

1. Razonar que $F = \mathbb{F}_2(\alpha)$.
2. Calcular el orden multiplicativo de α.
3. Resolver en F, expresando las soluciones en función de α, la ecuación $x^2 + x + 1 = 0$.

EJERCICIO 62. Sea $\alpha = \sqrt{2} + i\sqrt{3} \in \mathbb{C}$.

1. Demostrar que $\sqrt{2} \in \mathbb{Q}(\alpha)$ y calcular $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.
2. Calcular, definiendo explícitamente todos sus elementos, el grupo de Galois de $\mathrm{Irr}(\alpha; \mathbb{Q})$.
3. ¿Son las raíces de $\mathrm{Irr}(\alpha; \mathbb{Q})$ construibles con regla y compás?

EJERCICIO 63. Sea K el cuerpo de descomposición de $f = X^6 - 3 \in \mathbb{Q}[X]$.

1. Calcular $[K : \mathbb{Q}]$.
2. Demostrar que $i + \sqrt{3} \in K$.
3. Calcular, definiendo explícitamente todos sus elementos, el grupo $G = \mathrm{Aut}_{\mathbb{Q}(i+\sqrt{3})}(K)$.
4. ¿Es G un subgrupo normal del grupo de Galois de f?

EJERCICIO 64. Sea $F = \mathbb{F}_3(a)$ un cuerpo con a satisfaciendo la ecuación $a^3 + a - 1 = 0$.

1. Calcular el cardinal de F.
2. Calcular el grado de $\mathrm{Irr}(a^2, \mathbb{F}_3)$.
3. Calcular $\mathrm{Irr}(a^2, \mathbb{F}_3)$.

EJERCICIO 65. Calcular el número de polinomios mónicos irreducibles de grado menor o igual que 3 en $\mathbb{F}_5[X]$.

EJERCICIO 66. Sean $\sqrt{2}, \sqrt[3]{2} \in \mathbb{R}$.

1. Calcular razonadamente $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}), \mathbb{Q}]$.
2. Decidir razonadamente si $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, i\sqrt{3})$ es una extensión de Galois de $\mathbb{Q}$.
3. Calcular $\mathrm{Aut}(K)$ definiendo explícitamente todos sus elementos.
4. Calcular razonadamente el grado del polinomio
$$f = \mathrm{Irr}(\sqrt{2} + \sqrt[3]{2}, \mathbb{Q}).$$
5. Decidir razonadamente quién es el grupo de Galois de f. ¿Es f resoluble por radicales? ¿Son las raíces complejas de este polinomio construibles con regla y compás?

EJERCICIO 67. Sea K el cuerpo de descomposición de $f = X^{12} - 1 \in \mathbb{Q}[X]$.

1. Calcular el grupo de Galois G de f, definiendo explícitamente todos sus elementos.
2. Calcular todos los subgrupos de G.
3. Calcular todos los subcuerpos de K, indicando a qué subgrupo de G corresponde cada uno de ellos mediante la Conexión de Galois.

EJERCICIO 68. Sea $F = \mathbb{F}_3(a)$ un cuerpo con a satisfaciendo la ecuación $a^3 + a^2 - 1 = 0$.

1. Calcular el cardinal de F.
2. Calcular el grado de $\mathrm{Irr}(a^2, \mathbb{F}_3)$.
3. Calcular $\mathrm{Irr}(a^2, \mathbb{F}_3)$.

EJERCICIO 69. Formular y demostrar una extensión del Teorema 1.34 para S no necesariamente finito.

EJERCICIO 70. Realizar las siguientes tareas.

1. Demostrar que existe $a \in \mathbb{F}_{16}$ tal que $\mathbb{F}_{16} = \mathbb{F}_2(a)$ y $a^4 + a + 1 = 0$.
2. Demostrar que a genera el grupo cíclico $\mathbb{F}_{16}^{\times}$.
3. Resolver en $\mathbb{F}_{16}$, expresando la solución en función de a, la ecuación $x^2 + x + 1 = 0$.
4. Calcular el número de homomorfismos de cuerpos $\mathbb{F}_4 \to \mathbb{F}_{16}$.

EJERCICIO 71. Calcular $\mathrm{Aut}(E)$, para $E = \mathbb{Q}(\sqrt[3]{5}, i\sqrt{5})$.

EJERCICIO 72. Tomemos $f = (X^4 + 2)(X^2 - 2) \in \mathbb{Q}[X]$ y K el cuerpo de descomposición de f.

1. Demostrar que K es también cuerpo de descomposición de $X^4 - 2 \in \mathbb{Q}[X]$.
2. Describir explícitamente los elementos del grupo $\mathrm{Aut}(K)$.
3. Calcular, listando sus elementos, $\mathrm{Aut}_{\mathbb{Q}(i\sqrt{2})}(K) \cap \mathrm{Aut}_{\mathbb{Q}(\sqrt{2})}(K)$.
4. Calcular el número de subcuerpos de K de grado 4 sobre $\mathbb{Q}$.

EJERCICIO 73. Sea α una raíz real de $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$. ¿Es $\mathbb{Q}(\alpha)$ un cuerpo de descomposición de f?

EJERCICIO 74. Sea F un cuerpo de característica 2 y $a \in F$ tal que $F = \mathbb{F}_2(a)$ y $a^6 = a^3 + 1$.

1. Calcular el cardinal de F.
2. Calcular $\mathrm{Irr}(a^{21}, \mathbb{F}_2)$ y todos los homomorfismos de cuerpos de $\mathbb{F}_2(a^{21})$ a F.

EJERCICIO 75. Sea $\omega \in \mathbb{C}$ una raíz décima primitiva de la unidad.

1. Calcular $\mathrm{Irr}(\omega, \mathbb{Q})$.
2. Calcular, expresando sus generadores en términos de ω, todos los subcuerpos de $\mathbb{Q}(\omega)$.

EJERCICIO 76. Sea $f = X^4 + 3X^2 - 2 \in \mathbb{Q}[X]$ y K su cuerpo de descomposición.

1. Demostrar que f tiene una raíz real positiva α tal que $\alpha \notin \mathbb{Q}(\alpha^2)$.
2. Demostrar que $i\sqrt{2} \in K$ y calcular $[K : \mathbb{Q}]$.
3. Calcular $\mathrm{Aut}(K)$ definiendo explícitamente todos sus elementos.
4. Calcular los subgrupos de $\mathrm{Aut}(K)$ correspondientes por la Conexión de Galois con los subcuerpos $\mathbb{Q}(\alpha^2)$ y $\mathbb{Q}(i\sqrt{2})$ de K, listando sus elementos.
5. Decidir razonadamente cuál es el grado del polinomio
$$g = \mathrm{Irr}(\alpha + i\sqrt{2}, \mathbb{Q}).$$
¿Es g resoluble por radicales? ¿Son las raíces complejas de f constructibles con regla y compás?

EJERCICIO 77. Sea $\eta \in \mathbb{C}$ una raíz decimocuarta primitiva de la unidad.

1. Calcular el decimocuarto polinomio ciclotómico $\phi_{14} \in \mathbb{Q}[X]$.
2. Calcular, definiendo explícitamente todos sus elementos, $\mathrm{Aut}(\mathbb{Q}(\eta))$ y todos sus subgrupos.
3. Calcular, expresando sus generadores en función de η, todos los subcuerpos de $\mathbb{Q}(\eta)$.

EJERCICIO 78. Vimos en clase que $\mathbb{F}_{64} = \mathbb{F}_2(a)$ con a satisfaciendo la ecuación $a^6 + a + 1 = 0$, y que a es un elemento primitivo del $\mathbb{F}_{64}$. Calcular, expresándolas en función de a, las raíces en $\mathbb{F}_{64}$ del polinomio $h = X^3 + X + 1 \in \mathbb{F}_2[X]$.

5.2. Ejercicios resueltos

Solución al Ejercicio 5. Puesto que $\sqrt{2}$ es de grado 2 sobre $\mathbb{Q}$ e i es de grado 2 sobre[1] $\mathbb{Q}(\sqrt{2})$, tenemos, por el Lema de la torre, que $[\mathbb{Q}(\sqrt{2}, i) :$

[1] i no puede ser de grado 1 porque no pertenece a $\mathbb{Q}(\sqrt{2})$.

$\mathbb{Q}] = 4$. Pongamos $\alpha = \sqrt{2} + i$. Obviamente, $\mathbb{Q}(\alpha) \leq \mathbb{Q}(\sqrt{2}, i)$. Si razonamos que $\sqrt{2}, i \in \mathbb{Q}(\alpha)$, deducimos que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i)$.

Como $\alpha - \sqrt{2} = i$, elevando al cuadrado, obtenemos que $\alpha^2 - 2\sqrt{2}\alpha + 2 = -1$. Despejando $\sqrt{2}$, vemos que es un elemento de $\mathbb{Q}(\alpha)$. Análogamente, elevando al cuadrado ambos miembros de la igualdad $\alpha - i = \sqrt{2}$, deducimos que $i \in \mathbb{Q}(\alpha)$.

Por tanto, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. De modo que $\mathrm{Irr}(\alpha, \mathbb{Q})$ es un polinomio de grado 4. Si encontramos un polinomio mónico $f(X)$ de grado 4 en $\mathbb{Q}[X]$ del que α es raíz, entonces $f(X)$ ha de ser un múltiplo de $\mathrm{Irr}(\alpha, \mathbb{Q})$, por lo que se trata necesariamente de $\mathrm{Irr}(\alpha, \mathbb{Q})$.

Finalicemos: $\alpha^2 = 2 + 2\sqrt{2}i\alpha - 1$ de donde, $2\sqrt{2}i\alpha = \alpha^2 - 1$. Elevando al cuadrado, deducimos que $\alpha^4 - 2\alpha^2 + 9 = 0$. Por lo razonado anteriormente, $\mathrm{Irr}(\alpha, \mathbb{Q}) = X^4 - 2X^2 + 9$.

Solución al Ejercicio 50. Puesto que $i \in \mathbb{C}$ es una raíz cuarta primitiva de la unidad, sabemos que $K = \mathbb{Q}(\sqrt[4]{5}, i)$ es cuerpo de descomposición del polinomio irreducible $X^4 - 5 \in \mathbb{Q}[X]$, de donde la extensión $\mathbb{Q} \leq K$ es de Galois. Además, $\#\mathrm{Aut}(K) = [K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 8$, por un argumento reiterado que, en caso de examen, hay que hacer explícito. Sabemos que estos automorfismos se obtienen extendiendo cada homomorfismo $\mathbb{Q}(\sqrt[4]{5}) \to K$, determinado por una de las raíces de $X^4 - 5$ en K, a dos automorfismos de K, uno para cada raíz del polinomio irreducible $X^2 + 1 \in \mathbb{Q}(\sqrt[4]{5})[X]$. Con este razonamiento, tenemos que

$$\mathrm{Aut}(K) = \{\tau_{jk} : j \in \mathbb{Z}_4, k \in U(\mathbb{Z}_4)\},$$

donde

$$\tau_{jk} : \begin{cases} \sqrt[4]{5} & \mapsto & i^j \sqrt[4]{5} \\ i & \mapsto & i^k \end{cases}$$

De hecho, por el Ejercicio 49, la aplicación

$$\mathrm{Aut}(K) \to \mathrm{GL}_2(\mathbb{Z}_4), \quad \tau_{jk} \mapsto \begin{pmatrix} 1 & 0 \\ j & k \end{pmatrix} \tag{5.1}$$

es un homorfismo inyectivo de grupos.

De acuerdo con la conexión de Galois, los subcuerpos de K de grado 4 sobre $\mathbb{Q}$ están en correspondencia biyectiva con los subgrupos de $\mathrm{Aut}(K)$ de índice cuatro. O, lo que es lo mismo, con los elementos de orden 2. La representación (5.1) de los automorfismos facilita el cálculo $\tau_{jk}^2 = \tau_{j+kj\,k^2}$. Por tanto, $\tau_{jk}^2 = \tau_{01}$ si, y sólo si, $j(k+1) = 0, k^2 = 1$. Las soluciones (en $\mathbb{Z}_4$) dan $\tau_{21}, \tau_{03}, \tau_{13}, \tau_{23}, \tau_{33}$. Ahora razonamos como sigue: $\mathbb{Q}(\sqrt[4]{5})$ tiene grado 4 sobre $\mathbb{Q}$. Puesto que $\tau_{03}(\sqrt[4]{5}) = \sqrt[4]{5}$, obtenemos, con ayuda de la Conexión de Galois, que $K^{\langle \tau_{03} \rangle} = \mathbb{Q}(\sqrt[4]{5})$. Un razonamiento análogo da que $K^{\langle \tau_{23} \rangle} = \mathbb{Q}(i\sqrt[4]{5})$. Como τ_{21} deja fijos $i, \sqrt{5}$ y el cuerpo $\mathbb{Q}(i, \sqrt{5})$ tiene grado 4 sobre $\mathbb{Q}$, deducimos igualmente que $K^{\langle \tau_{21} \rangle} = \mathbb{Q}(i, \sqrt{5})$.

En este punto, hemos identificado como subcuerpos fijos por subgrupos de índice cuatro a los "obvios". Quedan dos por describir. Observemos que $\tau_{13}(\sqrt[4]{5}(1+i)) = \sqrt[4]{5}(1+i)$. Un sencillo cálculo muestra que $(\sqrt[4]{5}(1+i))^4 = -20$, así que $\mathrm{Irr}(\sqrt[4]{5}(1+i), \mathbb{Q}) = X^4 + 20$, puesto que dicho polinomio es irreducible por Eisenstein. El consabido argumento usando la conexión de Galois muestra que $K^{\langle \tau_{13} \rangle} = \mathbb{Q}(\sqrt[4]{5}(1+i))$. Por análogas razones, tenemos que $K^{\langle \tau_{33} \rangle} = \mathbb{Q}(\sqrt[4]{5}(1-i))$. En resumen, los 5 subcuerpos

de K de grado 4 son

$$K^{\langle\tau_{03}\rangle} = \mathbb{Q}(\sqrt[4]{5}); K^{\langle\tau_{23}\rangle} = \mathbb{Q}(i\sqrt[4]{5}); K^{\langle\tau_{21}\rangle} = \mathbb{Q}(i, \sqrt{5});$$
$$K^{\langle\tau_{13}\rangle} = \mathbb{Q}(\sqrt[4]{5}(1+i)); K^{\langle\tau_{33}\rangle} = \mathbb{Q}(\sqrt[4]{5}(1-i)).$$

Por último, los subcuerpos de K de grado 2 sobre $\mathbb{Q}$ están en correspondencia con los subgrupos de índice 2 de $Aut(K)$, es decir, subgrupos de 4 elementos. Por otra parte, el único grupo de 8 elementos que tiene 5 subgrupos de orden 2 es, salvo isomorfismos, el grupo diédrico D_4 de simetrías del cuadrado. Este grupo tiene, exactamente, 3 subgrupos de orden 4, luego hay tres subcuerpos de K de grado 2. Que son evidentes: $\mathbb{Q}(i), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(i\sqrt{5})$, y han de corresponderse con los tres subgrupos de cardinal 4. Con ello, hemos completado la descripción de los subcuerpos de K.

Como complemento, podemos completar la descripción de los subgrupos de $Aut(K)$ usando la conexión de Galois. Sabemos que $\langle\tau_{21}\rangle = Aut_{\mathbb{Q}(\sqrt{5},i)}(K)$, por lo que los grupos de índice 2, que son

$$Aut_{\mathbb{Q}(i)}(K),\ Aut_{\mathbb{Q}(\sqrt{5})}(K),\ Aut_{\mathbb{Q}(i\sqrt{5})}(K),$$

han de contener a τ_{21}.

Como $\tau_{11}(i) = i$, y este elemento tiene orden 4, deducimos que $Aut_{\mathbb{Q}(i)}(K) = \langle\tau_{11}\rangle$. Para completar los otros dos grupos de automorfismos, hemos de añadir dos elementos escogidos de entre $\{\tau_{03}, \tau_{13}, \tau_{23}, \tau_{33}\}$. Como $\tau_{03}(\sqrt{5}) = \tau_{23}(\sqrt{5}) = \sqrt{5}$, tenemos que

$$Aut_{\mathbb{Q}(\sqrt{5})}(K) = \{\tau_{01}, \tau_{21}, \tau_{03}, \tau_{23}\} = \langle\tau_{03}, \tau_{23}\rangle.$$

Análogamente, se comprueba que

$$Aut_{\mathbb{Q}(i\sqrt{5})}(K) = \{\tau_{01}, \tau_{21}, \tau_{13}, \tau_{33}\} = \langle\tau_{13}, \tau_{33}\rangle.$$

Solución al Ejercicio 53. Dado que $f \in \mathbb{F}_2[X]$ es irreducible, $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = \deg f = 3$. Así que $F(\alpha)$ es un cuerpo de 8 elementos. Toda extensión de cuerpos finitos es de Galois, así lo es $\mathbb{F}_2 \leq \mathbb{F}_2(\alpha)$. Puesto que f tiene una raíz en $\mathbb{F}_2(\alpha)$, ha de tenerlas todas, luego es un cuerpo de descomposición de f. Así, $\mathbb{F}_2(\alpha) = F$.

El resto de las raíces de f se obtienen, de acuerdo con el Teorema 4.50, aplicando a α el automorfismo de Frobenius. Resultan así $\alpha, \alpha^2, \alpha^4 = \alpha + \alpha^2$. Estas son, claro, las soluciones en F de $x^3 + x + 1 = 0$.

Las soluciones en F de $x^3 + x^2 + 1 = 0$ son las raíces de $g = X^3 + X^2 + 1 \in \mathbb{F}_2[X]$. Este polinomio de grado 3 es irreducible. Deducimos del Teorema 4.53 que g es un divisor de $X^8 - X$. Como los elementos de F son todos raíces de este polinomio, resulta que todas las raíces de g han de estar en F. Dado que ninguna puede coincidir, por la identidad de Bezout, con las de f, son, necesariamente, $\alpha + 1, \alpha^2 + 1, \alpha^2 + \alpha + 1$.

Por último, una solución $\beta \in F$ de la ecuación $x^2 + x + 1 = 0$ sería una raíz del polinomio irreducible $X^2 + X + 1 \in \mathbb{F}_2[X]$. Por tanto, $[\mathbb{F}_2(\beta) : \mathbb{F}_2] = 2$, lo que es imposible por la fórmula de la torre.

Solución al Ejercicio 54. Vamos a demostrar que $f \in \mathbb{F}_4[X]$ es irreducible, esto es, visto su grado, que no tiene ninguna raíz en $\mathbb{F}_4$. Supongamos que tuviera una, digamos $\beta \in \mathbb{F}_4$. Como f es irreducible sobre $\mathbb{F}_2$, deducimos que $\mathbb{F}_4 = \mathbb{F}_2(\beta)$. Lo que implica que $Irr(\beta, \mathbb{F}_2)$ tiene grado 2. Pero éste ha de ser un factor de $f \in \mathbb{F}_2[X]$, lo cual no es posible. Por tanto, $f \in \mathbb{F}_4[X]$ es irreducible. Razonando como en el Ejercicio 53, deducimos que $K = \mathbb{F}_4(\alpha)$, un cuerpo de 64 elementos.

Las soluciones en K de $x^3+x+1=0$ son las raíces en K de f así que, por el Teorema 4.52, son $\alpha, \alpha^4, \alpha^{16}$. Comparando con la solución del Ejercicio 53, puesto que $F \leq K$, hemos de tener que las soluciones son $\alpha, \alpha^2, \alpha^4$. No hay contradicción ninguna, ya que, por ser F un cuerpo de 8 elementos, $\alpha^8 = \alpha$, por lo que $\alpha^{16} = \alpha^2$. La observación $F \leq K$ también permite deducir que las soluciones de la segunda ecuación son las dadas en el Ejercicio 53.

Con respecto de la ecuación $x^2 + x + 1 = 0$, ahora sí que tiene solución en $\mathbb{F}_4$, ya que este es cuerpo de descomposición de $X^2 + X + 1 \in \mathbb{F}_2[X]$ y, por tanto, basta con tomar $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$ para que γ sea solución. La base pedida es, en vista de la demostración del Lema 1.16,

$$\{\gamma^j \alpha^k : j = 0, 1; k = 0, 1, 2\}.$$

Solución al Ejercicio 57. Sea K cuerpo de descomposición de f sobre $\mathbb{Q}$. Obviamente, $\mathbb{Q}(i) \leq K$. Tenemos que K es cuerpo de descomposición de $g = X^3 + X + 1$ sobre $\mathbb{Q}(i)$. Vamos a demostrar que $g \in \mathbb{Q}(i)[X]$ es irreducible, lo que equivale a mostrar que g no tiene raíces en $\mathbb{Q}(i)$.

Como $g' = 3X^2 + 1$, tenemos que $g(x)$, vista como función en una variable real x, tiene primera derivada estrictamente positiva, por lo que es estrictamente creciente. La consecuencia para el polinomio g es que tiene una única raíz real r. Y, por tanto, dos raíces complejas no reales conjugadas, digamos $\alpha, \overline{\alpha}$.

Bien, $r \notin \mathbb{Q}(i)$, ya que, de lo contrario, $r \in \mathbb{Q}$, lo que implica que $r = \pm 1$ cosa que no es cierta.

Si $\alpha \in \mathbb{Q}(i)$, entonces $\overline{\alpha} \in \mathbb{Q}(i)$. En tal caso, $h = (X-\alpha)(X-\overline{\alpha}) \in \mathbb{Q}[X]$. Pero, entonces, el cociente de g entre h tiene coeficientes en $\mathbb{Q}$. Este cociente es $X - r$, lo que implica que $r \in \mathbb{Q}$, lo que no es cierto.

Colegimos que ninguna de las raíces de g pertenece a $\mathbb{Q}(i)$, por lo que g es irreducible.

En este punto, sabemos que el grupo de Galois de g sobre $\mathbb{Q}(i)$ es isomorfo a A_3 o a S_3, disyuntiva que se decide viendo si el discriminante de g es un cuadrado en $\mathbb{Q}(i)$. Dicho discriminante vale -31. Si $\sqrt{-31} = i\sqrt{31} \in \mathbb{Q}(i)$, entonces $\sqrt{31} \in \mathbb{Q}(i)$ o, lo que es lo mismo, $\sqrt{31} \in \mathbb{Q}$. Esto no es posible, ya que $X^2 - 31 \in \mathbb{Q}[X]$ es irreducible.

Ahora ya sabemos que $\mathrm{Aut}_{\mathbb{Q}(i)}(K)$ es isomorfo a S_3. Por tanto, $[K : \mathbb{Q}(i)] = 6$. Concluimos:

$$\#\mathrm{Aut}(K) = [K : \mathbb{Q}] = [K : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 6 \times 2 = 12.$$

Solución al Ejercicio 58. Las raíces de f en $\mathbb{C}$ son

$$\sqrt{3}, -\sqrt{3}, \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2},$$

donde $\omega = e^{i2\pi/3} = -1/2 + i\sqrt{3}/2$. Por tanto,

$$K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}).$$

Observemos que $-1/2 + i\sqrt{3}/2 = \omega = (\omega\sqrt[3]{2})/\sqrt[3]{2} \in K$, de donde, puesto que $\sqrt{3} \in K$, deducimos que $i \in K$. Por tanto, $i + \sqrt{3} \in K$.

El anterior razonamiento muestra también que $\mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2}) \leq K$ y, como la inclusión recíproca es clara, deducimos que

$$K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2}).$$

Esta última igualdad permite escribir, por el Lema de la Torre,

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})][\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}].$$

Calculemos cada uno de los factores involucrados. En primer lugar,

$$\mathrm{Irr}(i, \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})) = X^2 + 1,$$

puesto que este último polinomio es irreducible al ser de grado dos y tener como raíces $\pm i \notin \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})$, ya que este último cuerpo sólo contiene números reales. Por tanto, $[K : \mathbb{Q}(\sqrt{3}, \sqrt[3]{2})] = 2$. Para el último factor, como $\sqrt{3}$ es raíz de $X^2 - 3$, que es irreducible por el criterio de Eisenstein, deducimos que $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Un argumento análogo muestra que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Si se tuviese que $\sqrt[3]{2} \in \mathbb{Q}(\sqrt{3})$, entonces $\mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{Q}(\sqrt{3})$ lo que, en vista de los grados sobre $\mathbb{Q}$ de ambas extensiones es imposible. Como las otras dos raíces de $X^3 - 2$ no son reales, deducimos que este polinomio de grado tres no tiene raíces en $\mathbb{Q}(\sqrt{3})$ por lo que es irreducible sobre dicho cuerpo. Por tanto, $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{3})] = 3$. Deducimos así que $[K : \mathbb{Q}] = 2 \times 3 \times 2 = 12$.

Como K es cuerpo de descomposición de f sobre $\mathbb{Q}$, sabemos que la extensión $\mathbb{Q} \leq K$ es de Galois y, por tanto, $\mathrm{Aut}(K)$ tiene 12 elementos. Para calcularlos, usamos que $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}, i)$ y aplicamos reiteradamente la extensión de homomorfismos dada por la Proposición 2.12. Así, los dos homomorfismos de cuerpos $\eta_0, \eta_1 : \mathbb{Q}(\sqrt{3}) \to K$ están determinados por las raíces $\pm\sqrt{3}$ del polinomio irreducible $X^2 - 3 \in \mathbb{Q}[X]$, concretamente, $\eta_0(\sqrt{3}) = \sqrt{3}, \eta_1(\sqrt{3}) = -\sqrt{3}$. Cada uno de éstos da tres extensiones $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) \to K$ determinadas por las raíces de $X^3 - 2$, que, según hemos visto antes, es irreducible sobre $\mathbb{Q}(\sqrt{3})$. Y, por último, cada uno de los seis homomorfismos descritos se extiende a 2 automorfismos $K \to K$ según las raíces $\pm i$ de $X^2 + 1$. En resumen, tenemos que $\mathrm{Aut}(K) = \{\eta_{jkl} : j = 0, 1; k = 0, 1, 2, l = 0, 1\}$, donde

$$\eta_{jkl} : \begin{cases} \sqrt{3} & \mapsto & (-1)^j\sqrt{3} \\ \sqrt[3]{2} & \mapsto & \omega^k \sqrt[3]{2} \\ i & \mapsto & (-1)^l i \end{cases}$$

Por último, $\mathrm{Aut}_{\mathbb{Q}(i+\sqrt{3})}(K)$ consiste en los automorfismos de K que dejan fijo $i + \sqrt{3}$. Como $\eta_{jkl}(i + \sqrt{3}) = (-1)^l i + (-1)^j\sqrt{3}$, deducimos que

$$\mathrm{Aut}_{\mathbb{Q}(i+\sqrt{3})}(K) = \{\eta_{0k0} : k = 0, 1, 2\}.$$

Un cálculo sencillo muestra que $\mathrm{Aut}_{\mathbb{Q}(i,\sqrt{3})}(K) = \{\eta_{0k0} : k = 0, 1, 2\}$, de modo que las extensiones de cuerpos $\mathbb{Q}(i+\sqrt{3}) \leq K$ y $\mathbb{Q}(i, \sqrt{3}) \leq K$ tienen el mismo grupo de Galois, luego, por la conexión de Galois, $\mathbb{Q}(i+\sqrt{3}) = \mathbb{Q}(i, \sqrt{3})$. Así, vemos que $\mathbb{Q}(i + \sqrt{3})$ es el cuerpo de descomposición de $(X^2 + 1)(X^2 - 3) \in \mathbb{Q}[X]$, lo que muestra que la extensión $\mathbb{Q} \leq \mathbb{Q}(i + \sqrt{3})$ es de Galois y, por tanto, $\mathrm{Aut}_{\mathbb{Q}(i+\sqrt{3})}(K)$ es un subgrupo normal de $\mathrm{Aut}(K)$.

Solución al Ejercicio 59. El polinomio f es irreducible ya que es de grado 3 y no tiene raíces en $\mathbb{Q}$, puesto que las únicas posibles no lo son: $f(1) = -1 \neq 0, f(-1) = 3 \neq 0$. Por tanto, su grupo de Galois es un subgrupo transitivo de S_3. Por otra parte, $\mathrm{Disc}(f) = 81 = 9^2$, lo que implica que dicho grupo de Galois es A_3. Ahora, si α es una raíz real de f, tenemos que $\mathrm{Irr}(\alpha, \mathbb{Q}) = f$, luego $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Pero, si K es el cuerpo de descomposición de f, tenemos que $\mathbb{Q}(\alpha) \leq K$ y, por otro lado, $[K : \mathbb{Q}] = \#A_3 = 3$. Conclusión: $K = \mathbb{Q}(\alpha)$.

Solución al Ejercicio 60. Las raíces del polinomio f son los números complejos $\pm i\sqrt{3}, \sqrt[3]{3}, \sqrt[3]{3}\omega, \sqrt[3]{3}\omega^2$, donde $\omega = -1/2 + i\sqrt{3}/2$. Obviamente, $\mathbb{Q}(\sqrt[3]{3}, i\sqrt{3}) \leq K$. Como $\omega \in \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$, deducimos que todas las raíces de

f están en ese cuerpo, de donde $K = \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$. Podemos, por el Lema de la Torre, que

$$[K : \mathbb{Q}] = [\mathbb{Q}(i\sqrt{3})(\sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{3})][\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}]. \tag{5.2}$$

Ahora bien, como $X^3 - 3 \in \mathbb{Q}[X]$ es irreducible por el criterio de Eisenstein, tenemos que $\mathrm{Irr}(\sqrt[3]{3}, \mathbb{Q}) = X^3 - 3$, lo que implica que $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$.

Por otra parte, $i\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{3})$, puesto que se trata de un número no real. Como es raíz de $X^2 + 3$, deducimos que $[\mathbb{Q}(i\sqrt{3})(\sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{3})] = 2$ y, como consecuencia, $X^2 + 3$ es irreducible sobre $\mathbb{Q}(\sqrt[3]{3})$.

Tenemos ya, en virtud de (5.2), que $[K : \mathbb{Q}] = 6$.

Como K es cuerpo de descomposición del polinomio separable f, la extensión $\mathbb{Q} \leq K$ es de Galois. Así, la conexión de Galois nos muestra en este caso que $\mathrm{Aut}_{\mathbb{Q}}(K)$ es un grupo de seis elementos. Describámoslos mediante la Proposición de Extensión. Como $X^3 - 3 \in \mathbb{Q}[X]$ es irreducible y K contiene sus tres raíces, hay exactamente tres homomorfismos de cuerpos $\eta_0, \eta_1, \eta_2 : \mathbb{Q}(\sqrt[3]{3}) \to K$, determinados por las condiciones $\eta_j(\sqrt[3]{3}) = \omega^j \sqrt[3]{3}$, para $j = 0, 1, 2$. Para cada uno de ellos, puesto que $X^2 + 3 \in \mathbb{Q}(\sqrt[3]{3})[X]$ es irreducible, tiene dos extensiones $\eta_{jk} : K \to K$, con $\eta_{jk}(i\sqrt{3}) = (-1)^k i\sqrt{3}$, $k = 0, 1$. En resumen,

$$G = \mathrm{Aut}_{\mathbb{Q}}(K) = \{\eta_{jk} : j = 0, 1, 2; k = 0, 1\},$$

donde

$$\begin{cases} \eta_{jk}(\sqrt[3]{3}) = \omega^j \sqrt[3]{3} \\ \eta_{jk}(i\sqrt{3}) = (-1)^k i\sqrt{3}. \end{cases}$$

Calculemos todos los subgrupos de $\mathrm{Aut}_{\mathbb{Q}}(K)$. La siguiente tabla recoge los órdenes de todos los elementos de este grupo

η_{00}	η_{01}	η_{10}	η_{11}	η_{20}	η_{21}
1	2	3	2	3	2

Por ejemplo, veamos el orden de η_{11}. Tenemos que

$$\eta_{11}(\eta_{11}(\sqrt[3]{3})) = \eta_{11}(\omega \sqrt[3]{3}) = \eta_{11}(\omega)\eta_{11}(\sqrt[3]{3}) = \overline{\omega}\omega \sqrt[3]{3} = \sqrt[3]{3}.$$

Como $\eta_{11}^2(i\sqrt{3}) = i\sqrt{3}$, deducimos que $\eta_{11}^2 = 2$.

En fin, vemos que este grupo es isomorfo a S_3, lo que permite describir fácilmente sus subgrupos (los no triviales son tres de orden 2 y uno de orden 3). Este último es $\langle \eta_{10} \rangle$. Sabemos, por la conexión de Galois, que $[K^{\langle \eta_{10} \rangle} : \mathbb{Q}] = (G : \langle \eta_{10} \rangle) = 2$. Como, obviamente, $i\sqrt{3} \in K^{\langle \eta_{10} \rangle}$, tenemos que $\mathbb{Q}(i\sqrt{3}) \leq K^{\langle \eta_{10} \rangle}$ y, al ser ambas extensiones de grado 2 de $\mathbb{Q}$, deducimos que $K^{\langle \eta_{10} \rangle} = \mathbb{Q}(i\sqrt{3})$.

Argumentos análogos, que el alumno ha de hacer explícitos, muestran que

$$K^{\langle \eta_{01} \rangle} = \mathbb{Q}(\sqrt[3]{3}), \quad K^{\langle \eta_{11} \rangle} = \mathbb{Q}(\omega^2 \sqrt[3]{3}), \quad K^{\langle \eta_{21} \rangle} = \mathbb{Q}(\omega \sqrt[3]{3}).$$

La conexión de Galois muestra que los cuatro subcuerpos de K descritos, junto con el propio K y el subcuerpo primo $\mathbb{Q}$, constituyen la lista completa de los subcuerpos de K.

Por último, $E = \mathbb{Q}(\sqrt[3]{3} + i\sqrt{3})$ ha de ser uno de los subcuerpos calculados. Primero, E no puede ser $\mathbb{Q}$ ni $\mathbb{Q}(\sqrt[3]{3})$ porque estos dos cuerpos sólo contienen números reales. Si $E = K^{\eta_{11}}$, entonces $\sqrt[3]{3} + i\sqrt{3}$ ha de ser fijo por η_{11}. Pero

$$\eta_{11}(\sqrt[3]{3} + i\sqrt{3}) = \omega \sqrt[3]{3} - i\sqrt{3},$$

elemento que, de ser igual a $\sqrt[3]{3}+i\sqrt{3}$, daría $2i\sqrt{3} = (\omega-1)\sqrt[3]{3}$. La parte real del miembro de la izquierda es cero, cosa que no ocurre para el miembro de la derecha.

Un argumento similar descarta que $E = K^{\eta_{21}}$, con lo que la única salida es admitir que $E = K$.

Solución al Ejercicio 62. 1. Tenemos que $\alpha - \sqrt{2} = i\sqrt{3}$. Elevando al cuadrado,

$$\alpha^2 - 2\sqrt{2}\alpha + 2 = -3.$$

Por tanto, $\sqrt{2} = \frac{\alpha^2+5}{2\alpha} \in \mathbb{Q}(\alpha)$. Como $i\sqrt{3} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$, deducimos que $\mathbb{Q}(\sqrt{2}, i\sqrt{3}) \leq \mathbb{Q}(\alpha)$. Como la inclusión recíproca es clara, obtenemos que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$. De modo que, usando el Lema de la Torre,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(i\sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4,$$

ya que ambos factores valen 2: el segundo, porque $X^2-2 \in \mathbb{Q}[X]$ es irreducible (por el criterio de Eisenstein), y el segundo porque $X^2 + 1 \in \mathbb{Q}(\sqrt{2})[X]$ es irreducible al ser de grado 2 y no tener raíces reales y, por tanto, tampoco en $\mathbb{Q}(\sqrt{2})$.

2. Hemos visto en el apartado anterior que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$. La segunda descripción muestra que $\mathbb{Q}(\alpha)$ es cuerpo de descomposición de $(X^2 - 2)(X^2 + 3) \in \mathbb{Q}[X]$. Como estamos en característica 0, deducimos que la extensión $\mathbb{Q} \leq \mathbb{Q}(\alpha)$ es de Galois. En particular, es normal, por lo que, dado que $\mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Q}[X]$ tiene una raíz en $\mathbb{Q}(\alpha)$ y es irreducible, ha de tener todas sus raíces en $\mathbb{Q}(\alpha)$. Deducimos, pues, que $\mathbb{Q}(\alpha)$ es cuerpo de descomposición[2] de $\mathrm{Irr}(\alpha, \mathbb{Q})$ y el grupo de Galois de éste es $\mathrm{Aut}(\mathbb{Q}(\alpha))$.

Usando la descripción $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$ y la Proposición de Extensión, argumentamos que existen dos homomorfismos de cuerpos, $\eta_0, \eta_1 : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\alpha)$ (tantos como raíces de $X^2 - 2$ en $\mathbb{Q}(\alpha)$), determinados por $\eta_j(\sqrt{2}) = (-1)^j\sqrt{2}$ para $j = 0, 1$. De manera similar, cada homomorfismo η_j se extiende a dos homomorfismos de cuerpos $\eta_{jk} : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ determinados por $\eta_{jk}(i\sqrt{3}) = (-1)^k i\sqrt{3}$ con $k = 0, 1$. Éstos resultan ser automorfismos porque son en particular aplicaciones $\mathbb{Q}$–lineales de un espacio vectorial racional de dimensión 4 sobre sí mismo. En resumen, el grupo de Galois de $\mathrm{Irr}(\alpha, \mathbb{Q})$ es $\{\eta_{jk} : j, k = 0, 1\}$.

3. Todas las raíces de $\mathrm{Irr}(\alpha, \mathbb{Q})$ pertenecen a $\mathbb{Q}(\alpha)$, que hemos visto es una extensión de Galois de $\mathbb{Q}$ de grado $4 = 2^2$. Por tanto, se trata de números construibles [3].

Solución al Ejercicio 63. 1. Las raíces complejas de $f = X^6 - 3$ son $\{\omega^k \sqrt[6]{3} : k = 0, \ldots, 5\}$ para $\omega \in \mathbb{C}$ una raíz sexta primitiva de la unidad. Podemos tomar $\omega = 1/2 + i\sqrt{3}/2$. Como $\omega = \frac{\omega \sqrt[6]{3}}{\sqrt[6]{3}}$, deducimos fácilmente que $K = \mathbb{Q}(\sqrt[6]{3}, \omega)$. Podemos simplificar algo más los generadores de esta extensión de $\mathbb{Q}$, ya que la forma de ω nos da que $K = \mathbb{Q}(\sqrt[6]{3}, i\sqrt{3})$. Aplicando el Lema de la Torre,

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[6]{3})][\mathbb{Q}(\sqrt[6]{3}) : \mathbb{Q}] = 2 \times 6 = 12.$$

[2] Un argumento alternativo, basado también en el apartado 1, es calcular $\mathrm{Irr}(\alpha, \mathbb{Q})$ y comprobar que se trata de una cuártica bicuadrática. De modo que sus raíces son $\alpha, -\alpha, \overline{\alpha}, -\overline{\alpha}$, números todos pertenecientes a $\mathbb{Q}(\sqrt{2}, i\sqrt{3}) = \mathbb{Q}(\alpha)$.

[3] Un argumento alternativo es que todas las raíces, $\alpha, -\alpha, \overline{\alpha}, -\overline{\alpha}$ son construibles porque, por ejemplo, tienen partes real e imaginaria raíces cuadradas de números enteros, que son construibles.

El segundo factor vale 6 porque $X^6-3 \in \mathbb{Q}[X]$ es irreducible por el criterio de Eisenstein. El primer factor vale 2 ya que $X^2+3 \in \mathbb{Q}(\sqrt[6]{3})[X]$ es irreducible por se un polinomio de grado 2 sin raíces reales y, por tanto, en $\mathbb{Q}(\sqrt[6]{3})$.

2. Bien $\sqrt{3} = (\sqrt[6]{3})^3 \in K$. Como, según el apartado anterior, $i\sqrt{3} \in K$, obtenemos que $i = \frac{i\sqrt{3}}{\sqrt{3}} \in K$. Por tanto, $i+\sqrt{3} \in K$.

3. Vamos a dar una descripción adecuada de los elementos de $Aut(K)$. Puesto que $i = \frac{i\sqrt{3}}{\sqrt{3}} \in K$, tenemos que $K = \mathbb{Q}(\sqrt[6]{3}, i)$. Por la Proposición de Extensión, hay exactamente un homomorfismo de cuerpos $\sigma_j : \mathbb{Q}(\sqrt[6]{3}) \to K$ determinado por la condición $\sigma_j(\sqrt[6]{3}) = \omega^j \sqrt[6]{3}$, para cada $j = 0, \dots, 5$. Cada uno de éstos se extiende a un automofismo $\sigma_{jk} : K \to K$ tal que $\sigma_{jk}(i) = (-1)^k i$ para $k = 0, 1$. De manera que $Aut(K) = \{\sigma_{jk} : j = 0 \dots, 5; k = 0, 1\}$, donde

$$\sigma_{jk}(\sqrt[6]{3}) = \omega^j \sqrt[6]{3}, \quad \sigma_{jk}(i) = (-1)^k i.$$

De acuerdo con la conexión de Galois, $\#Aut_{\mathbb{Q}(i+\sqrt{3})}(K) = [K : \mathbb{Q}(i+\sqrt{3})]$. Por otra parte, $\mathbb{Q}(i+\sqrt{3}) = \mathbb{Q}(i, \sqrt{3})$, ya que, si denotamos $\beta = i+\sqrt{3}$, entonces $\sqrt{3} = \frac{\beta^2+4}{2\beta}$ e $i = \beta - \sqrt{3}$. Esto muestra, por el Lema de la Torre, que $[\mathbb{Q}(i+\sqrt{3}) : \mathbb{Q}] = 4$ y, por el mismo lema, que $[K : \mathbb{Q}(i+\sqrt{3})] = 12/4 = 3$. Deducimos que $Aut_{\mathbb{Q}(i+\sqrt{3})}(K)$ tiene 3 elementos. Puesto que los elementos de este grupo son aquellos σ_{jk} que dejan fijo a $i+\sqrt{3}$ y

$$\sigma_{20}(\sqrt{3}+i) = \sigma_{20}((\sqrt[6]{3})^3) + \sigma_{20}(i) = \omega^6\sqrt{3} + i = \sqrt{3} + i,$$

$$\sigma_{40}(\sqrt{3}+i) = \sigma_{40}((\sqrt[6]{3})^3) + \sigma_{40}(i) = \omega^{12}\sqrt{3} + i = \sqrt{3} + i,$$

tenemos que

$$Aut_{\mathbb{Q}(i+\sqrt{3})}(K) = \{\sigma_{00}, \sigma_{20}, \sigma_{40}\}.$$

4. Según el apartado anterior, $\mathbb{Q}(i+\sqrt{3}) = \mathbb{Q}(i, \sqrt{3})$. Esta última descripción muestra que $\mathbb{Q}(i+\sqrt{3})$ es cuerpo de descomposición de $(X^2+1)(X^2-3) \in \mathbb{Q}[X]$. Por tanto, $\mathbb{Q} \leq \mathbb{Q}(i+\sqrt{3})$ es una extensión de Galois. El grupo correspondiente por la conexión de Galois, $Aut_{\mathbb{Q}(i+\sqrt{3})}(K)$, es, por tanto, normal en $Aut(K)$.

Solución al Ejercicio 64. 1. El elemento a es raíz del polinomio $f = X^3 + X - 1 \in \mathbb{F}_3[X]$. Como $f(-1) = 0$, se trata de un polinomio reducible. De hecho, se tiene que $f = (X+1)(X^2-X-1)$ es la factorización en irreducibles de f en $\mathbb{F}_3[X]$. Así que tenemos dos casos: o bien $a = -1$, o bien $a^2-a-1 = 0$. En el primero, $F = \mathbb{F}_3(-1) = \mathbb{F}_3$, cuyo cardinal es 3. En el segundo, el cardinal de $\mathbb{F}_3(a)$ es 9, puesto que $[F : \mathbb{F}_3] = 2$.

2. En el caso $a = -1$, $a^2 = 1$ e $Irr(1, \mathbb{F}_3) = X - 1$, grado 1. En el segundo caso, $a = a^2 - 1$, de donde $\mathbb{F}_3(a^2) = \mathbb{F}_3(a) = F$, luego $Irr(a^2, \mathbb{F}_3)$ tiene grado 2.

3. Según el apartado anterior, en el caso $a \neq -1$, a^2 ha de ser raíz de alguno de los tres polinomios mónicos irreducibles de grado 2 en $\mathbb{F}_3[X]$. Podemos descartar $X^2 - X - 1$, ya que sus raíces son $a, a^3 = 1 - a$, hecho que deducimos de aplicar el automorfismo de Frobenius. De los dos que quedan, observamos que

$$(a^2)^2 = a^4 = (a+1)^2 = a^2 + 2a + 1 = a + 1 + 2a + 1 = 2 = -1.$$

Luego $Irr(a^2, \mathbb{F}_3) = X^2 + 1$.

Solución al Ejercicio 65. Los polinomios mónicos de grado 1 en $\mathbb{F}_5[X]$ son cinco: $X + k$, con $k = 0, \dots, 4$. Puesto que $25 = 5^2$, la factorización

completa de $X^{25} - X \in \mathbb{F}_5[X]$ contiene a todos los polinomios mónicos irreducibles de grado 1 y 2 (los divisores de 2). Por tanto, el producto de los segundos ha de tener grado $25 - 5 = 20$, lo que implica que hay 10 polinomios mónicos irreducibles de grado 2. El mismo razonamiento, aplicado a la factorización completa de $X^{125} - X \in \mathbb{F}_5[X]$, nos da que hay $120/3 = 40$ polinomios mónicos irreducibles de grado 3 sobre $\mathbb{F}_5$. En total, el número pedido es $5 + 10 + 40 = 55$.

Solución al Ejercicio 66. 1. Consideremos la torre de cuerpos $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Puesto que $\sqrt[3]{2}$ es raíz del polinomio $X^3 - 2 \in \mathbb{Q}(\sqrt{2})[X]$, el polinomio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}(\sqrt{2})$ tiene grado menor o igual que 3. Así que, por el Lema de la Torre,

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] \leq 2 \times 3 = 6,$$

ya que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, por ser $X^2 - 2 \in \mathbb{Q}[X]$ irreducible por el criterio de Eisenstein. Además, $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$ es un múltiplo de 2. Pero también es un múltiplo de 3, aplicando un razonamiento análogo a la torre de cuerpos $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Conclusión: $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$.

2. Vamos a demostrar que K es cuerpo de descomposición del polinomio $(X^2 - 2)(X^3 - 2) \in \mathbb{Q}[X]$ lo que, en característica 0, sabemos que implica que la extensión $\mathbb{Q} \leq K$ es de Galois. Las raíces del polinomio son $\pm\sqrt{2}, \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ para $\omega = -1/2 + i\sqrt{3}/2$. Todas ellas pertenecen a K, luego el cuerpo de descomposición está contenido en K. Observemos que $\omega = \omega\sqrt[3]{2}/\sqrt[3]{2}$ está en dicho cuerpo de descomposición, de donde lo está $i\sqrt{3}$. Concluimos que K es el cuerpo de descomposición buscado.

3. Para describir los elementos del grupo $\mathrm{Aut}(K)$ usaremos reiteradamente la Proposición de Extensión. Así, puesto que las raíces del polinomio irreducible $X^2 - 2 \in \mathbb{Q}[X]$ pertenecen a K, hay exactamente dos homomorfismos de cuerpos $\tau_j : \mathbb{Q}(\sqrt{2}) \to K$, para $j = 0, 1$, determinados por $\tau_j(\sqrt{2}) = (-1)^j\sqrt{2}$. Del apartado 1 y el Lema de la Torre deducimos que $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 3$, lo que implica que $X^3 - 2 \in \mathbb{Q}(\sqrt{2})[X]$ es irreducible. Como las raíces de este polinomio están en K, hay exactamente tres extensiones de cada τ_j, digamos $\tau_{jk} : \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \to K$, para $k = 0, 1, 2$, determinadas por $\tau_{jk}(\sqrt[3]{2}) = \omega^k\sqrt[3]{2}$. Por último, cada una de éstos se extiende a dos automofismos $\tau_{jkl} : K \to K$, con $l = 0, 1$, uno por cada raíz del polinomio $X^2 + 3$, irreducible sobre $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ al carecer de raíces en ese cuerpo y ser de grado 2. En resumen,

$$\mathrm{Aut}(K) = \{\tau_{jkl} : j = 0, 1; k = 0, 1, 2; l = 0, 1\},$$

donde

$$\tau_{jkl} : \begin{cases} \sqrt{2} & \mapsto & (-1)^j\sqrt{2} \\ \sqrt[3]{2} & \mapsto & \omega^k\sqrt[3]{2} \\ i\sqrt{3} & \mapsto & (-1)^l i\sqrt{3}. \end{cases}$$

4. Llamemos $\alpha = \sqrt{2} + \sqrt[3]{2}$. El grado pedido es $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Observemos que $\{\tau_{00l} : l = 0, 1\} \subseteq \mathrm{Aut}_{\mathbb{Q}(\alpha)}(K)$. Razonemos que esta inclusión es una igualdad. Si $\tau_{jkl}(\alpha) = \alpha$, entonces

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

El número de la izquierda es real, en tanto que el de la derecha, si $k \neq 0$, no lo es. Luego $k = 0$. Lo que implica que el número del miembro a la

izquierda es 0 y, por tanto, $j = 0$. Tenemos, pues, que

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = (\mathrm{Aut}(K) : \mathrm{Aut}_{\mathbb{Q}(\alpha)}(K)) = \frac{\#\mathrm{Aut}(K)}{\#\mathrm{Aut}_{\mathbb{Q}(\alpha)}(K)} = \frac{12}{2} = 6.$$

5. Como $\mathbb{Q} \leq K$ es de Galois y contiene una raíz del irreducible $f \in \mathbb{Q}[X]$, deducimos que todas las raíces de f están en K. Por tanto, el cuerpo de descomposición de f, digamos E, está incluido en K. Tenemos la torre de cuerpos $\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq E \leq K$. Por otro lado, $\mathbb{Q}(\alpha) \leq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ y ambas extensiones tienen grado 6 sobre $\mathbb{Q}$. Por tanto, se tiene la igualdad y, en particular, $\sqrt[3]{2} \in \mathbb{Q}(\alpha)$. Por tanto, E debe contener a todas las raíces de $X^3 - 2$, lo que entraña que E es estrictamente mayor que $\mathbb{Q}(\alpha)$, ya que contiene números no reales. La única posibilidad es $E = K$ y, por tanto, el grupo de Galois de f es $\mathrm{Aut}(K)$. Este grupo tiene orden 12, por lo que es resoluble, así que f es resoluble por radicales. En contraste, todas las raíces de f tienen grado 6, luego ninguna es construible con regla y compás.

Solución al Ejercicio 70. 1. El polinomio $f = X^4 + X + 1 \in \mathbb{F}_2[X]$ es irreducible porque no tiene factores de grado 1 al carecer de raíces en $\mathbb{F}_2$ y el único posible factor irreducible de grado 2, X^2+X+1 no lo es. Esto último es evidente en cuanto se observa que $(X^2 + X + 1)^2 = X^4 + X^2 + 1$. Por tanto, $F = \mathbb{F}[X]/\langle f \rangle$ es un cuerpo, cuyo cardinal es 16, al tener dimensión como $\mathbb{F}_2$–espacio vectorial igual a 4. Así, $\mathbb{F}_{16}$ es isomorfo a F. Como $F = \mathbb{F}_2(X + \langle f \rangle)$, podemos tomar $a \in \mathbb{F}_{16}$ como la imagen de $X + \langle f \rangle$ bajo el mencionado isomorfismo.

2. El grupo multiplicativo $\mathbb{F}_{15}^\times$ es cíclico de orden 15. Así que el orden multiplicativo de a ha de ser un divisor de 15. Observemos que $\{1, a, a^2, a^3\}$ es una $\mathbb{F}_2$–base de $\mathbb{F}_{16}$. Esto implica que $a \neq 1, a^3 \neq 1$, por lo que el orden de a no es ni 1 ni 3. También tenemos que

$$a^5 = aa^4 = a(a + 1) = a^2 + a \neq 1,$$

lo que implica que el orden de a no es 5. Por tanto, a tiene orden 15, es decir, es un generador de $\mathbb{F}_{16}^\times$.

3. Si b es solución de $x^2 + x + 1 = 0$, entonces $\mathrm{Irr}(b, \mathbb{F}_2) = X^2 + X + 1 \in \mathbb{F}_2[X]$, que es irreducible. Por tanto, $\mathbb{F}_2(b)$ es un cuerpo de 4 elementos. Eso implica que el orden multiplicativo de b es 3. Estos elementos son a^5, a^{10}. Observemos que

$$(a^5)^2 + a^5 + 1 = (a^2 + a)^2 + a^2 + a + 1 = a^4 + a^2 + a^2 + a + 1 = a + 1 + a + 1 = 0.$$

Por tanto, a^5 es solución y, aplicándole el automorfismo de Frobenius, tenemos que también lo es a^{10}. Como la ecuación tiene grado 2, hemos obtenido todas sus soluciones.

4. Puedo poner $\mathbb{F}_4 = \mathbb{F}_2(b)$ con $b^2 + b + 1 = 0$. Por la proposición de extensión, los homomorfismos de cuerpos de $\mathbb{F}_4$ a $\mathbb{F}_{16}$, están en correspondencia biyectiva con las raíces de $X^2 + X + 1$ en $\mathbb{F}_{16}$, que hemos visto son 2. Luego hay 2 homomorfismos.

Solución al Ejercicio 72. 1. Comencemos describiendo K. Las raíces complejas de f son los cuatro valores de $\sqrt[4]{-2}$, junto con $\pm\sqrt{2}$. Un valor de $\sqrt[4]{-2}$ es

$$\alpha = \sqrt[4]{2}\frac{\sqrt{2} + i\sqrt{2}}{2} = \frac{1 + i}{\sqrt[4]{2}}.$$

Así, los valores de $\sqrt[4]{-2}$ son $\pm\alpha, \pm\overline{\alpha}$. Por tanto, $K = \mathbb{Q}(\sqrt{2}, \alpha, \overline{\alpha})$. Puesto que $\alpha\overline{\alpha} = \sqrt{2}$, tenemos que $K = \mathbb{Q}(\alpha, \overline{\alpha})$. Como $\alpha + \overline{\alpha} = 2/\sqrt[4]{2}$, deducimos que $K = \mathbb{Q}(\alpha, \alpha + \overline{\alpha}) = \mathbb{Q}(\alpha, \sqrt[4]{2})$. Y, dado que $\sqrt[4]{2}\alpha = 1 + i$, obtenemos que

$K = \mathbb{Q}(\alpha\sqrt[4]{2}, \sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2})$. Como las raíces de $X^4 - 2$ son $i^k\sqrt[4]{2}$, para $k = 0, 1, 2, 3$, deducimos que K es también cuerpo de descomposición de $X^4 - 2$ sobre $\mathbb{Q}$.

2. Por el Lema de la Torre,

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]. \tag{5.3}$$

Puesto que $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$, el polinomio de grado dos $X^2 + 1$, cuyas raíces son $\pm i$, es irreducible sobre $\mathbb{Q}(\sqrt[4]{2})$, de donde $\mathrm{Irr}(i, \mathbb{Q}(\sqrt[4]{2})) = X^2 + 1$. De aquí que $[K : \mathbb{Q}(\sqrt[4]{2})] = [\mathbb{Q}(\sqrt[4]{2})(i) : \mathbb{Q}(\sqrt[4]{2})] = 2$. Por otra parte, $X^4 - 2 \in \mathbb{Q}[X]$ es irreducible por el criterio de Eisenstein, lo que nos da que $\mathrm{Irr}(\sqrt[4]{2}, \mathbb{Q}) = X^4 - 2$ y, consecuentemente, $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Sustituyendo los valores calculados en (5.3), obtenemos $[K : \mathbb{Q}] = 8$.

La extensión $\mathbb{Q} \leq K$ es de Galois, porque K es cuerpo de descomposición de un polinomio con coeficientes en $\mathbb{Q}$ y estamos en característica 0. Consecuentemente, $\#\mathrm{Aut}(K) = \#\mathrm{Aut}_{\mathbb{Q}}(K) = 8$. Calculemos los elementos de este grupo usando la Proposición de Extensión para las dos extensiones sucesivas usadas en (5.3). Así, los homomorfismos de cuerpos desde $\mathbb{Q}(\sqrt[4]{2})$ a K están en correspondencia biyectiva con las raíces de $\mathrm{Irr}(\sqrt[4]{2}, \mathbb{Q}) = X^4 - 2$ en K. Luego hay cuatro, digamos $\eta_0, \eta_1, \eta_2, \eta_3$, determinados por $\eta_j(\sqrt[4]{2}) = i^j\sqrt[4]{2}$, para $j = 0, 1, 2, 3$.

Cada uno de los anteriores se extiende a dos homomorfismos de K a K, según las raíces de $\mathrm{Irr}(i, \mathbb{Q}(\sqrt[4]{2})) = X^2 + 1$. Esto nos da los ocho automorfismos buscados. En resumen,

$$\mathrm{Aut}(K) = \{\eta_{jk} : j = 0, 1, 2, 3; k = 0, 1\}$$

con η_{jk} determinado por $\eta_{jk}(\sqrt[4]{2}) = i^j\sqrt[4]{2}, \eta_{jk}(i) = (-1)^k i$.

3. Tenemos que

$$\mathrm{Aut}_{\mathbb{Q}(i\sqrt{2})}(K) \cap \mathrm{Aut}_{\mathbb{Q}(\sqrt{2})}(K) = \mathrm{Aut}_{\mathbb{Q}(\sqrt{2}, i\sqrt{2})}(K).$$

Por un argumento similar al usado en el apartado anterior, tenemos que $[\mathbb{Q}(\sqrt{2}, i\sqrt{2}) : \mathbb{Q}] = 4$. La Conexión de Galois nos da entonces que

$$(\mathrm{Aut}(K) : \mathrm{Aut}_{\mathbb{Q}(\sqrt{2}, i\sqrt{2})}(K)) = [\mathbb{Q}(\sqrt{2}, i\sqrt{2}) : \mathbb{Q}] = 4,$$

lo que indica que $\mathrm{Aut}_{\mathbb{Q}(\sqrt{2}, i\sqrt{2})}(K)$ tiene 2 elementos. Como

$$\eta_{20}(\sqrt{2}) = \eta_{20}((\sqrt[4]{2})^2) = \eta_{20}(\sqrt[4]{2})^2 = (-\sqrt[4]{2})^2 = \sqrt{2}, \quad \eta_{20}(i) = i,$$

deducimos que $\mathrm{Aut}_{\mathbb{Q}(\sqrt{2}, i\sqrt{2})}(K) = \{\eta_{00}, \eta_{20}\}$.

4. La Conexión de Galois nos dice de nuevo que los subcuerpos de K que buscamos están ligados a los subgrupos de orden dos de $\mathrm{Aut}(K)$. Es decir, estamos buscando contar los elementos de orden dos de este grupo. Puesto que $\eta_{jk}^2(i) = i$ para cualquier par j, k, los automorfismos de orden dos son aquellos que, distintos de η_{00}, satisfacen que $\eta_{jk}^2(\sqrt[4]{2}) = \sqrt[4]{2}$. Calculando, obtenemos

$$\eta_{jk}^2(\sqrt[4]{2}) = \eta_{jk}(i^j\sqrt[4]{2}) = (-1)^{kj} i^{2j}\sqrt[4]{2}.$$

Para $k = 0$ con $j \neq 0$, la condición $\eta_{jk}^2(\sqrt[4]{2}) = \sqrt[4]{2}$ se da, exactamente, cuando $j = 2$. Para $k = 1$, se tiene que $(-1)^j i^{2j} = 1$ para cualquier valor de j. Por lo que los elementos de orden dos son $\eta_{20}, \eta_{01}, \eta_{11}, \eta_{21}, \eta_{31}$. Concluimos que hay 5 subcuerpos de grado 4 de K.

Solución al Ejercicio 73. Como $f(1) = -1$ y $f(-1) = 3$, ninguna de las posibles raíces racionales de f lo es, luego f no tiene factores de grado 1. Al ser de grado 3, esto implica que es irreducible. Por tanto, su grupo de

Galois es isomorfo a A_3 o a S_3. Ahora bien, $\mathrm{Disc}(f) = 81 = 9^2$, luego la opción correcta es la primera. Así, si K es el cuerpo de descomposición de f, sabemos que $[K : \mathbb{Q}] = \#A_3 = 3$. De la torre de cuerpos $\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq K$ deducimos, mediante el Lema de la Torre, que $K = \mathbb{Q}(\alpha)$.

Solución al Ejercicio 74. 1. El elemento a es raíz del polinomio $f = X^6 + X^3 + 1 \in \mathbb{F}_2[X]$. Obviamente, f no tiene raíces en $\mathbb{F}_2$, por lo que la única forma en que podría ser reducible es que tuviera un factor irreducible de grado 2 o de grado 3. Todos estos posibles factores son $X^2 + X + 1, X^3 + X + 1, X^3 + X^2 + 1$. Anora, el resto de dividir $X^6 + X^3 + 1$ entre $X^2 + X + 1$ es 1; el de dividirlo entre $X^3 + X + 1$ es $X^2 + X + 1$ y entre $X^3 + X^2 + 1$ es X. Conclusión, ninguna de las divisiones es exacta, luego f es irreducible. Sabemos que, en tal caso, F tiene dimensión 6 sobre $\mathbb{F}_2$, es decir, tiene $2^6 = 64$ elementos.

2. Tenemos que el grupo multiplicativo $F^\times$ es cíclico de orden 63. Así que $(a^{21})^3 = a^{63} = 1$. Por tanto, a^{21} es raíz del polinomio $X^3 + 1 \in \mathbb{F}_2[X]$. Como $X^3 + 1 = (X + 1)(X^2 + X + 1)$, deducimos que, o bien $a^{21} = 1$, o bien $\mathrm{Irr}(a^{21}, \mathbb{F}_2) = X^2 + X + 1$. Descartemos la primera opción: $a^7 = aa^6 = a(a^3 + 1)$. Por tanto,

$$a^{21} = a^3(a^3 + 1)^3 = a^3(a^9 + a^6 + a^3 + 1) = a^3a^9.$$

Ahora, $a^9 = a^6a^3 = (a^3 + 1)a^3 = a^6 + a^3 = a^3 + 1 + a^3 = 1$, de modo que, después de todo, $a^{21} = a^3 \neq 1$, ya que $\{1, a, a^2, a^3, a^4, a^5\}$ es un conjunto $\mathbb{F}_2$–linealmente independiente.

Por la Proposición de Extensión, los homomorfismos de $\mathbb{F}_2(a^{21})$ a F están determinados por las raíces de $\mathrm{Irr}(a^{21}, \mathbb{F}_2) = X^2 + X + 1$. Estas raíces son a^{21} y a^{42}, por aplicación del automorfismo de Frobenius. En resumen, tenemos los dos homomorfismos $\eta_j : \mathbb{F}_2(a^{21}) \to F$, con $\eta_j(a^{21}) = a^{j \times 21}$ para $j = 1, 2$. Obviamente, η_1 es la inclusión.

Solución al Ejercicio 75. 1. Sabemos que $\mathrm{Irr}(\omega, \mathbb{Q}) = \phi_{10}$, el décimo polinomio ciclotómico sobre $\mathbb{Q}$. Como

$$\phi_{10} = \frac{X^{10} - 1}{\phi_1\phi_2\phi_5} = \frac{X^{10} - 1}{(X^5 - 1)\phi_2} = \frac{X^5 + 1}{X + 1},$$

realizando la última división obtenemos que $\phi_{10} = X^4 - X^3 + X^2 - X + 1$.

2. Como la décima extensión ciclotómica $\mathbb{Q} \leq \mathbb{Q}(\omega)$ es de Galois, vamos a usar la Conexión de Galois. Tenemos que

$$\mathrm{Aut}(\mathbb{Q}(\omega)) = \{\tau_j : j \in U(\mathbb{Z}_{10})\} = \{\tau_j : j = 1, 3, 7, 9\},$$

donde $\tau_j(\omega) = \omega^j$. Observemos que $\tau_3^2(\omega) = \omega^9 \neq \omega$, ya que ω tiene orden multiplicativo 10. De modo que τ_3 tiene orden mayor que 2, de donde, por el Teorema de Lagrange, su orden es 4. Es decir, $\mathrm{Aut}(\mathbb{Q}(\omega))$ es cíclico con generador τ_3. Por lo que su único subgrupo propio, de cardinal dos, es $\langle\tau_9\rangle$. Como $\tau_9(\omega^9) = \omega^{81} = \omega$, deducimos que $\omega + \omega^9 \in \mathbb{Q}(\omega)^{\langle\tau_9\rangle}$ y $\mathbb{Q}(\omega + \omega^9) \leq \mathbb{Q}(\omega)^{\langle\tau_9\rangle}$. La igualdad se dará, por el Lema de la Torre, siempre y cuando comprobemos que $\omega + \omega^9 \notin \mathbb{Q}$. Bien, como, al tener orden multiplicativo 2, $\omega^5 = -1$, deducimos que

$$\omega^9 + \omega = -\omega^4 + \omega = \omega^3 - \omega^2 + \omega - 1 + \omega \notin \mathbb{Q},$$

ya que $\{1, \omega, \omega^2, \omega^3\}$ es un conjunto $\mathbb{Q}$–linealmente independiente.

La Conexión de Galois nos dice, entonces, que los subcuerpos de $\mathbb{Q}(\omega)$ son $\mathbb{Q}, \mathbb{Q}(\omega + \omega^9), \mathbb{Q}(\omega)$.

Solución al Ejercicio 76. 1. Como f es bicuadrático, podemos calcular sus raíces como sigue. Si r es una, entonces r^2 lo es de $X^2 + 3X - 2$, por lo

que

$$r^2 = \frac{-3 \pm \sqrt{17}}{2}.$$

Esto da cuatro valores complejos para r, que son $\alpha, -\alpha, \beta, -\beta$, donde

$$\alpha = \sqrt{\frac{-3+\sqrt{17}}{2}}, \qquad \beta = i\sqrt{\frac{3+\sqrt{17}}{2}}.$$

De estos números, α es el único real y positivo. Observemos que $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\frac{-3+\sqrt{17}}{2}) = \mathbb{Q}(\sqrt{17})$. Puesto que el polinomio $X^2 - 17 \in \mathbb{Q}[X]$ es irreducible por el criterio de Eisenstein, deducimos que se trata de $\mathrm{Irr}(\sqrt{17}, \mathbb{Q})$, de donde $[\mathbb{Q}(\sqrt{17}) : \mathbb{Q}] = 2$ y $\{1, \sqrt{17}\}$ es una $\mathbb{Q}$–base de $\mathbb{Q}(\sqrt{17})$.

Si $\alpha \in \mathbb{Q}(\alpha^2)$ deducimos de lo anterior que existen $a, b \in \mathbb{Q}$ tales que $\alpha = a + b\sqrt{17}$. Elevando al cuadrado, obtenemos que

$$\frac{-3+\sqrt{17}}{2} = a^2 + 17b^2 + 2ab\sqrt{17}.$$

Igualando coordenadas con respecto de la base $\{1, \sqrt{17}\}$, obtenemos que $-3/2 = a^2 + 17b^2 \geq 0$. Esta contradicción fuerza que $\alpha \notin \mathbb{Q}(\alpha^2)$.

2. Es claro que $K = \mathbb{Q}(\alpha, \beta)$. Por tanto, $\alpha\beta \in K$. Pero

$$\alpha\beta = i\sqrt{\left(\frac{-3+\sqrt{17}}{2}\right)\left(\frac{3+\sqrt{17}}{2}\right)} = i\sqrt{\frac{8}{4}} = i\sqrt{2}.$$

Por otra parte, $K = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \alpha\beta) = \mathbb{Q}(\alpha, i\sqrt{2})$. Usando el Lema de la Torre, obtenemos

$$[K : \mathbb{Q}] = [\mathbb{Q}(\alpha)(i\sqrt{2}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)][\mathbb{Q}(\alpha^2) : \mathbb{Q}]. \tag{5.4}$$

Como $i\sqrt{2}$ raíz de $X^2 + 2 \in \mathbb{Q}(\alpha)[X]$, el primer factor es, a lo sumo, 2. Ya que $i\sqrt{2} \notin \mathbb{Q}(\alpha)$, por ser α real, resulta ser 2. Puesto que $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{17})$ y $\sqrt{17} \notin \mathbb{Q}$, según se ha argumentado en el apartado anterior, deducimos que $[\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 2$. Para calibrar el factor central, observemos que α es raíz de $X^2 - \alpha^2 \in \mathbb{Q}(\alpha^2)[X]$, por lo que $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] \leq 2$. Como $\alpha \notin \mathbb{Q}(\alpha^2)$, deducimos que este valor es 2. Así, la igualdad (5.4) muestra que $[K : \mathbb{Q}] = 2 \times 2 \times 2 = 8$.

3. Puesto que K es cuerpo de descomposición de un polinomio separable[4], $\mathbb{Q} \leq K$ es de Galois, por lo que $\#\mathrm{Aut}(K) = 8$. Comenzamos usando la Proposición de Extensión para determinar los homomorfismos de cuerpos desde $\mathbb{Q}(\alpha)$ a K, que no son más que las extensiones de la inclusión $\mathbb{Q} \leq \mathbb{Q}(\alpha)$. Los citados homomorfismos están en correspondencia con las raíces en K de $\mathrm{Irr}(\alpha, \mathbb{Q})$. El grado de este polinomio es $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, valor que, según se colige de lo expuesto en el apartado anterior, es 4. Como α es raíz de f, y f alcanza el mínimo grado entre los polinomios que se anulan en α, deducimos que $f = \mathrm{Irr}(\alpha, \mathbb{Q})$. De modo que hay cuatro homomorfismos $\eta_j : \mathbb{Q}(\alpha) \to K$, con $j = 0, 1, 2, 3$, determinados por. $\eta_j(\alpha) = (-1)^j\alpha$ para $j = 0, 1$ y $\eta_j(\alpha) = (-1)^j\beta$, para $j = 2, 3$.

Cada η_j se extiende, por la misma Proposición de Extensión, a tantos homomorfismos de $K = \mathbb{Q}(\alpha)(i\sqrt{2})$ a K como raíces tenga en K el polinomio $\mathrm{Irr}(i\sqrt{2}, \mathbb{Q}(\alpha))^{\eta_j}$. Pero $i\sqrt{2}$ es raíz de $X^2 + 2$ e $i\sqrt{2} \notin \mathbb{Q}$, por lo que $\mathrm{Irr}(i\sqrt{2}, \mathbb{Q}(\alpha)) = X^2 + 2$. Deducimos, por tanto, que η_j tiene dos extensiones

[4] también valdría aquí invocar que estamos en característica cero

$\eta_{j\ell} : K \to K$, determinadas por $\eta_{j\ell}(i\sqrt{2}) = (-1)^\ell i\sqrt{2}$ para $\ell = 0, 1$. Obtenemos, pues, que

$$\mathrm{Aut}(K) = \{\eta_{j\ell} : j = 0, 1, 2, 3, \ell = 0, 1\},$$

para $\eta_{j\ell}$ determinado por

$$\eta_{j\ell} : \begin{cases} \alpha & \mapsto (-1)^j \alpha, \quad (j = 0, 1) \\ \alpha & \mapsto (-1)^j \beta, \quad (j = 2, 3) \\ i\sqrt{2} & \mapsto (-1)^\ell i\sqrt{2} \quad (\ell = 0, 1) \end{cases} \tag{5.5}$$

4. Tenemos que calcular los subgrupos $\mathrm{Aut}_{\mathbb{Q}(\alpha^2)}(K)$ y $\mathrm{Aut}_{\mathbb{Q}(i\sqrt{2})}(K)$. Por la Conexión de Galois, conocemos sus tamaños: para el primero, tenemos

$$\#\mathrm{Aut}_{\mathbb{Q}(\alpha^2)}(K) = (\mathrm{Aut}_{\mathbb{Q}(\alpha^2)}(K) : \mathrm{id}_K) = [K : \mathbb{Q}(\alpha^2)] = \frac{[K : \mathbb{Q}]}{[\mathbb{Q}(\alpha^2) : \mathbb{Q}]} = 8/2 = 4.$$

Aquí, hemos usado información de los apartados anteriores. Análogamente, se obtiene que $\#\mathrm{Aut}_{\mathbb{Q}(i\sqrt{2})}(K) = 4$. Para el primer grupo, hemos de buscar cuatro automorfismos de K que dejen fijo α^2. A la vista de (5.5),

$$\mathrm{Aut}_{\mathbb{Q}(\alpha^2)}(K) = \{\eta_{00}, \eta_{01}, \eta_{10}, \eta_{11}\}.$$

Con el mismo argumento, los cuatro automorfismos que dejan fijo $i\sqrt{2}$ son

$$\mathrm{Aut}_{\mathbb{Q}(i\sqrt{2})}(K) = \{\eta_{00}, \eta_{10}, \eta_{20}, \eta_{30}\}.$$

5. Como $\alpha + i\sqrt{2} \in K$, tenemos que $\mathbb{Q}(\alpha + i\sqrt{2})$ es un subcuerpo de K que, por la Conexión de Galois, ha de ser el subcuerpo fijo por un subgrupo de $\mathrm{Aut}(K)$. Veamos quién es dicho subgrupo. Observemos que

$$\eta_{j\ell}(\alpha + i\sqrt{2}) = (-1)^j \alpha + (-1)^\ell i\sqrt{2} \qquad (j = 0, 1),$$
$$\eta_{j\ell}(\alpha + i\sqrt{2}) = (-1)^j \beta + (-1)^\ell i\sqrt{2} \qquad (j = 2, 3).$$

En el primer caso, que $\eta_{j\ell}(\alpha + i\sqrt{2}) = \alpha + i\sqrt{2}$ implica, igualando partes reales e imaginarias, que $\alpha = (-1)^j \alpha$ y $(-1)^\ell i\sqrt{2}$. Por tanto, $j = \ell = 0$. En el segundo caso, si $\ell = 0$, y $\alpha + i\sqrt{2}$ queda fijo por η_{j0}, deducimos que $\alpha = (-1)^j \beta$, lo que implicaría que un número sea real e imaginario puro al mismo tiempo. El subcaso restante da la igualdad

$$\alpha + i\sqrt{2} = (-1)^j \beta - i\sqrt{2}.$$

Lo que implica que $\alpha = -2i\sqrt{2} + (-1)^j \beta$. Esto es también imposible porque, en tal caso, α sería un número imaginario. En conclusión, $\mathrm{Aut}_{\mathbb{Q}(\alpha + i\sqrt{2})}(K) = \{\eta_{00}\}$. La Conexión de Galois implica que $K = \mathbb{Q}(\alpha + i\sqrt{2})$. Luego el grado de $g = \mathrm{Irr}(\alpha + i\sqrt{2})$ es igual a $[K : \mathbb{Q}] = 8$.

Como $\mathbb{Q} \leq K$ es de Galois, todas las raíces de g están, al estar una y ser irreducible, en K. Es decir, K es cuerpo de descomposición de $g \in \mathbb{Q}[X]$. Así, su grupo de Galois, que es $\mathrm{Aut}(K)$, tiene 8 elementos, luego es resoluble. Por tanto, g es resoluble por radicales.

Por último, f es resoluble por radicales porque sus raíces están en K, que es una extensión de Galois de grado $8 = 2^3$ sobre $\mathbb{Q}$. Alternativamente, podemos decir dichas raíces se obtienen partiendo de $\mathbb{Q}$ mediante extracción de raíces cuadradas y operaciones de cuerpo, por lo que son números construibles.

Solución al Ejercicio 77. 1. Sabemos que $X^{14} - 1 = \phi_1 \phi_2 \phi_7 \phi_{14}$. Como $\phi_1 \phi_7 = X^7 - 1$, deducimos que $\phi_2 \phi_{14} = \frac{X^{14}-1}{X^7-1} = X^7 + 1$. Luego $\phi_{14} = \frac{X^7+1}{X+1}$. Realizando esta división euclidiana de polinomios, obtenemos que

$$\phi_{14} = X^6 - X^5 + X^4 - X^3 + X^2 - X + 1.$$

2. Sabemos que $\mathrm{Aut}(\mathbb{Q}(\eta))$ es isomorfo al grupo de unidades $\mathcal{U}(\mathbb{Z}_{14})$. De hecho, ese isomorfismo viene de la descripción explícita

$$\mathrm{Aut}(\mathbb{Q}(\eta)) = \{\tau_j : j = 1, 3, 5, 9, 11, 13\},$$

donde $\tau_j(\eta) = \eta^j$ para cada j. Como es un grupo abeliano de cardinal 6, ha de ser cíclico de orden 6, luego tiene, aparte del subgrupo trivial y del total, dos subgrupos de orden 2 y 3, respectivamente. Calculemos éstos. Comencemos con el orden de τ_3, aplicándolo sucesivamente a η, según se indica en el siguiente esquema:

$$\eta \xrightarrow{\tau_3} \eta^3 \xrightarrow{\tau_3} \eta^9 \xrightarrow{\tau_3} \eta^{27} = \eta^{13} \ . \tag{5.6}$$

Las raíces decimocuartas de la unidad forman un grupo cíclico de orden 14 generado por η. Por tanto, $\eta^{12} \neq 1$, por lo que $\eta^{13} \neq \eta$. Deducimos que el orden de τ_3 es mayor que 3. El Teorema de Lagrange nos dice que ha de ser 6, esto es, $\mathrm{Aut}(\mathbb{Q}(\eta)) = \langle\tau_3\rangle$. El subgrupo de orden 2 ha de ser $\langle\tau_3^3\rangle$, en tanto que el de orden 3 es $\langle\tau_3^2\rangle$. El propio cálculo (5.6) indica que estos grupos son, respectivamente, $\langle\tau_{13}\rangle$ y $\langle\tau_9\rangle$.

3. Como sabemos que $\mathbb{Q} \leq \mathbb{Q}(\eta)$ es una extensión de Galois, podemos usar la Conexión de Galois para asegurar que los subcuerpos de $\mathbb{Q}(\eta)$ son, exactamente, los fijos por los subgrupos del grupo $\mathrm{Aut}(\mathbb{Q}(\eta))$, descritos en el apartado anterior. Así, aparte de $\mathbb{Q}$ y $\mathbb{Q}(\eta)$, los subcuerpos propios serán $\mathbb{Q}(\eta)^{\langle\tau_9\rangle}$ y $\mathbb{Q}(\eta)^{\langle\tau_{13}\rangle}$.

Tenemos que $[\mathbb{Q}(\eta)^{\langle\tau_9\rangle} : \mathbb{Q}] = (\mathrm{Aut}(\mathbb{Q}(\eta)) : \langle\tau_9\rangle) = 2$. Hemos de buscar elementos fijos por τ_9. Vemos que $\tau_9(\eta^7) = \eta^{63} = \eta^7$, pero η^7 tiene orden multiplicativo 2, luego $\eta^7 = -1$. Así que $\mathbb{Q}(\eta^7) = \mathbb{Q}$, luego hemos de buscar otro elemento fijo por τ_9.

Describamos la órbita de η por la acción de τ_9:

$$\eta \xrightarrow{\tau_9} \eta^9 = \eta^7\eta^2 = -\eta^2 \xrightarrow{\tau_9} -\eta^{18} = -\eta^4 \xrightarrow{\tau_9} -\eta^{36} = -\eta^8 = \eta \ .$$

De donde obtenemos que

$$\tau_9(\eta - \eta^2 - \eta^4) = -\eta^2 - \eta^4 + \eta.$$

De modo que $\eta - \eta^2 - \eta^4 \in \mathbb{Q}^{\langle\tau_9\rangle}$. Podemos afirmar que $\eta - \eta^2 - \eta^4 \notin \mathbb{Q}$ ya que $[\mathbb{Q}(\eta) : \mathbb{Q}] = 6$ y $\{1, \eta, \ldots, \eta^5\}$ es $\mathbb{Q}$–linealmente independiente. Por tanto, $\mathbb{Q}^{\langle\tau_9\rangle} = \mathbb{Q}(\eta - \eta^2 - \eta^4)$.

Puesto que $\eta^{13} = \eta^{-1}$, tenemos que $\tau_{13}(\eta + \eta^{-1}) = \eta^{-1} + \eta$, luego $\mathbb{Q}(\eta + \eta^{-1}) \leq \mathbb{Q}(\eta)^{\langle\tau_{13}\rangle}$. Además, $\eta + \eta^{-1} \notin \mathbb{Q}$, ya que, usando que ϕ_{14} es el polinomio mínimo de η sobre $\mathbb{Q}$, obtenemos que

$$\eta + \eta^{-1} = \eta - \eta^6 = \eta - \eta^5 + \eta^4 - \eta^3 + \eta^2 - \eta + 1 = -\eta^5 + \eta^4 - \eta^3 + \eta^2 - 1$$

y que $\{1, \eta, \ldots, \eta^5\}$ es $\mathbb{Q}$–linealmente independiente. La Conexión de Galois nos da, como antes, que $[\mathbb{Q}(\eta)^{\langle\tau_{13}\rangle} : \mathbb{Q}] = 3$, por lo que hemos de admitir, por el Lema de la Torre, la igualdad $\mathbb{Q}(\eta + \eta^{-1}) = \mathbb{Q}(\eta)^{\langle\tau_{13}\rangle}$.

Solución al Ejercicio 78. Puesto que $h \in \mathbb{F}_2[X]$ no tiene raíces en $\mathbb{F}_2$ y tiene grado 3, ha de ser irreducible. Vimos en clase que cualquier cuerpo de descomposición de h es isomorfo a uno de $2^3 = 8$ elementos. También sabemos, puesto que $64 = 2^6$ y 3 divide a 6, que $\mathbb{F}_{64} = \mathbb{F}_2(a)$ contiene un único subcuerpo F con 8 elementos. Dicho cuerpo es de la forma $F = \mathbb{F}_2(b)$ para $b \in \mathbb{F}_{64}$ tal que $\mathrm{Irr}(b, \mathbb{F}_2)$ tiene grado 3. Buscamos, pues, $b \in \mathbb{F}_2(a)$ de manera que $\mathrm{Irr}(b, \mathbb{F}_2) = h$.

Sabemos que $F^\times$ es un grupo cíclico de orden 7. Como, de acuerdo con el enunciado, a es un generador del grupo cíclico $\mathbb{F}_2(a)^\times$, que tiene

orden 63, $F^\times$ ha de ser el único subgrupo cíclico de orden 7 de $\mathbb{F}_2(a)^\times$. Como consecuencia, $b \in \{a^9, a^{18}, a^{27}, a^{36}, a^{45}, a^{54}\}$, ya que $b \neq 1$. Probemos a evaluar h en el más sencillo: hemos de calcular $h(a^9) = (a^9)^6 + a^9 + 1$. Tenemos que

$$a^9 = a^3(a+1) = a^4 + a^3;$$

$$(a^9)^6 = (a^6)^9 = (a+1)^8(a+1) = (a^8+1)(a+1) = (a^2a^6+1)(a+1)$$
$$= (a^2(a+1)+1)(a+1) = (a^3+a^2+1)(a+1) = a^4+a^2+a+1,$$

luego

$$h(a^9) = a^4+a^2+a+1+a^4+a^3+1 = a^2+a+a^3,$$

elemento que es no nulo porque $\{1, a, a^2, a^3, a^4, a^5\}$ es una $\mathbb{F}_2$–base de $\mathbb{F}_2(a)$.

Ahora podríamos seguir "probando" a evaluar más candidatos, pero preferimos usar un poco más de teoría: Recordemos que los elementos de F son, exactamente, las raíces de $X^8 + X$ en $\mathbb{F}_2(a)$. De la factorización completa $X^8 + X = X(X+1)(X^3+X+1)(X^3+X^2+1)$ deducimos, puesto que no lo es de h, que a^9 ha de ser raíz del último factor. Sus otras dos raíces se obtienen aplicando el automorfismo de Frobenius de F: son a^{18}, a^{36}. De modo que las raíces de h tienen que ser los tres elementos que quedan en $F^\times$ distintos de 1, a saber, a^{27}, a^{45}, a^{54}.

Bibliografía

1. J. B. Fraleigh, Álgebra Abstracta, Addison-Wesley Iberoamericana, 1987.
2. J. Gómez Torrecillas, Álgebra I, Universidad de Granada, 2018-2022, http://hdl.handle.net/10481/76682
3. N. Jacobson, Basic Algebra I, W H Freeman & Co, 1985.
4. S. Lang, Algebra, revised third edition. Springer, 2002.
5. J. S. Milne, Fields and Galois Theory (v. 5.00), 2021. Available at www.jmilne.org/math/.
6. J. P. Tignol, Galois' Theory of Algebraic Equations, World Scientific, 2001.
7. B.L. Van der Waerden, Algebra vol. 1, seventh edition, Frederik Ungar Publishing co., 1970.