Álgebra III

Versión 2.3. Cursos 22/23, 23/24 y 24/25. [1] **Advertencia: al tratarse de un borrador, puede contener erratas, y acaso algún error, así que estos apuntes han de usarse con prudencia, leerse críticamente y preguntar en caso de duda. En particular, declino cualquier responsabilidad por un uso ignorante de esta advertencia. Comentarios y sugerencias serán bienvenidos.**

José Gómez Torrecillas
Departamento de Álgebra
Universidad de Granada

[1] versión: 1 de octubre de 2024

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* [1] de cuerpos.

Dada cualquier extensión de cuerpos $F \leq K$, la propia multiplicación de K proporciona una estructura de F–espacio vectorial sobre 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. $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$. La segunda igualdad se deduce de que $\mathbb{R}$ no tiene cardinal numerable.

Dado cualquier conjunto 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 $S = \emptyset$, obtenemos el menor subcuerpo de K, que se llama *subcuerpo primo* de K.

La característica de un anillo A se denotará por $car(A)$.

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* $car(K) = 0$.

[1] Más tarde, daremos una definición algo más general de extensión de cuerpos.

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

Si $p > 0$, entonces tenemos un isomorfismo de anillos $\mathbb{Z}/p\mathbb{Z} \cong \mathrm{Im}\chi$, así que $\mathrm{Im}\chi$ es un subcuerpo de K isomorfo a $\mathbb{Z}_p$. Como $\mathrm{Im}\chi \subseteq \Pi$, deducimos que $\mathrm{Im}\chi = \Pi$.

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

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 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. 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

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

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

[2]Ver Sección 2.3 para una demostración en el contexto de este curso, que no necesita variable compleja.

cualquiera de ellas, entonces un cuerpo de descomposición de $X^n - 1$ 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.

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 $F(\alpha) \cong F[X]/\langle f\rangle$ 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 (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, por el isomorfismo (1.1), 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 $\{X^i + \langle f\rangle : i < \deg f\}$. 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 $\operatorname{Irr}(\alpha, F)$. Al grado de $\operatorname{Irr}(\alpha, F)$ 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.

EJERCICIO 3. 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 $\operatorname{Irr}(\alpha, F)$.

EJERCICIO 4. Calcular $\operatorname{Irr}(\omega, \mathbb{Q}(\sqrt[3]{2}))$, para $\omega = e^{i2\pi/3}$.

EJERCICIO 5. Sea p un número primo y $\omega \neq 1$ una raíz p–ésima compleja de la unidad. Calcular $\operatorname{Irr}(\omega, \mathbb{Q})$.

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 referencia, 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. Cada inclusión es estricta, ya que $\omega \notin \mathbb{Q}(\sqrt[3]{2})$ por no ser un número real. 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 están en ese subcuerpo. Así,

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

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 de este 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 $F \le K$ y $\alpha \in K$, se tiene que α es algebraico sobre F si, y sólo si, existe una sub-extensión $F \le L \le K$ tal que $F \le L$ 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 $F(\alpha) \le L$, deducimos del Lema 1.16 que $F(\alpha)$ es un F–espacio vectorial de dimensión finita. Por tanto, existe un natural $n \ge 1$ 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 $F \le K$ 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 $F \le K$ es finita si, y sólo si, es algebraica y finitamente generada.*

DEMOSTRACIÓN. Si $F \le K$ 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 $F \le F(\alpha_1) \le F(\alpha_1,\alpha_2) \le \cdots \le F(\alpha_1,\ldots,\alpha_n) = K$. Por tanto, $F \le K$ es finita. □

COROLARIO 1.23. *Dada una extensión $F \le K$, el conjunto Λ de los elementos de K que son algebraicos sobre F es un subcuerpo de K. Obviamente, la extensión $F \le \Lambda$ es algebraica.*

DEMOSTRACIÓN. Si $\alpha,\beta \in K$ son algebraicos sobre F, entonces $\alpha+\beta, \alpha\beta \in F(\alpha,\beta)$. Como la extensión $F \le F(\alpha,\beta)$ es finita, deducimos que es algebraica, así que $\alpha+\beta, \alpha\beta$ son algebraicos. Luego Λ es un subanillo de K. Por último, si $\alpha \ne 0$, entonces $\alpha^{-1} \in F(\alpha)$, y resulta ser algebraico sobre F. Así que Λ es un subcuerpo de K. □

DEFINICIÓN 1.24. El subcuerpo Λ de K descrito en el Corolario 1.23 se llama *clausura algebraica de F en K*.

EJEMPLO 1.25. 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 6. Calcular $\mathrm{Irr}(\sqrt{2}+i, \mathbb{Q})$.

EJERCICIO 7. Calcular $\mathrm{Irr}(\sqrt{2}+i\sqrt{3}, \mathbb{Q})$.

EJERCICIO 8. Calcular un cuerpo de descomposición de $X^4+16 \in \mathbb{Q}[X]$ y su grado sobre $\mathbb{Q}$.

EJERCICIO 9. Calcular $\mathrm{Irr}(\sqrt{2}+\sqrt[3]{2}, \mathbb{Q})$.

1.3. Construcciones con regla y compás

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 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 S junto con las circunferencias con centros en S y radio determinado por este centro y cualquier otro punto de S. Llamemos S^c a los puntos obtenidos al intersecar cualquier par de elementos de Γ. Es claro que $S \subseteq S^c$.

DEFINICIÓN 1.26. Dado un conjunto finito de puntos S del plano euclidiano, definimos recursivamente la sucesión de subconjuntos S_n del plano como sigue: $S_0 = S$, $S_{n+1} = S_n^c$, para $n \in \mathbb{N}$. El conjunto de los *puntos constructibles* (con regla y compás) a partir de S es

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

LEMA 1.27. *Dados tres puntos P, Q, R del plano, con P, Q distintos, se puede construir con regla y compás 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 trazamos 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 un 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 isósceles. 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.

□

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 con contenido en ella, construir, usando regla y compás, el simétrico de A con respecto de r.

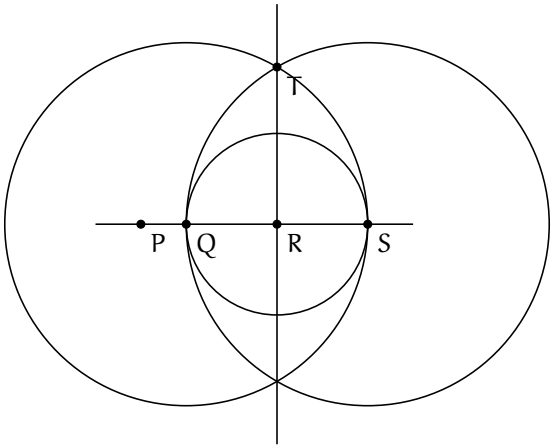


FIGURA 1. Recta perpendicular, caso 1

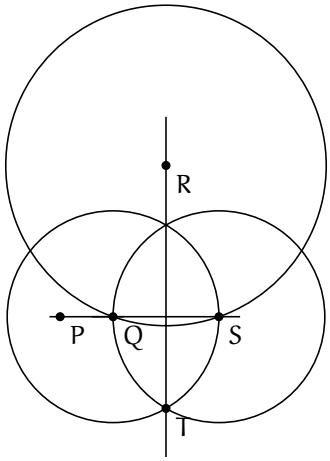


FIGURA 2. Recta perpendicular, caso 2

Elijamos dos puntos en 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 $C(S)$ de los puntos constructibles a partir de S es un subconjunto de $\mathbb{C}$. Con esta perspectiva, lo que estamos suponiendo es que S contiene a los números 0 y 1.

LEMA 1.28. *Dado $z = x+iy \in \mathbb{C}$ se tiene que $z \in C(S)$ si, y sólo si, $x,y \in C(S)$.*

DEMOSTRACIÓN. Observemos que $i \in C(S)$, 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 $r \in C(S)$ si, y sólo si, $ri \in C(S)$.

Bien, si $x+iy \in C(S)$, entonces obtenemos x, iy como proyecciones ortogonales sobre el eje real y el eje imaginario. Por tanto, $x,y \in C(S)$. Recíprocamente, si $x,y \in C(S)$, entonces podemos obtener $x+iy$ como la

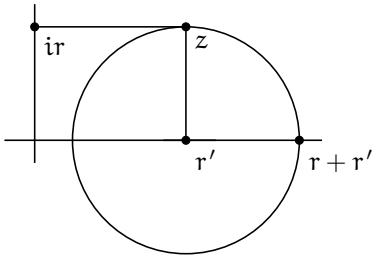


FIGURA 3. Suma de números reales

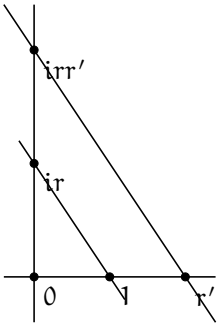


FIGURA 4. Producto de números reales

intersección de la recta perpendicular al eje imaginario que pasa por iy y la perpendicular al eje real que pasa por x. □

PROPOSICIÓN 1.29. *El conjunto* $C(S)$ *es un subcuerpo de* $\mathbb{C}$*. Además, si* $z \in C(S)$*, entonces* $\overline{z} \in C(S)$*.*

DEMOSTRACIÓN. En virtud del Lema 1.28, y de la expresión de las operaciones suma, producto e inversión de números complejos en función de sus componentes real e imaginaria, basta que que demostremos que $C(S) \cap \mathbb{R}$ es un subcuerpo.

Vayamos con la suma y el producto: dados $r, r' \in C(S) \cap \mathbb{R}$, sabemos que $z = r' + ir \in C(S)$. El corte de la circunferencia con centro r' que pasa por z con el eje real es el número $r + r'$.

Para el producto rr', supongamos que $r, r' > 0$, ya que el resto de los casos se deduce de éste teniendo en cuenta que si $x \in C(S)$, entonces $-x \in C(S)$. 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 triángulos de vértices $0, 1, ir$ y $0, r', iy$ son semejantes, lo que implica que $y = rr'$ y, por tanto, $rr' \in C(S)$.

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 $r^{-1} \in C(S)$.

□

LEMA 1.30. *Si* $z \in C(S)$*, entonces* $\sqrt{z} \in C(S)$*.*

DEMOSTRACIÓN. Escribiendo z en forma polar, reducimos el problema a un número de módulo 1 demostrando que, si $r \in C(S)$ es real y positivo, entonces $\sqrt{r} \in C(S)$. Para ello, construimos la circunferencia con centro

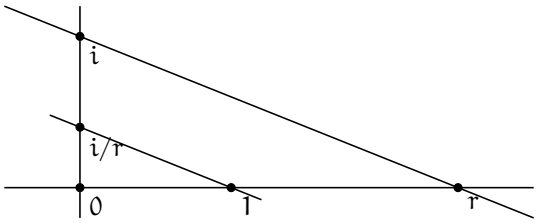


FIGURA 5. Inversión de números reales

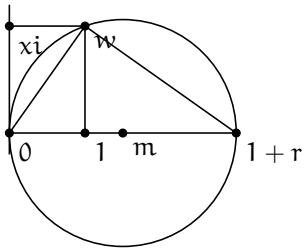


FIGURA 6. Extracción de raíces cuadradas de números reales positivos

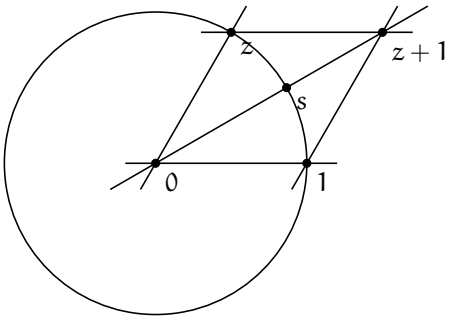


FIGURA 7. Construcción de la raíz cuadrada $s = \sqrt{z}$

$m = (1 + r)/2$ 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 $x \in C(S)$ 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 $x^2 = r$.

Finalmente, tomemos $z = e^{i\theta} \in C(S)$. El número $z+1 \in C(S)$ es entonces de la forma $re^{i\theta/2}$ para $r = |z + 1|$ (usar la regla del paralelogramo para sumar z y 1). Como $|z+1| = \sqrt{(z + 1)(\overline{z + 1})}$, deducimos que $s = e^{i\theta/2} \in C(S)$, lo que prueba el lema.

□

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

DEMOSTRACIÓN. Ya sabemos que $C(S)$ es un subcuerpo de $\mathbb{C}$ que contiene a S y es cerrado por conjugación y raíces cuadradas. Tomemos otro subcuerpo C' con las mismas propiedades, y demostremos que $C(S) \subseteq C'$. En vista de (1.3), basta con que demostremos que $S_n \subseteq C'$ para todo $n \in \mathbb{N}$. Obviamente, $S_0 = S \subseteq C'$. Supongamos $S_n \subseteq C'$ para algún $n \in \mathbb{N}$. Dado $z \in S_{n+1}$, tenemos que $z \in X \cap Y$ para X, Y rectas o circunferencias trazadas a partir de 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 1.32. 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 $i = 1, \ldots, t-1$.

TEOREMA 1.33. *Sea $S = \{z_1, \ldots, z_n\} \subseteq \mathbb{C}$ y $F = \mathbb{Q}(z_1, \ldots, z_n, \overline{z}_1, \ldots, \overline{z}_n)$. Denotemos por $\mathcal{T}$ el conjunto de todas las torres por raíces cuadradas sobre F contenidas en $\mathbb{C}$. Entonces*

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

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, 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 $F \leq C(S)$, se deduce del Lema 1.30 que $L \leq C(S)$. 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 1.31, que $C(S) \leq L$. Por tanto, $L = C(S)$. □

COROLARIO 1.34. *El cuerpo $C(S)$ es una extensión algebraica de F. De hecho, todo número en $C(S)$ tiene como grado sobre F una potencia de 2.*

DEMOSTRACIÓN. Si $\alpha \in C(S)$ entonces, por el Teorema 1.33, 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 1.35. Un número complejo z se dice *constructible* si lo es a partir de $\{0, 1\}$.

COROLARIO 1.36. *Todo número constructible es algebraico con grado sobre $\mathbb{Q}$ una potencia de 2.*

EJEMPLO 1.37. Consideremos la circunferencia de radio 1 centrada en 0. Si el lado ℓ de un cuadrado de igual área fuera constructible, entonces $\ell^2 = \pi$. Eso implica que π es constructible y, por el Corolario 1.36, algebraico. Lo que contradice el Teorema de Lindemann-Weierstrass.

EJEMPLO 1.38. 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 $e^{i\pi/3}$. En caso de que la respuesta fuese positiva, tendríamos que $\cos\pi/9$ sería constructible a partir de $e^{i\pi/3}$. De acuerdo con el Teorema 1.33, esto significaría que $\cos\pi/9$ pertenecería a una torre por raíces cuadradas sobre $F = \mathbb{Q}(e^{i\pi/3}) = \mathbb{Q}(\sqrt{-3})$. En particular, su grado sobre F sería una potencia de 2. Por otra parte, $[F : \mathbb{Q}] = 2$, así que, si $\cos\pi/9$ perteneciese a una torre por raíces cuadradas de F, entonces su grado 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 constructible a partir de $e^{i\pi/3}$ y deducimos que el ángulo de 20^o no se puede construir con regla y compás a partir del ángulo de 60^o.

1.4. Homomorfismos de cuerpos. Cuerpos de descomposición

Nuestro próximo objetivo es buscar cuerpos donde un polinomio dado tenga todas sus raíces.

LEMA 1.39. *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 1.40. 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 1.41. Dado un homomorfismo de cuerpos $\sigma : F \to K$, el Lema 1.39 indica que F es isomorfo, vía σ, al subcuerpo $\sigma(F) = \mathrm{Im}\sigma$ de

K. Tenemos 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

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

EJEMPLO 1.42. 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 1.42, enunciándola como lema, para su uso posterior.

LEMA 1.43. *Si $f \in F[X]$ es no constante, existe un homomorfismo de cuerpos $\sigma : F \to K$ y $\alpha \in K$ tal que $f^\sigma(\alpha) = 0$ y $\sigma(F)(\alpha) = K$.*

PROPOSICIÓN 1.44. *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. Recordemos que f admite una factorización única. Mirándola, podemos descomponer $f = gh$, donde $g \in F[X]$ es producto de polinomios lineales 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 $E = F$ y $\sigma = id_F$.

Vayamos al caso propio, que ocurre cuando h tiene algún divisor irreducible p de grado mayor que 1. Aplicando la construcción descrita en el Ejemplo 1.42 obtenemos un homomorfismo de cuerpos $\tau : F \to K$ tal que h^τ tiene una raíz $\alpha \in K$ y $K = \tau(F)(\alpha)$. 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 $\rho : K \to E$ tal que E es un cuerpo de descomposición de $(f^\tau)^\rho$. Tomando la composición $\sigma = \rho\tau : F \to E$, f^σ se descompone como producto de polinomios lineales en $E[X]$. Además, $E = \rho(K)(\sigma(\alpha_1), \dots, \sigma(\alpha_t), \rho(\beta_1), \dots, \rho(\beta_r), \gamma_1, \dots, \gamma_r)$, para $\gamma_1, \dots, \gamma_r \in E$ las raíces de k. Por último, puesto que $\alpha_1, \dots, \alpha_t \in F$ y $\beta_1, \dots, \beta_s \in \tau(F)(\alpha)$, deducimos que $E = \sigma(F)(\rho(\alpha), \gamma_1, \dots, \gamma_r)$ y, a fortiori,

$$E = \sigma(F)(\sigma(\alpha_1), \dots, \sigma(\alpha_t), \rho(\beta_1), \dots, \rho(\beta_r), \gamma_1, \dots, \gamma_r).$$

□

Extendemos la definición de cuerpo de descomposición que habíamos dado para recoger la situación descrita por la anterior proposición.

DEFINICIÓN 1.45. 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.

EJEMPLO 1.46. 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 1.47. 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 1.42, 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

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

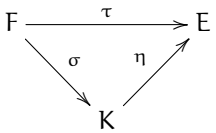
Por tanto, L es un cuerpo de descomposición de f. Más adelante, daremos alguna información general sobre los cuerpos de descomposición de polinomios con coeficientes en cuerpos finitos.

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

LEMA 1.48. *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 $\sigma_\alpha : F[X]/\langle p\rangle \cong \sigma(F)(\alpha)$ 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. □

DEFINICIÓN 1.49. 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 $\mathrm{Ex}(\tau, \sigma)$.



PROPOSICIÓN 1.50 (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 1.48. 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 $\tau(F)(\beta) \subseteq E$. Tenemos que

$$\eta(\alpha) = \tau_\beta(X + \langle p\rangle) = \beta. \tag{1.4}$$

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

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

□

OBSERVACIÓN 1.51. Obsérvese que la Proposición 1.50 no excluye el caso en que $\mathrm{Ex}(\tau, \sigma) = \emptyset$, que se da cuando f^τ no tiene raíces en E.

LEMA 1.52. *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*

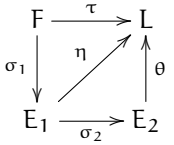
$$\mathrm{Ex}(\tau, \sigma_2\sigma_1) = \bigcup_{\eta \in \mathrm{Ex}(\tau, \sigma_1)} \mathrm{Ex}(\eta, \sigma_2).$$

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



□

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

PROPOSICIÓN 1.53. *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, este es el único elemento de $Ex(\tau, \sigma)$ en este caso.

Supongamos que $n > 1$, lo que implica que existe $\alpha \in K$ tal que $[\sigma(F)(\alpha) : \sigma(F)] > 1$. Por tanto, $[K : \sigma(F)(\alpha)] < n$.

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 1.52, 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 1.50, $\#Ex(\tau, \sigma')$ es igual al número de raíces de p^τ en E. Así,

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

□

PROPOSICIÓN 1.54. *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 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, como en la Proposición 1.53, 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 1.53, 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 1.53, deducimos que

$$\#Ex(\tau, \sigma) = \sum_{\eta \in Ex(\tau, \sigma')} \#Ex(\eta, \iota). \tag{1.5}$$

De la Proposición 1.50 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 $Ex(\tau, \sigma)$ tiene cardinal mayor que 0, es decir, 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 (1.5), implica que

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

□

EJERCICIO 14. 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 1.55 (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 1.54, 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 inyectivo, 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. □

1.5. 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 1.56. *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 15. 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 1.57. *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 $f' = -1$, 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 1.56, que E es cuerpo de descomposición de f. El Teorema 1.55 garantiza que E es isomorfo a F. □

Usaremos la notación $\mathbb{F}_q$ para referirnos "al" cuerpo finito con q elementos.

1.6. 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 bajo 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.

EJERCICIO 16. Demostrar que, si Π denota el subcuerpo primo de K, entonces $\mathrm{Aut}_\Pi(K) = \mathrm{Aut}(K)$.

OBSERVACIÓN 1.58. Sea $F \leq K$ una extensión finita de cuerpos e $\iota : F \to K$ el homomorfismo inclusión. Se sigue del Ejercicio 14 que $\mathrm{Aut}_F(K) = \mathrm{Ex}(\iota, \iota)$, para $\iota : F \to K$ la inclusión.

PROPOSICIÓN 1.59. *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 1.54 a $\mathrm{Ex}(\iota, \iota)$, teniendo en cuenta el Ejercicio 1.58. □

EJEMPLO 1.60. Vamos a describir $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega))$ para $\omega = e^{i2\pi/3}$. Para ello, haremos uso de que $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ es cuerpo de descomposición de $f = X^3 - 2 \in \mathbb{Q}[X]$, con lo que, según el Ejercicio 1.58, hemos de calcular $\mathrm{Ex}(\iota, \iota)$, para $\iota : \mathbb{Q} \to K$ el homomorfismo inclusión. Además, como las tres raíces $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ de f son distintas, tenemos que $\#\mathrm{Aut}(K) = 6$. Vamos a utilizar la Proposición 1.50, concretamente, la construcción de homomorfismos a partir de raíces dada por (1.4). Así que, primero, vamos a describir los homomorfismos de $\eta_0, \eta_1, \eta_2 : \mathbb{Q}(\sqrt[3]{2}) \to K$. Según dicha proposición, éstos están determinados por las condiciones

$$\eta_i(\sqrt[3]{2}) = \omega^i \sqrt[3]{2}, \qquad (i = 0, 1, 2).$$

Ahora, como $K = \mathbb{Q}(\sqrt[3]{2})(\omega)$ e $\mathrm{Irr}(\omega, \mathbb{Q}(\sqrt[3]{2})) = X^2 + X + 1$, la Proposición 1.50 indica que, para cada η_i hay, exactamente, dos homomorfismos $\eta_{ij} : K \to K$, $j = 1, 2$, que extienden a η_i. Así, $\mathrm{Aut}(K)$ consiste en estos seis automorfismos, que están determinados por las condiciones

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

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

TEOREMA 1.61. *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 1.56, $\mathbb{F}_q$ es cuerpo de descomposición de $X^q - X \in \mathbb{F}_p$, deducimos de la Proposición 1.54 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

$$\tau : \mathbb{F}_q \to \mathbb{F}_q, \qquad (x \mapsto x^p). \tag{1.6}$$

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 1.62. El generador τ de $\mathrm{Aut}(\mathbb{F}_q)$ definido según (1.6) se llama *automorfismo de Frobenius* del cuerpo $\mathbb{F}_q$.

1.7. Ejercicios

EJERCICIO 17. 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?

EJERCICIO 18. 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 19. 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 20. Calcular $\mathrm{Irr}(\omega, \mathbb{Q}(\sqrt[3]{2}))$, para $\omega = e^{i2\pi/3}$.

EJERCICIO 21. Sea p un número primo y $\omega \neq 1$ una raíz p-ésima compleja de la unidad. Calcular $\mathrm{Irr}(\omega, \mathbb{Q})$.

EJERCICIO 22. Calcular un cuerpo de descomposición de $X^4+16 \in \mathbb{Q}[X]$.

EJERCICIO 23. 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 24. 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 25. 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 26. Calcular $\mathrm{Irr}(\alpha, \mathbb{Q})$ para los siguientes valores de α:

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

EJERCICIO 27. 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 28. 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 29. 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 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. 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 32. 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 $\mathbb{C}$.

Capítulo 2

Extensiones de Galois

2.1. Extensiones de Galois

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 2.1 (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 $m > n$. 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 entradas 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

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

La igualdad $vA = 0$ es equivalente a

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

Si aplicamos σ_k a la anterior igualdad, obtenemos que

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

Como $G = \{\sigma_k\sigma_1, \ldots, \sigma_k\sigma_n\}$, resulta que $\sigma_k(v)A = 0$. Tenemos, pues, que $(v - \sigma_k(v))A = 0$. Pero $v - \sigma_k(v) \neq 0$ y 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 da la relación de dependencia lineal sobre K^G

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

□

PROPOSICIÓN 2.2. *Si $F \leq K$ es finita, entonces $\#\mathrm{Aut}_F(K) \leq [K : F]$.*

DEMOSTRACIÓN. Llamemos $\iota : F \to K$ a la inclusión. Como $\mathrm{Aut}_F(K) = \mathrm{Ex}(\iota, \iota)$, la desigualdad se sigue de la Proposición 1.53. □

LEMA 2.3. *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 $\mathrm{Aut}_F(K) \supseteq \mathrm{Aut}_E(K)$.*

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

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. Se trata de comprobaciones rutinarias. □

TEOREMA 2.4. *Si* G *es un subgrupo finito de* $\mathrm{Aut}(K)$, *entonces* $G = \mathrm{Aut}_{K^G}(K)$.

DEMOSTRACIÓN. Sabemos, por el Lema 2.3, que $G \subseteq \mathrm{Aut}_{K^G}(K)$. Aplicando las proposiciones 2.1 y 2.2, obtenemos

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

luego $G = \mathrm{Aut}_{K^G}(K)$. □

Seguidamente, vamos a exponer algunos hechos básicos de las extensiones de Galois, que serán definidas en su momento.

DEFINICIÓN 2.5. Un polinomio no constante $f \in F[X]$ se dice *separable* si todas sus raíces en un cuerpo de descomposición son simples. Sabemos que esto es equivalente a que f es coprimo con su polinomio derivado f'.

EJEMPLO 2.6. Si F es de característica 0, entonces todo polinomio irreducible $f \in F[X]$ es separable. Esto es porque $f' \neq 0$ de grado menor que el de f y, por ser f irreducible, deducimos que $\mathrm{mcd}(f, f') = 1$.

EJEMPLO 2.7. El polinomio $X^q - X \in \mathbb{F}_p[X]$ para $q = p^n$ es separable.

EJEMPLO 2.8. Sea $\mathbb{F}_p(t)$ el cuerpo de fracciones del anillo de polinomios $\mathbb{F}_p[t]$. Entonces el polinomio irreducible $f = X^p - t \in \mathbb{F}_p(t)[X]$ no es separable, ya que $f' = 0$.

DEFINICIÓN 2.9. Una extensión algebraica $F \leq K$ es *separable* si el polinomio $\mathrm{Irr}(\alpha, F)$ es separable para todo $\alpha \in K$.

EJEMPLO 2.10. Toda extensión algebraica de cuerpos de característica cero es separable.

DEFINICIÓN 2.11. 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 2.12. La extensión $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ no es normal (aunque es separable).

TEOREMA 2.13. *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* $F = K^{\mathrm{Aut}_F(K)}$*;*
*(*III*)* $F = K^G$ *para un subgrupo finito* G *de* $\mathrm{Aut}(K)$*;*
*(*IV*)* $F \leq K$ *es finita, normal y separable.*

DEMOSTRACIÓN. (I) ⇒ (II). Sea $f \in F[X]$ tal que K es cuerpo de descomposición de f. Sabemos que $F \leq K$ es finita. Tenemos que $F' = K^{\mathrm{Aut}_F(K)} \geq F$. Aplicando el Teorema 2.4 para $G = \mathrm{Aut}_F(K)$, obtenemos que $\mathrm{Aut}_F(K) = \mathrm{Aut}_{F'}(K)$. Como K es también cuerpo de descomposición de $f \in F'[X]$, la Proposición 1.59 nos da que

$$[K : F] = \#\mathrm{Aut}_F(K) = \#\mathrm{Aut}_{F'}(K) = [K : F'],$$

de donde $F' = F$.

(II) ⇒ (III). Tomamos $G = \mathrm{Aut}_F(K)$ que es finito por la Proposición 2.2.

(III) $\Rightarrow$ (IV). Por la Proposición 2.1, $F \leq K$ es finita. Sea $\alpha \in K$, y $f = \mathrm{Irr}(\alpha, F)$. Tomamos $\{\alpha_1, \ldots, \alpha_t\}$ la órbita de α bajo la acción de G sobre K, y construyamos el 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 f divide a g en $F[X]$. Ahora, aplicando cada $\sigma \in G$ a la igualdad $f(\alpha) = 0$, obtenemos que todos los elementos $\alpha_1, \ldots, \alpha_t$ son raíces de f. Esto sólo es posible si $f = g$. Así, f se factoriza en $K[X]$ como producto de factores 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 $f_i = \mathrm{Irr}(\alpha_i, F)$, eliminando repeticiones. Como cada f_i se factoriza como producto de factores lineales distintos en $K[X]$, obtenemos que K es cuerpo de descomposición de f, que resulta ser, además, separable. □

OBSERVACIÓN 2.14. En la demostración del Teorema 2.13, hemos visto que, si $F = K^G$ para G un subgrupo finito de $\mathrm{Aut}(K)$, entonces $\mathrm{Irr}(\alpha, F) = \prod_i (X - \alpha_i)$, donde $\{\alpha_1, \ldots, \alpha_t\}$ es la órbita de α bajo la acción de G. Estos elementos son los llamados *conjugados de* α.

DEFINICIÓN 2.15. Si $F \leq K$ satisface las condiciones equivalentes del Teorema 2.13, entonces diremos que es una extensión de Galois, al grupo $\mathrm{Aut}_F(K)$ se le llama *Grupo de Galois* de la extensión.

COROLARIO 2.16. *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 2.17. *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 2.13, 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. □

COROLARIO 2.18. *Toda extensión de cuerpos finitos es de Galois.*

DEMOSTRACIÓN. Sea $F \leq K$ una extensión de cuerpos finitos. Denotemos por p a su característica. De acuerdo con la Proposición 1.56, 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 2.17 nos da que $F \leq K$ es de Galois. □

EJEMPLO 2.19. 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 $-3 = a^2 - 5b^2 + 2abi\sqrt{5}$. De aquí, $a^2 - 5b^2 + 3 = 0$ y $ab = 0$. Si $a = 0$, 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. Si $b = 0$, obtenemos que $a^2 + 3 = 0$, también imposible para el número racional a.

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

2.2. 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 $\mathrm{Subex}(F \leq K)$, 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 cogerse a izquierda o a la derecha, el índice no cambia. El conjunto de los subgrupos de G, ordenado por inclusión, será denotado como $\mathrm{Subgr}(G)$.

TEOREMA 2.20. *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 2.13.

Dado $H \in \mathrm{Subgr}(G)$, el Teorema 2.4 asegura que $\mathrm{Aut}_{K^H}(K) = H$. Por otra parte, dado $E \in \mathrm{Subex}(F \leq K)$, tenemos que $E = K^{\mathrm{Aut}_E(K)}$, ya que $E \leq K$ es de Galois de acuerdo con el Corolario 2.17. Esto demuestra que las aplicaciones del enunciado son biyectivas e inversas una de la otra. En virtud del Lema 2.3, resultan anti-isomorfismos de conjuntos ordenados.

Dados ahora $H_1 \subseteq H_2$ subgrupos de G, las subextensiones correspondientes son $E_1 = K^{H_1}$, $E_2 = K^{H_2}$. Bien, como $E_i \leq K$ es de Galois, tenemos que $[K : E_i] = \#H_i$, 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 2.21. A la biyección establecida en el Teorema 2.20 la llamaremos *conexión de Galois* para $F \leq K$.

EJEMPLO 2.22. Vamos a calcular los subcuerpos de $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ para $\omega = e^{i2\pi/3}$. Dichos subcuerpos coinciden con las subextensiones de la extensión de Galois $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}, \omega)$. Por el Teorema 2.20, los subcuerpos son los fijos bajo los subgrupos de $G = Aut(\mathbb{Q}(\sqrt[3]{2}, \omega))$. Usamos la descripción de este grupo dada en el Ejemplo 1.60. De allí deducimos que es un grupo no conmutativo con 6 elementos, así que ha de ser isomorfo a S_3. Por tanto, tiene cuatro subgrupos propios: tres de orden 2 y uno de orden tres. Estos resultan ser, tras calcular el orden de los elementos G:

$$A = \{\eta_{01}, \eta_{11}, \eta_{21}\}, C_0 = \{\eta_{01}, \eta_{02}\}, C_1 = \{\eta_{01}, \eta_{12}\}, C_2 = \{\eta_{01}, \eta_{22}\}.$$

Los subcuerpos fijos resultan ser, respectivamente,

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

Razonemos esto último: puesto que $Irr(\omega, \mathbb{Q}) = X^2 + X + 1$, obtenemos que $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. Según el Teorema 2.20, esto muestra que $\mathbb{Q}(\omega)$ ha de ser el subcuerpo fijo de K bajo un subgrupo de índice 2 en G. Como el único que hay es A, deducimos que $K^A = \mathbb{Q}(\omega)$. Por otra parte, vemos, ya que $Irr(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$, que $[\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}] = 3$, luego, de nuevo por el Teorema 2.20, tenemos que $\mathbb{Q}(\sqrt[3]{2})$ es un subcuerpo fijo de K bajo un subgrupo de índice 3 en G. Ahora hay tres opciones, pero, como $\eta_{02}(\sqrt[3]{2}) = \sqrt[3]{2}$, deducimos que $\mathbb{Q}(\sqrt[3]{2}) \leq K^{C_0}$. Lo que, en vista de que son ambos $\mathbb{Q}$–subespacios vectoriales de dimensión 3 de K, fuerza que $K^{C_0} = \mathbb{Q}(\sqrt[3]{2})$. Los razonamientos para obtener que $\mathbb{Q}(\omega\sqrt[3]{2}) = K^{C_1}$ y $\mathbb{Q}(\omega^2\sqrt[3]{2}) = K^{C_2}$ son análogos; se anima al estudiante a hacerlos explícitos.

EJEMPLO 2.23. Vamos a describir los subcuerpos de $\mathbb{F}_q$, para $q = p^n$. Sabemos 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 2.20, 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 $[\mathbb{F}_q^{\langle\tau^d\rangle} : \mathbb{F}_p] = (G : \langle\tau^d\rangle) = d$. Así, 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 33. Supongamos que hemos expresado

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

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

EJERCICIO 34. Generalizar la descripción de los subcuerpos de cualquier $\mathbb{F}_q$ según la pauta descrita en el Ejercicio 33.

LEMA 2.24. *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. Tenemos que $E = K^H$ y hemos de demostrar 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 2.25. *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 2.24, $\sigma(E) = E$ 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 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 2.13.

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 $\sigma(\alpha_i) = \alpha_j \in E$. Por tanto, $\sigma(E) = E$. Del Lema 2.24 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. □

EJERCICIO 35. 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 36. 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?.

2.3. El Teorema Fundamental del Álgebra

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 $\bar{f}$ denotaremos, en esta sección, el polinomio obtenido de aplicar el automorfismo conjugación a sus coeficientes.

TEOREMA 2.26 (Fundamental del Álgebra). *Si* $f \in \mathbb{C}[X]$ *es no constante, entonces* f *tiene todas sus raíces en* $\mathbb{C}$.

DEMOSTRACIÓN. Observemos que $g = f\bar{f} \in \mathbb{R}[X]$ 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 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 2.20, $\mathbb{C} \leq$

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 2.27. *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 37. 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 3

Teoría de Galois de ecuaciones

3.1. Grupo de Galois de un polinomio

Definamos el *discriminante* de un polinomio mónico $f \in F[X]$ con raíces $\alpha_1, \ldots, \alpha_n$ 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. Supondremos implícitamente que todos nuestros polinomios son mónicos, ya que 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.

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 $\{\alpha_1, \ldots, \alpha_n\}$. 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 de f. Dicho homomorfismo es inyectivo, porque cada automorfismo del grupo de Galois está determinado por su valor sobre las raíces de f, así que podemos considerar 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

$$\sigma(\Delta(f)) = \mathrm{sign}(\sigma)\Delta(f), \qquad \sigma(\mathrm{Disc}(f)) = \mathrm{Disc}(f), \tag{3.1}$$

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

PROPOSICIÓN 3.1. *Para un polinomio separable $f \in F$ con grupo de Galois $G = \mathrm{Aut}_F(K)$, se tiene que $\mathrm{Disc}(f) \in F$. Además, el subcuerpo fijo 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 (3.1) que $\mathrm{Disc}(f) \in K^G = F$. También se deduce de (3.1) que $\Delta(f) \in K^{G \cap A_n}$. Así, $F(\Delta(f)) \le K^{G \cap A_n}$. Como $[K^{G \cap A_n} : F] = (G : G \cap A_n) \le 2$, deducimos que sólo se pueden dar dos casos: $F(\Delta(f)) = F$ o bien $F(\Delta(f)) = K^{G \cap A_n}$. En el primer caso, se sigue de (3.1) que $G \subseteq A_n$. □

EJEMPLO 3.2. Dado un polinomio $f = X^n + \sum_{i=0}^{n-1} a_i X^i$, con raíces

$$\alpha_1, \ldots, \alpha_n,$$

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* 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 fácilmente 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 obtiene 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

$$\mathrm{Disc}(f) = -4p^3 - 27q^2. \tag{3.2}$$

PROPOSICIÓN 3.3. *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 1.50 da una extensión $\tau : F(\alpha) \to K$ de la inclusión $F \leq F(\alpha)$ tal que $\tau(\alpha) = \beta$. Ahora, la Proposición 1.54 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 3.4. 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 3.5. Para $f \in F[X]$ separable e irreducible de grado 3 sabemos que su grupo de Galois G es un subgrupo transitivo 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 3.6. 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 los elementos β_i, resulta que $g^\sigma = g$ y, por tanto, los coeficientes de g están en $K^G = F$. Este polinomio el lo que se llama *una resolvente cúbica* de f. Si

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

entonces

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

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 $\mathrm{Disc}(f) = \mathrm{Disc}(g)$. Además, g es separable y $E = F(\beta_1, \beta_2, \beta_3)$ es su cuerpo de descomposición. Por tanto, $F \leq E$ 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

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

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 y su núcleo es

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

Tenemos el diagrama conmutativo de homomorfismos de grupos con filas exactas[1]

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

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 3.7. Tomemos $f = X^4 - 2 \in \mathbb{Q}[X]$. La resolvente cúbica de g es

$$g = X^3 + 8X.$$

Por tanto, $\mathrm{Disc}(f) = \mathrm{Disc}(g) = -4 \times 8^3$, que no es un cuadrado en $\mathbb{Q}$. Esto implica que el grupo de Galois G de f no está contenido en A_4. Por otra parte, las raíces de g son $\beta_1 = 0, \beta_2 = i2\sqrt{2}, \beta_3 = -i2\sqrt{2}$. Así, $E = \mathbb{Q}(i\sqrt{2})$. Tenemos, por tanto, que $G/G \cap V \cong \mathrm{Aut}_F(E)$, por lo que $(G : G \cap V) = 2$. De esta forma, $G \neq S_4$. Sólo quedan dos posibilidades: G es isomorfo a uno de los subgrupos de S_4 isomorfos a D_4 o lo es a uno de los cíclicos de orden 4. Calculando el grado del cuerpo de descomposición, se deshace la ambigüedad.

EJERCICIO 38 (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

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

[1] 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.

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

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

EJERCICIO 39. 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 40. 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 39).

EJERCICIO 41. Demostrar que el grupo de Galois de $f = X^5 - 4X - 1 \in \mathbb{Q}[X]$ es isomorfo a S_5.

3.2. 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 $K^\times$, 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 3.8. 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 3.9. Las raíces n–ésimas de la unidad sobre $\mathbb{Q}$ son los números complejos $\{e^{i2\pi k/n} : k = 0, 1, \dots, n-1\}$, y la n–ésima extensión ciclotómica de $\mathbb{Q}$ es $\mathbb{Q}(e^{i2\pi/n})$. Obviamente, podemos tomar otras raíces n–ésimas primitivas de la unidad como generadores.

Dado $n \geq 2$ natural, denotamos por $U(\mathbb{Z}_n)$ el grupo de unidades de $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, que sabemos es abeliano de orden $\varphi(n)$ (función de Euler). 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) abuso de notación. Las raíces primitivas son, así,

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

PROPOSICIÓN 3.10. *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 primitiva n–ésima de la unidad. Dado $\sigma \in G = \mathrm{Aut}_F(F(\zeta))$, entonces es fácil ver que $\sigma(\zeta)$ es otra raíz primitiva n–ésima de la unidad. Por tanto, $\sigma(\zeta) = \zeta^k$ para algún $k \in U(\mathbb{Z}_n)$. Este k es único, por 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 3.11. Definimos el n–ésimo polinomio ciclotómico como

$$\Phi_n = \prod_{k \in U(\mathbb{Z}_n)} (X - \zeta^k). \tag{3.3}$$

PROPOSICIÓN 3.12. *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 (3.3). □

PROPOSICIÓN 3.13. *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 (3.3), 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 muestra que Φ_n también los tiene.

En el caso de característica 0, razonemos por inducción sobre n que $\Phi_n \in \mathbb{Z}[X]$ y es un polinomio primitivo. 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 $\Phi_n = f \in \mathbb{Z}[X]$ es primitivo. □

EJEMPLO 3.14. 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 $\Phi_6 = X^2 - X + 1$.

EJERCICIO 42. Calcular, en característica 0, Φ_8.

TEOREMA 3.15. *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 una raíz compleja ζ de f. Al ser raíz de Φ_n, se trata de una raíz n–ésima primitiva de la unidad. Si probamos que todas las demás son también raíces de f, deduciremos que $f = \Phi_n$. Así, tomemos un exponente k coprimo con n y mostremos que ζ^k es también raíz de f. Descomponiendo k en factores primos, vemos que basta con demostrar que cada uno de esos factores p da ζ^p como 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 para $\Phi_n = fg$. Así que $g(\zeta^p) = 0$. 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 y h es un divisor de h en $\mathbb{Q}[X]$. Pero f es primitivo, es un divisor de h en $\mathbb{Z}[X]$ (ver [**2**, Lema 4.25]).

Finalmente, 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 $\mathbb{F}_p$. □

COROLARIO 3.16. *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 3.15, 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,

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

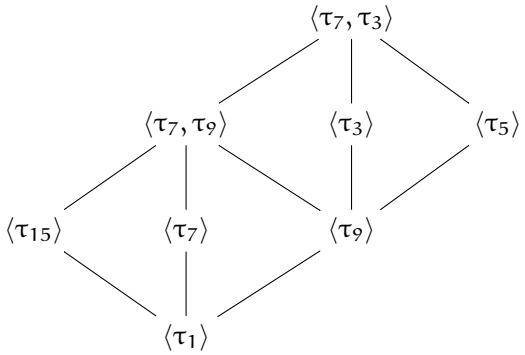
Deducimos de la Proposición 3.10 que $\mathrm{Aut}(\mathbb{Q}(\zeta))$ es isomorfo a $U(\mathbb{Z}_n)$. □

EJEMPLO 3.17. 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 el retículo de subcuerpos de K. Por el Corolario 3.16,

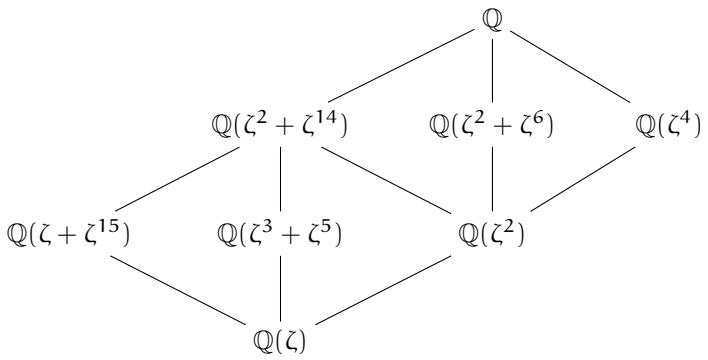
$$\mathrm{Aut}(K) = \{\tau_j : j \in U(\mathbb{Z}_{16})\},$$

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

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



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



3.3. Polígonos regulares constructibles

Complementamos el Teorema 1.33 sobre números complejos constructibles 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 $S = \{z_1, \ldots, z_n\}$ de números complejos, consideramos el subcuerpo $F = \mathbb{Q}(z_1, \ldots, z_n, \overline{z_1}, \ldots, \overline{z_n})$ de $\mathbb{C}$.

TEOREMA 3.18. *Un número complejo z es constructible 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 constructible a partir de S. De acuerdo con el Teorema 1.33, 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 $i = 0, \ldots, s$, 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 la fórmula 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

$$F = K_0 \leq K_1 \leq \cdots \leq K_n = K, \tag{3.4}$$

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 (3.4) es por raíces cuadradas y, de acuerdo con el Teorema 1.33, z es constructible a partir de S. □

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

COROLARIO 3.19. *Un polígono regular de n lados es constructible si, y sólo si, $\varphi(n)$ es una potencia de 2.*

DEMOSTRACIÓN. La idea clave es que el polígono del enunciado será constructible si, y sólo si, lo es la raíz n–ésima primitiva de la unidad $e^{i2\pi/n}$. Según el Teorema 3.18, 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 constructible, 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 3.16. Recíprocamente, el mismo corolario da que puedo tomar $K = \mathbb{Q}(e^{i2\pi/n})$, que es de Galois, y aplicar el Teorema 3.18. □

EJEMPLO 3.20. Si p es un número primo, el Corolario 3.19 muestra que un polígono regular de p lados es constructible 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 constructibles. No obstante, el heptágono regular no lo es y, para encontrar otro polígono regular constructible con un número primo de lados, hay que subir hasta $p = 17$.

OBSERVACIÓN 3.21. 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 43. Demostrar que un polígono regular de n lados es constructible si, y sólo si, n es producto de una potencia de 2 y primos de Fermat distintos entre sí.

3.4. Extensiones cíclicas

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

TEOREMA 3.22. *Supongamos que $X^n - a \in F[X]$, con $0 \neq a$, es separable y sea K su cuerpo de descomposición. Entonces K contiene una raíz n–ésima primitiva de la unidad ζ. Además, el grupo de Galois de la extensión $F(\zeta) \leq K$ es cíclico con orden un divisor de n.*

DEMOSTRACIÓN. 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 rs^{-1} 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 $r, \zeta r, \ldots, \zeta^{n-1}r \in K$.

Consideramos ahora $\sigma \in \mathrm{Aut}_{F(\zeta)}(K)$ y $\sigma(r) = r\zeta^j$ para $j \in \mathbb{Z}_n$. Como ζ es raíz primitiva, resulta que σ determina de manera única j, podemos escribir así $j = j(\sigma)$ 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

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

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 3.22.

COROLARIO 3.23. *$X^n - a$ 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 3.24. Una extensión $F \leq K$ se dirá *cíclica* si es de Galois con grupo de Galois cíclico.

EJEMPLO 3.25. 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 3.22.

EJERCICIO 44. Razonar que toda extensión de cuerpos finitos es cíclica.

LEMA 3.26 (de independencia de Dedekind). *Sean $\sigma_1, \ldots, \sigma_n : F \to E$ homomorfismos de cuerpos distintos. Si $\lambda_1, \ldots, \lambda_n \in E$ 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

$$\lambda_1\sigma_1(x) + \cdots + \lambda_n\sigma_n(x) = 0, \qquad \forall x \in F. \tag{3.5}$$

Tomamos, de entre todas las listas $\lambda_1, \ldots, \lambda_n$ satisfaciendo (3.37), 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,

$$\lambda_1\sigma_1(yx) + \cdots + \lambda_m\sigma_m(yx) = 0. \tag{3.6}$$

Ya que cada σ_i es multiplicativo, restando (3.6) de (3.37) 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 3.27. *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 3.26 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 $id, \sigma, \ldots, \sigma^{n-1}$ son F–automorfismos distintos de $F(\beta)$. La Proposición 2.2 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 $Irr(\beta, F)$ tiene grado n, luego $Irr(\beta, F) = X^n - a$.

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

PROPOSICIÓN 3.28. *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 3.10. Además, sabemos por el Teorema 2.25 que el mismo es isomorfo a $Aut_F(K)/Aut_{F(\zeta)}(K)$. Tenemos así la serie normal

$$\{id_K\} \subseteq Aut_{F(\zeta)}(K) \subseteq Aut_F(K)$$

con factores abelianos, en vista del Teorema 3.15. Así, $Aut_F(K)$ es resoluble. □

EJEMPLO 3.29. 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 $\sqrt{2} \notin \mathbb{Q}(\sqrt[8]{3})$. Esto no es completamente obvio y, a falta de un argumento sencillo, vamos a 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 $N(r) = N(s) = 3$. 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 $[K : \mathbb{Q}] = 32$.

EJERCICIO 45. 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 $\sigma \in \mathrm{Aut}_F(K)$, 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

$$\mathrm{Aut}_F(K) \to \mathrm{GL}_2(\mathbb{Z}_n), \qquad (\sigma \mapsto \begin{pmatrix} 1 & 0 \\ j(\sigma) & k(\sigma) \end{pmatrix}).$$

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

EJERCICIO 46. 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 $\mathrm{Aut}(K)$.
3. Calcular todos los subcuerpos de K que tienen grado 4 sobre $\mathbb{Q}$.
4. Calcular todos los subcuerpos de K.

3.5. 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 3.30. 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 $X^{n_1} - a_j \in E_{j-1}[X]$ para $j = 1, \ldots, t$.

DEFINICIÓN 3.31. 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 3.32. Diremos que una extensión $F \leq K$ es *radical* si K es cuerpo de descomposición de un polinomio de la forma $X^n - a \in F[X]$ y F contiene una raíz n–ésima primitiva de la unidad. 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.

PROPOSICIÓN 3.33. *Supongamos una extensión $E \leq E(\alpha)$, para α una raíz de $X^n - a \in E[X]$, con $a \neq 0$. Si $F \leq E$ es Galois, entonces existe una extensión radical iterada $E \leq K$ tal que $E(\alpha) \leq K$ y $F \leq K$ es Galois.*

DEMOSTRACIÓN. Consideremos el polinomio

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

Puesto que, claramente, $f^\sigma = f$, sus coeficientes están en $E^G = F$. Por otra parte, E es el cuerpo de descomposición de un polinomio $g \in F[X]$. Definamos K como el cuerpo de descomposición del polinomio $fg \in F[X]$.

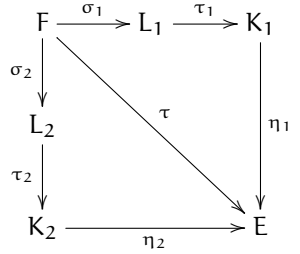
Así que $F \leq K$ es una extensión normal. Como estamos en característica 0, es también separable, por lo que es Galois. Obviamente, $\alpha \in K$, así que $E(\alpha) \leq K$. Como K contiene todas las raíces de $X^n - a$, ha de contener una raíz primitiva n–ésima de la unidad ζ, y el cuerpo de descomposición 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 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. □

Para el siguiente paso, necesitamos la siguiente construcción. Supongamos homomorfismos de cuerpos $\sigma_1 : F \to L_1, \sigma_2 : F \to L_2$ tales que las extensiones $\sigma_i(F) \leq L_i$ sean ambas finitas. Tomando productos de polinomios irreducibles de generadores para ambas extensiones, tenemos $f_1, f_2 \in F[X]$ tales que los cuerpos de descomposición de $f_i^{\sigma_i}$, visto como polinomio en L_i, vienen dados por $\tau_i : L_i \to K_i$. Tenemos también un cuerpo de descomposición $\tau : F \to E$ de $f_1 f_2$. Por la Proposición 1.54, existen homomorfismos $\eta_i : F \to K_i$ tales que $\eta_i \tau_i \sigma_i = \tau$.



Tenemos así las extensiones de cuerpos $\tau(F) \leq \eta_i \tau_i(L_i) \leq E$. Identificando cuerpos por sus imágenes por homomorfismos, tenemos las extensiones $F \leq L_i \leq E$. Además, la extensión $F \leq E$ es finita y, en característica 0 es, además, de Galois.

PROPOSICIÓN 3.34. *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 pasemos 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 3.33 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 3.35. *Si $F \leq K$ es una extensión radical iterada, entonces $\mathrm{Aut}_F(K)$ 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 la conexión de Galois tenemos una cadena de subgrupos

$$\mathrm{Aut}_F(K) = \mathrm{Aut}_{K_0}(K) \supseteq \mathrm{Aut}_{K_1}(K) \supseteq \cdots \supseteq \mathrm{Aut}_{K_{t-1}}(K) \supseteq \mathrm{Aut}_{K_t}(K) = \{\mathrm{id}_K\}.$$

Ahora bien, $\mathrm{Aut}_{K_i}(K)$ es normal en $\mathrm{Aut}_{K_{i-1}}(K)$ para cada $i = 1, \ldots, t$, ya que $K_{i-1} \leq K_i$ es de Galois, por el Teorema 2.25. Por último, el mismo teorema nos dice que

$$\mathrm{Aut}_{K_{i-1}}(K)/\mathrm{Aut}_{K_i}(K) \cong \mathrm{Aut}_{K_{i-1}}(K_i),$$

y éste último grupo es cíclico por el Teorema 3.22. Por tanto, $\mathrm{Aut}_F(K)$ es resoluble. □

EJERCICIO 47. 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 $\mathrm{Aut}_E(K)$ es isomorfo a un subgrupo de $\mathrm{Aut}_F(L)$.

TEOREMA 3.36. *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. Por hipótesis, tenemos una torre de cuerpos $F \leq L \leq E$ tal que E es una extensión por radicales de F. La Proposición 3.34 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 2.25, $\mathrm{Aut}_L(K)$ es un subgrupo normal de $\mathrm{Aut}_F(K)$ y $\mathrm{Aut}_F(L) \cong \mathrm{Aut}_F(K)/\mathrm{Aut}_L(K)$. Según el Lema 3.35, $\mathrm{Aut}_F(K)$ es resoluble, luego así lo es también $\mathrm{Aut}_F(L)$.

Recíprocamente, supongamos que $\mathrm{Aut}_F(L)$ es resoluble y pongamos $n = [L : F]$. Consideramos la extensión $K = L(\zeta)$, para ζ una raíz n–ésima primitiva de la unidad. Como, de acuerdo con el Ejercicio 47, $\mathrm{Aut}_{F(\zeta)}(K)$ es isomorfo a un subgrupo de $\mathrm{Aut}_F(L)$, tenemos que $\mathrm{Aut}_{F(\zeta)}(K)$ es resoluble y que $\#\mathrm{Aut}_{F(\zeta)}(K)$ divide a $n = \#\mathrm{Aut}_F(L)$. Tomemos una serie de composición

$$\mathrm{Aut}_{F(\zeta)}(K) = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_{t-1} \supseteq G_t = \mathrm{id}_K. \tag{3.7}$$

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 (3.7) obtenemos una torre de cuerpos

$$F(\zeta) = K^{G_0} \leq K^{G_1} \leq \cdots \leq K^{G_{t-1}} \leq K^{G_t} = K. \tag{3.8}$$

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 3.27, cada extensión $K^{G_{i-1}} \leq K^{G_i}$ es radical y, a la vista de (3.8), $F(\zeta) \leq K$ 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. □

Un ejemplo de quíntica no resoluble por radicales sobre $\mathbb{Q}$ es la que aparece en el Ejemplo 41. Otros ejemplos se pueden dar a partir del siguiente teorema que no vamos a demostrar.

TEOREMA 3.37 (Dedekind). *Sea $f \in \mathbb{Z}[X]$ un polinomio mónico de grado n y p un primo tal que la reducción $\overline{f}$ módulo p de f es separable. Supongamos que $\overline{f} = f_1 \cdots f_t$, con $f_i \in \mathbb{F}_p[X]$ irreducible de grado n_i para $i = 1, \ldots, t$. Entonces el grupo de Galois de f sobre $\mathbb{Q}$ contiene una permutación cuya descomposición en ciclos disjuntos tiene estructura $n = n_1 + \cdots + n_t$.*

DEMOSTRACIÓN. Quizás más adelante. □

EJEMPLO 3.38. Sea $f = X^5 - X - 1 \in \mathbb{Z}[X]$. Su reducción módulo 3 es

$$\overline{f} = X^5 + 2X + 2 \in \mathbb{F}_3[X].$$

Este polinomio no tiene raíces en $\mathbb{F}_3$, así, no tiene factores de grado 1. En vista de su grado, será irreducible si, y sólo si, no tiene factores de grado 2. Los candidatos a factores son $X^2 + 1, X^2 + X + 2, X^2 + 2X + 2$. Realizando las tres divisiones con resto, comprobamos que éstos son no nulos y, por tanto, $\overline{f} \in \mathbb{F}_3[X]$ es irreducible. Esto tiene varias consecuencias: $f \in \mathbb{Q}[X]$ es irreducible, su grupo de Galois es un subgrupo transitivo de S_5 y contiene un ciclo de longitud 5.

Reduciendo módulo 2, obtenemos $\widetilde{f} \in \mathbb{F}_2[X]$, cuya factorización completa es

$$\widetilde{f} = X^5 + X + 1 = (X^2 + X + 1)(X^3 + X^2 + 1).$$

Por el Teorema 3.37 de nuevo, el grupo de Galois de f contiene una permutación del tipo $\sigma = (ij)(klm)$. Resulta que $\sigma^3 = (ij)$, así que el grupo de Galois buscado es S_5. Conclusión: $f = X^5 - X - 1$ no es resoluble por radicales sobre $\mathbb{Q}$.

3.6. 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 $i = 1, \ldots, n$. Éste da 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 $\mathrm{Aut}_F(E)$. Denotemos por G su imagen.

DEFINICIÓN 3.39. El cuerpo E^G se llama cuerpo de las funciones racionales simétricas en $X_1, \ldots, X_n$ con coeficientes en F.

PROPOSICIÓN 3.40. *Para cada $k = 1, \ldots, n$, escribamos*

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

Entonces

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

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,

$$f = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n. \tag{3.9}$$

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

Observemos que E es cuerpo de descomposición de f sobre $F(s_1, \ldots, s_n)$. Como f es separable, tenemos que $F(s_1, \ldots, s_n) \leq E$ es de Galois, gracias al Teorema 2.13. Además, $G \subseteq \mathrm{Aut}_{F(s_1,\ldots,s_n)}(E)$. Pero, si $\tau : E \to E$ es $F(s_1, \ldots, s_n)$–lineal, entonces, para cada $i = 1, \ldots, n$, 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 $F(s_1, \ldots, s_n) \leq E$, de donde $E^G = F(s_1, \ldots, s_n)$. □

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

$$g = X^n - \lambda_1 X^{n-1} + \cdots + (-1)^n \lambda_n \in F(\lambda_1, \ldots, \lambda_n)[X], \tag{3.10}$$

donde $\lambda_1, \ldots, \lambda_n$ son indeterminadas y $F(\lambda_1, \ldots, \lambda_n)$ es el cuerpo de fracciones del anillo de polinomios $F[\lambda_1, \ldots, \lambda_n]$. Los cambios de signo que aparecen en (3.10) son para facilitar la exposición.

LEMA 3.41. *Sea* $h \in F[\lambda_1, \ldots, \lambda_n]$ *no nulo. Entonces* $h(s_1, \ldots, s_n) \neq 0$.

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

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

de donde

$$s_k(X_1, \ldots, X_{n-1}, 0) = s_k(X_1, \ldots, X_{n-1}), \quad (k = 1, \ldots, n). \tag{3.11}$$

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 $h(s_1, \ldots, s_n) = 0$. 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 $h_0, \ldots, h_{n-1} \in F[\lambda_1, \ldots, \lambda_{n-1}]$.

Tenemos que

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

es nulo. Evaluando ahora en $X_n = 0$, obtenemos, puesto que $s_n(X_1, \ldots, X_n) = X_1 \cdots X_n$, que

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

Según (3.11), hemos obtenido que

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

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

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

Evaluando en $(s_1, \ldots, s_n)$, obtenemos que

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

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

PROPOSICIÓN 3.42. *El polinomio* g *en* (3.10) *es irreducible, separable y su grupo de Galois es isomorfo a* S_n.

DEMOSTRACIÓN. Consideremos, con la notación de la Proposición 3.40, el homomorfismo F–lineal de anillos $\epsilon : F[\lambda_1, \ldots, \lambda_n] \to F(s_1, \ldots, s_n)$ determinado por las condiciones $\epsilon(\lambda_k) = s_k$, para $k = 1, \ldots, n$ que existe por la propiedad universal del anillo de polinomios. Como $F(s_1, \ldots, s_n)$ es un cuerpo, dicho homomorfismo, que es inyectivo por el Lema 3.41, se extiende de manera única, por la propiedad universal del cuerpo de fracciones, a un homomorfismo de cuerpos, que denotamos igual, $\epsilon : F(\lambda_1, \ldots, \lambda_n) \to F(s_1, \ldots, s_n)$. Dicho homomorfismo es, obviamente, sobreyectivo y, por tanto, es un isomorfismo F–lineal de cuerpos. Además, $g^\epsilon = f$, en la notación de (3.9). Como $E = F(X_1, \ldots, X_n)$ es cuerpo de descomposición de f sobre $E^G = F(s_1, \ldots, s_n)$, se sigue que $\epsilon : F(\lambda_1, \ldots, \lambda_n) \to E$ da un cuerpo de descomposición de g sobre $F(\lambda_1, \ldots, \lambda_n)$. Así, el grupo de Galois de g sobre $F(\lambda_1, \ldots, \lambda_n)$ 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 3.3 que g es irreducible. □

TEOREMA 3.43 (Abel-Ruffini). *Si* F *es de característica* 0*, entonces el polinomio* g *dado en* (3.10) *no es resoluble por radicales sobre* $F(\lambda_1, \ldots, \lambda_n)$ *para* $n \geq 5$.

DEMOSTRACIÓN. Por la Proposición 3.42, el grupo de Galois de g sobre $F(\lambda_1, \ldots, \lambda_n)$ es isomorfo a S_n, que no es resoluble para $n \geq 5$. Por el Teorema 3.36, f no es resoluble por radicales sobre $F(\lambda_1, \ldots, \lambda_n)$. □

3.7. Resolución de las ecuaciones de grado hasta 4

Las ecuaciones de grado hasta 4 son resolubles por radicales en característica cero, gracias al Teorema 3.36. En realidad, lo son para casi todas las características. Vamos a dar procedimientos clásicos en cada una de ellas.

3.7.1. 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

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

3.7.2. 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. 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. Tomemos

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

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

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

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 3.44. 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:

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

3.7.3. 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

$$\begin{array}{rcl} \rho_1 & = & -(\beta_1+\beta_2)(\beta_3+\beta_4) \\ \rho_2 & = & -(\beta_1+\beta_3)(\beta_2+\beta_4) \\ \rho_3 & = & -(\beta_1+\beta_4)(\beta_2+\beta_3). \end{array} \tag{3.12}$$

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. De hecho, de las relaciones de Cardano-Vieta para g deducimos, aparte de la igualdad

$$\beta_1 + \beta_2 + \beta_3 + \beta_4 = 0, \tag{3.13}$$

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,

$$h(Y) = Y^3 + 2pY^2 + (p^2-4r)Y - q^2, \tag{3.14}$$

polinomio que es *una resolvente cúbica* de g. Supuesta resuelta, conocemos ρ_1, ρ_2, ρ_3. Deducimos de (3.12) y (3.13) que

$$\begin{array}{rclrcl} \beta_1+\beta_2 & = & \sqrt{\rho_1}, & \beta_3+\beta_4 & = & -\sqrt{\rho_1} \\ \beta_1+\beta_3 & = & \sqrt{\rho_2}, & \beta_2+\beta_4 & = & -\sqrt{\rho_2} \\ \beta_1+\beta_4 & = & \sqrt{\rho_3}, & \beta_2+\beta_3 & = & -\sqrt{\rho_3} \end{array} \tag{3.15}$$

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:

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

donde hemos usado (3.13) y, de nuevo, las identidades de Cardano-Vieta.

Por último, sumando de tres en tres ecuaciones adecuadas de (3.15), obtenemos

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

EJERCICIO 48. Demostrar que el discriminante de una resolvente cúbica, de entre las definidas durante este curso, de una cuártica coincide con el de ésta.

EJERCICIO 49. Determinar, salvo isomorfismos, el grupo de Galois del polinomio $X^4 + X + 1 \in \mathbb{Q}[X]$.

3.8. Ecuaciones sobre cuerpos finitos

Recordemos que un cuerpo finito tiene $q = p^k$ elementos, para p su característica y que dos cuerpos finitos con el mismo cardinal son isomorfos. Sabemos, también, que cualquier extensión de cuerpos finitos es de Galois.

TEOREMA 3.45. *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 2.18, la torre de extensiones de Galois $\mathbb{F}_p \leq \mathbb{F}_{p^k} \leq \mathbb{F}_{p^{kn}}$. Tenemos 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 $\mathbb{F}_{q^n}$ es cuerpo de descomposición sobre $\mathbb{F}_p$ de $X^{q^n} - X$. □

DEFINICIÓN 3.46. El automorfismo ϕ del enunciado del Teorema 3.45 se llama *automorfismo de Frobenius* de la extensión $\mathbb{F}_q \leq \mathbb{F}_{q^n}$.

TEOREMA 3.47. *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, que ha de ser un cuerpo finito con q^n elementos. Como, según el Corolario 2.18,. 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 2.13. 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 3.3. La descripción de todas ellas se sigue de aquí. □

TEOREMA 3.48. *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 3.47, 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 3.47, 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 $X^{q^m} - X$. □

Capítulo 4

Algunos ejercicios

4.1. Ejercicios propuestos

EJERCICIO 50. 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 51. 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 52. 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 53. 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 54. Calcular el cardinal del grupo de Galois sobre $\mathbb{Q}$ del polinomio $f = (X^3 + X + 1)(X^2 + 1)$.

EJERCICIO 55. 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 56. 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 $\mathbb{Q}(\alpha)$.

4.2. Ejercicios resueltos

Solución al Ejercicio 6. 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 $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. 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 $i \in \mathbb{Q}(\alpha)$.

[1] i no puede ser de grado 1 porque no pertenece a $\mathbb{Q}(\sqrt{2})$.

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 46. 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

$$\mathrm{Aut}(K) = \{\tau_{jk} : j \in \mathbb{Z}_4, k \in \mathcal{U}(\mathbb{Z}_4)\},$$

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 45, la aplicación

$$\mathrm{Aut}(K) \to \mathrm{GL}_2(\mathbb{Z}_4), \quad \tau_{jk} \mapsto \begin{pmatrix} 1 & 0 \\ j & k \end{pmatrix} \tag{4.1}$$

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 (4.1) 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 $\mathrm{Aut}(K)$, 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 $\mathrm{Aut}(K)$ usando la conexión de Galois. Sabemos que $\langle \tau_{21} \rangle = \mathrm{Aut}_{\mathbb{Q}(\sqrt{5},i)}(K)$, por lo que los grupos de índice 2, que son

$$\mathrm{Aut}_{\mathbb{Q}(i)}(K),\ \mathrm{Aut}_{\mathbb{Q}(\sqrt{5})}(K),\ \mathrm{Aut}_{\mathbb{Q}(i\sqrt{5})}(K),$$

han de contener a τ_{21}.

Como $\tau_{11}(i) = i$, y este elemento tiene orden 4, deducimos que $\mathrm{Aut}_{\mathbb{Q}(i)}(K) = \langle \tau_{11} \rangle$. 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

$$\mathrm{Aut}_{\mathbb{Q}(\sqrt{5})}(K) = \{\tau_{01}, \tau_{21}, \tau_{03}, \tau_{23}\} = \langle \tau_{03}, \tau_{23} \rangle.$$

Análogamente, se comprueba que

$$\mathrm{Aut}_{\mathbb{Q}(i\sqrt{5})}(K) = \{\tau_{01}, \tau_{21}, \tau_{13}, \tau_{33}\} = \langle \tau_{13}, \tau_{33} \rangle.$$

Solución al Ejercicio 49. Comprobemos primero que $f = X^4 + X + 1 \in \mathbb{Q}[X]$ es irreducible. Al tener coeficientes enteros y ser primitivo, basta con que demostremos que es irreducible en $\mathbb{Z}[X]$. Reduciéndolo módulo 2, obtenemos $X^4 + X + 1 \in \mathbb{F}_2[X]$ que no tiene raíces y cuyo único posible factor irreducible, $X^2 + X + 1$, no lo es, lo que se comprueba realizando la división con resto de f entre éste y viendo que da resto no nulo.

Como f es irreducible, su grupo de Galois, visto como grupo de permutaciones de sus raíces, es un subgrupo transitivo de S_4, en virtud de la Proposición 3.3.

Vamos a calcular el discriminante de f, para lo que usamos su resolvente cúbica dada en (3.14). Ésta resulta $h = Y^3 - 4Y - 1$. Usando el Ejercicio 48 y (3.2), tenemos que

$$\mathrm{Disc}(f) = \mathrm{Disc}(h) = -4(-4)^3 - 27 = 229.$$

Observemos que 229 es un entero primo, ya que no es divisible por $2, 3, 5, 7, 11, 13$, por lo que el Criterio de Eisenstein aplicado a $X^2 - 229 \in \mathbb{Z}[X]$ implica que este polinomio es irreducible en $\mathbb{Z}[X]$ y, así, en $\mathbb{Q}[X]$. La consecuencia que nos interesa es que $\sqrt{229} \notin \mathbb{Q}$. En vista de la Proposición 3.1, tenemos que el grupo de Galois de f no está incluido en A_4.

Pero esta misma información puede usarse para el polinomio de grado tres h, que es irreducible en $\mathbb{Q}[X]$, ya que no tiene raíces racionales (las únicas posibles, ± 1, no lo son). En este caso, deducimos que el grupo de Galois de h es un subgrupo transitivo de S_3 que no es A_3. O sea, es S_3.

Reunamos toda la información teniendo en cuenta la torre de cuerpos

$$\mathbb{Q} \leq E = \mathbb{Q}(\rho_1, \rho_2, \rho_3) \leq K = \mathbb{Q}(\beta_1, \beta_2, \beta_3, \beta_4),$$

que involucra los cuerpos de descomposición de h y de f.

La conexión de Galois da la cadena de grupos

$$\mathrm{Aut}(K) \supseteq \mathrm{Aut}_E(K) \supseteq \{\mathrm{id}\}.$$

Además, según el Teorema 2.25, $\mathrm{Aut}_E(K)$ es normal en $\mathrm{Aut}(K)$ y $\mathrm{Aut}(E) \cong \mathrm{Aut}(K)/\mathrm{Aut}_E(K)$. Como $\mathrm{Aut}(E) \cong S_3$, deducimos que $\mathrm{Aut}(K)$ tiene cardinal

un múltiplo de 6. Como es un subgrupo transitivo de S_4 y no es A_4, la única posibilidad es que sea S_4.

Solución al Ejercicio 50. 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 3.45, 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 3.48 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 51. 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 $\mathrm{Irr}(\beta, \mathbb{F}_2)$ 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 50, 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 3.47, son $\alpha, \alpha^4, \alpha^{16}$. Comparando con la solución del Ejercicio 50, 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 50.

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 54. 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 g 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, $[K : \mathbb{Q}(i)] = 6$. Ahora ya podemos concluir:

$$\#\mathrm{Aut}(K) = [K : \mathbb{Q}] = [K : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 6 \times 2 = 12.$$

Solución al Ejercicio 55. 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 calcularlod, usamos que $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}, i)$ y aplicamos reiteradamente la extensión de homomorfismos dada por la Proposición 1.50. 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 $\mathrm{Aut}_{\mathbb{Q}(i,\sqrt{3})} = \{\eta_{0k0} : k = 0, 1, 2\}$, 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 este cuerpo es el 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 56. 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: $K = \mathbb{Q}(\alpha)$.

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.