Ejercicios

Ejercicio 1. *Hallar el polinomio mínimo de* $\sqrt{2}+\sqrt{5}$ *sobre* $\mathbb{Q}$.

Solución. Llamemos $\alpha = \sqrt{2}+\sqrt{5}$. Entonces

$$\alpha^2 = 7 + 2\sqrt{2}\sqrt{5},$$

es decir,

$$\alpha^2 - 7 = 2\sqrt{10}$$

Elevando al cuadrado,

$$\alpha^4 + 49 - 14\alpha^2 = 40,$$

así que un polinomio en $\mathbb{Q}[X]$ que anula a α es $f(X) = X^4 - 14X^2 + 9$. Veamos que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2},\sqrt{5})$. La contencion $\subset$ es clara; para la otra, probemos que $\sqrt{2},\sqrt{5} \in \mathbb{Q}(\alpha)$. Se tiene que $\alpha^2 = 7+2\sqrt{10} \in \mathbb{Q}(\alpha)$, luego $\sqrt{10} \in \alpha$, así que $\sqrt{10}\alpha = 2\sqrt{5}+5\sqrt{2} \in \mathbb{Q}(\alpha)$, y entonces $2\sqrt{5}+5\sqrt{2}-2\alpha = 3\sqrt{2} \in \mathbb{Q}(\alpha)$, luego $\sqrt{2} \in \mathbb{Q}(\alpha)$ y $\sqrt{5} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$.

Tenemos entonces que $[\mathbb{Q}(\sqrt{2}+\sqrt{5})\colon \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{5})\colon \mathbb{Q}] = 4$ (se prueba fácilmente que $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$ y de ahí la última igualdad sale sola). La conclusión es que $X^4 - 14X^2 + 9 = \mathrm{Irr}(\alpha, X, \mathbb{Q})$, pues es un polinomio mónico de grado mínimo que anula a α. □

Ejercicio 2. *Sea* u *un elemento trascendente sobre un cuerpo* $\mathbb{F}$. *Probar que no existe ningún cuerpo* $\mathbb{K}$ *tal que* $\mathbb{F} \subsetneq \mathbb{K} \subsetneq \mathbb{F}(u)$ *con* $[\mathbb{K}\colon \mathbb{F}]$ *finito.*

Solución. Sea u un elemento trascendente sobre $\mathbb{F}$ y considérese una torre de extensiones

$$\mathbb{F} \subsetneq \mathbb{K} \subsetneq \mathbb{F}(u)$$

Veamos que $[\mathbb{K}\colon \mathbb{F}] = \infty$. Para ello, se va a probar que u es algebraico sobre $\mathbb{K}$. Sea $v \in \mathbb{K}$ con $v \notin \mathbb{F}$. Como $v \in \mathbb{F}(u)$, existen $p(X), q(X) \in \mathbb{F}[X]$ tales que

$$v = \frac{p(u)}{q(u)},$$

luego $q(u)v - p(u) = 0$ y entonces $q(X)v - p(X)$ es un polinomio en $\mathbb{K}[X]$ que anula a u. Como u es algebraico sobre $\mathbb{K}$, entonces $[\mathbb{K}(u)\colon \mathbb{K}] < \infty$ y por tanto $[\mathbb{F}(u)\colon \mathbb{K}] < \infty$. Pero es que $[\mathbb{F}(u)\colon \mathbb{F}] = \infty$ por ser u trascendente sobre $\mathbb{F}$, luego $[\mathbb{K}\colon \mathbb{F}] = \infty$. □

Ejercicio 3. *Sea* $\xi = 1_{\frac{2\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. *Probar que* $i \notin \mathbb{Q}(\sqrt{2},\xi)$.

Solución. Consideremos las torres de extensiones

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2},\xi) \qquad \text{y} \qquad \mathbb{Q} \subset \mathbb{Q}(\xi) \subset \mathbb{Q}(\sqrt{2},\xi)$$

Se tiene que

- $[\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}] = 2$ porque $X^2 - 2 \in \mathbb{Q}[X]$ es mónico e irreducible (no tiene raíces en $\mathbb{Q}$) y anula a $\sqrt{2}$.
- $[\mathbb{Q}(\xi)\colon \mathbb{Q}] = 2$ porque $X^2 + X + 1 \in \mathbb{Q}[X]$ es mónico e irreducible (pues $X^3 - 1 = (X-1)(X^2+X+1)$ y 3 es primo) y anula a ξ.
- $[\mathbb{Q}(\sqrt{2},\xi)\colon \mathbb{Q}(\sqrt{2})]$ no puede ser mayor que 2 porque $X^2 + X + 1 \in \mathbb{Q}(\sqrt{2})[X]$ y anula a ξ. Tampoco puede ser 1 porque entonces sería $\mathbb{Q}(\sqrt{2},\xi) = \mathbb{Q}(\sqrt{2})$, que es imposible porque en $\mathbb{Q}(\sqrt{2},\xi)$ hay números complejos y en $\mathbb{Q}(\sqrt{2})$ no. Por tanto, $[\mathbb{Q}(\sqrt{2},\xi)\colon \mathbb{Q}(\sqrt{2})] = 2$.

En consecuencia,

$$[\mathbb{Q}(\sqrt{2},\xi):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\xi):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q})] = 2\cdot 2 = 4$$

Como $\{1,\sqrt{2}\}$ es base de $\mathbb{Q}(\sqrt{2})$ y $\{1,\xi\}$ es base de $\mathbb{Q}(\xi)$, entonces una base de $\mathbb{Q}(\sqrt{2},\xi)$ como $\mathbb{Q}$-espacio vectorial se obtiene multiplicando los elementos de las bases anteriores, quedando $\{1,\sqrt{2},\xi,\xi\sqrt{2}\}$.

Supongamos, por reducción al absurdo, que $i \in \mathbb{Q}(\sqrt{2},\xi)$. Entonces existen $a,b,c,d \in \mathbb{Q}$ tales que

$$\begin{aligned} i &= a + b\sqrt{2} + c\xi + d\xi\sqrt{2} \\ &= a + b\sqrt{2} + c\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) + d\sqrt{2}\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) \\ &= a + b\sqrt{2} - \frac{c}{2} + i\frac{c\sqrt{3}}{2} - \frac{d\sqrt{2}}{2} + i\frac{d\sqrt{6}}{2} \\ &= a + b\sqrt{2} - \frac{c}{2} - \frac{d\sqrt{2}}{2} + i\left(\frac{c\sqrt{3}+d\sqrt{6}}{2}\right) \end{aligned}$$

Comparando las partes imaginarias, debe cumplirse

$$\frac{c\sqrt{3}+d\sqrt{6}}{2} = 1,$$

luego

$$c\sqrt{3}+d\sqrt{6} = 2$$

Se distinguen varios casos:

- Si $c \neq 0$ y $d \neq 0$, elevando al cuadrado se obtiene

  $$(c\sqrt{3}+d\sqrt{6})^2 = 4 \iff 3c^2+6d^2+2cd\sqrt{18} = 4 \iff \sqrt{18} = \frac{4-3c^2-6d^2}{2cd} \in \mathbb{Q},$$

  que es imposible.

- Si $c = 0$ y $d \neq 0$, entonces

  $$d\sqrt{6} = 2,$$

  y al dividir por d se obtiene $\sqrt{6} \in \mathbb{Q}$, que es imposible.

- Si $c \neq 0$ y $d = 0$, entonces

  $$c\sqrt{3} = 2,$$

  y al dividir por c se obtiene $\sqrt{3} \in \mathbb{Q}$, que es imposible.

- El caso $c = 0$, $d = 0$ tampoco es posible, evidentemente.

En cualquier caso obtenemos una contradicción, luego $i \notin \mathbb{Q}(\sqrt{2},\xi)$. □

Ejercicio 4. *Sea $\mathbb{F} \subset \mathbb{K}$ una extensión de cuerpos, sea $f(X) \in \mathbb{K}[X]$ irreducible y de grado n, sea $\mathbb{L}$ el cuerpo de descomposición de $f(X)$ sobre $\mathbb{K}$ y sean $u_1,\ldots,u_t$ las raíces de $f(X)$ en $\mathbb{L}$. Demostrar que $[\mathbb{F}[u_1,\ldots,u_t]:\mathbb{F}]$ es múltiplo de n.*

Solución. Sin perder generalidad, se va a suponer que $f(X)$ es un polinomio mónico. Así,

$$f(X) = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + X^n$$

Sean $v_1,\ldots,v_n$ las n raíces de $f(X)$ en $\mathbb{L}$ (no necesariamente distintas). Entonces

$$f(X) = (X-v_1)\ldots(X-v_n),$$

y por tanto los coeficientes de $f(X)$ son suma, resta y producto de los v_i, con $i \in \{1,\ldots,n\}$. Esto nos dice

$$\mathbb{F}[a_0,a_1,\ldots,a_{n-1},v_1,\ldots,v_n] = \mathbb{F}[v_1,\ldots,v_n] = \mathbb{F}[u_1,\ldots,u_t]$$

Así, tenemos la torre de extensiones

$$\mathbb{F} \subset \mathbb{F}[a_0, a_1, \ldots, a_{n-1}, u_1] \subset \mathbb{F}[u_1, \ldots, u_t]$$

Como $f(X)$ es un polinomio mónico e irreducible en $\mathbb{F}[a_0, a_1, \ldots, a_{n-1}][X]$ y anula a u_1, entonces

$$[\mathbb{F}[a_0, a_1, \ldots, a_{n-1}, u_1] \colon \mathbb{F}] = n,$$

y en consecuencia,

$$[\mathbb{F}[u_1, \ldots, u_t] \colon \mathbb{F}] = n \cdot [\mathbb{F}[u_1, \ldots, u_t] \colon \mathbb{F}[a_0, a_1, \ldots, a_{n-1}, u_1]],$$

concluyéndose que $[\mathbb{F}[u_1, \ldots, u_t] \colon \mathbb{F}]$ es múltiplo de n. □

Ejercicio 5. *Sea $\mathbb{F} \subset \mathbb{K}$ una extensión de cuerpos normal y finita y sea $f(X) \in \mathbb{F}[X]$ irreducible. Probar que todos los polinomios de la factorización de $f(X)$ como producto de irreducibles en $\mathbb{K}[X]$ tienen el mismo grado.*

Solución. Factoricemos $f(X)$ como producto de irreducibles en $\mathbb{K}[X]$:

$$f(X) = f_1(X) \ldots f_k(X)$$

Sea $i \in \{2, 3, \ldots, k\}$ (si fuese $k = 1$ no hay nada que probar) y veamos que $f_1(X)$ y $f_i(X)$ tienen el mismo grado.

En primer lugar, como la extensión $\mathbb{F} \subset \mathbb{K}$ es normal y finita, entonces existe $g(X) \in \mathbb{F}[X]$ tal que $\mathbb{K}$ es el cuerpo de descomposición de $g(X)$ sobre $\mathbb{F}$. Ahora, si $\mathbb{L}$ es el cuerpo de descomposición de $f(X)g(X)$ sobre $\mathbb{F}$, entonces $\mathbb{K} \subset \mathbb{L}$, pues todas las raíces de $g(X)$ están en $\mathbb{L}$.

Por otra parte, sean $\alpha, \beta \in \mathbb{L}$ raíces de $f_1(X)$ y $f_i(X)$, respectivamente. Como $f(X) = \mathrm{Irr}(\alpha, X, \mathbb{F})$ (no hay problema en suponer que $f(X)$ es mónico) y β es raíz de $f(X)$, por el teorema de extensión, existe un único isomorfismo $\sigma \colon \mathbb{F}[\alpha] \to \mathbb{F}[\beta]$ extensión de $id \colon \mathbb{F} \to \mathbb{F}$ con $\sigma(\alpha) = \beta$. Además, tenemos que $\mathbb{L}$ es el cuerpo de descomposición de $f(X)$ sobre $\mathbb{F}[\alpha]$ y también es el cuerpo de descomposición de $f^\sigma(X) = f(X)$ sobre $\mathbb{F}[\beta]$, así que existe un isomorfismo $\overline{\sigma} \colon \mathbb{L} \to \mathbb{L}$ que extiende a σ.

$$\begin{array}{ccc} \mathbb{F} & \xrightarrow{id} & \mathbb{F} \\ \downarrow & & \downarrow \\ \mathbb{F}[\alpha] & \xrightarrow{\sigma} & \mathbb{F}[\beta] \\ \downarrow & & \downarrow \\ \mathbb{L} & \xrightarrow{\overline{\sigma}} & \mathbb{L} \end{array}$$

Como además $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$ y las extensiones $\mathbb{F} \subset \mathbb{K}$ y $\mathbb{F} \subset \mathbb{L}$ son normales, entonces $\overline{\sigma}(\mathbb{K}) \subset \mathbb{K}$. Así, tenemos que $f_1^{\overline{\sigma}}(X)$ es un polinomio mónico e irreducible en $\mathbb{K}[X]$ que anula a $\overline{\sigma}(\alpha) = \sigma(\alpha) = \beta$. Pero $f_i(X)$ es otro polinomio mónico e irreducible en $\mathbb{K}[X]$ que anula a β, luego $f_i(X) = f_1^{\overline{\sigma}}(X)$, y como $\overline{\sigma}$ preserva los grados (pues es un isomorfismo), se concluye que $f_1(X)$ y $f_i(X)$ tienen el mismo grado. □

Ejercicio 6. *Sea $\mathbb{F} \subset \mathbb{K}$ una extensión algebraica de cuerpos con $\mathbb{K} = \mathbb{F}[S]$ y tal que $[F[s] \colon \mathbb{F}] \leq 2$ para todo $s \in S$. Demostrar que la extensión es normal.*

Solución. Sea $f(X) \in \mathbb{F}[X]$ un polinomio irreducible y sea $\alpha \in \mathbb{K}$ una raíz de $f(X)$. Veamos que todas las raíces de $f(X)$ están en $\mathbb{K}$.

Como $\alpha \in \mathbb{F}[S]$, existe $p(X_1, \ldots, X_k) \in \mathbb{F}[X_1, \ldots, X_k]$ tales que $\alpha = p(s_1, \ldots, s_k)$, con $s_1, \ldots, s_k \in S$. Así, tenemos una extensión de cuerpos $\mathbb{F} \subset \mathbb{F}[s_1, \ldots, s_k]$ y $\alpha \in \mathbb{F}[s_1, \ldots, s_k]$. Veamos que esta extensión es normal.

Dado $i \in \{1, \ldots, k\}$, sea $g_i(X) = \mathrm{Irr}(s_i, X, \mathbb{F})$. Como $[F[s_i] \colon \mathbb{F}] \leq 2$, entonces la extensión $\mathbb{F} \subset \mathbb{F}[s_i]$ es normal y por tanto todas las raíces de $g_i(X)$ están en $\mathbb{F}[s_i]$. Así, si consideramos

$$g(X) = \prod_{i=1}^{n} g_i(X),$$

tenemos que todas las raíces de $g(X)$ están en $\mathbb{F}[s_1,\ldots,s_k]$, luego este es el cuerpo de descomposición de $g(X)$ sobre $\mathbb{F}$ y por tanto la extensión $\mathbb{F}\subset\mathbb{F}[s_1,\ldots,s_k]$ es normal.

Para terminar, como $\alpha\in\mathbb{F}[s_1,\ldots,s_k]$ es raíz de $f(X)$ y la extensión $\mathbb{F}\subset\mathbb{F}[s_1,\ldots,s_k]$ es normal, entonces todas las raíces de $f(X)$ están en $\mathbb{F}[s_1,\ldots,s_k]$ y por tanto están en $\mathbb{K}$, concluyéndose que la extensión $\mathbb{F}\subset\mathbb{K}$ es normal. □

Ejercicio 7. *Sea $f(X)\in\mathbb{F}[X]$ un polinomio irreducible y separable de grado n, sea $\mathbb{K}$ el cuerpo de descomposición de $f(X)$ sobre $\mathbb{F}$ y sea $\alpha\in\mathbb{K}$ una raíz de $f(X)$.*

(a) Dada otra raíz $\beta\in\mathbb{F}[\alpha]$ de $f(X)$, demostrar que existe $g(X)\in\mathbb{F}[X]$ de grado menor que n y con $g(\alpha)=\beta$.

(b) Demostrar que si γ es raíz de $f(X)$, entonces $g(\gamma)$ también lo es.

(c) ¿Es cierto el resultado del apartado anterior si $f(X)$ es separable pero no irreducible?

Solución.

(*a*) Como $f(X)=\mathrm{Irr}(\alpha,X,\mathbb{F})$ y $\deg(f(X))=[\mathbb{F}[\alpha]\colon\mathbb{F}]=n$, entonces $\{1,\alpha,\ldots,\alpha^{n-1}\}$ es una base de $\mathbb{F}[\alpha]$ como $\mathbb{F}$-espacio vectorial, luego $\beta=a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1}$ para ciertos $a_0,a_1,\ldots,a_{n-1}\in\mathbb{F}$. El polinomio $g(X)=a_0+a_1X+\ldots+a_{n-1}X^{n-1}\in\mathbb{F}[X]$ es de grado menor que n y $g(\alpha)=\beta$.

(*b*) Sea $\gamma\in\mathbb{K}$ otra raíz de $f(X)$. Por el teorema de extensión, existe un isomorfismo $\sigma\colon\mathbb{F}[\alpha]\to\mathbb{F}[\gamma]$ que extiende a $id\colon\mathbb{F}\to\mathbb{F}$ y con $\sigma(\alpha)=\gamma$.

$$\begin{array}{ccc}\mathbb{F} & \xrightarrow{\ id\ } & \mathbb{F}\\ \downarrow & & \downarrow\\ \mathbb{F}[\alpha] & \xrightarrow{\ \sigma\ } & \mathbb{F}[\gamma]\end{array}$$

Como $\beta=a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1}$, entonces

$$\sigma(\beta)=a_0+a_1\sigma(\alpha)+\ldots+a_{n-1}\sigma(\alpha)^{n-1}=a_0+a_1\gamma+\ldots+a_{n-1}\gamma^{n-1}=g(\gamma)$$

Por otra parte, se observa que $\mathbb{F}[\beta]=\mathbb{F}[\alpha]$ porque $\mathbb{F}[\beta]\subset\mathbb{F}[\alpha]$ (por ser $\beta\in\mathbb{F}[\alpha]$) y la dimensión de ambos como $\mathbb{F}$-espacios vectoriales es la misma: el grado de $f(X)$. Así, como $f(X)=\mathrm{Irr}(\beta,X,\mathbb{F})$ y tenemos un isomorfismo $\sigma\colon\mathbb{F}[\beta]\to\mathbb{F}[\gamma]$, entonces $\sigma(\beta)=g(\gamma)$ es raíz de $f^\sigma(X)=f(X)$.

(*c*) Si $f(X)$ es separable pero no irreducible, entonces el resultado no es cierto. En efecto, tomemos $f(X)=(X-1)(X-2)\in\mathbb{Q}[X]$. El polinomio $g(X)=X+1$ es de grado menor que el de $f(X)$ y verifica $g(1)=2$. Sin embargo, $g(2)=3$ no es raíz de $f(X)$. □

Ejercicio 8. *Sea $\mathbb{F}\subset\mathbb{K}$ una extensión algebraica de cuerpos con $\mathbb{K}=\mathbb{F}[a_1,\ldots,a_n]$ y tal que $a_i^2\in\mathbb{F}$ para todo $i\in\{1,\ldots,n\}$. Supóngase que la característica de $\mathbb{F}$ es distinta de 2 y que $[\mathbb{K}\colon\mathbb{F}]=2^n$. Demostrar que $a_1+\ldots+a_n$ es un elemento primitivo de la extensión.*

Solución. Lo primero que se va a probar es que $[\mathbb{F}[a_1,\ldots,a_i]\colon\mathbb{F}[a_1,\ldots,a_{i-1}]]=2$ para todo $i\in\{1,\ldots,n\}$ (se entiende que para $i=1$ la igualdad es $[\mathbb{F}[a_1]\colon\mathbb{F}]=2$). Nótese que $X^2-a_i^2\in\mathbb{F}[X]$ es un polinomio que anula a a_i, luego $[\mathbb{F}[a_1,\ldots,a_i]\colon\mathbb{F}[a_1,\ldots,a_{i-1}]]\leq 2$. Por reducción al absurdo, supongamos que existe $i_0\in\{1,\ldots,n\}$ tal que $[\mathbb{F}[a_1,\ldots,a_{i_0}]\colon\mathbb{F}[a_1,\ldots,a_{i_0-1}]]=1$. Por comodidad en la notación, supongamos que $i_0=n$ (no se pierde ninguna generalidad). Entonces

$$[\mathbb{K}\colon\mathbb{F}]=\underbrace{[\mathbb{F}[a_1]\colon\mathbb{F}]}_{\leq 2}\cdot\underbrace{[\mathbb{F}[a_1,a_2]\colon\mathbb{F}[a_1]]}_{\leq 2}\cdot\ldots\cdot\underbrace{[\mathbb{F}[a_1,\ldots,a_{n-1}]\colon\mathbb{F}[a_1,\ldots,a_{n-2}]]}_{\leq 2}\cdot\underbrace{[\mathbb{K}\colon\mathbb{F}[a_1,\ldots,a_{n-1}]]}_{=1}\leq 2^{n-1}$$

Esto es imposible porque $[\mathbb{K}\colon\mathbb{F}]=2^n$. Así, para cada $i\in\{1,\ldots,n\}$ es $[\mathbb{F}[a_1,\ldots,a_i]\colon\mathbb{F}[a_1,\ldots,a_{i-1}]]=2$ y en consecuencia

$$X^2-a_i^2=\mathrm{Irr}(a_i,X,\mathbb{F}[a_1,\ldots,a_{i-1}])$$

Las raíces de este polinomio son a_i y $-a_i$ (y son distintas porque son no nulas y la característica de $\mathbb{F}$ no de 2). En el caso $i=1$, por el teorema de extensión, hay exactamente dos inmersiones de $\mathbb{F}[a_1]$

en $\mathbb{F}[a_1]$ que extienden a $id\colon \mathbb{F}\to\mathbb{F}$, y vienen dadas por $\sigma_{j_1}(a_1)=(-1)^{j_1}a_1$, $j_1\in\{0,1\}$. Para $i=2$, hay exactamente dos inmersiones de $\mathbb{F}[a_1,a_2]$ en $\mathbb{F}[a_1,a_2]$ que extienden a $\sigma_{j_1}\colon \mathbb{F}[a_1]\to\mathbb{F}[a_1]$, y vienen dadas por $\sigma_{j_1,j_2}(a_2)=(-1)^{j_2}a_2$, $j_2\in\{0,1\}$, y se verifica $\sigma_{j_1,j_2}(a_1+a_2)=(-1)^{j_1}a_1+(-1)^{j_2}a_2$. Continuamos este razonamiento hasta llegar a $i=n$.

$$\begin{array}{ccc}
\mathbb{F} & \xrightarrow{\quad id\quad} & \mathbb{F} \\
\downarrow & & \downarrow \\
\mathbb{F}[a_1] & \xrightarrow{\quad\sigma_{j_1}\quad} & \mathbb{F}[a_1] \\
a_1 & \longmapsto & (-1)^{j_1}a_1 \\
\downarrow & & \downarrow \\
\mathbb{F}[a_1,a_2] & \xrightarrow{\quad\sigma_{j_1,j_2}\quad} & \mathbb{F}[a_1,a_2] \\
a_1+a_2 & \longmapsto & (-1)^{j_1}a_1+(-1)^{j_2}a_2 \\
\downarrow & & \downarrow \\
(\ldots) & & (\ldots) \\
\downarrow & & \downarrow \\
\mathbb{F}[a_1,\ldots,a_n] & \xrightarrow{\quad\sigma_{j_1,\ldots,j_n}\quad} & \mathbb{F}[a_1,\ldots,a_n] \\
a_1+\ldots+a_n & \longmapsto & (-1)^{j_1}a_1+\ldots+(-1)^{j_n}a_n
\end{array}$$

Sea $I=\{1,2\}^n$ y, dado $(j_1,\ldots,j_n)\in I$, llamemos $\tau_{j_1,\ldots,j_n}$ a la restricción de $\sigma_{j_1,\ldots,j_n}$ a $\mathbb{F}[a_1+\ldots+a_n]$. Es claro que $\tau_{j_1,\ldots,j_n}$ es una inmersión de $\mathbb{F}[a_1+\ldots+a_n]$ en $\mathbb{K}$, pues es la restricción de $\sigma_{j_1,\ldots,j_n}\in \mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$. Así,

$$\begin{aligned}
\tau_{j_1,\ldots,j_n}\colon \mathbb{F}[a_1+\ldots+a_n] &\longrightarrow \mathbb{K} \\
a_1+\ldots+a_n &\longmapsto (-1)^{j_1}a_1+\ldots+(-1)^{j_n}a_n
\end{aligned}$$

Veamos que todas estas inmersiones son distintas. Por reducción al absurdo, supóngase que existen $(j_1,\ldots,j_n),(k_1,\ldots,k_n)\in I$ tales que

$$\tau_{j_1,\ldots,j_n}(a_1+\ldots+a_n)=\tau_{k_1,\ldots,k_n}(a_1+\ldots+a_n)$$

Entonces

$$(-1)^{j_1}a_1+(-1)^{j_2}a_2+\ldots+(-1)^{j_n}a_n=(-1)^{k_1}a_1+(-1)^{k_2}a_2+\ldots+(-1)^{k_n}a_n,$$

es decir,

$$\left((-1)^{j_1}+(-1)^{k_1+1}\right)a_1+\ldots+\left((-1)^{j_n}+(-1)^{k_n+1}\right)a_n=0$$

El coeficiente de cada a_i es 0, 2 o -2, así que podemos reordenar la suma para que se tenga

$$\left((-1)^{j_1}+(-1)^{k_1+1}\right)a_1+\ldots+\left((-1)^{j_s}+(-1)^{k_s+1}\right)a_s=0$$

para algún $s\in\mathbb{N}$ con $s\leq n$. El coeficiente de cada a_i ahora es 2 o -2. Si el coeficiente de a_i es 2, llamamos $b_i=a_i$, y en otro caso, $b_i=-a_i$. Tenemos entonces

$$2b_1+\ldots+2b_s=0$$

Como la característica de $\mathbb{F}$ no es 2, debe ser

$$b_1+\ldots+b_s=0,$$

Esto implica $a_s\in\mathbb{F}[a_1,\ldots,a_{s-1}]$, que no puede ser porque $[F[a_1,\ldots,a_s]\colon \mathbb{F}[a_1,\ldots,a_{s-1}]]=2$. Así, queda probado que que todas las inmersiones $\tau_{j_1,\ldots,j_n}$ son distintas, luego hay al menos 2^n inmersiones de $\mathbb{F}[a_1+\ldots+a_n]$ en $\mathbb{K}$ que extienden a $id\colon\mathbb{F}\to\mathbb{F}$. Pero un teorema visto en clase nos permite afirmar que el número de estas inmersiones es menor o igual que $[\mathbb{F}[a_1+\ldots+a_n]\colon\mathbb{F}]$, y por tanto es menor o igual que $[\mathbb{K}\colon\mathbb{F}]=2^n$. La única posibilidad es que sea $[\mathbb{F}[a_1+\ldots+a_n]\colon\mathbb{F}]=2^n$, concluyéndose que $\mathbb{K}=\mathbb{F}[a_1+\ldots+a_n]$. □

Ejercicio 9. *Hallar todos los ángulos $\alpha \in \mathbb{Q}$ entre $0°$ y $360°$ tales que $\cos(\alpha) \in \mathbb{Q}$.*

Solución. Sea $\alpha \in \mathbb{Q}$ un ángulo entre $0°$ y $360°$ con $\cos(\alpha) \in \mathbb{Q}$. En primer lugar, se va a probar que $\xi = \cos(\alpha) + i\,\mathrm{sen}(\alpha)$ es una raíz primitiva n-ésima de la unidad para algún $n \in \mathbb{N}$.

En efecto, como $\alpha \in \mathbb{Q}$ está medido en grados y $0° \leq \alpha \leq 360°$, podemos escribir $\alpha = \frac{360°}{n}$ para cierto $n \in \mathbb{N}$, de forma que $\xi = 1_{\frac{2\pi}{n}}$, que es una raíz primitiva n-ésima de la unidad.

Consideremos la torre de extensiones $\mathbb{Q} \subset \mathbb{Q}[\cos(\alpha)] \subset \mathbb{Q}[\xi]$. Se tiene que

(a) $[\mathbb{Q}[\cos(\alpha)]\colon \mathbb{Q}] = 1$ porque $\cos(\alpha) \in \mathbb{Q}$.

(b) $[\mathbb{Q}[\xi]\colon \mathbb{Q}[\cos(\alpha)]] \leq 2$ porque $\mathbb{Q}[\xi] = \mathbb{Q}[\cos(\alpha), \mathrm{sen}(\alpha)]$ y $X^2 + \cos^2\alpha - 1 \in \mathbb{Q}[\cos(\alpha)][X]$ anula a $\mathrm{sen}(\alpha)$.

Por tanto, $[\mathbb{Q}[\xi]\colon \mathbb{Q}] \leq 2$. Pero ξ es una raíz primitiva n-ésima de la unidad, así que $[\mathbb{Q}[\xi]\colon \mathbb{Q}] = \phi(n)$, y por tanto $\phi(n) = 2$ o $\phi(n) = 1$. Hallemos todos los $n \in \mathbb{N}$ tales que $\phi(n) = 2$ o $\phi(n) = 1$.

Si $n \neq 1$, factorizamos n: supongamos que $n = p_1^{n_1} \dots p_k^{n_k}$. Entonces

$$\phi(n) = 2 \iff p_1^{n_1} \dots p_k^{n_k} \left(\frac{p_1 - 1}{p_1}\right) \dots \left(\frac{p_k - 1}{p_k}\right) = 2 \iff p_1^{n_1 - 1} \dots p_k^{n_k - 1} (p_1 - 1) \dots (p_k - 1) = 2$$

De esto se deduce que uno de los miembros del producto anterior debe ser 2 y el resto debe ser 1, y esto nos dice que hay, como mucho, dos primos distintos. Ahora se distinguen dos casos:

(a) El 2 está en $p_1^{n_1 - 1} p_k^{n_k - 1}$. Entonces todos los $p_i - 1$ son iguales (valen 1), luego solo hay un primo distinto y debe ser 2. Además, como $2^{n_1 - 1} = 2$, ha de ser $n_1 = 2$. La conclusión de este caso es que $n = 4$.

(b) El 2 está en $(p_1 - 1) \dots (p_k - 1)$. Ahora podrían haber uno o dos primos distintos. Supongamos primero que son dos. Entonces $p_1 = 3$, $p_2 = 2$ y

$$p_1^{n_1 - 1} p_2^{n_2 - 1} \cdot 2 \cdot 1 = 2,$$

luego $p_1^{n_1 - 1} = p_2^{n_2 - 1} = 1$, o sea, $n_1 = 1$ y $n_2 = 1$. La conclusión de este caso es que $n = 6$. Si solo hubiese un primo distinto, tendría que ser $p_1 = 3$, y además

$$p_1^{n_1 - 1} \cdot 2 = 2,$$

de donde $n_1 - 1 = 1$. La conclusión de este caso es que $n = 3$.

Por otra parte,

$$\phi(n) = 1 \iff p_1^{n_1 - 1} \dots p_k^{n_k - 1} (p_1 - 1) \dots (p_k - 1) = 1,$$

luego todos los miembros del producto anterior valen 1. Esto nos dice que solo hay un primo distinto (que debe ser 2 para que se tenga $p_1 - 1 = 1$) y además $n_1 - 1 = 0$, es decir, $n_1 = 1$. La conclusión de este caso es que $n = 2$.

Lo que se ha probado es que

$$\phi(n) \in \{1, 2\} \iff n \in \{1, 2, 3, 4, 6\}$$

Además, para todos estos valores de n se tiene que $\cos(\frac{360°}{n}) \in \mathbb{Q}$. Los ángulos pedidos serían entonces $60°$, $90°$, $120°$, $180°$ y $360°$. □

Ejercicio 10. *Sea $\mathbb{F}$ un cuerpo de característica p, sea $\mathbb{F} \subset \mathbb{K}$ una extensión de cuerpos y sea $a \in \mathbb{K}$ un elemento algebraico sobre $\mathbb{F}$. Demostrar que a es separable sobre $\mathbb{F}$ si y solo si $\mathbb{F}[a] = \mathbb{F}[a^p]$.*

Solución. Supongamos que a es separable sobre $\mathbb{F}$. Sea $n = [\mathbb{F}[a]\colon \mathbb{F}]$ y veamos que $[\mathbb{F}[a^p]\colon \mathbb{F}] = n$. Para ello, se probará que hay n inmersiones de $\mathbb{F}[a^p]$ en $\overline{\mathbb{K}}$ que extienden a $id\colon \mathbb{F} \to \mathbb{F}$, donde $\overline{\mathbb{K}}$ es la clausura normal de la extensión $\mathbb{F} \subset \mathbb{K}$. Como a es separable sobre $\mathbb{F}$, el número de extensiones de $\mathbb{F}[a]$ en $\overline{\mathbb{K}}$ que extienden a $id\colon \mathbb{F} \to \mathbb{F}$ es n.

$$\begin{array}{ccc} \mathbb{F} & \xrightarrow{id} & \mathbb{F} \\ \downarrow & & \downarrow \\ \mathbb{F}[a] & \xrightarrow{\sigma_i} & \overline{\mathbb{K}} \end{array}$$

Para cada $i \in \{1,\dots,n\}$ la aplicación

$$\begin{aligned} \tau_i : \mathbb{F}[a^p] &\longrightarrow \overline{\mathbb{K}} \\ a^p &\longmapsto \sigma_i(a^p) \end{aligned}$$

es una $\mathbb{F}$-inmersión (por ser la restricción de una $\mathbb{F}$-inmersión) de $\mathbb{F}[a^p]$ en $\overline{\mathbb{K}}$. Veamos que todas las τ_i son distintas. Por reducción al absurdo, supongamos que existen $i,j \in \{1,\dots,n\}$ con $\sigma_i(a^p) = \sigma_j(a^p)$, es decir, $\sigma_i(a)^p = \sigma_j(a)^p$. Entonces

$$\sigma_i(a)^p - \sigma_j(a)^p = 0,$$

o lo que es lo mismo, por ser $\mathbb{F}$ de característica p,

$$(\sigma_i(a) - \sigma_j(a))^p = 0,$$

luego $\sigma_i(a) = \sigma_j(a)$ y esto nos dice que $i = j$, pues las inmersiones σ_i quedan totalmente determinadas por la imagen de a. En consecuencia, como las inmersiones τ_i quedan totalmente determinadas por la imagen de a^p, podemos afirmar que son todas distintas, luego el número de inmersiones de $\mathbb{F}[a^p]$ en $\overline{\mathbb{K}}$ que extienden a $id\colon \mathbb{F} \to \mathbb{F}$ es al menos n. Por otro lado, este número es menor o igual que $[\mathbb{F}[a^p]\colon \mathbb{F}]$, que, a su vez, es menor o igual que $[\mathbb{F}[a]\colon \mathbb{F}] = n$. La única posibilidad es que sea $[\mathbb{F}[a^p]\colon \mathbb{F}] = n$, así que $\mathbb{F}[a] = \mathbb{F}[a^p]$.

Recíprocamente, supongamos que a no es separable sobre $\mathbb{F}$ y veamos que $\mathbb{F}[a^p] \subsetneq \mathbb{F}[a]$. Sea

$$f(X) = \mathrm{Irr}(a, X, \mathbb{F}) = a_0 + a_1 X + \ldots + a_{n-1}X^{n-1} + X^n$$

Como $f(X)$ es irreducible y no separable, entonces $f'(X) = 0$, es decir,

$$a_1 + 2a_2 X + \ldots + (n-1)a_{n-1}X^{n-2} + nX^n = 0$$

Esto nos dice que si $i \in \{1,\dots,n\}$ no es múltiplo de p, entonces $a_i = 0$. En consecuencia,

$$f(X) = a_0 + a_p X^p + \ldots + a_{(s-1)p}X^{(s-1)p} + X^{sp},$$

con $sp = n$. Sea

$$g(X) = a_0 + a_p X + \ldots + a_{(s-1)p}X^{s-1} + X^s$$

Entonces $g(X) \in \mathbb{F}[X]$ es un polinomio mónico e irreducible (por ser $f(X)$ irreducible) que anula a a^p, luego $g(X) = \mathrm{Irr}(a^p, X, \mathbb{F})$. En consecuencia,

$$[\mathbb{F}[a^p]\colon \mathbb{F}] = \deg(g(X)) = s < sp = \deg(f(X)) = [\mathbb{F}[a]\colon \mathbb{F}],$$

concluyéndose que $\mathbb{F}[a^p] \subsetneq \mathbb{F}[a]$. □

Ejercicio 11. *Sea $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$ una torre de extensiones con $[\mathbb{K}\colon \mathbb{F}] = n$ y sea $\sigma\colon \mathbb{F} \to \mathbb{L}$ una inmersión. Demostrar que si la extensión $\mathbb{F} \subset \mathbb{K}$ no es separable, entonces el número de inmersiones $\overline{\sigma}\colon \mathbb{K} \to \mathbb{L}$ que extienden a σ es menor que n.*

Solución. Se sabe que:

(*a*) La extensión $\mathbb{F} \subset \mathbb{K}$ es separable si y solo si existe una extensión de cuerpos $\mathbb{L} \subset \mathbb{L}'$ tal que el número de inmersiones de $\mathbb{K}$ en $\mathbb{L}'$ que extienden a σ es $[\mathbb{K}\colon \mathbb{F}]$.

(*b*) Dada una extensión $\mathbb{L} \subset \mathbb{L}'$, el número de inmersiones de $\mathbb{K}$ en $\mathbb{L}'$ que extienden a σ es menor o igual que $[\mathbb{K}\colon \mathbb{F}]$.

Como la extensión $\mathbb{F} \subset \mathbb{K}$ no es separable, por (*a*), para toda extensión de cuerpos $\mathbb{L} \subset \mathbb{L}'$ se tiene que el número de inmersiones de $\mathbb{K}$ en $\mathbb{L}'$ que extienden a σ es distinto de $[\mathbb{K}\colon \mathbb{F}]$. Es más, por (*b*), el número de estas inmersiones debe ser menor que $[\mathbb{K}\colon \mathbb{F}]$. En particular, tomando $\mathbb{L}' = \mathbb{L}$, el número de inmersiones de $\mathbb{K}$ en $\mathbb{L}$ que extienden a σ es menor que $[\mathbb{K}\colon \mathbb{F}] = n$. □

Ejercicio 12. *Sea* $\sigma\colon \mathbb{Q}(i\sqrt{3}) \to \mathbb{Q}(i\sqrt{3})$ *el automorfismo dado por* $\sigma(i\sqrt{3}) = -i\sqrt{3}$. *Sea* α *una raíz de* $X^4 - 2X^2 + 4 \in \mathbb{Q}[X]$. *Determinar el número de inmersiones* $\overline{\sigma}\colon \mathbb{Q}(i\sqrt{3},\alpha) \to \mathbb{C}$ *que extienden a* σ.

Solución. Como la extensión $\mathbb{Q} \subset \mathbb{Q}(i\sqrt{3},\alpha)$ es separable (ya que $\mathbb{Q}$ es perfecto) y $\mathbb{Q}(i\sqrt{3})$ es un cuerpo intermedio de la extensión, entonces $\mathbb{Q}(i\sqrt{3}) \subset \mathbb{Q}(i\sqrt{3},\alpha)$ también es separable y, en consecuencia, el número de inmersiones de $\mathbb{Q}(i\sqrt{3},\alpha)$ en $\mathbb{C}$ coincide con $[\mathbb{Q}(i\sqrt{3},\alpha)\colon \mathbb{Q}(i\sqrt{3})]$. Por otra parte, como se tiene $(\alpha^2)^2 - 2\alpha^2 + 4 = 0$, entonces

$$\alpha^2 \in \left\{ \frac{2+\sqrt{4-16}}{2}, \frac{2-\sqrt{4-16}}{2} \right\} = \left\{ 1+i\sqrt{3}, 1-i\sqrt{3} \right\}$$

De aquí se deduce que alguno de los polinomios $X^2 - 1 - i\sqrt{3}$ o $X^2 - 1 + i\sqrt{3}$, ambos en $\mathbb{Q}(i\sqrt{3})[X]$, anula a α, así que

$$[\mathbb{Q}(i\sqrt{3},\alpha)\colon \mathbb{Q}(i\sqrt{3})] \leq 2$$

De hecho, el grado de la extensión es 2, pues si llamamos $f(X) = \mathrm{Irr}(\alpha, X, \mathbb{Q}(i\sqrt{3}))$, tenemos que α es una raíz de $f(X)$, luego $\overline{\alpha}$ también lo es, y como $\alpha^2 \in \mathbb{C}$, entonces $\alpha \in \mathbb{C}$, así que $\overline{\alpha} \neq \alpha$ y, al tener dos raíces distintas, el grado de $f(X)$ no puede ser 1. En consecuencia, $[\mathbb{Q}(i\sqrt{3},\alpha)\colon \mathbb{Q}(i\sqrt{3})] = 2$ y el número de inmersiones de $\mathbb{Q}(i\sqrt{3},\alpha)$ en $\mathbb{C}$ que extienden a σ es 2. □

Ejercicio 13. *Sea* $\mathbb{F} \subset \mathbb{K}$ *una extensión de Galois finita. Sea* $G = \mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$ *y sea* $u \in \mathbb{K}$. *Demostrar que existe* $m \in \mathbb{N}$ *tal que*

$$\prod_{\sigma \in G} (X - \sigma(u)) = \mathrm{Irr}(u, X, \mathbb{F})^m$$

Solución. Sea

$$f(X) = \prod_{\sigma \in G} (X - \sigma(u))$$

Si $\tau \in G$, entonces

$$\tau(f(X)) = \prod_{\sigma \in G} (X - \tau \circ \sigma(u)) = f(X),$$

donde se ha usado que la aplicación

$$\begin{aligned} \Psi\colon G &\to G \\ \sigma &\mapsto \tau \circ \sigma \end{aligned}$$

es biyectiva. Por tanto, $f(X) \in \mathbb{K}^G[X]$, y como la extensión es finita y de Galois, entonces $\mathbb{K}^G = \mathbb{F}$, luego $f(X) \in \mathbb{F}[X]$. Como $f(X)$ es un polinomio en $\mathbb{F}[X]$ que anula a u, se tiene $f(X) \mid \mathrm{Irr}(u, X, \mathbb{F})$. Factoricemos $f(X)$ como producto de irreducibles:

$$f(X) = f_1(X) \dots f_m(X)$$

Dado $i \in \{1, \dots, m\}$, cualquier raíz de $f_i(X)$ es de la forma $u_i = \sigma_i(u)$ con $\sigma_i \in G$, y como u es raíz de $\mathrm{Irr}(u, X, \mathbb{F})$, entonces $\sigma_i(u) = u_i$ también lo es. Tenemos entonces que todas las raíces de $f_i(X)$ son raíces de $\mathrm{Irr}(u, X, \mathbb{F})$, así que $f_i(X) \mid \mathrm{Irr}(u, X, \mathbb{F})$. Pero ambos son mónicos e irreducibles, luego $f_i(X) = \mathrm{Irr}(u, X, \mathbb{F})$ y concluimos que

$$f(X) = \prod_{i=1}^{m} \mathrm{Irr}(u, X, \mathbb{F}) = \mathrm{Irr}(u, X, \mathbb{F})^m$$ □

Ejercicio 14. *Sea* $\mathbb{F}$ *un cuerpo, sea* $f(X) \in \mathbb{F}[X]$ *un polinomio irreducible y separable y sea* $\mathbb{K}$ *el cuerpo de descomposición de* $f(X)$ *sobre* $\mathbb{F}$. *Si* $\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$ *es abeliano, demostrar que* $\mathbb{K} = \mathbb{F}[a]$ *para cualquier raíz* $a \in \mathbb{K}$ *de* $f(X)$.

Solución. Sean $u_1, \dots, u_t$ las raíces de $f(X)$. Como la extensión $\mathbb{F} \subset \mathbb{K}$ es de Galois (ya que $\mathbb{K}$ es el cuerpo de descomposición de un polinomio separable sobre $\mathbb{F}$), entonces $n = \#\mathrm{Gal}_{\mathbb{F}}(\mathbb{K}) = [\mathbb{K}\colon \mathbb{F}]$. Veamos que $\mathbb{K} = \mathbb{F}[u_1]$. Para ello, se va a demostrar que el número de inmersiones de $\mathbb{F}[a]$ en $\mathbb{K}$ es al menos n.

Si $\sigma \in \mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$, entonces $\sigma\big|_{\mathbb{F}[u_1]}$ es una inmersión de $\mathbb{F}[u_1]$ en $\mathbb{K}$ que extiende a $id\colon \mathbb{F} \to \mathbb{F}$. Veamos que cada elemento de $\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$ restringido a $\mathbb{F}[u_1]$ proporciona una inmersión diferente.

Sean $\sigma, \tau \in \mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$ con $\sigma(u_1) = \tau(u_1)$ y veamos que $\sigma = \tau$. Para ello, basta probar que $\sigma(u_i) = \tau(u_i)$ para todo $i \in \{2, \ldots, n\}$, pues $\mathbb{K} = \mathbb{F}[u_1, \ldots, u_n]$ y por tanto cada elemento de $\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$ queda totalmente determinado por la imagen de $u_1, \ldots, u_n$. Sea $i \in \{2, \ldots, n\}$. Por el teorema de extensión, existe una única $\mathbb{F}$-inmersión $\overline{\rho}\colon \mathbb{F}[u_1] \to \mathbb{K}$ con $\overline{\rho}(u_1) = u_i$, que puede extenderse a un isomorfismo $\rho \in \mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$ por ser $\mathbb{K}$ el cuerpo de descomposición de un polinomio sobre $\mathbb{F}$. Como $\rho(u_1) = u_i$, aplicando σ y usando que $\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$ es abeliano,

$$\sigma(u_i) = \sigma \circ \rho(u_1) = \rho \circ \sigma(u_1) = \rho \circ \tau(u_1) = \tau \circ \rho(u_1) = \tau(u_i)$$

Esto implica $\sigma = \tau$ y por tanto hay al menos n $\mathbb{F}$-inmersiones de $\mathbb{F}[u_1]$ en $\mathbb{K}$. Pero el número de estas inmersiones es menor o igual que $[\mathbb{F}[u_1]\colon \mathbb{F}]$, que, a su vez, es menor o igual que $[\mathbb{K}\colon \mathbb{F}] = n$. La conclusión es que $[\mathbb{F}[u_1]\colon \mathbb{F}] = n$ y por tanto $\mathbb{K} = \mathbb{F}[u_1]$. □

Ejercicio 15. *Sea $\mathbb{F}$ un cuerpo finito y sea $\mathbb{F} \subset \mathbb{K}$ una extensión de cuerpos de grado n. Demostrar que para cada divisor d de n existe un único cuerpo intermedio de grado d entre $\mathbb{F}$ y $\mathbb{K}$.*

Solución. Si $\#\mathbb{F} = p^k$ y $[\mathbb{K}\colon \mathbb{F}] = n$, entonces

(*a*) la extensión es cíclica por un teorema visto en clase;

(*b*) $\#\mathbb{K} = p^{nk}$, así que $\mathbb{K}$ es el cuerpo de descomposición del polinomio $f(X) = X^{p^{nk}} - X \in \mathbb{F}[X]$, que es separable porque $f'(X) = -1$ y $\mathrm{mcd}(f(X), f'(X)) = -1$.

Por tanto, la extensión $\mathbb{F} \subset \mathbb{K}$ es finita, de Galois y cíclica. Por ser cíclica, $\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$ tiene un único subgrupo de orden d para cada divisor d de n, o lo que es lo mismo, en virtud del teorema fundamental, la extensión $\mathbb{F} \subset \mathbb{K}$ tiene un único cuerpo intermedio de grado d para cada divisor d de n. □

Ejercicio 16. *Sea $\mathbb{F}$ un cuerpo finito.*

(a) Sea $f(X) \in \mathbb{F}[X]$ un polinomio irreducible de grado n. Probar que $f(X)$ se descompone totalmente en cualquier extensión de $\mathbb{F}$ de grado n.

(b) Sea $f(X) \in \mathbb{F}[X]$ un polinomio cuya factorización en producto de irreducibles es

$$f_4(X) g_4(X) g_3(X) h_5(X),$$

donde $\deg(f_4(X)) = \deg(g_4(X)) = 4$, $\deg(g_3(X)) = 3$ y $\deg(h_5(X)) = 5$. Calcular el orden de $\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$, donde $\mathbb{K}$ es el cuerpo de descomposición de $f(X)$ sobre $\mathbb{F}$.

Solución.

(*a*) Sea u una raíz de $f(X)$ en su cuerpo de descomposición sobre $\mathbb{F}$. La extensión $\mathbb{F} \subset \mathbb{F}[u]$ es normal (toda extensión finita de un cuerpo finito es normal) y por tanto $f(X)$ se descompone totalmente en $\mathbb{F}[u]$, luego $\mathbb{F}[u]$ es el cuerpo de descomposición de $f(X)$ sobre $\mathbb{F}$. Pero $[\mathbb{F}[u]\colon \mathbb{F}] = n$ y $\mathbb{F}[u]$ es, salvo isomorfismo, el único cuerpo con $\#\mathbb{F}[u] = p^{nk}$ elementos (donde $\#F = p^k$). En consecuencia, si $\mathbb{F} \subset \mathbb{K}$ es cualquier extensión de grado n, entonces $\mathbb{K}$ y $\mathbb{F}[u]$ son isomorfos, y como $f(X)$ se descompone totalmente en $\mathbb{F}[u]$, también lo hace en $\mathbb{K}$.

(*b*) Nótese que toda extensión finita de un cuerpo finito es de Galois, luego $\#\mathrm{Gal}_{\mathbb{F}}(\mathbb{K}) = [\mathbb{K}\colon \mathbb{F}]$. Sean $\alpha, \beta, \gamma \in \mathbb{K}$ raíces de $f_4(X)$, $g_3(X)$ y $h_5(X)$, respectivamente. Por el apartado anterior,

- $f_4(X)$ y $g_4(X)$ se descomponen totalmente en $\mathbb{F}[\alpha]$;
- $g_3(X)$ se descompone totalmente en $\mathbb{F}[\beta]$;
- $h_5(X)$ se descompone totalmente en $\mathbb{F}[\gamma]$.

Por tanto, el cuerpo de descomposición de $f(X)$ sobre $\mathbb{F}$ es $\mathbb{F}[\alpha, \beta, \gamma]$. Como $[\mathbb{F}[\alpha]\colon \mathbb{F}] = 4$, $[\mathbb{F}[\beta]\colon \mathbb{F}] = 3$, $[\mathbb{F}[\alpha]\colon \mathbb{F}] = 5$ y 3, 4 y 5 son primos relativos, entonces

$$[\mathbb{F}[\alpha, \beta, \gamma]\colon \mathbb{F}] = 3 \cdot 4 \cdot 5 = 60,$$

concluyéndose que $\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$ tiene orden 60. □

Ejercicio 17. *Construir un cuerpo finito $\mathbb{F}$ que tenga 125 elementos. ¿Existe alguna extensión $\mathbb{K}$ de $\mathbb{F}$ de grado 4?*

Solución. Dado un $n \in \mathbb{N}$ con $\mathrm{mcd}(n,5) = 1$, se sabe que $\mathbb{F}_{5^3}$ es el cuerpo de descomposición de $X^n - 1$ sobre $\mathbb{Z}_5[X]$, con 3 el menor natural tal que $5^3 \equiv 1 \bmod n$. El problema se reduce a encontrar un n adecuado. Puede tomarse, por ejemplo, $n = 31$, así que el cuerpo pedido es $\mathbb{Z}_5(\xi)$, donde ξ es una raíz primitiva 31-ésima de la unidad.

Cualquier extensión $\mathbb{F} \subset \mathbb{K}$ con $[\mathbb{K} : \mathbb{F}] = 4$ es tal que $\#\mathbb{K} = 125^4 = 5^{12}$. También se sabe que $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ si y solo si n divide a m. Como 3 divide a 12, sí existe alguna extensión $\mathbb{K}$ de $\mathbb{F}$ de grado 4: basta tomar cualquier cuerpo con 125^4 elementos. □

Ejercicio 18. *Encontrar una extensión de Galois de $\mathbb{Q}$ de grado 15 y con grupo de Galois cíclico.*

Solución. Lo primero que hay que observar es que el grupo de Galois de la extensión buscada tendrá grado 15 y el único grupo de grado 15 es $\mathbb{Z}_{15}$ (pues $15 = 3 \cdot 5$, 3 y 5 son primos y 3 no divide a $5 - 1 = 4$). El problema se reduce entonces a encontrar una extensión de Galois de grado 15. Para ello, primero buscaremos extensiones de Galois de grado 3 y 5.

Para hallar la extensión de grado 3, buscamos un cuerpo intermedio en una extensión del tipo $\mathbb{Q} \subset \mathbb{Q}[\xi]$, donde ξ es una raíz primitiva n-ésima de la unidad de forma que $\phi(n)$ sea múltiplo de 3. Lo más sencillo es tomar $n = 7$.

Tomemos entonces una raíz primitiva séptima de la unidad, ξ. Como $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\xi]) \approx \mathbb{Z}_6$, hay un subgrupo normal H de orden 2 (por ser cíclico, existe un único subgrupo de orden d para cada divisor d de 6, y por ser abeliano, todo subgrupo es normal). Por el teorema fundamental, la extensión $\mathbb{Q} \subset \mathrm{Inv}(H)$ es de grado 3 y de Galois (normal porque H es un subgrupo normal; separable porque $\mathbb{Q}$ es perfecto).

Razonando análogamente, si τ es una raíz primitiva onceava de la unidad, entonces $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\tau]) \approx \mathbb{Z}_{10}$ y por tanto existe un subgrupo normal K de orden 2. Por el teorema fundamental, la extensión $\mathbb{Q} \subset \mathrm{Inv}(K)$ es de grado 5 y de Galois.

Lo siguiente será hallar elementos primitivos de ambas extensiones. Empecemos por la de grado 3. Los elementos de $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\xi])$ son de la forma

$$\begin{aligned} \sigma_k : \mathbb{Q}[\xi] &\longrightarrow \mathbb{Q}[\xi] \\ \xi &\longmapsto \xi^k \end{aligned}$$

para $k \in \{1,2,3,4,5,6\}$. Calculamos el orden de los elementos:

$$\circ\sigma_1 = 1, \qquad \circ\sigma_2 = 3, \qquad \circ\sigma_3 = 6, \qquad \circ\sigma_4 = 3, \qquad \circ\sigma_5 = 6, \qquad \circ\sigma_6 = 2$$

Por tanto, $H = \langle \sigma_6 \rangle$, y tenemos que hallar el cuerpo $\mathrm{Inv}\langle \sigma_6 \rangle$. Una base de $\mathbb{Q}[\xi]$ es $\{1, \xi, \xi^2, \xi^3, \xi^4, \xi^5\}$. Así, dados $a, b, c, d, e, f \in \mathbb{Q}$, se tiene que

$$\begin{aligned} \sigma_6(a + b\xi + c\xi^2 + d\xi^3 + e\xi^4 + f\xi^5) &= a + b\xi^6 + c\xi^5 + d\xi^4 + e\xi^3 + f\xi^2 \\ &= a - b - b\xi - b\xi^2 - b\xi^3 - b\xi^4 - b\xi^5 + c\xi^5 + d\xi^4 + e\xi^3 + f\xi^2 \\ &= a - b - b\xi + (f - b)\xi^2 + (e - b)\xi^3 + (d - b)\xi^4 + (c - b)\xi^5 \end{aligned}$$

donde se ha usado que $\xi^6 = -1 - \xi - \xi^2 - \xi^3 - \xi^4 - \xi^5$ porque $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = \mathrm{Irr}(\xi, X, \mathbb{Q})$. En consecuencia,

$$\sigma_6(a + b\xi + c\xi^2 + d\xi^3 + e\xi^4 + f\xi^5) = a + b\xi + c\xi^2 + d\xi^3 + e\xi^4 + f\xi^5 \iff \begin{cases} a = a - b \\ -b = b \\ f - b = c \\ e - b = d \\ d - b = e \\ c - d = f \end{cases}$$

$$\iff b = 0, c = f, d = e$$

Por tanto,

$$\mathrm{Inv}\langle\sigma_6\rangle = \{a + c(\xi^2+\xi^5) + d(\xi^3+\xi^4) \colon a,c,d \in \mathbb{Q}\} \overset{(*)}{=} \mathbb{Q}[\xi^2+\xi^5, \xi^3+\xi^4]$$

La contención $\subset$ en $(*)$ es trivial, y la contención $\supset$ casi que también, pues

$$\{a + c(\xi^2+\xi^5) + d(\xi^3+\xi^4) \colon a,c,d \in \mathbb{Q}\}$$

es un cuerpo que contiene a $\mathbb{Q}$, a $\xi^2+\xi^5$ y a $\xi^3+\xi^4$, y $\mathbb{Q}[\xi^2+\xi^5, \xi^3+\xi^4]$ es el menor cuerpo verificando esta propiedad. Observamos además que $\xi^2+\xi^5 \notin \mathbb{Q}$, pues si existiese $q \in \mathbb{Q}$ tal que $\xi^2+\xi^5 = q$, entonces ξ sería raíz del polinomio $X^5 + X^2 - q \in \mathbb{Q}[X]$, y esto es imposible porque $[\mathbb{Q}[\xi] \colon \mathbb{Q}] = 6 > 5$. Así, tenemos la torre de extensiones

$$\mathbb{Q} \subset \mathbb{Q}[\xi^2+\xi^5] \subset \mathbb{Q}[\xi^2+\xi^5, \xi^3+\xi^4] = \mathrm{Inv}\langle\sigma_6\rangle$$

Como $[\mathrm{Inv}\langle\sigma_6\rangle \colon \mathbb{Q}] = 3$, que es primo, entonces $[\mathbb{Q}[\xi^2+\xi^5] \colon \mathbb{Q}] \in \{1,3\}$. Pero este grado no puede ser 1 porque $\xi^2+\xi^5 \notin \mathbb{Q}$, así que

$$\mathrm{Inv}\langle\sigma_6\rangle = \mathbb{Q}[\xi^2+\xi^5]$$

Vamos ahora con la extensión de grado 5; el procedimiento va a ser totalmente análogo. Los elementos de $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\tau])$ son de la forma

$$\begin{aligned} \mu_k \colon \mathbb{Q}[\tau] &\longrightarrow \mathbb{Q}[\tau] \\ \tau &\longmapsto \tau^k \end{aligned}$$

para $k \in \{1,2,3,4,5,6,7,8,9,10\}$. Calculamos el orden de los elementos:

$$\circ\mu_1 = 1, \quad \circ\mu_2 = 10, \quad \circ\mu_3 = 5, \quad \circ\mu_4 = 5, \quad \circ\mu_5 = 5, \quad \circ\mu_6 = 10 \quad \circ\mu_7 = 10, \quad \circ\mu_8 = 10, \quad \circ\mu_9 = 5, \quad \circ\mu_{10} = 2$$

Por tanto, $K = \langle\mu_{10}\rangle$, y tenemos que hallar el cuerpo $\mathrm{Inv}\langle\mu_{10}\rangle$. Llegados a este punto, se ve venir que las cuentas a realizar van a resultar bastante desagradables, así que simplemente se afirma que

$$\mathrm{Inv}\langle\mu_{10}\rangle = \mathbb{Q}[\tau_2 + \tau_9]$$

Llamando $\alpha = \xi^2+\xi^5$, $\beta = \tau^2+\tau^9$, tenemos que la extensión

$$\mathbb{Q} \subset \mathbb{Q}[\alpha,\beta] = \mathbb{K}$$

es de orden 15 (pues $\mathrm{mcd}(n,m) = 1$) y es de Galois (es normal porque es el cuerpo de descomposición de $f(X)g(X)$, donde $f(X) = \mathrm{Irr}(\alpha,X,\mathbb{Q})$ y $g(X) = \mathrm{Irr}(\beta,X,\mathbb{Q})$; es separable porque $\mathbb{Q}$ es perfecto). Aunque ya se ha razonado que $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$ es cíclico, lo demostramos de otra manera: construyamos un generador de $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$. Como $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\alpha]) \approx \mathbb{Z}_3$ y $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\alpha]) \approx \mathbb{Z}_{10}$, existen $\sigma_1 \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\alpha])$, $\sigma_2 \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\beta])$ tales que

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\alpha]) = \langle\sigma_1\rangle \qquad \text{y} \qquad \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\beta]) = \langle\sigma_2\rangle$$

En primer lugar, nótese que

$$15 = [\mathbb{Q}[\alpha,\beta] \colon \mathbb{Q}] = [\mathbb{Q}[\alpha,\beta] \colon \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] \colon \mathbb{Q}] = [\mathbb{Q}[\alpha,\beta] \colon \mathbb{Q}[\alpha]] \cdot 3,$$

lo que implica $[\mathbb{Q}[\alpha,\beta] \colon \mathbb{Q}[\alpha]] = 5$ y por tanto $\mathrm{Irr}(\beta,X,\mathbb{Q}) = \mathrm{Irr}(\beta,X,\mathbb{Q}[\alpha])$.

Por otro lado, tenemos que $\alpha' = \sigma_1(\alpha)$ es raíz de $\mathrm{Irr}^{id_{\mathbb{Q}}}(\alpha,X,\mathbb{Q}) = \mathrm{Irr}(\alpha,X,\mathbb{Q})$, luego $\sigma_1 \colon \mathbb{Q}[\alpha] \to \mathbb{Q}[\alpha]$ es el único isomorfismo que extiende a $id_{\mathbb{Q}}$ y con $\sigma_1(\alpha) = \alpha'$ (nótese que $\sigma_1(\mathbb{Q}[\alpha]) = \mathbb{Q}[\alpha]$ porque la extensión es normal). Además, como $\beta' = \sigma_2(\beta)$ es raíz de $\mathrm{Irr}(\beta,X,\mathbb{Q}) = \mathrm{Irr}(\beta,X,\mathbb{Q}[\alpha]) = \mathrm{Irr}^{\sigma_1}(\beta,X,\mathbb{Q}[\alpha])$, existe un único isomorfismo $\sigma \colon \mathbb{Q}[\alpha,\beta] \to \mathbb{Q}[\alpha,\beta]$ que extiende a σ_1 y con $\sigma(\beta) = \beta'$.

$$\begin{array}{ccc} \mathbb{Q} & \xrightarrow{id} & \mathbb{Q} \\ \downarrow & & \downarrow \\ \mathbb{Q}[\alpha] & \xrightarrow{\sigma_1} & \mathbb{Q}[\alpha] \\ \downarrow & & \downarrow \\ \mathbb{Q}[\alpha,\beta] & \xrightarrow{\sigma} & \mathbb{Q}[\alpha,\beta] \\ \alpha & \longmapsto & \alpha' \\ \beta & \longmapsto & \beta' \end{array}$$

Tenemos entonces que $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\alpha,\beta])$, y como σ_1 tiene orden 3 y σ_2 tiene orden 5, se deduce que σ tiene orden $\mathrm{mcm}(3,5) = 15$. Pero

$$\#\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\alpha,\beta]) = [\mathbb{Q}[\alpha,\beta]\colon \mathbb{Q}] = 15,$$

así que es un grupo cíclico. □

Ejercicio 19. *Sea* $\mathbb{K} = \mathbb{Q}(\sqrt{3}, \sqrt{3}+\sqrt[3]{3}, \sqrt[3]{3}+\sqrt[5]{3})$ *y* $\mathbb{L} = \mathbb{K}(\xi_{15})$*, donde* ξ_{15} *es una raíz primitiva quinceava de la unidad.*

(a) Calcular $[\mathbb{K}\colon \mathbb{Q}]$.

(b) ¿Es $\mathbb{Q} \subset \mathbb{K}$ *normal?*

(c) Demostrar que $\mathbb{L}$ *es la clausura normal de* $\mathbb{Q} \subset \mathbb{K}$.

(d) Demostrar que $\sqrt{3} \notin \mathbb{Q}(\xi_5)$*, donde* ξ_5 *es una raíz primitiva quinta de la unidad.* Ayuda*: obsérvese que* $\sqrt{5} \in \mathbb{Q}(\xi_5)$.

(e) Usar (d) *para comprobar que* $[\mathbb{L}\colon \mathbb{Q}] = 240$.

(f) ¿Es el polinomio ciclotómico $\Phi_{15}(X)$ *irreducible sobre* $\mathbb{K}$*?*

(g) Sea $G = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{L})$*. Probar que* G *tiene subgrupos normales* H_1 *y* H_2 *de orden* 60 *tales que* G/H_1 *es cíclico y* G/H_2 *es isomorfo a* $C_2 \times C_2$.

(h) Probar que G *tiene un subgrupo no normal de orden* 48.

(i) ¿Es G *abeliano?*

(j) Calcular el subgrupo de G *correspondiente a la extensión intermedia* $\mathbb{K}$ *en el teorema fundamental.*

Solución.

(a) Veamos primero que $\mathbb{K} = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \sqrt[5]{3})$. La contención $\subset$ es trivial. Para la otra, como $\sqrt{3}+\sqrt[3]{3} \in \mathbb{K}$ y $\sqrt{3} \in \mathbb{K}$, entonces $\sqrt{3}+\sqrt[3]{3}-\sqrt{3} = \sqrt[3]{3} \in \mathbb{K}$. Usando esto y el hecho de que $\sqrt[3]{3}+\sqrt[5]{3} \in \mathbb{K}$ obtenemos que $\sqrt[3]{3}+\sqrt[5]{3}-\sqrt[3]{3} = \sqrt[5]{3} \in \mathbb{K}$. Como $\sqrt{3}$, $\sqrt[3]{3}$, $\sqrt[5]{3} \in \mathbb{K}$, entonces $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \sqrt[5]{3}) \subset \mathbb{K}$.

Hallamos ahora el grado de la extensión. Se tiene que

- $[\mathbb{Q}(\sqrt{3})\colon \mathbb{Q}] = 2$, pues $X^2 - 3$ es mónico e irreducible (Eisenstein con $p = 3$) y anula a $\sqrt{3}$.
- $[\mathbb{Q}(\sqrt[3]{3})\colon \mathbb{Q}] = 3$, pues $X^3 - 3$ es mónico e irreducible (Eisenstein con $p = 3$) y anula a $\sqrt[3]{3}$.
- $[\mathbb{Q}(\sqrt[5]{3})\colon \mathbb{Q}] = 5$, pues $X^5 - 3$ es mónico e irreducible (Eisenstein con $p = 3$) y anula a $\sqrt[5]{3}$.

Por ser 2, 3 y 5 coprimos,

$$[\mathbb{K}\colon \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \sqrt[5]{3})\colon \mathbb{Q}] = 2 \cdot 3 \cdot 5 = 30$$

(b) Se tiene que $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \sqrt[5]{3})\colon \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})] \leq 5$, pues $X^5 - 3 \in \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})[X]$ anula a $\sqrt[5]{3}$. Asimismo, $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{3})\colon \mathbb{Q}(\sqrt{3})] \leq 3$, pues $X^3 - 3 \in \mathbb{Q}(\sqrt{3})[X]$ anula a $\sqrt[3]{3}$. Además, $[\mathbb{Q}(\sqrt{3})\colon \mathbb{Q}] = 2$ como se ha visto antes. Por tanto,

$$30 = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \sqrt[5]{3})\colon \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \sqrt[5]{3})\colon \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})][\mathbb{Q}(\sqrt{3}, \sqrt[3]{3})\colon \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3})\colon \mathbb{Q}] \leq 5 \cdot 3 \cdot 2 = 30$$

Debe ser entonces

$$[\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \sqrt[5]{3})\colon \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})] = 5, \qquad [\mathbb{Q}(\sqrt{3}, \sqrt[3]{3})\colon \mathbb{Q}(\sqrt{3})] = 3$$

La primera igualdad nos dice que $\mathrm{Irr}(\sqrt[5]{3}, X, \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})) = X^5 - 3$, que tiene como raíces a $\xi_5^k \sqrt[5]{3}$, donde $k \in \{0,1,2,3,4\}$. Como al menos una de estas raíces es compleja y en $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \sqrt[5]{3})$ no hay elementos complejos, tenemos que la extensión $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) \subset \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \sqrt[5]{3})$ no es normal, y, por tanto, la extensión $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \sqrt[5]{3}) = \mathbb{K}$ tampoco lo es.

(*c*) Se va a utilizar a lo largo del ejercicio que $\mathbb{K}(\xi_{15}) = \mathbb{K}(\xi_3, \xi_5)$, igualdad que es cierta porque $\text{mcd}(3,5) = 1$.

Sea $\mathbb{L}'$ la clausura normal de la extensión $\mathbb{Q} \subset \mathbb{K}$. Recuperamos del apartado anterior la igualdad $[\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}(\sqrt{3})] = 3$, que nos dice que $X^3 - 3 = \text{Irr}(\sqrt[3]{3}, X, \mathbb{Q}(\sqrt{3}))$. Las raíces de este polinomio son $\xi_3^k \sqrt[3]{3}$, $k \in \{0,1,2\}$. Como $\mathbb{L}'$ debe contener a los elementos $\xi_3^k \sqrt[3]{3}$, en particular, contiene a $\sqrt[3]{3}$ y a $\xi_3 \sqrt[3]{3}$, luego también contiene a ξ_3.

Asimismo, como las raíces del polinomio $X^5 - 3 = \text{Irr}(\sqrt[5]{3}, X, \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}))$ son $\xi_5^k \sqrt[5]{3}$, $k \in \{0,1,2,3,4\}$, entonces en $\mathbb{L}'$ también deben estar ξ_5 y $\sqrt[5]{3}$. Evidentemente, también debe estar $\sqrt{3}$ (porque es raíz de $X^2 - 3 = \text{Irr}(\sqrt{3}, X, \mathbb{Q})$).

Pero $\mathbb{L} = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \sqrt[5]{3}, \xi_3, \xi_5)$ es, por definición, el menor cuerpo que contiene a $\mathbb{Q}$, $\sqrt{3}$, $\sqrt[3]{3}$, $\sqrt[5]{3}$, ξ_3 y ξ_5, así que basta comprobar que la extensión $\mathbb{Q} \subset \mathbb{L}$ es normal para que se tenga $\mathbb{L} = \mathbb{L}'$. Pero esto es trivial porque $\mathbb{L}$ contiene a todas las raíces los polinomios $X^2 - 3$, $X^3 - 3$ y $X^5 - 3$, luego es el cuerpo de descomposición del producto de los tres sobre $\mathbb{Q}$. En consecuencia, la extensión $\mathbb{Q} \subset \mathbb{L}$ es normal y $\mathbb{L} = \mathbb{L}'$.

(*d*) Lo primero que observamos es que $\sqrt{3} \notin \mathbb{Q}(\sqrt{5})$. En efecto, supóngase que existen $a, b \in \mathbb{Q}$ tales que $\sqrt{3} = a + b\sqrt{5}$ (se está usando que $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$). Se distinguen tres casos:

- Si $a = 0$, entonces $\sqrt{3} = b\sqrt{5}$ y $3 = 5b^2 = 5\frac{m^2}{n^2}$ ($m, n \in \mathbb{N}$, $\text{mcd}(m,n) = 1$), luego $3n^2 = 5m^2$ y esto es imposible porque $\text{mcd}(n,m) = 1$.
- Si $b = 0$, entonces $\sqrt{3} = a \in \mathbb{Q}$, que es imposible.
- Si $a \neq 0$, $b \neq 0$, al elevar al cuadrado en $\sqrt{3} - b\sqrt{5} = a$ se obtiene $3 + 5b^2 - 2b\sqrt{15} = a^2$, luego

$$\sqrt{15} = -\frac{a^2 - 5b^2 - 3}{2b} \in \mathbb{Q},$$

que es imposible.

Al llegarse a contradicción en todos los casos, hay que admitir que $\sqrt{3} \notin \mathbb{Q}(\sqrt{5})$ y, en consecuencia, $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{5})] \geq 2$. De hecho, $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{5})] = 2$ porque $X^2 - 3$ anula a $\sqrt{3}$. Por reducción al absurdo, supongamos que $\sqrt{3} \in \mathbb{Q}(\xi_5)$. Como también es $\sqrt{5} \in \mathbb{Q}(\xi_5)$, entonces $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subset \mathbb{Q}(\xi_5)$. Pero $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subset \mathbb{Q}] = 4$ y $[\mathbb{Q}(\xi_5) : \mathbb{Q}] = \phi(5) = 4$, así que $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\xi_5)$ y esto es imposible porque en $\mathbb{Q}(\xi_5)$ hay números complejos y en $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ no.

(*e*) Vamos a probar que $\xi_3 \notin \mathbb{Q}(\xi_5, \sqrt{3})$. Para ello, se va a demostrar que las extensiones $\mathbb{Q} \subset \mathbb{Q}(\xi_5, \sqrt{3})$ y $\mathbb{Q} \subset \mathbb{Q}(\xi_5, \xi_3, \sqrt{3})$ tienen distintos grupos de Galois. En primer lugar, como $\xi_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, entonces $\mathbb{Q}(\xi_5, \xi_3, \sqrt{3}) = \mathbb{Q}(\xi_5, i, \sqrt{3})$.

- Los elementos de $\text{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi_5, \sqrt{3}))$ quedan totalmente determinados por

$$\sigma_{ij}(\xi_5) = \xi_5^i, \qquad \sigma_{ij}(\sqrt{3}) = (-1)^j \sqrt{3},$$

con $i \in \{1,2,3,4\}$, $j \in \{0,1\}$. Se comprueba fácilmente que hay 3 elementos de orden 2.

- Los elementos de $\text{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi_5, i, \sqrt{3}))$ quedan totalmente determinados por

$$\sigma_{ijk}(\xi_5) = \xi_5^i, \qquad \sigma_{ijk}(i) = (-1^j)i, \qquad \sigma_{ijk}(\sqrt{3}) = (-1)^k \sqrt{3},$$

con $i \in \{1,2,3,4\}$, $j \in \{0,1\}$, $k \in \{0,1\}$. Se comprueba fácilmente que hay más de 3 elementos de orden 2.

Con todo esto puede afirmarse que $\xi_3 \notin \mathbb{Q}(\xi_5, \sqrt{3})$, así que

$$[\mathbb{Q}(\xi_5, \xi_3, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\xi_5, \xi_3, \sqrt{3}) : \mathbb{Q}(\xi_5, \sqrt{3})][\mathbb{Q}(\xi_5, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 8 = 16,$$

y como $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$, $[\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = 5$ y 3, 5 y 16 son primos relativos, entonces

$$[\mathbb{L} : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \sqrt[5]{3}, \xi_3, \xi_5) : \mathbb{Q}] = 3 \cdot 5 \cdot 16 = 240$$

(*f*) Sí, porque

$$[\mathbb{L}:\mathbb{K}] = [\mathbb{K}(\xi_{15}):\mathbb{K}] = \frac{[\mathbb{L}:\mathbb{Q}]}{[\mathbb{K}:\mathbb{Q}]} = \frac{240}{30} = 8 = \phi(15)$$

y $\Phi_{15}(X)$ es un polinomio de grado $\phi(15)$ que anula a ξ_{15}, luego es su polinomio mínimo sobre $\mathbb{K}$ y, en consecuencia, es irreducible.

(*g*) Consideremos la torre de extensiones

$$\mathbb{Q} \subset \mathbb{Q}(\xi_5) \subset \mathbb{L}$$

Como $[\mathbb{Q}(\xi_5):\mathbb{Q}] = 4$ y $[\mathbb{L}:\mathbb{Q}(\xi_5)] = \frac{[\mathbb{L}:\mathbb{Q}]}{[\mathbb{Q}(\xi_5):\mathbb{Q}]} = 60$, por el teorema fundamental, $H_1 = \mathrm{Gal}_{\mathbb{Q}(\xi_5)}(\mathbb{L})$ es un subgrupo de $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{L})$ de orden 60. De hecho, como la extensión $\mathbb{Q} \subset \mathbb{Q}(\xi_5)$ es normal (pues $\mathbb{Q}(\xi_5)$ es el cuerpo de descomposición sobre $\mathbb{Q}$ de $X^5 - 1$), entonces el subgrupo es normal y, además,

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi_5)) = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{L}) \big/ \mathrm{Gal}_{\mathbb{Q}(\xi_5)}(\mathbb{L}) = G \big/ H_1$$

Pero $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi_5)) \cong \mathbb{Z}_5^* \cong \mathbb{Z}_4$, que es cíclico, así que $G \,/\, H_1$ también lo es.

Por otra parte, consideremos la torre de extensiones

$$\mathbb{Q} \subset \mathbb{Q}(\xi_3, \sqrt{3}) \subset \mathbb{L}$$

Como $[\mathbb{Q}(\xi_3, \sqrt{3}):\mathbb{Q}] = 4$ y $[\mathbb{L}:\mathbb{Q}(\xi_3, \sqrt{3})] = \frac{[\mathbb{L}:\mathbb{Q}]}{[\mathbb{Q}(\xi_3, \sqrt{3}):\mathbb{Q}]} = 60$, aplicando el teorema fundamental, $H_2 = \mathrm{Gal}_{\mathbb{Q}(\xi_3, \sqrt{3})}(\mathbb{L})$ es un subgrupo de $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{L})$ de orden 60. Es más, como la extensión $\mathbb{Q} \subset \mathbb{Q}(\xi_3, \sqrt{3})$ es normal (pues $\mathbb{Q}(\xi_3, \sqrt{3})$ es el cuerpo de descomposición sobre $\mathbb{Q}$ de $(X^3 - 1)(X^2 - 3)$), entonces el subgrupo es normal y, además,

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi_3, \sqrt{3})) = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{L}) \big/ \mathrm{Gal}_{\mathbb{Q}(\xi_3, \sqrt{3})}(\mathbb{L}) = G \big/ H_2$$

Veamos que $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi_3, \sqrt{3})) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Sus elementos vienen dados por

$$\sigma_{ij}(\xi_3) = \xi_3^i, \qquad \sigma_{ij}(\sqrt{3}) = (-1)^j \sqrt{3},$$

con $i \in \{1,2\}$ y $j \in \{1,2\}$. Calculando el orden de los elementos, se obtiene

$$\circ\sigma_{11} = 2, \qquad \circ\sigma_{12} = 1, \qquad \circ\sigma_{21} = 2, \qquad \circ\sigma_{22} = 2,$$

Los únicos grupos de orden 4 son $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$, y como no hay elementos de orden 4, debe ser $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi_3, \sqrt{3})) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(*h*) Consideremos la torre de extensiones

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[5]{3}) \subset \mathbb{L}$$

Como $[\mathbb{Q}(\sqrt[5]{3}):\mathbb{Q}] = 5$ y $[\mathbb{L}:\mathbb{Q}(\sqrt[5]{3})] = \frac{[\mathbb{L}:\mathbb{Q}]}{[\mathbb{Q}(\sqrt[5]{3}):\mathbb{Q}]} = 48$, por el teorema fundamental, $H = \mathrm{Gal}_{\mathbb{Q}(\sqrt[5]{3}))}(\mathbb{L})$ es un subgrupo de $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{L})$ de orden 48. Es más, como la extensión $\mathbb{Q} \subset \mathbb{Q}(\sqrt[5]{3})$ no es normal (pues $\mathrm{Irr}(\sqrt[5]{3}) = X^5 - 3$ tiene como raíces a $\xi_5^k \sqrt[5]{3}$, $k \in \{0,1,2,3,4\}$, y en $\mathbb{Q}(\sqrt[5]{3})$ no hay números complejos), entonces H no es un subgrupo normal de G.

(*i*) G no es abeliano, pues si lo fuese, todos sus subgrupos serían normales, y esto no se tiene por el apartado anterior.

(*j*) El subgrupo de G correspondiente a la extensión $\mathbb{F} \subset \mathbb{K}$ es $\mathrm{Gal}_{\mathbb{K}}(\mathbb{L})$, que es un subgrupo de G de orden $[\mathbb{L}:\mathbb{K}] = \frac{[\mathbb{L}:\mathbb{Q}]}{[\mathbb{K}:\mathbb{Q}]} = 8$. Como $\mathbb{L} = \mathbb{K}(\xi_{15})$, un automorfismo $\sigma \in \mathrm{Gal}_{\mathbb{K}}(\mathbb{L})$ queda totalmente determinado por la imagen de ξ_{15}, $\sigma(\xi_{15})$, que debe ser una raíz de $\mathrm{Irr}(\xi_{15}, X, \mathbb{K}) = \Phi_{15}(X)$ (esta igualdad se razonó en el apartado (*f*)). Las raíces de $\Phi_{15}(X)$ son las raíces primitivas quinceavas, es decir, los elementos de la forma ξ_{15}^k, donde $k \in \mathbb{N}$ es tal que $\mathrm{mcd}(15,k) = 1$. Así, $\sigma(\xi_{15}) = \xi_{15}^k$ y observamos que el orden de σ coincide con el orden de k en $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$. La conclusión es que $\mathrm{Gal}_{\mathbb{K}}(\mathbb{L}) = \mathbb{Z}_{15}^*$. □

Ejercicio 20. *Sean $\alpha, \beta \in \mathbb{C}$ tales que $[\mathbb{Q}(\alpha)\colon \mathbb{Q}] = 2 = [\mathbb{Q}(\beta)\colon \mathbb{Q}]$ y $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$.*

(a) Calcular $[\mathbb{Q}(\alpha, \beta)\colon \mathbb{Q}]$.

(b) Determinar $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\alpha, \beta))$.

(c) Encontrar $\alpha' \in \mathbb{Q}(\alpha, \beta)$ tal que $\mathbb{Q}(\alpha') = \mathbb{Q}(\alpha)$ y $\alpha'^2 \in \mathbb{Q}$.

(d) Probar que la aplicación $f\colon \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ dada por $f(a + b\alpha') = a - b\alpha'$ es un isomorfismo de anillos.

(e) Encontrar $\gamma \in \mathbb{Q}(\alpha, \beta)$ tal que $\mathbb{Q}(\gamma)$ es el tercer cuerpo intermedio de la extensión $\mathbb{Q}(\alpha, \beta)$.

(f) Demostrar que $\mathbb{Q}(\alpha + c\beta) = \mathbb{Q}(\alpha, \beta)$ para cualquier $c \in \mathbb{Q}$ no nulo.

Solución.

(*a*) Sean $f(X) = \mathrm{Irr}(\alpha, X, \mathbb{Q})$ y $g(X) = \mathrm{Irr}(\beta, X, \mathbb{Q})$. Tenemos que $\deg(f(X)) = \deg(g(X)) = 2$. Por tanto, $[\mathbb{Q}(\alpha, \beta)\colon \mathbb{Q}(\alpha)] \leq 2$ ($g(X) \in \mathbb{Q}(\alpha)[X]$ anula a β y es de grado 2). El grado de la extensión no puede ser 1 porque $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$, luego $[\mathbb{Q}(\alpha, \beta)\colon \mathbb{Q}(\alpha)] = 2$ y entonces

$$[\mathbb{Q}(\alpha, \beta)\colon \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta)\colon \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha)\colon \mathbb{Q}] = 4$$

(*b*) Las raíces de $f(X)$ son $\alpha, \overline{\alpha} \in \mathbb{Q}(\alpha)$, mientras que las raíces de $g(X)$ son $\beta, \overline{\beta} \in \mathbb{Q}(\beta)$. Además, por ser $[\mathbb{Q}(\alpha, \beta)\colon \mathbb{Q}(\alpha)] = 2$, tenemos $g(X) = \mathrm{Irr}(\beta, X, \mathbb{Q}(\alpha))$. Con todo esto, podemos construir los elementos de $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\alpha, \beta))$. Sean $\alpha_1 = \alpha$, $\alpha_2 = \overline{\alpha}$, $\beta_1 = \beta$, $\beta_2 = \overline{\beta}$.

$$\begin{array}{ccc}
\mathbb{Q} & \xrightarrow{id} & \mathbb{Q} \\
\downarrow & & \downarrow \\
\mathbb{Q}(\alpha) & \xrightarrow{\sigma_i} & \mathbb{Q}(\alpha) \\
\alpha & \longmapsto & \alpha_i \\
\downarrow & & \downarrow \\
\mathbb{Q}(\alpha, \beta) & \xrightarrow{\sigma_{ij}} & \mathbb{Q}(\alpha, \beta) \\
\alpha & \longmapsto & \alpha_i \\
\beta & \longmapsto & \beta_j
\end{array}$$

Nótese que

$$\circ\sigma_{11} = 1, \qquad \circ\sigma_{12} = 2, \qquad \circ\sigma_{21} = 2, \qquad \circ\sigma_{22} = 2,$$

luego $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\alpha, \beta)) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(*c*) Si $f(X) = X^2 + bX + a$, entonces

$$\alpha \in \left\{ \frac{-b + \sqrt{b^2 - 4a}}{2}, \frac{-b - \sqrt{b^2 - 4a}}{2} \right\}$$

Es claro que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{b^2 - 4a})$, luego basta tomar $\alpha' = \sqrt{b^2 - 4a}$.

(*d*) Sea $f\colon \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ la aplicación dada por $f(c + d\alpha') = c - d\alpha'$. Nótese que f está bien definida porque $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$ y $\{1, \alpha'\}$ es una base de $\mathbb{Q}(\alpha')$ como $\mathbb{Q}$-espacio vectorial. Supongamos que

$$\alpha = \frac{-b + \sqrt{b^2 - 4a}}{2} = -\frac{b}{2} + \frac{1}{2}\alpha'$$

Entonces

$$f(\alpha) = \frac{b}{2} - \frac{1}{2}\alpha' = \frac{-b - \sqrt{b^2 - 4ac}}{2} = \overline{\alpha}$$

En consecuencia, $f\colon \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ es una aplicación que extiende a la identidad en $\mathbb{Q}$ y que verifica $f(\alpha) = \overline{\alpha}$. Como α y $\overline{\alpha}$ son raíces de $f(X) = \mathrm{Irr}(\alpha, X, \mathbb{Q})$, existe un único isomorfismo de $\mathbb{Q}(\alpha)$ en $\mathbb{Q}(\overline{\alpha}) = \mathbb{Q}(\alpha)$ que extiende a la identidad en $\mathbb{Q}$ y que envía α en $\overline{\alpha}$. Pero f es precisamente esta aplicación, así que, en particular, es un isomorfismo.

(*e*) Como $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\alpha,\beta)) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, hay tantas extensiones intermedias en la extensión $\mathbb{Q} \subset \mathbb{Q}(\alpha,\beta)$ como subgrupos en $\mathbb{Z}_2 \times \mathbb{Z}_2$. Los subgrupos propios de $\mathbb{Z}_2 \times \mathbb{Z}_2$ son $\mathbb{Z}_2 \times \{0\}$, $\{0\} \times \mathbb{Z}_2$, $\langle (1,1) \rangle$. Hay que identificar los elementos de $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\alpha,\beta))$ con los de $\mathbb{Z}_2 \times \mathbb{Z}_2$: se observa que $\mathbb{Z}_2 \times \{0\} \cong \langle \sigma_{21} \rangle$ y $\{0\} \times \mathbb{Z}_2 \cong \langle \sigma_{12} \rangle$, luego los subgrupos propios de $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\alpha,\beta))$ serían $\langle \sigma_{21} \rangle$, $\langle \sigma_{12} \rangle$ y $\langle \sigma_{22} \rangle$. Los cuerpos intermedios que corresponden a estos subgrupos son $\mathrm{Inv}(\langle \sigma_{12} \rangle)$, $\mathrm{Inv}(\langle \sigma_{21} \rangle)$ y $\mathrm{Inv}(\langle \sigma_{22} \rangle)$. Dos de estos cuerpos son $\mathbb{Q}(\alpha)$ y $\mathbb{Q}(\beta)$, y el tercero es el que buscamos. Se comprueba fácilmente que $\mathbb{Q}(\alpha) = \mathrm{Inv}(\langle \sigma_{12} \rangle)$ y que $\mathbb{Q}(\beta) = \mathrm{Inv}(\langle \sigma_{21} \rangle)$. Hallemos $\mathrm{Inv}(\langle \sigma_{22} \rangle)$. Sea $a_1 + a_2\alpha + a_3\beta + a_4\alpha\beta \in \mathbb{Q}(\alpha,\beta)$. Se tiene que

$$\sigma_{22}(a_1+a_2\alpha+a_3\beta+a_4\alpha\beta)=a_1+a_2\alpha+a_3\beta+a_4\alpha\beta \iff a_1+a_2\overline{\alpha}+a_3\overline{\beta}+a_4\overline{\alpha}\,\overline{\beta}=a_1+a_2\alpha+a_3\beta+a_4\alpha\beta \qquad (*)$$

En un apartado anterior se probó que $\alpha' = \alpha - \overline{\alpha}$ es tal que $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$ y $\alpha'^2 \in \mathbb{Q}$. Análogamente se demuestra que $\beta' = \beta - \overline{\beta}$ es tal que $\mathbb{Q}(\beta) = \mathbb{Q}(\beta')$ y $\beta'^2 \in \mathbb{Q}$. Seguimos con la cadena de equivalencias anterior:

$$\begin{aligned}
(*) &\iff a_1 + a_2(\alpha-\alpha') + a_3(\beta-\beta') + a_4(\alpha-\alpha')(\beta-\beta') = a_1 + a_2\alpha + a_3\beta + a_4\alpha\beta \\
&\iff a_1 + a_2\alpha - a_2\alpha' + a_3\beta - a_3\beta' + a_4\alpha\beta - a_4\alpha\beta' - a_4\alpha'\beta + a_4\alpha'\beta' = a_1 + a_2\alpha + a_3\beta + a_4\alpha\beta \\
&\iff -a_4(\alpha'\beta + \alpha\beta') - a_2\alpha' - a_3\beta' + a_4\alpha'\beta' = 0 \qquad (**)
\end{aligned}$$

Nótese que $\mathbb{Q}(\alpha',\beta') = \mathbb{Q}(\alpha,\beta)$ y una base suya como $\mathbb{Q}$-espacio vectorial es $\{1,\alpha',\beta',\alpha'\beta'\}$. Sería bastante conveniente escribir $\alpha'\beta - \alpha\beta'$ en términos de α', β' y $\alpha'\beta'$ para tener una combinación lineal nula de los elementos de la base. Pero α, α', β, β' son de la forma

$$\alpha = -\frac{b}{2} + \frac{1}{2}\sqrt{b^2-4a}, \quad \alpha' = \sqrt{b^2-4a}, \quad \beta = -\frac{c}{2} + \frac{1}{2}\sqrt{c^2-4d}, \quad \beta' = \sqrt{c^2-4d},$$

con $a,b,c,d \in \mathbb{Q}$. Por tanto,

$$\begin{aligned}
\alpha'\beta + \alpha\beta' &= -\frac{c}{2}\sqrt{b^2-4a} + \frac{1}{2}\sqrt{b^2-4a}\sqrt{c^2-4d} - \frac{b}{2}\sqrt{c^2-4d} + \frac{1}{2}\sqrt{b^2-4a}\sqrt{c^2-4d} \\
&= -\frac{c}{2}\sqrt{b^2-4a} - \frac{b}{2}\sqrt{c^2-4d} + \sqrt{b^2-4a}\sqrt{c^2-4d} \\
&= -\frac{c}{2}\alpha' - \frac{b}{2}\beta' + \alpha'\beta'
\end{aligned}$$

En consecuencia,

$$\begin{aligned}
(**) &\iff a_4\frac{c}{2}\alpha' + a_4\frac{b}{2}\beta' - a_2\alpha' - a_3\beta' = 0 \iff \left(a_4\frac{c}{2} - a_2\right)\alpha' + \left(a_4\frac{b}{2} - a_3\right)\beta' = 0 \\
&\iff a_2 = a_4\frac{c}{2},\ a_3 = a_4\frac{b}{2}
\end{aligned}$$

Así,

$$\mathrm{Inv}(\langle \sigma_{22} \rangle) = \left\{ a_1 + a_4\frac{c}{2}\alpha + a_4\frac{b}{2}\beta + a_4\alpha\beta \colon a_1, a_4 \in \mathbb{Q} \right\} = \left\{ a_1 + a_4\left(\frac{c}{2}\alpha + \frac{b}{2}\beta + \alpha\beta\right) \colon a_1, a_4 \in \mathbb{Q} \right\}$$

Se tiene que

$$\frac{c}{2}\alpha + \frac{b}{2}\beta + \alpha\beta = -\frac{bc}{4} + \frac{c}{4}\cancel{\alpha'} - \frac{b\cancel{c}}{4} + \frac{b}{4}\cancel{\beta'} + \frac{b\cancel{c}}{4} - \frac{b}{4}\cancel{\beta'} - \frac{c}{4}\cancel{\alpha'} + \frac{1}{4}\alpha'\beta' = -\frac{bc}{4} + \frac{1}{4}\alpha'\beta'$$

Por tanto,

$$\mathrm{Inv}(\langle \sigma_{22} \rangle) = \mathbb{Q}(-bc + \alpha'\beta') = \mathbb{Q}(\alpha'\beta')$$

(*f*) Sea $q \in \mathbb{C}$ con $q \neq 0$ y veamos que $\mathbb{Q}(\alpha + q\beta) = \mathbb{Q}(\alpha,\beta)$.

- Veamos que $\mathbb{Q}(\alpha + q\beta) \neq \mathbb{Q}$. Si existiese $q' \in \mathbb{Q}$ con $\alpha + q\beta = q'$, entonces $\alpha = q' - q\beta \in \mathbb{Q}(\beta)$, que es imposible porque $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$.

- Veamos que $\mathbb{Q}(\alpha+q\beta)\neq\mathbb{Q}(\alpha)$. Si fuese $\mathbb{Q}(\alpha+q\beta)=\mathbb{Q}(\alpha)$, entonces $\alpha+q\beta\in\mathbb{Q}(\alpha)$ y $\alpha\in\mathbb{Q}(\alpha)$, luego $\alpha+q\beta-\alpha=q\beta\in\mathbb{Q}(\alpha)$, y como $q\neq 0$, sería $\beta\in\mathbb{Q}(\alpha)$, que es imposible porque $\mathbb{Q}(\alpha)\neq\mathbb{Q}(\beta)$.
- Veamos que $\mathbb{Q}(\alpha+q\beta)\neq\mathbb{Q}(\beta)$. Si fuese $\mathbb{Q}(\alpha+q\beta)=\mathbb{Q}(\beta)$, entonces $\alpha+q\beta\in\mathbb{Q}(\beta)$ y $q\beta\in\mathbb{Q}(\beta)$, luego $\alpha+q\beta-q\beta=\alpha\in\mathbb{Q}(\beta)$, que también es imposible porque $\mathbb{Q}(\alpha)\neq\mathbb{Q}(\beta)$.
- Veamos que $\mathbb{Q}(\alpha+q\beta)\neq\mathbb{Q}(\alpha'\beta')$. Se tiene que

$$\alpha+q\beta=-\frac{b}{2}+\frac{1}{2}\alpha'+q\left(-\frac{c}{2}+\frac{1}{2}\beta'\right)=-\frac{b}{2}-\frac{cq}{2}+\frac{1}{2}\alpha'+\frac{q}{2}\beta'=q'+\frac{1}{2}\alpha'+\frac{q}{2}\beta',$$

donde $q'\in\mathbb{Q}$. Por tanto,

$$\mathbb{Q}(\alpha+q\beta)=\mathbb{Q}(q'+\frac{1}{2}\alpha'+\frac{q}{2}\beta')=\mathbb{Q}(\alpha'+q\beta')$$

Por reducción al absurdo, supongamos que $\mathbb{Q}(\alpha'+q\beta')=\mathbb{Q}(\alpha'\beta')$. Entonces

$$(\alpha'+q\beta')\alpha'\beta'=\alpha'^2\beta'+q\alpha'\beta'^2\in\mathbb{Q}(\alpha'\beta')$$

Pero $\alpha'^2\in\mathbb{Q}$, así que podemos dividir por α'^2 (que es no nulo porque si fuese $\sqrt{b^2-4a}=0$ entonces $\alpha\in\mathbb{Q}$, que es falso). Así, $\beta'+q\alpha'\frac{\beta'^2}{\alpha'^2}\in\mathbb{Q}(\alpha'\beta')$. Pero también es $\beta'^2\in\mathbb{Q}$, luego $q'=(q\frac{\alpha'^2}{\beta'^2})^{-1}\in\mathbb{Q}$ y por tanto $q'\beta'+\alpha'\in\mathbb{Q}(\alpha'\beta')$. Tenemos entonces $\alpha'+q\beta'\in\mathbb{Q}(\alpha'\beta')$ y $\alpha'+q'\beta'\in\mathbb{Q}(\alpha'\beta')$, así que al restarlos y dividir por $q-q'$ (que es no nulo, probablemente) se obtiene $\beta'\in\mathbb{Q}(\alpha'\beta')$, luego $\mathbb{Q}(\beta)=\mathbb{Q}(\beta')=\mathbb{Q}(\alpha'\beta)$ y esto es imposible por el apartado anterior.

Como no hay más cuerpos intermedios en la extensión $\mathbb{Q}\subset\mathbb{Q}(\alpha,\beta)$, no queda más remedio que admitir que $\mathbb{Q}(\alpha+q\beta)=\mathbb{Q}(\alpha,\beta)$. □

Ejercicio 21. *Encontrar todos los subgrupos de* $\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$*, siendo* $\mathbb{K}$ *el cuerpo de descomposición de* $f(X)$ *sobre* $\mathbb{F}$*, donde*

(a) $\mathbb{F}=\mathbb{Q}(i)$*,* $f(X)=X^6-1$*;*

(b) $\mathbb{F}=\mathbb{Q}$*,* $f(X)=X^{10}-1$*.*

Solución.

(*a*) Si ξ es una raíz primitiva sexta de la unidad, el cuerpo de descomposición de $\mathbb{F}$ sobre $f(X)$ es $\mathbb{K}=\mathbb{F}(\xi)=\mathbb{Q}(i,\xi)$. Veamos que $i\notin\mathbb{Q}(\xi)$, lo que nos ayudará a calcular el grado de la extensión. Como $\xi=\cos(60°)+i\,\mathrm{sen}(60°)=\frac{1}{2}+i\frac{\sqrt{3}}{2}$, entonces $i\frac{\sqrt{3}}{2}\in\mathbb{Q}(\xi)$, y si fuese $i\in\mathbb{Q}(\xi)$, tendríamos $\sqrt{3}\in\mathbb{Q}(\xi)$, y como $[\mathbb{Q}(\xi)\colon\mathbb{Q}]=\phi(6)=2=[\mathbb{Q}(\sqrt{3})\colon\mathbb{Q}]$, luego $\mathbb{Q}(\sqrt{3})=\mathbb{Q}(\xi)$ y esto es imposible porque $\mathbb{Q}(\sqrt{3})\subset\mathbb{R}$ y hemos supuesto que $i\in\mathbb{Q}(\xi)$. Por tanto, $[\mathbb{Q}(i,\xi)\colon\mathbb{Q}(\xi)]=2$ (es menor o igual que 2 porque X^2+1 anula a i; no puede ser 1 por lo que se acaba de probar). En consecuencia,

$$[\mathbb{Q}(i,\xi)\colon\mathbb{Q}]=[\mathbb{Q}(i,\xi)\colon\mathbb{Q}(\xi)][\mathbb{Q}(\xi)\colon\mathbb{Q}]=4$$

Si $\sigma\in\mathrm{Gal}_{\mathbb{Q}(i)}(\mathbb{Q}(i,\xi))$, entonces $\sigma(\xi)$ es una raíz de $\mathrm{Irr}(\xi,X,\mathbb{Q}(i))=\mathrm{Irr}(\xi,X,\mathbb{Q})=\Phi_6(X)$ (igualdad que se tiene porque $[\mathbb{Q}(i,\xi)\colon\mathbb{Q}(i)]=2$), es decir, solo hay dos posibilidades, $\sigma(\xi)=\xi$ y $\sigma(\xi)=\xi^5$. Se tiene que $\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})\cong\mathbb{Z}_2$ y el único subgrupo propio es $\langle\sigma\rangle$, donde $\sigma\in\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$ es tal que $\sigma(\xi)=\xi^5$.

Como $\mathrm{Gal}_{\mathbb{Q}(i)}(K)$ es un grupo abeliano, todos los subgrupos son normales, luego todos los cuerpos intermedios $\mathbb{Q}(i)\subset\mathbb{E}\subset\mathbb{K}$ son tales que $\mathbb{Q}(i)\subset\mathbb{E}$ es normal. Pero $\mathbb{Q}\subset\mathbb{Q}(i)$ también es normal (es de grado 2), así que $\mathbb{Q}\subset\mathbb{E}$ es normal.

(*b*) Se verifica que $\mathbb{K}=\mathbb{Q}(\xi)$, donde ξ es una raíz primitiva décima de la unidad. Además, se tiene $\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})\cong\mathbb{Z}_{10}^*=\{1,3,7,9\}$, que es isomorfo a $\mathbb{Z}_4$ porque 3 tiene orden 4. Por tanto, como $\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$ es cíclico, existe un único subgrupo de orden d para cada divisor d de 4, es decir, solo hay un subgrupo no trivial y este es de orden 2. Basta tomar el subgrupo generado por cualquier elemento de $\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$ de orden 2, que puede hallarse fácilmente.

Por ser $\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})$ un grupo abeliano, todos los cuerpos intermedios $\mathbb{Q}\subset\mathbb{E}\subset\mathbb{K}$ verifican que $\mathbb{Q}\subset\mathbb{E}$ es normal. □

Ejercicio 22. *Sean α la raíz real de X^3-2 en $\mathbb{C}$, ξ_6 una raíz primitiva sexta de la unidad, $\mathbb{F}=\mathbb{Q}(\alpha)$ y $\mathbb{K}=\mathbb{Q}(\alpha,\xi_6)$.*

(a) Comprobar que $\mathbb{K}$ es la clausura normal de $\mathbb{Q}\subset\mathbb{F}$.

(b) ¿Existe un elemento primitivo de $\mathbb{Q}\subset\mathbb{K}$?

(c) ¿Se puede dar un polinomio $f(X)\in\mathbb{Q}[X]$ tal que $\mathbb{F}$ sea el cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$? ¿Y para $\mathbb{Q}\subset\mathbb{K}$?

(d) Calcular $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{F})$.

(e) Calcular $[\mathbb{K}:\mathbb{Q}]$ y $|G|$, donde $G=\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$.

(f) Determinar el orden del subgrupo H de G correspondiente a $\mathbb{F}$ en el teorema fundamental.

(g) Demostrar que G tiene un subgrupo normal S tal que G/S es isomorfo a $\mathbb{Z}_6^*$.

(h) ¿Se pueden encontrar dos subgrupos de G de orden 2?

Solución.

(*a*) Las raíces de X^3-2 son $\xi_3^k\sqrt[3]{2}$, donde $k\in\{0,1,2\}$ y ξ_3 es una raíz primitiva tercera de la unidad. Se tiene entonces $\alpha=\sqrt[3]{2}$. Además,

$$\xi_3=\cos(120^\circ)+i\,\mathrm{sen}(120^\circ)=-\frac{1}{2}+i\frac{\sqrt{3}}{2},\qquad \xi_6=\cos(60^\circ)+i\,\mathrm{sen}(60^\circ)=\frac{1}{2}+i\frac{\sqrt{3}}{2}$$

En consecuencia, $\mathbb{K}=\mathbb{Q}(\alpha,\xi_6)=\mathbb{Q}(\alpha,\xi_3)$. Observamos además que la clausura normal de $\mathbb{Q}\subset\mathbb{Q}(\alpha)$ contiene a α, luego debe contener a todas las raíces de X^3-2. En particular, también contiene a $\xi_3\alpha$, y dividiendo por α obtenemos que debe contener a ξ_3. Pero, por definición, $\mathbb{K}=\mathbb{Q}(\alpha,\xi_3)$ es el menor cuerpo que contiene a $\mathbb{Q}$, α y ξ_3, y además la extensión $\mathbb{Q}\subset\mathbb{K}$ es normal (pues $\mathbb{K}$ es el cuerpo de descomposición de X^3-2 sobre $\mathbb{Q}$). Concluimos que $\mathbb{K}$ es la clausura normal de $\mathbb{Q}\subset\mathbb{Q}(\alpha)$.

(*b*) Como $\mathbb{Q}$ es perfecto, entonces la extensión $\mathbb{Q}\subset\mathbb{K}$ es separable, y como es finita, el teorema del elemento primitivo asegura la existencia de un elemento primitivo de dicha extensión.

(*c*) Para la extensión $\mathbb{Q}\subset\mathbb{Q}(\alpha)$ no existe ningún polinomio $f(X)\in\mathbb{Q}[X]$ tal que $\mathbb{Q}(\alpha)$ sea el cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$. En efecto, si existiese un polinomio en estas condiciones, entonces la extensión $\mathbb{Q}\subset\mathbb{Q}(\alpha)$ sería normal, pero esto es falso porque α es raíz de $X^3-2\in\mathbb{Q}(\alpha)$ y las otras dos raíces de α no están en $\mathbb{Q}(\alpha)$, pues son complejas y $\mathbb{Q}(\alpha)\subset\mathbb{R}$.

En cuanto a la extensión $\mathbb{Q}\subset\mathbb{K}$, tenemos que $\mathbb{K}=\mathbb{Q}(\alpha,\xi_3)$ es el cuerpo de descomposición de $X^3-2\in\mathbb{Q}[X]$ sobre $\mathbb{Q}$.

(*d*) Cualquier automorfismo $\sigma\colon\mathbb{Q}(\alpha)\to\mathbb{Q}(\alpha)$ que extienda a $id\colon\mathbb{Q}\to\mathbb{Q}$ debe enviar α en una raíz de $\mathrm{Irr}^{id}(\alpha,X,\mathbb{Q})=X^3-2$. Las raíces de este polinomio son α, $\xi_3\alpha$ y $\xi_3^2\alpha$. Pero $\xi_3\alpha$ y $\xi_3^2\alpha$ no están en $\mathbb{Q}(\alpha)$ (son números complejos), así que la única posibilidad es que $\sigma(\alpha)=\alpha$ y, en consecuencia, σ es la identidad. En resumen: $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{F})=\{id\}$.

(*e*) Tenemos que $[\mathbb{Q}(\alpha,\xi_3)\colon\mathbb{Q}(\alpha)]\leq 2$, ya que X^2+X+1 anula a ξ_3. Pero no puede ser 1 porque $\xi_3\notin\mathbb{Q}(\alpha)$, luego $[\mathbb{Q}(\alpha,\xi_3)\colon\mathbb{Q}(\alpha)]=2$ y, en consecuencia,

$$[\mathbb{K}:\mathbb{Q}]=[\mathbb{Q}(\alpha)\colon\mathbb{Q}][\mathbb{Q}(\alpha,\xi_3)\colon\mathbb{Q}(\alpha)]=6$$

La extensión $\mathbb{Q}\subset\mathbb{K}$ es normal y separable, luego es de Galois y, en consecuencia, $|G|=[\mathbb{K}:\mathbb{Q}]=6$.

(*f*) El subgrupo pedido es $H=\mathrm{Gal}_{\mathbb{F}}(\mathbb{K})=\mathrm{Gal}_{\mathbb{Q}(\alpha)}(\mathbb{Q}(\alpha,\xi_3))$. Un automorfismo $\sigma\colon\mathbb{Q}(\alpha,\xi_3)\to\mathbb{Q}(\alpha,\xi_3)$ que extiende a $id\colon\mathbb{Q}(\alpha)\to\mathbb{Q}(\alpha)$ queda totalmente determinado por la imagen de ξ_3, que es enviado a una raíz de $\mathrm{Irr}(\xi_3,X,\mathbb{Q}(\alpha))=\mathrm{Irr}(\xi_3,X,\mathbb{Q})=X^2+X+1$, donde en la primera igualdad se ha usado que $[\mathbb{Q}(\alpha,\xi_3)\colon\mathbb{Q}(\alpha)]=2$. Las raíces de este polinomio son ξ_3 y ξ_3^2, así que hay dos posibles automorfismos: la identidad y el determinado por $\sigma(\xi_3)=\xi_3^2$. Tenemos entonces

$$H=\{id,\sigma\}\cong\mathbb{Z}_2$$

(g) Consideremos la torre de extensiones

$$\mathbb{Q} \subset \mathbb{Q}(\xi_3) \subset \mathbb{Q}(\alpha, \xi_3)$$

Sea $S = \mathrm{Gal}_{\mathbb{Q}(\xi_3)}(\mathbb{Q}(\alpha,\xi_3))$. Como la extensión $\mathbb{Q} \subset \mathbb{Q}(\xi_3)$ es normal (pues $\mathbb{Q}(\xi_3)$ es el cuerpo de descomposición de X^3-1 sobre $\mathbb{Q}$), por el teorema fundamental, S es un subgrupo normal de G y además

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi_3)) \cong {}^{G}\!/_{S}$$

Pero $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\xi_3)) \cong \mathbb{Z}_3^* \cong \mathbb{Z}_6^*$, donde el último isomorfismo se tiene porque $\mathbb{Z}_3^*$ y $\mathbb{Z}_6^*$ son grupos de $\phi(3) = \phi(6) = 2$ elementos.

(h) Se prueba fácilmente que los elementos de G vienen dados por

$$\sigma_{ij}(\alpha) = \xi_3^i \alpha, \qquad \sigma_{ij}(\xi_3) = \xi_3^j,$$

con $i \in \{0,1,2\}$, $j \in \{1,2\}$. También se comprueba fácilmente que

$$\circ\sigma_{01} = 1, \qquad \circ\sigma_{02} = 2, \qquad \circ\sigma_{11} = 3, \qquad \circ\sigma_{12} = 2, \qquad \circ\sigma_{21} = 3, \qquad \circ\sigma_{22} = 2$$

Se tiene entonces que $G \cong S_3$ (los grupos de orden 6 son S_3 y $\mathbb{Z}_6$, y no hay elementos de orden 6), y en S_3 hay tres subgrupos distintos de orden 2, así que la respuesta a la pregunta del enunciado es afirmativa. □

Ejercicio 23. *Sea $\mathbb{F} \subset \mathbb{K}$ una extensión finita, de Galois y de grado n con grupo de Galois*

$$G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$$

Demostrar que $\gamma \in \mathbb{K}$ es un elemento primitivo de $\mathbb{F} \subset \mathbb{K}$ si y solo si

$$\sigma_1(\gamma), \sigma_2(\gamma), \ldots, \sigma_n(\gamma)$$

son todos diferentes.

Solución. Supongamos que $\mathbb{K} = \mathbb{F}(\gamma)$. Cada automorfismo $\sigma \in G$ queda totalmente determinado por la imagen de γ, que debe ser enviado a una raíz de $f(X) = \mathrm{Irr}(\gamma, X, \mathbb{F})$ que esté en $\mathbb{F}(\gamma)$. Pero $\mathbb{F} \subset \mathbb{F}(\gamma)$ es normal, así que todas las raíces de $f(X)$ están en $\mathbb{F}(\gamma)$, y $f(X)$ es separable (pues la extensión es de Galois), así que tiene $[\mathbb{F}(\alpha)\colon \mathbb{F}]$ raíces distintas. Y, además, $[\mathbb{F}(\alpha)\colon \mathbb{F}] = \#G = n$ por ser la extensión de Galois. La conclusión es que las raíces de $f(X)$ son

$$\sigma_1(\gamma), \sigma_2(\gamma), \ldots, \sigma_n(\gamma),$$

y además son todas distintas.

Recíprocamente, supongamos que existe $\gamma \in \mathbb{K}$ tal que

$$\sigma_1(\gamma), \sigma_2(\gamma), \ldots, \sigma_n(\gamma)$$

son todas diferentes, y veamos que $\mathbb{K} = \mathbb{F}(\gamma)$. Basta comprobar que

$$[\mathbb{F}(\gamma)\colon \mathbb{F}] = [\mathbb{K}\colon \mathbb{F}] = \#G = n$$

Para cada $i \in \{1,2,\ldots,n\}$, $\overline{\sigma}_i = \sigma_i\big|_{\mathbb{F}(\gamma)}$ es una inmersión de $\mathbb{F}(\gamma)$ en $\mathbb{K}$, y además, como cada una de estas inmersiones queda totalmente determinada por la imagen de γ, por hipótesis, todas las inmersiones $\overline{\sigma}_i$ son diferentes. Así, el número de inmersiones de $\mathbb{F}(\gamma)$ en $\mathbb{K}$ es al menos $n \geq [\mathbb{F}(\alpha)\colon \mathbb{F}]$. Pero también se sabe que el número de inmersiones de $\mathbb{F}(\gamma)$ en $\mathbb{K}$ que extienden a $id\colon \mathbb{F} \to \mathbb{F}$ es menor o igual que $[\mathbb{F}(\gamma)\colon \mathbb{F}]$ (nótese que $\mathbb{K}$ contiene al cuerpo de descomposición de $\mathrm{Irr}(\gamma, X, \mathbb{F})$ sobre $\mathbb{F}$ porque la extensión $\mathbb{F} \subset \mathbb{K}$ es normal, y por tanto puede aplicarse el resultado sobre el número de inmersiones). Todo esto nos dice que

$$n = [\mathbb{F}(\gamma)\colon \mathbb{F}],$$

concluyéndose que $\mathbb{K} = \mathbb{F}(\gamma)$. □

Ejercicio 24. *Sea p un número primo y sea $f(X)$ un factor irreducible de $X^{p^n} - X$ en $\mathbb{Z}_p[X]$.*

(a) ¿Qué se puede decir sobre el grado de $f(X)$?

(b) Sea α una raíz de $f(X)$ en algún cuerpo de descomposición. Determinar los grados de los factores irreducibles de $f(X)$ en $\mathbb{Z}_p(\alpha)[X]$.

(c) ¿Cuántas extensiones intermedias tiene el cuerpo de descomposición de $f(X)$ sobre $\mathbb{Z}_p$?

(d) Si d es un entero que divide a n, ¿existe un factor irreducible de $X^{p^n} - X$ cuyo grupo de Galois sea cíclico y de orden d?

(e) Si d es un entero que divide a n, ¿existe un factor irreducible de $X^{p^n} - X$ cuyo grupo de Galois sea isomorfo a S_d?

Solución.

(*a*) Veamos que $m = \deg(f(X))$ divide a n. Sea $\mathbb{K}$ el cuerpo de descomposición de $X^{p^n} - X$ sobre $\mathbb{Z}_p$ y sea $\mathbb{F}$ el cuerpo de descomposición de $f(X)$ sobre $\mathbb{Z}_p$. Sabemos que $\#\mathbb{K} = p^n$ y que $f(X)$ divide a $X^{p^n} - X$, luego $\mathbb{F} \subset \mathbb{K}$ y tenemos la torre de extensiones

$$\mathbb{Z}_p \subset \mathbb{F} \subset \mathbb{K}$$

Además, $[\mathbb{F} : \mathbb{Z}_p] = m$, ya que podemos considerar cualquier raíz $\alpha \in \mathbb{F}$ de $f(X)$ y tenemos que la extensión $\mathbb{Z}_p \subset \mathbb{Z}_p(\alpha)$ es normal, así que $\mathbb{Z}_p(\alpha)$ es el cuerpo de descomposición de $f(X)$ sobre $\mathbb{Z}_p$, es decir, $\mathbb{F} = \mathbb{Z}_p(\alpha)$. Tenemos entonces

$$n = [\mathbb{K} : \mathbb{Z}_p] = [\mathbb{K} : \mathbb{F}][\mathbb{F} : \mathbb{Z}_p] = [\mathbb{K} : \mathbb{F}] \cdot \deg(f(X)),$$

luego m divide a n.

(*b*) Como se ha visto en el apartado anterior, $\mathbb{Z}_p(\alpha)$ es el cuerpo de descomposición de $f(X)$ sobre $\mathbb{Z}_p$. Pero además $f(X)$ es separable (porque $\mathbb{Z}_p$ es finito y, por tanto, perfecto), así que todos los factores irreducibles de $f(X)$ en $\mathbb{Z}_p(\alpha)[X]$ tienen grado 1.

(*c*) El cuerpo de descomposición de $f(X)$ sobre $\mathbb{Z}_p$ es $\mathbb{Z}_p(\alpha)$, y sabemos que toda extensión finita de un cuerpo finito es cíclica. Además, la extensión es de Galois, así que

$$\#\mathrm{Gal}_{\mathbb{Z}_p}(\mathbb{Z}_p(\alpha)) = [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = m$$

Por tanto, como $\mathrm{Gal}_{\mathbb{Z}_p}(\mathbb{Z}_p(\alpha))$ es cíclico, existe un único subgrupo de orden d para cada divisor d de m, luego, por el teorema fundamental, existe un único cuerpo intermedio de la extensión $\mathbb{Z}_p \subset \mathbb{Z}_p(\alpha)$ para cada divisor d de m.

(*d*) Veamos que sí existe. Sea d un divisor de n. Sabemos que en la factorización de $X^{p^n} - X$ aparecen todos los polinomios mónicos sobre $\mathbb{Z}_p$ de grado un divisor de n. En particular, existe un factor irreducible de $X^{p^n} - X$ de grado d, y, repitiendo los razonamientos anteriores, su grupo de Galois es cíclico y de grado d.

(*e*) Como se ha visto en los apartados anteriores, todo factor irreducible de $X^{p^n} - X$ tiene grupo de Galois cíclico, así que no puede ser isomorfo a S_d para ningún divisor d de n. □

Ejercicio 25. *Sean α, β raíces reales positivas de $X^4 - 2$ y $X^6 - 2$ respectivamente, y sea $\mathbb{K} = \mathbb{Q}(\alpha, \beta)$.*

(a) Probar que $\frac{\alpha}{\beta}$ es un elemento primitivo de $\mathbb{Q} \subset \mathbb{K}$.

(b) Demostrar que el polinomio mínimo de α sobre $\mathbb{Q}(\beta)$ es $X^2 - \sqrt{2}$.

(c) ¿Existe $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$ tal que $\sigma(\beta) = -\beta$?

(d) Demostrar que $\mathbb{K}^{\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})} = \mathbb{Q}(\beta)$.

(e) *Explicar por qué la clausura normal de* $\mathbb{Q} \subset \mathbb{K}$ *es*

$$\mathbb{L} = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2}, \sqrt[4]{2})$$

(f) *Calcular* $[\mathbb{L} : \mathbb{Q}]$.

(g) *Demostra que existe un polinomio irreducible* $f(X) \in \mathbb{Q}[X]$ *de grado* 12 *con grupo de Galois soluble y de orden* 48. *¿Son las raíces de este polinomio construibles con regla y compás?*

(h) *Sea* $G = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{L})$. *Encontrar dos subgrupos* H_1, H_2 *de* G *de orden* 6 *tales que* H_1 *sea un subgrupo normal y* H_2 *no lo sea.*

(i) *Probar que existe un subgrupo normal* S *de* G *tal que* $G \,/\, S$ *es isomorfo a* $\mathbb{Z}_{12}^*$.

(j) *¿Es* H_1 *un subgrupo de* S*?*

Solución. Las raíces de $X^4 - 2$ son $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$ y $-i\sqrt[4]{2}$, mientras que las raíces de $X^6 - 2$ son $\xi^k \sqrt[6]{2}$, $k \in \{0,1,2,3,4,5\}$, donde ξ es una raíz primitiva sexta de la unidad. Por tanto, $\alpha = \sqrt[4]{2}$ y $\beta = \sqrt[6]{2}$.

(a) Veamos que $\alpha, \beta \in \mathbb{Q}(\frac{\alpha}{\beta})$, lo que probará que $\frac{\alpha}{\beta}$ es un elemento primitivo de la extensión. Se tiene que

$$\left(\frac{\alpha}{\beta}\right)^{12} = \frac{8}{4} = 2,$$

luego $(\frac{\alpha}{\beta})^3$ es una raíz de $X^4 - 2$. Como α y β son reales y positivos, entonces $(\frac{\alpha}{\beta})^3$ también lo es. Pero α es la única raíz real y positiva de $X^4 - 2$, así que $(\frac{\alpha}{\beta})^3 = \alpha \in \mathbb{Q}(\frac{\alpha}{\beta})$ y de aquí se sigue inmediatamente que $\mathbb{Q}(\frac{\alpha}{\beta}) = \mathbb{Q}(\alpha, \beta)$.

(b) Como $X^2 - \sqrt{2} \in \mathbb{Q}(\beta)[X]$ (pues $\beta^3 = \sqrt{2}$) y anula a α, entonces $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\beta)] \leq 2$. Veamos que este grado es 2. Si fuese 1, entonces $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\frac{\alpha}{\beta})$ y tenemos la torre de extensiones

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$$

Esto no tiene ningún sentido porque $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ ($X^4 - 2$ es irreducible por Eisenstein), que no divide a $[\mathbb{Q}(\beta) : \mathbb{Q}] = 6$ ($X^6 - 2$ es irreducible por Eisenstein). Por tanto, $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\beta)] = 2$ y entonces $X^2 - \sqrt{2} = \mathrm{Irr}(\alpha, X, \mathbb{Q}(\beta))$.

(c) Un automorfismo $\sigma : \mathbb{Q}(\alpha,\beta) \to \mathbb{Q}(\alpha,\beta)$ debe enviar β en una raíz de $\mathrm{Irr}(\beta, X, \mathbb{Q}(\alpha))$, que es un polinomio de grado $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)] = \frac{[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = 3$. Pero las raíces de este polinomio son β, γ y $\overline{\gamma}$ para algún $\gamma \in \mathbb{C}$, y no puede ser $\gamma \in \mathbb{R}$ porque entonces $\mathrm{Irr}(\beta, X, \mathbb{Q}(\alpha))$, que es separable por ser $\mathbb{Q}$ perfecto, tendría una raíz doble. Como $-\beta \in \mathbb{R}$ y $\beta \neq -\beta$, todo esto nos dice que $-\beta$ no puede ser raíz de $\mathrm{Irr}(\beta, X, \mathbb{Q}(\alpha))$, así que no existe ningún $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$ que envíe β en $-\beta$.

(d) Sea $G = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$ y veamos que $\mathbb{K}^G = \mathbb{Q}(\beta)$. Por el apartado anterior, si $\sigma \in G$, entonces $\sigma(\beta) = \beta$ (no puede ser $\sigma(\beta) = \gamma$ o $\sigma(\beta) = \overline{\gamma}$ porque $\mathbb{Q}(\alpha,\beta) \subset \mathbb{R}$ y $\gamma \in \mathbb{C} \setminus \mathbb{R}$). Esto nos dice que $\mathbb{Q}(\beta) \subset \mathbb{K}^G$. Consideremos la torre de extensiones

$$\mathbb{Q}(\beta) \subset \mathbb{K}^G \subset \mathbb{K}$$

Como $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\beta)] = 2$, entonces solo hay dos posibilidades: $\mathbb{Q}(\beta) = \mathbb{K}^G$ o $\mathbb{K}^G = \mathbb{K}$. La segunda igualdad nos diría que todo elemento de G es el grupo trivial, y esto es imposible porque las raíces de $X^2 - 2 = \mathrm{Irr}(\alpha, X, \mathbb{Q}(\beta))$ son $\alpha, -\alpha \in \mathbb{K}$, así que la aplicación $\sigma : \mathbb{K} \to \mathbb{K}$ determinada por $\sigma(\alpha) = -\alpha$, $\sigma(\beta) = \beta$ es un automorfismo distinto de la identidad. Por tanto, debe ser $\mathbb{Q}(\beta) = \mathbb{K}^G$.

(e) La clausura normal de la extensión, $\mathbb{L}$, es el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $(X^4 - 2)(X^6 - 2)$, cuyas raíces son

$$\sqrt[4]{2},\ -\sqrt[4]{2},\ i\sqrt[4]{2},\ -i\sqrt[4]{2},\ \sqrt[6]{2},\ \xi\sqrt[6]{2},\ \xi^2\sqrt[6]{2},\ \xi^3\sqrt[6]{2},\ \xi^4\sqrt[6]{2},\ \xi^5\sqrt[6]{2}$$

Es claro que $\mathbb{L} = \mathbb{Q}(i, \xi, \sqrt[4]{2}, \sqrt[6]{2})$. Pero

$$\xi = \cos(60^\circ) + i\,\mathrm{sen}(60^\circ) = \frac{1}{2} + i\frac{\sqrt{3}}{2}$$

De aquí se deduce fácilmente que

$$\mathbb{L} = \mathbb{Q}(i, \sqrt{3}, \sqrt[4]{2}, \sqrt[6]{2})$$

(*f*) Se tiene que $[\mathbb{Q}(\sqrt{3}, \sqrt[4]{2}) \colon \mathbb{Q}] = 8$ (tiene que dividir a 4 porque $[\mathbb{Q}(\sqrt[4]{2}) \colon \mathbb{Q}] = 4$; no puede ser 4 porque $\sqrt[4]{2} \notin \mathbb{Q}(\sqrt{3})$, como se prueba fácilmente). Por tanto, como 8 y $[\mathbb{Q}(\sqrt[3]{2}) \colon \mathbb{Q}] = 3$ son coprimos, entonces $[\mathbb{Q}(\sqrt{3}, \sqrt[4]{2}, \sqrt[3]{2}) \colon \mathbb{Q}] = 24$. Y como $\mathbb{Q}(\sqrt{3}, \sqrt[4]{2}, \sqrt[3]{2}) \subset \mathbb{R}$, entonces $[\mathbb{Q}(i, \sqrt{3}, \sqrt[4]{2}, \sqrt[3]{2}) \colon \mathbb{Q}] = 48$.

(*g*) Observamos que la extensión $\mathbb{Q} \subset \mathbb{L}$ es de Galois, luego $G = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{L})$ es de orden $48 = [\mathbb{L} \colon \mathbb{Q}]$, y es soluble porque la extensión $\mathbb{Q} \subset \mathbb{L}$ es claramente radical. Tratamos de encontrar una torre de extensiones

$$\mathbb{Q} \subset \mathbb{E} \subset \mathbb{L}$$

de forma que $\mathbb{Q} \subset \mathbb{E}$ sea de Galois y de grado 12. Por el teorema fundamental, esto es equivalente a encontrar un subgrupo normal H de G de orden 4. Por el primer teorema de Sylow ($|G| = 2^4 \cdot 3$), existe un subgrupo H de orden $2^2 = 4$, y como los grupos de orden 4 son abelianos, H es un subgrupo normal de G. En consecuencia, la extensión $\mathbb{Q} \subset \mathrm{Inv}(H)$ es de Galois. En particular, es primitiva, luego existe $u \in \mathbb{L}$ tal que $\mathrm{Inv}(H) = \mathbb{Q}(u)$ y el polinomio buscado es $f(X) = \mathrm{Irr}(u, X, \mathbb{Q})$.

Veamos que una raíz v de $f(X)$ no es construible con regla y compás. Como la extensión $\mathbb{Q} \subset \mathbb{Q}(u)$ es normal, entonces $v \in \mathbb{Q}(u)$; de hecho, $\mathbb{Q}(u) = \mathbb{Q}(v)$. Además, v es construible con regla y compás si y solo existe una cadena de cuerpos

$$\mathbb{Q} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \ldots \subset \mathbb{F}_s$$

con $v \in \mathbb{F}_s$ y $[\mathbb{F}_k : \mathbb{F}_{k-1}]$, $k \in \{1, 2, \ldots, s\}$. Pero si $v \in \mathbb{F}_s$, entonces tenemos la torre de extensiones

$$\mathbb{Q} \subset \mathbb{Q}(v) \subset \mathbb{F}_s$$

Esto carece de sentido porque $[\mathbb{F}_s \colon \mathbb{Q}]$ es potencia de dos y $[\mathbb{Q}(v) \colon \mathbb{Q}] = 12$ es múltiplo de 3.

(*h*) De nuevo por causa del teorema fundamental, encontrar subgrupos en G de orden 6 es lo mismo que encontrar torres de extensiones $\mathbb{Q} \subset \mathbb{E} \subset \mathbb{L}$ tales que $[\mathbb{E} \colon \mathbb{Q}] = 8$. Hay que encontrar una extensión que sea normal y otra que no lo sea. Para la normal, basta considerar $\mathbb{E} = \mathbb{Q}(i, \sqrt[4]{2})$ (como se comprueba fácilmente), y para la otra, puede escogerse $\mathbb{E}' = \mathbb{Q}(\sqrt{3}, \sqrt[4]{2})$ (como se comprueba aún más fácilmente). Los subgrupos buscados son $\mathrm{Gal}_{\mathbb{E}'}(\mathbb{L})$ y $\mathrm{Gal}_{\mathbb{E}}(\mathbb{L})$.

(*i*) Una raíz primitiva doceava de la unidad es

$$\tau = \cos(30^\circ) + i\,\mathrm{sen}(30^\circ) = \frac{\sqrt{3}}{2} + i\frac{1}{2}$$

Considérese la torre de extensiones

$$\mathbb{Q} \subset \mathbb{Q}(i, \sqrt{3}) \subset \mathbb{L}$$

Como $[\mathbb{Q}(\tau) \colon \mathbb{Q}] = \phi(12) = 4 = [\mathbb{Q}(i, \sqrt{3}) \colon \mathbb{Q}]$ y $\tau \in \mathbb{Q}(i, \sqrt{3})$, entonces $\mathbb{Q}(\tau) = \mathbb{Q}(i, \sqrt{3})$ y tenemos que $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(i, \sqrt{3})) \cong \mathbb{Z}_{12}^*$ y la extensión $\mathbb{Q} \subset \mathbb{Q}(i, \sqrt{3})$ es de Galois. Aplicando el teorema fundamental, $S = \mathrm{Gal}_{\mathbb{Q}(i,\sqrt{3})}(\mathbb{L})$ es un subgrupo normal de G y además

$$\mathbb{Z}_{12}^* \cong \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(i, \sqrt{3})) \cong {}^{G}\!/_{S}$$

(*j*) Como $\mathbb{Q}(i, \sqrt{3}) \not\subset \mathbb{Q}(i, \sqrt[4]{2})$, entonces H_1 no es un subgrupo de S. □