Teoría de Galois

Algunas soluciones e indicaciones a la Hoja 4

Carolina Vallejo Rodríguez

Una extensión E/K se dice de Galois si es normal y separable. Dado $f \in K[x]$, escribimos $E = K(f)$ para denotar al cuerpo de escisión de f sobre K. Por grupo de Galois de f sobre K, entenderemos $G(f) = \mathrm{Gal}(E/K)$.

1. Sea E un cuerpo y $F \subseteq E$ su subcuerpo primo. Demuestra que todo automorfismo de E fija a F, en particular, $\mathrm{Aut}(E) = \mathrm{Gal}(E/F)$.

2. Sea $E = \mathbb{F}_{p^n}$, con p primo y $n \geq 1$, y sea $\varphi \in \mathrm{Aut}(E)$ el automorfismo de Frobenius de E.

a) Prueba que $E/\mathbb{F}_p$ es una extensión de Galois y que $G = \mathrm{Gal}(E/\mathbb{F}_p) = \langle\varphi\rangle$. Por tanto, el grupo de Galois de la extensión $E/\mathbb{F}_p$ es cíclico de orden n.

b) Prueba que para cada divisor d de n, existe un único subcuerpo $\mathbb{F}_p \subseteq L \subseteq E$ de modo que $|L : \mathbb{F}_p| = d$. En particular $L = \mathbb{F}_{p^d}$ (salvo isomorfismo).

c) Sea d un divisor de n y $L = \mathbb{F}_{p^d}$, prueba que $L \subseteq E$ y $\mathrm{Gal}(E/L)$ es cíclico. Da un generador de $\mathrm{Gal}(E/L)$.

Solución. a) Sabemos que E es el cuerpo de escisión del polinomio $x^{p^n} - x \in \mathbb{F}_p[x]$. (De hecho, E es exactamente el conjunto de raíces de este polinomio.) Por tanto, la extensión $E/\mathbb{F}_p$ es normal. Además, $\mathbb{F}_p$ es perfecto por ser finito, luego $E/\mathbb{F}_p$ es separable. Por tanto $E/\mathbb{F}_p$ es de Galois. Como $|E : \mathbb{F}_p| = n$, tenemos que $|\mathrm{Gal}(E/\mathbb{F}_p)| = n$. Por el Teorema del Elemento Primitivo $E = \mathbb{F}_p(\alpha)$. Ahora, sabemos que $\varphi \in \mathrm{Gal}(E/\mathbb{F}_p)$. Sabemos que $\varphi^n(\alpha) = \alpha^{p^n} = \alpha$ (usando que E es exactamente el conjunto de raíces del polinomio $x^{p^n} - x$). Si $\varphi^m(\alpha) = \alpha$ con $m < n$, entonces $\varphi^m = 1|_E$ y eso implicaría que todo elemento de E es solución de $x^{p^m} - x$, y obtendríamos una contradicción porque $|E| = p^n > p^m$ siendo el segundo término el número máximo de raíces del polinomio. Hemos encontrado un elemento en $\mathrm{Gal}(E/\mathbb{F}_p)$ de orden el orden del grupo, esto implica que $\mathrm{Gal}(E/\mathbb{F}_p) = \langle\varphi\rangle$.

b) Como $G = \mathrm{Gal}(E/\mathbb{F}_p)$ es cíclico, tiene un único subgrupo $H \leq G$ de índice $|G : H| = d$. Por el Teorema Fundamental de la Teoría de Galois $L = E^H \subseteq E$ es la única subextensión de $E/\mathbb{F}_p$ de grado d sobre $\mathbb{F}_p$. (Además, como $H \triangleleft G$ se tiene que $L/\mathbb{F}_p$ es normal). Tenemos que $|L : \mathbb{F}_p| = d$ luego $|L| = p^d$ y por la unicidad de los cuerpos finitos $L = \mathbb{F}_{p^d}$ (salvo isomorfismo).

c) Las dos primeras partes del último apartado son consecuencia de los anteriores. Como $E/\mathbb{F}_p$ tiene una subextensión de grado d, entonces E contiene un cuerpo con p^d elementos, que por la unicidad de los cuerpos finitos ha de ser $\mathbb{F}_{p^d}$ (de nuevo, salvo isomorfismo). Además $\mathrm{Gal}(E/L) \leq G$, como los subgrupos de grupos cíclicos son cíclicos, tenemos que $\mathrm{Gal}(E/L)$ tiene un generador, cuyo orden debe ser $|\mathrm{Gal}(E/L)| = |E : L| = n/d$ (aquí estamos usando que E/L es de Galois y el Teorema de Transitividad de Grados). Notamos que $\varphi \in G$ pero φ no fija L elemento a elemento. En cambio, $\varphi^d(a) = a^{p^d}$, y todos los elementos de L son raíces de $x^{p^d} - x$. Por tanto, φ^d fija L elemento a elemento, por tanto, $\varphi^d \in \mathrm{Gal}(E/L)$. Sabemos también (por Teoría de Grupos) que el orden de $\varphi^d \in G$ es exactamente n/d. Si φ^d tuviera orden menor como elemento de $\mathrm{Gal}(E/L)$ llegaríamos a que E tiene menos de p^n (procediendo como en el apartado a)), es decir, a una contradicción. Luego $o(\varphi^d) = n/d$ y, por tanto, $\mathrm{Gal}(E/L) = \langle\varphi^d\rangle$.

3. Demuestra que la extensión $\mathbb{F}_3(t)/\mathbb{F}_3(t^3)$ no es de Galois y que, en cambio, la extensión $\mathbb{C}(t)/\mathbb{C}(t^3)$ sí es de Galois. Calcula el grupo de Galois de ambas extensiones.

4. Sea E/K una extensión finita con grupo de Galois G. Prueba que si $E^G = K$, entonces E/K es de Galois. Es decir, el recíproco del Teorema 4.3 es cierto.

Sugerencia: Dado un $\alpha \in E$ cualquiera, considera $\mathcal{O}_\alpha$ la órbita de α bajo la acción de G y el polinomio $f(x) = \prod_{\beta \in \mathcal{O}_\alpha}(x - \beta)$. Demuestra que $f \in K[x]$ usando el Teorema 4.3 y el hecho de que $\sigma(\mathcal{O}_\alpha) = \mathcal{O}_\alpha$ para todo $\sigma \in G$. Concluye que el polinomio mínimo de α sobre K se escinde en E y todas sus raíces son distintas. Deduce que E/K es separable, por definición, y normal, usando el criterio del Teorema 3.9.

5. Calcula el grupo de Galois de los siguientes polinomios sobre $\mathbb{Q}$:

$$x^{12} - 1,\ x^6 + 1,\ x^4 - 2,\ x^4 + 4x^2 + 2.$$

Solución. Lo primero que hay que hacer en cada caso es calcular el cuerpo de escisión de los polinomios y el grado de la extensión que define sobre $\mathbb{Q}$.

a) Notamos que $x^{12} - 6$ y $x^6 + 1$ tiene el mismo cuerpo de escisión $E = \mathbb{Q}(\sqrt{3}, i)$. Es fácil ver que $|E : \mathbb{Q}| = 4$ y que $G = \mathrm{Gal}(E/\mathbb{Q}) = \langle\sigma\rangle \times \langle\tau\rangle$ donde $\sigma(\sqrt{3}) = \sqrt{3}$, $\sigma(i) = i$ y $\tau(\sqrt{3}) = -\sqrt{3}$ y $\sigma(i) = i$. Es decir, G es un 4-grupo de Klein. Entonces $G = \{1, \sigma, \tau, \sigma\tau\}$ y cada elemento no trivial de G tiene orden 2. G tiene exactamente 5 subgrupos: 1, $\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\sigma\tau\rangle$, G y las subextensiones correspondientes son: $E^1 = E$, $E^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{3})$, $E^{\langle\tau\rangle} = \mathbb{Q}(i)$, $E^{\langle\sigma\tau\rangle} = \mathbb{Q}(\sqrt{3}i)$, E.

b) Sea $E = \mathbb{Q}(x^4 - 2) = \mathbb{Q}(\sqrt[4]{2}, i)$ vimos que $|E : \mathbb{Q}| = 8$. Como $\mathbb{Q}(\sqrt[4]{2})$ define una subextensión no normal, sabemos que $G = \mathrm{Gal}(E/\mathbb{Q})$ tiene un subgrupo no normal (de orden 2, por cierto). Por tanto, $G \cong \mathsf{D}_8$, puesto que es el único grupo de orden 8 que tiene subgrupos no normales. También calculamos todos sus automorfismos y encontramos una presentación de G tipo $\langle a, b \mid a^4 = b^2, a^b = a^{-1}\rangle$. Concretamente $a(\sqrt[4]{2}) = \sqrt[4]{2}i$, $a(i) = i$ y $b(\sqrt[4]{2}) = \sqrt[4]{2}$ y $b(i) = -i$. Con estos generadores podemos describir completamente los elementos de G según $G = \{1, a, a^2, a^3, b, ab, a^b, a^3b\}$. Notamos además que $\mathbf{Z}(G) = \langle a^2\rangle$ (porque conmuta con ambos generadores y es el único elemento no trivial que lo hace). Los subgrupos de G son:

$$1, \langle a^2\rangle, \langle b\rangle, \langle ab\rangle, \langle a^2b\rangle, \langle a^3b\rangle, \langle a\rangle, \langle a^2\rangle \times \langle b\rangle, \langle a^2\rangle \times \langle ab\rangle, G\,.$$

De izquierda a derecha el grupo trivial, 5 subgrupos de orden 2 (solo el primero de ellos normal), 2 subgrupos de orden 4 (normales) y el grupo total. Algunas de las subextensiones las podemos calcular simplemente encontrando elementos fijados que al adjuntarlos nos dan extensiones del grado correspondiente. De este modo podemos calcular:

$$E^{\langle a\rangle} = \mathbb{Q}(i), E^{\langle a^2\rangle} = \mathbb{Q}(\sqrt{2}, i), E^{\langle b\rangle} = \mathbb{Q}(\sqrt[4]{2}), E^{\langle ab\rangle} = \mathbb{Q}(\sqrt[4]{2}i), E^{\langle a^2\rangle\times\langle b\rangle} = \mathbb{Q}(\sqrt{2}) \text{ y } E^{\langle a^2\rangle\times\langle ab\rangle} = \mathbb{Q}(\sqrt{2}i)\,.$$

Por supuesto $E^1 = E$ y $E^G = \mathbb{Q}$. Para calcular $E^{\langle a^2b\rangle}$ y $E^{\langle a^3b\rangle}$ no hay más remedio que plantear los sistemas de ecuaciones asociados con respecto a la $\mathbb{Q}$-base $\{1, \alpha, \alpha^2, \alpha^3, i, \alpha i, \alpha^2 i, \alpha^3 i\}$, donde $\alpha = \sqrt[4]{2}$ y resolverlos.
Nota: Este ejemplo está resuelto con todo lujo de detalles en el capítulo 12 del libro "Galois Theory" de Ian Stewart.

c) Sea $E = \mathbb{Q}(x^4 + 4x^2 + 2)$ vimos que $E = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ donde $\alpha = \sqrt{-2 + \sqrt{2}}$, $\beta = \sqrt{-2 - \sqrt{2}}$ y $\{\pm\alpha, \pm\beta\}$ es el conjunto de raíces de $x^4 + 4x^2 + 2$. Por tanto, obtenemos el cuerpo de esición de este polinomio con solo añadir una cualquiera de sus raíces y $|E : \mathbb{Q}|$. Por tanto, $G = \mathrm{Gal}(E/\mathbb{Q})$ es abeliano y tenemos que distinguir si es isomorfo a un producto directo de dos cíclicos de orden 2 o a un cíclico de orden 4. Vimos que $G = \mathrm{Gal}(E/\mathbb{Q}) = \{1, \sigma, \tau, \gamma\}$ donde $\sigma(\alpha) = -\alpha$, $\tau(\alpha) = \beta$ y $\gamma(\alpha) = -\beta$. Es fácil notar que $o(\sigma) = 2$. Para saber si G es cíclico o un 4-grupo de Klein no hay más remedio que calcular el orden de τ. (Es suficiente porque si su orden es 4, entonces el grupo es cíclico y el orden de γ ha de ser 4 porque C_4 tiene dos generadores, por el mismo motivo, si su orden es 2, el orden de γ también debe ser 2.) Como $\tau^2(\alpha) = \tau(\beta)$, necesitamos calcular una expresión de β como combinación lineal de elementos sobre los que sabemos calcular τ, por ejemplo, en función de $\{1, \alpha, \alpha^2, \alpha^3\}$ (que sabemos es una $\mathbb{Q}$-base de E) o en función de α y α^{-1} (puesto que $\tau(\alpha^{-1}) = \tau(\alpha)^{-1} = \beta^{-1}$). Notamos que $\alpha\beta = \sqrt{2} = \alpha^2 + 2 = -\beta^2 + 2$. Luego, $\beta = \sqrt{2}\alpha^{-1} = (\alpha^2 + 2)\alpha^{-1} = \alpha + 2\alpha^{-1}$ y $\tau(\beta) = \beta + 2\beta^{-1}$. Podemos comprobar con un razonamiento

similar que $\beta + 2\beta^{-1} = -\alpha$ (ya que $\beta^2 + 2 = -\sqrt{2} = -\alpha\beta$). Por tanto $\tau^2 \neq 1_E$, $o(\tau) > 2$ y $o(\tau) = 4$. Hemos probado que $G \cong \mathsf{C}_4$ y podemos notar que $\sigma = \tau^2$ y $\gamma = \tau^3$. Por propiedades de los grupos cíclicos y el Teorema Fundamental de la Teoría de Galois sabemos que $E/\mathbb{Q}$ tiene una única subextensión propia, que es exactamente E^σ. Como $\sigma(\sqrt{2}) = \sigma(\alpha^2 + 2) = \alpha^2 + 2 = \sqrt{2}$ tenemos que $\sqrt{2} \in E^\sigma$, y como $|E^\sigma : \mathbb{Q}| = 2$ podemos concluir que $E^\sigma = \mathbb{Q}(\sqrt{2})$.

6. Sea $f(x) = (x^3 - 2)(x^2 - 3) \in \mathbb{Q}[x]$.

a) Calcula $E = \mathbb{Q}(f)$ y prueba que $L = \mathbb{Q}(\sqrt{3}) \subseteq E$.

b) Calcula el grado de $E/\mathbb{Q}$ y E/L.

c) Calcula $G = \mathrm{Gal}(E/\mathbb{Q})$ y $N = \mathrm{Gal(E/L)}$. ¿Qué relación existe entre estos grupos?

d) Prueba que $G = \langle \sigma, \tau \mid \sigma^6 = \tau^2 = 1,\ \sigma^\tau = \sigma^{-1} \rangle \cong \mathsf{D}_{12}$, y que $N \cong \mathsf{S}_3$.

e) Encuentra una subextensión $\mathbb{Q} \subseteq M \subseteq E$ tal que $G/\mathrm{Gal}(E/M) \cong \mathsf{S}_3$

Indicación.

a) $E = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}, i)$.

b) $|E : \mathbb{Q}| = 12$ y $|E : L| = 6$.

c) $L/\mathbb{Q}$ es una extensión normal luego $N \triangleleft G$.

d) Tenemos que $G \cong \mathsf{D}_{12}$ y $N \cong \mathsf{S}_3$. En el primer caso lo mejor es encontrar una presentación como sugiere el ejercicio, y en el segundo basta notar que N es un grupo de orden 6 no abeliano.

e) Sea $M = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$, sabemos que $\mathrm{Gal}(M/\mathbb{Q}) \cong \mathsf{S}_3$ por el ejemplo de la sección 4.3. Como $M/\mathbb{Q}$ es normal sabemos que $\mathrm{Gal}(E/M) \triangleleft G$ y además, $G/\mathrm{Gal}(E/M) \cong \mathrm{Gal}(M/\mathbb{Q})$.

7. Sea p es un primo y $f(x) = x^p - 1 \in \mathbb{Q}[x]$.

a) Halla $E = \mathbb{Q}(f)$.

b) Prueba que $E/\mathbb{Q}$ es simple de grado $p - 1$.

c) Demuestra que $G = \mathrm{Gal}(E/\mathbb{Q})$ es cíclico encontrando un isomorfismo explícito entre G y $\mathbb{F}_p^\times$.

d) Demuestra que si p es impar, entonces E contiene exactamente una extensión cuadrática de $\mathbb{Q}$ (es decir, una extensión de grado 2 sobre $\mathbb{Q}$).

8. Sea $E = \mathbb{Q}(\xi)$ donde $\xi = e^{\frac{2\pi i}{7}}$. Muestra que E es una extensión de Galois de $\mathbb{Q}$. Encuentra todos los subcuerpos intermedios de la extensión $E/\mathbb{Q}$, los subgrupos de $\mathrm{Gal}(E/\mathbb{Q})$ que les corresponden y determina qué subcuerpos intermedios se corresponden con extensiónes normales de $\mathbb{Q}$.

Solución. Por el ejercicio anterior, que hicimos en clase, sabemos que $G = \mathrm{Gal}(E/\mathbb{Q}) = \{\varphi_1, \ldots, \varphi_6\}$ donde $\varphi_j(\xi) = \xi^j$. Encontrar un generador de G es equivalente a encontrar un generador de $\mathbb{F}_7^\times$. Notamos que $\mathbb{F}_7^\times = \langle 3 \rangle$. Luego $\varphi = \varphi_3$ genera G. Como G es cíclico de orden 6, tiene solo dos subgrupos propios de orden 3 y 2 respectivamente. De hecho, los subgrupos de G son:

$$1, \langle \varphi^2 \rangle = \langle \varphi_2 \rangle, \langle \varphi^3 \rangle = \langle \varphi_6 \rangle, G\,.$$

Por el Teorema Fundamental de la Teoría de Galois los subcuerpos de la extensión son exactamente:

$$E, E^{\varphi_2}, E^{\varphi_6}, E\,.$$

En clase calculamos $E^{\varphi_2} = \mathbb{Q}(\xi + \xi^2 + \xi^4) = \mathbb{Q}(1 + 2(\xi + \xi^2 + \xi^4)) = \mathbb{Q}(\sqrt{-7})$, la última igualdad se sigue de la suma Gaussiana cuya fórmula forma parte de la sugerencia del ejercicio 11. Si no os convence, podéis calcular el valor de α^2 siendo $\alpha = 1 + 2(\xi + \xi^2 + \xi^4)$. Desarrollando vemos que $\alpha^2 = 1 + 8(\xi + \xi^2 + \xi^3 + \xi^4 + \xi^5 + \xi^6)$. Recordando que $\mathrm{Irr}(\mathbb{Q}, \xi) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, concluimos que $\alpha^2 = 1 + 8(-1) = -7$. También comenté que para hallar el valor de $\beta = \xi + \xi^2 + \xi^4$ sin usar la fórmula de Gauss podríais hallar el polinomio

mínimo de β. En este caso, podéis comprobar que $\mathrm{Irr}(\mathbb{Q},\beta) = x^2+x+2$ (hay que hacer los cálculos con mucho cuidado y usar distintas propiedades de las raíces de la unidad) y como β es solución se obtiene que $\beta = \frac{-1\pm\sqrt{-7}}{2}$, y $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{-7})$.

En clase no calculamos E^{φ_6}, pero como $\varphi_6(\xi) = \xi^6 = \xi^{-1}$ y $o(\varphi_6) = 2$, se tiene que $\xi + \xi^{-1} \in E^{\varphi_6}$. Además sabemos que $|E^{\varphi_6} : \mathbb{Q}| = |G : \langle\varphi_6\rangle| = 3$ y resulta que $|\mathbb{Q}(\xi+\xi^{-1}) : \mathbb{Q}| = 3$. En la Hoja 2 Ejercicio 6.c) ya vimos que $|\mathbb{Q}(\xi+\xi^{-1}) : \mathbb{Q}| = \frac{7-1}{2}$, siendo la clave que ξ es solución de un polinomio sobre $\mathbb{Q}(\xi+\xi^{-1})$ de grado 2. A veces, para calcular un cuerpo fijado, basta encontrar elementos fijados de forma que al adjuntarlos obtengamos una extensión del grado correcto. En cualquier caso, planetando un sistema de ecuaciones habríamos llegado al mismo resultado.

9. Halla el cuerpo de escisión E de $f(x) = x^4+x^3+x^2+x+1$ sobre $\mathbb{Q}$.

a) Calcula $G(f) = \mathrm{Gal}(E/\mathbb{Q})$.

b) Describe el retículo de subgrupos de $G(f)$.

c) Halla todas las subextensiones de $E/\mathbb{Q}$ indicando aquellas que se corresponden a extensiones normales de $\mathbb{Q}$.
Extra: Comprueba que $L = \mathbb{Q}(\sqrt{5}) \subseteq E$ y calcula la expresión radical de las soluciones de f.

Indicación. Sabemos que $G(f) \cong \mathbb{F}_5^\times$, luego un generador de $G(f)$ es φ con $\varphi(\omega) = \omega^2$, siendo $\omega = e^{\frac{2\pi i}{5}}$. Por tanto, $E/\mathbb{Q}$ tiene una única subextensión propia de grado 2 sobre $\mathbb{Q}$. Ahora $1/2(\omega+\omega^{-1})/2 = \cos 2\pi/5$, por tanto, ω es raíz del polinomio real $x^2 - 2\cos 2\pi/5 + 1$. Por el ejercicio 6.c) de la Hoja 2 sabemos que $\cos 2\pi/5 \notin \mathbb{Q}$ y que, de hecho, $|\mathbb{Q}(\cos 2\pi/5) : \mathbb{Q}| = 2$, así que $\mathbb{Q}(\cos 2\pi/5)/\mathbb{Q}$ es la única subextensión propia de $E/\mathbb{Q}$.

Para la parte extra, se puede comprobar que $1 + 2(\xi+\xi^4) = \sqrt{5}$ elevando la expresión al cuadrado. De otro modo, podéis notar que si $\alpha = \omega + \omega^4$, entonces ω es raíz de $x^2 - \alpha + 1 \in \mathbb{Q}(\cos 2\pi/5)$. Queremos hallar $\mathrm{Irr}(\mathbb{Q},\alpha)$. Notamos que $\alpha^2 = 2 + (\omega^2+\omega^3) = 1 - \alpha$, usando que $1+\omega+\omega^2+\omega^3+\omega^4 = 0$. De donde $\mathrm{Irr}(\mathbb{Q},\alpha) = x^2+x-1$, obtenemos que $\alpha \in \{\frac{-1\pm\sqrt{5}}{2}\}$. De donde $\mathbb{Q}(\cos 2\pi/5) = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5})$. Ahora, resolviendo $x^2 - \alpha + 1$ con los dos valores de α obtenemos la expresión radical de las raíces de f

$$\{\frac{\alpha \pm \sqrt{\alpha^2-4}}{2}\} = \{\alpha/2 \pm \frac{\sqrt{(2\alpha)^2-16}}{4}\} = \{-1/4 \pm \sqrt{5}/4 \pm \frac{\sqrt{-10\pm\sqrt{5}}}{4}\}.$$

10. Sea ξ una raíz 11-ésima primitiva de la unidad en $\mathbb{C}$.

a) Construye la menor subextensión normal E de $\mathbb{Q}$ que contiene a ξ.

b) Demuestra que $\mathrm{Gal}(E/\mathbb{Q})$ es cíclico. Encuentra un generador y expresa todos los automorfismos en función de este generador.

c) ¿Cuántas subextensiones propias tiene $\mathbb{Q}(\xi)/\mathbb{Q}$? ¿Qué grados tienen?

d) Decide cuáles de los siguientes cuerpos son subextensiones de $E/\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{11}),\ \mathbb{Q}(\sqrt{-11}),\ \mathbb{Q}(i),\ \mathbb{Q}(\sqrt[5]{5}).$$

Recuerda que si p es impar entonces,

$$\sum_{n=0}^{p-1} e^{\frac{2\pi i n^2}{p}} = \begin{cases} \sqrt{p} & \text{si } p \equiv 1 \mod 4 \\ \sqrt{-p} & \text{si } p \equiv 3 \mod 4 \end{cases}$$

Solución. d) $E/\mathbb{Q}$ tiene solo dos subextensiones propias, de grado 2 y 5 sobre $\mathbb{Q}$ respectivamente. La subextensión de grado 2 es $L = E^{\langle\varphi^2\rangle}$ donde $\varphi(\xi) = \xi^3$ (comprobad que φ genera el grupo de Galois en este aso). La subextensión de grado 5 no puede ser $\mathbb{Q}(\sqrt[5]{5})$ porque $\mathbb{Q}(\sqrt[5]{5})/\mathbb{Q}$ no es normal y por el Teorema

Fundamental de la Teoría de Galois se correspondería con un subgrupo no normal de G, lo que es absurdo pues todo subgrupo de G es normal (por ser abeliano).

11. Sea E/K una extensión de Galois con $G = \mathrm{Gal}(E/K)$ cíclico de orden n. Demuestra que:

a) Para cada divisor d de n existe exactamente un cuerpo intermedio L con $|E : L| = d$.

b) Si L_1 y L_2 son dos cuerpos intermedios, entonces $L_1 \subseteq L_2$ si, y solo si, $|E : L_2|$ divide a $|E : L_1|$.

c) Demuestra que la hipótesis E/K de Galois puede relajarse a que E/K sea finita en a).

Indicación. Para los apartados a) y b) la clave es usar el Teorema Fundamental de la Teoría de Galois y propiedades de los grupos cíciclos, concretamente, que para cada divisor del orden de un grupo cíclico (finito) existe un único subgrupo de orden tal divisor. Para el último apartado, considerar el subcuerpo intermedio $F = E^G$. Tenemos que $G = \mathrm{Gal}(E/F)$. Por el ejercicio 4 de esta hoja de problemas, E/F es de Galois con grupo de Galois cíciclo, así que por lo probado en a) para cada divisor de n existe $F \subseteq L \subseteq E$ con $|E : L| = d$ (en particular L/K es una subextensión de E/K).

12. Sea E el cuerpo de descomposición de $f(x) = x^p - 2$ sobre $\mathbb{Q}$, donde p es un primo.

a) Demuestra que $E = \mathbb{Q}(\alpha, \xi)$ donde $\xi^p = 1$, $\xi \neq 1$ y $\alpha^p = 2$.

b) Demuestra que $|E : \mathbb{Q}| = p(p-1)$.

c) Sea $H = \{\begin{pmatrix} 1 & c \\ 0 & d \end{pmatrix} \mid d \in \mathbb{F}_p^\times, c \in \mathbb{F}_p\} \leq \mathrm{GL}(2, p)$. Prueba que $\mathrm{Gal}(E/\mathbb{Q}) \cong H$.

d) Si $p = 5$, encuentra los subcuerpos de E fijados por los subgrupos de $\mathrm{Gal}(E/\mathbb{Q})$.

Indicación. d) Sea $G = \mathrm{Gal}(E/\mathbb{Q})$, sabemos que $|G| = 20$, además

$$G \cong H = \{\begin{pmatrix} 1 & c \\ 0 & d \end{pmatrix} \mid d \in \mathbb{F}_5^\times, c \in \mathbb{F}_5\} = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \rangle .$$

Aquí usamos que $\langle 2 \rangle = \mathbb{F}_5^\times$ y $\langle 1 \rangle = \mathbb{F}_5$. Sean $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ y $b = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, se puede comprobar que $G \cong \langle a, b \mid a^5 = b^4 = 1, a^b = a^2 \rangle$. Una razón por la cual la única relación que necesitamos conocer es a^b se deriva del Teorema Fundamental de la Teoría de Galois. La extensión $E/\mathbb{Q}$ contiene a $\mathbb{Q}(\xi)$ donde $1 \neq \xi$ y $\xi^5 = 1$ que es normal sobre $\mathbb{Q}$ y de grado 4. Por tanto, se corresponde con un subgrupo normal $P \triangleleft G$ de índice 4. Es decir, P tiene orden 5, y es el único subgrupo de orden 5 de G, además, bajo el isomorfismo con H, el grupo $P = \mathrm{Gal}(E/\mathbb{Q}(\xi))$ se corresponde con $\langle a \rangle$. Como $H = \langle a \rangle \langle b \rangle$ (simplemente calculando cardinales) tenemos que, de hecho, $H = \langle a \rangle \rtimes \langle b \rangle$ y basta especificar a^b para determinar completamente este producto semidirecto.

13. Sea $f(x) = x^{12} - 3 \in \mathbb{Q}[x]$. Considera el cuerpo de escisión E de f sobre $\mathbb{Q}$.

a) Calcula $|E : \mathbb{Q}|$.

b) Prueba que $\mathrm{Ł} = \mathbb{Q}(i) \subseteq E$ y, por tanto, E es el cuerpo de escisión de f sobre L.

c) Prueba que E/L es una extensión simple y concluye que f es irreducible sobre L.

d) Demuestra que $G = \mathrm{Gal}(E/L)$ tiene una presentación de la forma

$$\langle \tau, \sigma |\ \tau^6 = 1, \sigma^2 = \tau^3, \sigma^{-1}\tau\sigma = \tau^{-1} \rangle .$$

e) Calcula todas las subextensiones de E/L grado 3 y 4 sobre L.

Solución. (a) Sea $\alpha = \sqrt[12]{3} \in \mathbb{R}_{>0}$ y sea $\xi = i\omega$ donde $\omega = e^{2\pi/3} = \frac{1}{2}(1 + \sqrt{3}i)$. Notar que ξ es una raíz primitiva duodécima de la unidad. Como E es el cuerpo de escisión de $x^{12} - 3$ sobre $L = \mathbb{Q}(i)$, E

el cuerpo que se obtiene al adjuntar todas las raíces de $x^{12}-3$ a $L=\mathbb{Q}(i)$. Las raíces de $x^{12}-3$ son $\{\pm\alpha, \pm\alpha i, \pm\alpha\omega, \pm\alpha\omega^2, \pm\alpha\omega i, \pm\alpha\omega^2 i\}$. Notamos que tanto ω como i pertenecen a E. En particular, E es también el cuerpo de escisión sobre $\mathbb{Q}$ de $x^{12}-3$. De hecho, $E=\mathbb{Q}(\alpha,\xi)=\mathbb{Q}(\alpha)(\xi)=\mathbb{Q}(\alpha)(i)=L(\alpha)$. Para justificar la segunda igualdad tengamos en cuenta lo siguiente, $\xi=i\omega=1/2(i-\sqrt{3})\in\mathbb{Q}(\alpha,i)$ puesto que $\alpha^6=\sqrt{3}$. Por otro lado, $\xi^3=i^3\omega^3=-i$, por tanto $i\in\mathbb{Q}(\alpha,\xi)$.

Por el criterio de Einsestein $|\mathbb{Q}(\alpha):\mathbb{Q}|=12$. Por la transitividad de grados

$$|E:\mathbb{Q}|=|E:\mathbb{Q}(\alpha)||\mathbb{Q}(\alpha):\mathbb{Q}|.$$

Como $\mathbb{Q}(\alpha)\subseteq\mathbb{R}$, tenemos que $\mathbb{Q}(\alpha)$ está estrictamente contenido en $E=\mathbb{Q}(\alpha)(i)$. Además el polinomio x^2+1 no tiene raíces en $\mathbb{Q}(\alpha)$. En consecuencia $|E:\mathbb{Q}(\alpha)|=2$. Por tanto, $|E:\mathbb{Q}|=24$. Aplicando de nuevo la transitividad de grados $|E:L|=|E:\mathbb{Q}|/|L:\mathbb{Q}|=12$. En particular, $f=\mathrm{Irr}(L,\alpha)$.

(b) Sabemos que $E=L(\alpha)$, es decir, E es una extensión simple de L. En consecuencia, cada $\tau\in\mathrm{Gal}(E/L)=G$ queda determinado por su imagen sobre α y por el hecho de fijar elemento a elemento al cuerpo $L=\mathbb{Q}(i)$. Tenemos que $\omega=1/2(1-\alpha^6 i)$. Como E/L es Galois sabemos que $|G|=12$. Los 12 elementos de G, como ya hemos mencionado, quedan determinados por las 12 posibles imágenes de α, pues como $x^{12}-3$ es irreducible sobre L, para cada raíz β del polinomio, existe un $\tau\in G$ de modo que $\tau(\alpha)=\beta$. Podemos escribir la información relevante de $\mathrm{Gal}(E/L)$ en una tabla.

$\mathrm{Gal}(E/L)$	α	β	orden
$\tau_1=1_E$	α	ω	1
τ_2	$-\alpha$	ω	2
τ_3	αi	ω^2	4
τ_4	$-\alpha i$	ω^2	4
τ_5	$\alpha\omega$	ω	3
τ_6	$-\alpha\omega$	ω	6
τ_7	$\alpha\omega^2$	ω	3
τ_8	$-\alpha\omega^2$	ω	6
τ_9	$\alpha\omega i$	ω^2	4
τ_{10}	$-\alpha\omega i$	ω^2	4
τ_{11}	$\alpha\omega^2 i$	ω^2	4
τ_{12}	$-\alpha\omega^2 i$	ω^2	4

Si escribimos $\tau=\tau_6$ y $\sigma=\tau_3$. Es rutina comprobar que $\tau^3=\sigma^2$ y $\tau^\sigma=\tau^5=\tau^{-1}$.
Para ver que τ y σ generan G se puede comprobar que cada τ_j se puede obtener como producto de potencias de τ y σ. Otra forma de verlo es la siguiente: Sabemos que $|G|_3=3$, como G solo tiene dos elementos de orden 3, entonces G tiene un único subgrupo $Q=\langle\tau_5\rangle$ de orden 3. Sea $H=\langle\tau,\sigma\rangle\leq G$. En particular $Q\leq H$. Ahora H tiene un subgrupo P de orden 4 (generado por σ), por tanto, $H=QP$ y $Q\cap P=1$ implica que $|H|=|Q||P|=12$ divide $|G|=12$. Concluimos que $H=G$.

Sea $Q\in\mathrm{Syl}_3(G)$, sabemos que $Q\lhd G$. Si $P\in\mathrm{Syl}_2(G)$, entonces $G=QP$ con $Q\cap P=1$. Es decir, $G\cong Q\rtimes P$. Como G tiene elementos de orden 4 y $|P|=4$ concluimos que $P\cong\mathsf{C}_4$. Ahora bien $P/\mathbf{C}_P(Q)\leq\mathrm{Aut}(Q)\cong C_2$. Como P no es normal (si lo fuera habría solo 4 elementos de orden potencia de 2), sabemos que la acción de P sobre Q no es trivial. Entonces $P/\mathbf{C}_P(Q)\cong\mathsf{C}_2$. Como $Q\lhd G$, entonces $\mathsf{C}_2\cong\mathbf{C}_P(Q)\lhd G$. En particular, $\mathbf{C}_P(Q)=\mathbf{Z}(G)$ y $G/\mathbf{Z}(G)\cong\mathsf{S}_3$. Existen 5 clases de isomorfía de grupos de orden 12, G es isomorfo al producto semidirecto de C_3 con C_4 respecto a la única acción no trivial de C_4 sobre C_3.

Los apartados (c) y (d) piden encontrar subextensiones de L de un cierto grado. Podemos obtener el número de subextensiones $L\subseteq K\subseteq E$ de grado 3 y 4 sobre L de forma indirecta usando Teoría de Grupos (si queremos describirlas exactamente habrá que realizar la rutina habitual). Por el Teorema Fundamental de la Teoría de Galois y la transitividad de grados

$$\#\{L\subseteq K\subseteq E\mid |K:L|=3\}=\#\{H\leq G\,||H|=4\}$$

es el número de 2-subgrupos de Sylow, es decir, $|\mathrm{Syl}_2(G)| = |G : \mathbf{N}_G(P)|$. Como hay más de 4 elementos de orden potencia de 2 en G, tenemos que $\mathbf{N}_G(P) < G$ y en consecuencia $\mathbf{N}_G(P) = P$ ya que $|G : P| = 3$. Hay tres extensiones de L en E de grado 3 sobre L que se corresponden con los cuerpos fijados por cada uno de los tres 2-subgrupos de Sylow de G. De forma similar

$$\#\{L \subseteq K \subseteq E \mid |K : L| = 4\} = \#\{H \geq G \,||H| = 3\} = 1\,,$$

porque ya hemos mencionado que G tiene un 3-Sylow normal, y, por tanto, único. Existe una única extensión de L contenida en E de grado 4 sobre L, que se corresponde con el cuerpo fijado por el 3-subgrupo de Sylow de G.

Por los comentarios anteriores sabemos que G tiene 3 subgrupos de orden 4, todos ellos son conjugados y, por tanto, cíclicos (pues G tiene elementos de orden 4). Es fácil ver que $H_1 = \langle \tau_3 \rangle = \langle \tau_4 \rangle$, $H_2 = \langle \tau_9 \rangle = \langle \tau_{10} \rangle$, $H_2 = \langle \tau_{11} \rangle = \langle \tau_{12} \rangle$ son los 3 subgrupos de orden 4 de G. Por el Teorema Fundamental de la Teoría de Galois (la parte consecuencia del Teorema de Artin) $|E : E^{H_j}| = 4$ para $1 \leq j \leq 3$, por tanto, $|E^{H_j} : L| = 3$ para $1 \leq j \leq 3$. El método consiste en escribir los elementos de E en la base dada por el Teorema del elemento algebraico, es decir, $\{1, \alpha, \ldots, \alpha^{11}\}$ y ver qué expresión tienen los elementos fijados por τ_3, τ_9 y τ_{11} respectivamente. Como H_1, H_2 y H_3 son conjugados, bastará realizar este proceso una vez y luego conjugar.

Tenemos que $K_1 = E^{H_1} = L(\beta)$ donde $\beta = \alpha^4 = \sqrt[3]{3}$. Comprobar que $x = \sum_{j=0}^{11} a_j \alpha^j \in E$ satisface $\tau_3(x) = x$ si, y sólo si, $a_j = 0$ siempre que $j \equiv 1, 2, 3 \mod 4$, si, y sólo si, $x = a + b\alpha^4 + c\alpha^8$. Notar que $\alpha^4 = \sqrt[3]{3}$ es raíz del polinomio $x^3 - 3$ irreducible sobre L. Usando el resultado de conjugación en subgrupos de un grupo de Galois, podemos obtener el resto de subextensiones de grado 3 sobre L como sigue:

$$K_2 = E^{H_2} = E^{H_1^{\tau_{11}}} = \tau_{11}(K_1) = \mathbb{Q}(i)(\alpha^4\omega^2)\,,$$
$$K_3 = E^{H_3} = E^{H_1^{\tau_9}} = \tau_9(K_1) = \mathbb{Q}(i)(\alpha^4\omega)\,.$$

Los subcuerpos K_1, K_2 y K_3 definen las dos extensiones simples de $\mathbb{Q}(i)$ que se obtienen al adjuntar las distintas raíces del polinomio $x^3 + 3$ (irreducible sobre L por no tener raíces en L).

También podríamos darnos cuenta de que $L(\sqrt[3]{3})$ define una extensión de grado 3 sobre L contenida en E. Por tanto, ha de corresponder con el cuerpo fijado por algún 2-subgrupo de Sylow. Y luego el resto de extensiones de grao 3 sobre L se pueden obetener aplicando los distintos elementos de G a $L(\sqrt[3]{3})$. (Esta forma sirve si no nos piden decir a qué subgrupo se corresponde cada subextensión, aunque también podríamos hacer estos cálculos *a posteriori*.)

Por la discusión del apartado anterior y el párrafo que lo precede, tenemos que calcular $E^{\langle \tau_5 \rangle}$. Notamos que $\tau_5(\alpha^3) = \alpha^3$, luego $L(\alpha^3) = L(\sqrt[4]{3}) \subseteq E^{\tau_5}$, como además $|L(\sqrt[4]{3}) : L| = 4$ (aquí debemos probar que $x^4 - 3$ es irreducible sobre L) tenemos que $E^{\tau_5} = L(\alpha^3) = L(\sqrt[4]{3})$. (Si probamos directamente que $E^{\tau_5} = L(\alpha^3) = L(\sqrt[4]{3})$, que no es difícil, obtenemos como conclusión que $x^4 - 3$ es irreducible sobre L.)

También podríamos haber realizado este ejercicio tomando como raíz duodécima de la unidad $\eta = 1/2i + \sqrt{3}/2$. *La idea es que conociendo una raíz cuarta y una raíz cúbica de la unidad, tenemos una raíz duodécima sin necesidad de aprendernos de memoria su expresión; pero una buena manera de ver que entendéis el ejercicio es hacer todos los cálculos con respecto a* η.

14. * Sea $p(x) = x^4 - 2x^2 + 2 \in \mathbb{Q}[x]$ y $E = \mathbb{Q}(f)$.

a) Calcula el grado de $E/\mathbb{Q}$.

b) Describe el grupo de Galois de la extensión $E/\mathbb{Q}$ y determina su clase de isomorfía.

c) Encuentra todas las subextensiones de $E/\mathbb{Q}$ grado 4 sobre $\mathbb{Q}$.

Solución. Las raíces de p son $\{\pm\sqrt{1 \pm i}\}$. Notamos que p es irreducible por el criterio de Einsestein. Sean $\alpha = \sqrt{1+i}$ y $\beta = \sqrt{1-i}$. Entonces $\alpha\beta = \sqrt{2}$. La clave está en encontrar una forma manejable de describir

$E = \mathbb{Q}(\pm\sqrt{1 \pm i})$. Por ejemplo, notamos que $\sqrt{2} \in E$ y $\beta = \sqrt{2}\alpha^{-1} \in \mathbb{Q}(\alpha, \sqrt{2})$. Con esto ya podemos concluir que $E = \mathbb{Q}(\sqrt{2}, \alpha) = \mathbb{Q}(\sqrt{2}, \beta)$. La gran dificultad del ejercicio es calcular $|E : \mathbb{Q}|$. Para ello, podemos usar una extensión intermedia y el Teorema de Transitividad de Grados. Por ejemplo, notamos que $i \in E$. Por tanto, $L = \mathbb{Q}(\sqrt{2}, i) \subseteq E$. Además $|L : \mathbb{Q}| = 4$, de hecho, sabemos que $L/\mathbb{Q}$ es de Galois con $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathsf{C}_2 \times \mathsf{C}_2$. Ahora $\alpha^2 = 1 + i \in L$. Luego el polinomio irreducible de α sobre L divide a $x^2 - (1+i)$. Veamos que $\alpha \notin L$. Supongamos que $\alpha \in L$ por reducción al absurdo. Entonces $\mathbb{Q}(\alpha) = L = E$. Ahora bien, $\mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$ con $\sigma\tau = \tau\sigma$ y cada uno de los automorfismos no triviales de orden 2. Como p es irreducible, dadas dos raíces existe un automorfismo que nos lleva una en otra, por ejemplo $\tau(\alpha) = \beta$ y $\sigma(\alpha) = -\alpha$. La restricción $\sigma\tau = \tau\sigma$ implica que $\sigma(\beta) = -\beta$. Entonces la tabla de $\mathrm{Gal}(L/\mathbb{Q})$ tiene que ser de la forma

$\mathrm{Gal}(L/\mathbb{Q})$	α	β
1_L	α	β
τ	β	α
σ	$-\alpha$	$-\beta$
$\tau\sigma$	$-\beta$	$-\alpha$

Sabemos que $L^{\mathrm{Gal}(L/\mathbb{Q})} = \mathbb{Q}$ porque $L/\mathbb{Q}$ es de Galois, pero podemos ver que todos los automorfismos de L fijan $\alpha\beta = \sqrt{2}$, lo que es absurdo. Por tanto, concluimos que $\alpha \notin L$. Por tanto $L \neq E$ y $|E : \mathbb{Q}| = |E : L||L : \mathbb{Q}| = 8$. Notad que además hemos probado que $\mathbb{Q}(\alpha) \subseteq E$ no es normal sobre $\mathbb{Q}$, por tanto, $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathsf{D}_8$. Ya sabéis la clase de isomorfía, faltaría describir el grupo completamente, lo podéis hacer describiendo las imágenes de α y β por los distintos automorfismos, y usando que $\alpha\beta = \sqrt{2}$ para calcular los órdenes.

15. Sea $f = (x^2 - p)(x^2 - q) \in \mathbb{Q}[x]$ donde $p \neq q$ son primos. Determina la clase de isomorfía de $\mathrm{Gal}(f)$.
Indicación. Es fácil notar que $\mathrm{Gal}(f) \cong \mathsf{C}_2 \times \mathsf{C}_2$ puesto que $\mathbb{Q}(f)/\mathbb{Q}$ tiene más de una subextensión propia.

16. Sea $f(x) = x^4 + ax^2 + b$ un polinomio irreducible sobre K donde $\mathbb{Q} \subseteq K$, y sea $G = \mathrm{Gal}(f)$ su grupo de Galois. Demuestra que:

a) Si b es el cuadrado de un elemento de K, entonces $G \cong \mathsf{C}_2 \times \mathsf{C}_2$.

b) Si b no es el cuadrado de ningún elemento de K pero $b(a^2 - 4b)$ sí lo es, entonces $G \cong \mathsf{C}_4$.

17. Sea E/K una extensión de Galois con $\mathrm{Gal}(E/K) \cong \mathsf{C}_2 \times \mathsf{C}_2$ y $\mathrm{car}(K) \neq 2$. Probar que existen $a, b \in E$ tales que $E = K(a, b)$ con $a^2, b^2 \in K$.

18. Sea f un polinomio irreducible sobre $\mathbb{Q}$ cuyo grupo de Galois es abeliano y u una raíz de f en $\mathbb{C}$. Demuestra que el grado de f es primo si, y solo si, no hay extensiones intermedias entre $\mathbb{Q}$ y $\mathbb{Q}(u)$.
Solución. Sea $G = \mathrm{Gal}(f)$ abeliano por hipótesis. Tenemos que $\mathbb{Q} \subseteq \mathbb{Q}(u) \subseteq \mathbb{Q}(f)$ y $H = \mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}(u)) \triangleleft G$, por tanto, $\mathbb{Q}(u)/\mathbb{Q}$ es normal y tenemos que f se escinde en $\mathbb{Q}(u)$. Luego $\mathbb{Q}(f) = \mathbb{Q}(u)$. Además $|G| = |\mathbb{Q}(u) : \mathbb{Q}| = \delta(f)$. Ahora hay que recordar que $\mathbb{Q}(u)/\mathbb{Q}$ no tiene extensiones intermedias si, y solo si, G no tiene subgrupos propios si, y solo si, G es cíclico de orden primo.

19. Sea E/K una extensión de Galois, sea F/K una subextensión y sea $a \in F$. Demuestra que $F = K(a)$ si, y solo si, los elementos de $\mathrm{Gal}(E/K)$ que fijan a son exactamente $\mathrm{Gal}(E/F)$. Utilizando este resultado demuestra que:

a) $\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}) = \mathbb{Q}(\sqrt[3]{5} + \sqrt{5})$;

b) El cuerpo de escisión de $x^6 - 3x^3 + 2$ es $\mathbb{Q}(\sqrt[3]{2} + 2\sqrt{-3})$.

Sugerencia: usa el Teorema 4.3. aplicado a E/F que es de Galois. ¿Cómo sabes que un elemento pertenece a F?