Teoría de Galois

Hoja 5. Aplicaciones: Gran Teorema de Galois

1. Decimos que una extensión E/K es abeliana si E/K es de Galois y $\mathrm{Gal}(E/K)$ es un grupo abeliano. Demuestra que si E/K es abeliana y $K \subseteq L \subseteq E$ es un subcuerpo intermedio, entonces E/L y L/K son abelianas.

Solución. Como $H = \mathrm{Gal}(E/L) \leq G = \mathrm{Gal}(E/K)$ y G es abeliano, tenemos que $H \triangleleft G$ y tanto H como G/H son abelianos. En particular, E/L es de Galois con grupo de Galois H abeliano, luego E/L es abeliana.

Ahora, $H \triangleleft G$ implica por el Teorema Fundamental de la Teoría de Galois que $E^H = L$ define una extensión normal sobre K. En particular L/K es de Galois. También se tiene que $G/H \cong \mathrm{Gal}(L/K)$ es abeliano, luego L/K también es abeliana.

2. Sea E/K una extensión de Galois y $K \subseteq L, M \subseteq E$ subcuerpos intermedios. Se define $\langle L, M\rangle$ como la intersección de todos los subcuerpos de E que contienen a L y M. Prueba que

$$\mathrm{Gal}(E/L) \cap \mathrm{Gal}(E/M) = \mathrm{Gal}(E/\langle L, M\rangle).$$

3. Sea E/K de Galois y sean $K \subseteq L, M \subseteq E$ subcuerpos intermedios. Prueba que $L \subseteq M$ si, y solo si, $\mathrm{Gal}(E/M) \subseteq \mathrm{Gal}(E/L)$.

Sugerencia: La implicación directa se sigue de la definición de grupo de Galois de una extensión. Para el recíproco, nota que por el Teorema Fundamental de la Teoría de Galois basta probar que $\mathrm{Gal}(E/M) = \mathrm{Gal}(E/\langle L, M\rangle)$*, ya que la inyectividad de f en el Teorema Fundamental de la Teoría de Galois implica que $M = \langle L, M\rangle$ que contiene a L por definición. Usa el ejercicio 2.*

4. (Irracionalidades Naturales) Sea E/K y sean $K \subseteq L, M \subseteq E$ subcuerpos intermedios. Supongamos que $E = \langle L, M\rangle$ y sea $F = L \cap M$. Si M/K es de Galois, entonces E/L es de Galois y la restricción $\mathrm{Gal}(E/L) \to \mathrm{Gal}(M/F)$ es un isomorfismo de grupos.

Sugerencia: Prueba que E/L es de Galois. La restricción $\Theta\colon \mathrm{Gal}(E/L) \to \mathrm{Gal}(M/F)$ definida por $\tau \mapsto \tau_M$ es un homomorfismo de grupos, usando que M/F es una subextensión normal de E/F. Demuestra que Θ es inyectiva y sobreyectiva usando el ejercicio 2 y el Teorema Fundamental de la Teoría de Galois.

5. Sea $\xi \in \mathbb{C}$ es una raíz primitiva n-ésima de la unidad, y $\mathbb{Q}(\xi)/\mathbb{Q}$ la n-ésima extensión ciclotómica de $\mathbb{Q}$.

a) Demuestra que $\mathbb{Q}(\xi)/\mathbb{Q}$ es una extensión abeliana.

b) Nota que el apartados anterior sigue siendo cierto si sustituimos $\mathbb{Q}$ por K con $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$.

c) ¿Es $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ siempre cíclico?

Solución. a) Es fácil ver que $\mathbb{Q}(\xi) = \mathbb{Q}(x^n - 1)$, pues ξ genera todas las raíces n-ésimas de la unidad. Por tanto, $\mathbb{Q}(\xi)$ es el cuerpo de escisión de un polinomio racional, y $\mathbb{Q}(\xi)/\mathbb{Q}$ es de Galois. Además, un $\tau \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ queda completamente determinado por $\tau(\xi)$. Como $\tau(\xi)$ tiene que ir a otra raíz de $x^n - 1$ (del mismo orden que ξ), necesariamente $\tau(\xi) = \xi^j$ con $1 \leq j \leq n$ y $(k, n) = 1$. (En particular esto nos define un monomorfismo de grupos $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \to \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$.) Escribimos τ_j para denotar tal elemento del grupo de Galois. Entonces $\tau_j\tau_k = \tau_k\tau_j$ (porque $\xi^{jk} = \xi^{kj}$) para todo par $\tau_j, \tau_k \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$. El apartado b) se demuestra de forma similar. Para el apartado c) recordad que $\mathrm{Gal}(\mathbb{Q}(\xi_{12})/\mathbb{Q}) \cong \mathsf{C}_2 \times \mathsf{C}_2$, donde ξ es una raíz duocécima de la unidad.

6. Sea $\omega \in \mathbb{C}$ una raíz primitiva novena de la unidad y $E = \mathbb{Q}(\omega)$.

a) Calcula el polinomio mínimo de ω sobre $\mathbb{Q}$.

b) Encuentra todas las subextensiones de $E/\mathbb{Q}$.

c) Determina las órbitas que la acción de $\mathrm{Gal}(E/\mathbb{Q})$ define sobre las raíces novenas de la unidad.

Solución. a) Sabemos que ω satisface $\omega^9 = 1$, por tanto, es raíz del polinomio $x^9 - 1$. Por otro lado, todas las raíces cúbicas de la unidad son raíces novenas, luego $x^3 - 1$ divide a $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$. Por tanto, $\mathrm{Irr}(\mathbb{Q}, \omega)$ divide a $x^6 + x^3 + 1$. Queremos ver ahora que , $\mathrm{Irr}(\mathbb{Q}, \omega) = x^6 + x^3 + 1$. Sin conocer previamente el grado de la extensión $|E : \mathbb{Q}|$ lo mejor es probar que $f(x) = x^6 + x^3 + 1$ es irreducible usando el criterio de Einsestein sobre $f(x + 1)$, por ejemplo.

Podríamos pensar en que $\sigma(\omega) = \omega^2$ tiene "orden" 6 en $\mathrm{Gal}(E/\mathbb{Q})$. El problema aquí es justificar que σ define un automorfismo de E, si ω y ω^2 son raíces del mismo polinomio irreducible, entonces sabemos que σ define un automorfismo, pero como no lo sabemos a priori, deberíamos probarlo a mano, y podéis corroborar que es un trabajo de lo más pesado (y quizá infructuoso).

Siguiendo esta idea, lo que sí podemos notar es que $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^2)$ pues ambas son raíces primitivas novenas. Luego sus polinomios irreducibles sobre $\mathbb{Q}$ han de tener el mismo grado y ser divisores de x^6+x^3+1, esto nos permite concluir que si este polinomio se descompone sobre $\mathbb{Q}$, lo hará como producto de dos polinomios cúbicos o tres polinomios cuadráticos. En el primer caso $|\mathbb{Q}(\omega) : \mathbb{Q}| = 3$ (pues $x^6 + x^3 + 1$ no tien raíces en $\mathbb{Q}$) pero $\mathbb{Q}(\omega^3) \subseteq \mathbb{Q}(\omega)$ tiene grado 2, lo que es imposible por la transitividad de grados. Así que nos queda el caso en que $x^6 + x^3 + 1$ se descompone como producto de 3 polinomios irreducibles de grado 2, en este caso $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^3)$. Sea $\eta = \omega^3$, entonces $\omega = a + b\eta$ con $a, b \in \mathbb{Q}$; pero $|\omega| = 1 = |a + b\eta| = \sqrt{(a + b\eta)(a + b\overline{\eta})} = \sqrt{a^2 + b^2 - ab}$. Es decir, $a^2 + b^2 - ab = (a - b)^2 + ab = 1$ con $a, b \in \mathbb{Q}$, una contradicción.

b) Una vez sabemos que $|E : \mathbb{Q}| = 6$, el resto del ejercicio es fácil. Por el ejercicio anterior $G = \mathrm{Gal}(E/\mathbb{Q})$ es abeliano, luego $G \cong \mathsf{C}_6$. De hecho, como $\{\omega, \omega^2, \omega^4, \omega^5, \omega^7, \omega^8\}$ son las raíces de $x^6 + x^3 + 1$ que es irreducible, podemos describir todos los automorfismos de G y ver que $G = \langle\sigma\rangle$ con $\sigma(\omega) = \omega^2$. (Ahora sí, una resultado de teoría nos garantiza que σ es un automorfismo de E.) Por el Teorema Fundamental de la Teoría de Galois, $E/\mathbb{Q}$ tiene dos subextensiones propias de grados 2 y 3 sobre $\mathbb{Q}$. La de grado 2 es $K = \mathbb{Q}(\omega^2)$, la de grado 3 es $L = \mathbb{Q}(\omega + \omega^{-1}) = \mathbb{Q}(\cos 2\pi/9) \subseteq \mathbb{R}$. El hecho de que $|L : \mathbb{Q}| = 3$, se sigue de que ω es raíz del polinomio $x^2 - (\omega + \omega^{-1})x + 1 \in L[x]$ que es irreducible sobre L, luego $|E : L| = 2$. La conclusión se obtiene aplicando la transitividad de grados.

c) Es fácil una vez conocido G.

7. Prueba que la extensión $\mathbb{Q}(\sqrt{2 + \sqrt{2}}, \sqrt[3]{3}i)/\mathbb{Q}$ es radical.

Solución. Tenemos que $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2 + \sqrt{2}}) \subseteq \mathbb{Q}(\sqrt{2 + \sqrt{2}})(\sqrt[3]{3}i) = \mathbb{Q}(\sqrt{2 + \sqrt{2}}, \sqrt[3]{3}i)$ de modo que $(\sqrt{2})^2 \in \mathbb{Q}$, $(\sqrt{2 + \sqrt{2}})^2 \in \mathbb{Q}(\sqrt{2})$ y $(\sqrt[3]{3}i)^3 \in \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2 + \sqrt{2}})$.

8. Sea G un grupo finito.

a) Si G es resoluble y $H \leq G$, entonces H es resoluble.

b) Si $N \lhd G$, entonces G es resoluble si, y solo si, G/N y N son resolubles.

9. Sea G un grupo finito. Demuestra que G es resoluble si, y solo si, existe una serie $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_{k-1} \lhd G_k = G$ tal que G_j/G_{j-1} es cíclico de orden primo para cada $j \in \{1, \ldots, k\}$.
Sugerencia: Para la implicación directa nota que si A es abeliano existe tal serie con cocientes cíclicos de orden primo, y luego refina una serie normal con cocientes abelianos de G usando la misma idea. El recíproco es obvio porque los cocientes cíclicos son, en particular, abelianos.

10. Demuestra que S_4 es resoluble. Demuestra que S_n no es resoluble para todo $n \geq 5$.

11. Decide si los siguientes enunciados son verdaderos o falsos:

a) Si R/K es radical, entonces R/K es separable.

b) Si R/K es radical, entonces R/K es normal.

Soución. Los dos enunciados son falsos. Para a) considerad la extensión $\mathbb{F}_3(t)/\mathbb{F}_3(t^3)$. Para b) podéis considerar las extensiones $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ o $\mathbb{Q}(\sqrt{1+\sqrt{7}})/\mathbb{Q}$ (y tantas otras).

Nota. Recordad que f es resoluble por radicales si su cuerpo de escisión está **contenido** en una extensión radical. Podríais pensar por qué decimos contenido y no directamente que defina una extensión radical. La respuesta es que, en general, el cuerpo de escisión de un polinomio resoluble por radicales no define una extensión radical. Desafortunadamente, para probarlo, necesitaríamos haber tenido más horas de clase. Por ejemplo, el polinomio $x^3 - 3x + 1 \in \mathbb{Q}[x]$ es irreducible y resoluble por radicales. Todas sus raíces son reales. Se puede probar que si α es una de esas raíces entonces $\mathbb{Q}(\alpha)$ es el cuerpo de escisión de f, y que la extesión $\mathbb{Q}(\alpha)/\mathbb{Q}$ no es radical. Podéis consultar el libro *Fields and Galois Theory* de Patrick Morandi (pp. 149–152).

12. Sea $f \in \mathbb{Q}[x]$ de grado 5. Demuestra que si f es resoluble por radicales, entonces $|\mathrm{Gal}(f)| \leq 24$.

13. Sea p un primo y sea $f \in \mathbb{Q}[x]$ un polinomio irreducible de grado p. Supongamos que f tiene exactamente dos raíces no reales en $\mathbb{C}$. Demuestra que entonces $\mathrm{Gal}(f) \cong \mathsf{S}_p$.
Sugerencia: Utiliza que S_p *está generado por las permutaciones* (12) *y* $(12\dots p)$.

14. Demuestra que el polinomio $x^5 - 6x + 3 \in \mathbb{Q}[x]$ no es resoluble por radicales.