TEORÍA DE GALOIS

Hoja 4. El Teorema Fundamental de la Teoría de Galois.

Recuerda que una extensión E/K es Galois si es normal, finita y separable. Dado $f \in K[x]$, escribimos $E = K(f)$ para denotar al cuerpo de descomposión de f sobre K; en tal caso diremos que el grupo de Galois de f sobre K es $\mathrm{Gal}(E/K)$ y lo denotaremos por $\mathrm{G}(f)$.

---

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

2. Demuestra que la extensión $\mathbb{C}(x)/\mathbb{C}(x^6)$ es normal y separable. Calcula su grupo de Galois.

3. Calcula los siguientes grupos de Galois.

a) Prueba que $\mathrm{Aut}\mathbb{Q} = \{\mathrm{Id}\}$ y $\mathrm{Aut}\mathbb{R} = \mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = \{\mathrm{Id}\}$.

b) Definimos $\sigma\colon \mathbb{C} \to \mathbb{C}$ como $\sigma(a + bi) = a - bi$. Prueba que $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$.

Sugerencia: para el primer apartado, observa que si $0 < x \in \mathbb{R}$ *entonces* $x = y^2$ *y entonces para todo* $f \in \mathrm{Aut}\mathbb{R}$ *se tiene que* $x < y$ *implica que* $f(x) < f(y)$*; después usa que entre dos números reales siempre hay un racional.*

4. 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. Prueba que $E/\mathbb{F}_p$ es una extensión Galois y que $\mathrm{Gal}(E/\mathbb{F}_p) = \langle\varphi\rangle$. En particular, el grupo de Galois de la extensión $E/\mathbb{F}_p$ tiene orden n.

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

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

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

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

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

7. Calcula el grupo de Galois de los siguientes polinomios sobre $\mathbb{Q}$: $x^{12} - 1,\ x^6 + 1,\ x^4 - 2,\ x^4 + x^2 - 6$.

8. 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 $\mathrm{Gal}(E/\mathbb{Q})$ es cíclico encontrando un generador del grupo.

9. 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 $\mathbb{Q}$.

10. 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 $\mathbb{Q}$.

11. 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 el grupo de Galois de $E/\mathbb{Q}$ es cíclico. Encuentra un generador y expresa todos los automorfismos de $\mathrm{Gal}(E/\mathbb{Q})$ 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 $E/\mathbb{Q}$: $\mathbb{Q}(\sqrt{11})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt[5]{5})$. *Sugerencia: Para las de grado dos, calcula un generador del cuerpo fijo correspondiente y a continuacin encuentra su polinomio mínimo.*

12. Sea E/K una extensión Galois con $G = \mathrm{Gal}(E/K)$ un grupo 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, $|E : L_1|$ divide a $|E : L_2|$.

c) Si la extensión E/K es sólo normal, ¿siguen valiendo los apartados anteriores?

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

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

14. 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 Ł $= \mathbb{Q}(i) \subset E$ y, por tanto, E es el cuerpo de escisión de f sobre L.

c) Calcula $[E : L]$ y concluye que f es irreducible sobre L.

d) Decide de manera razonada la clase de isomorfía de $\mathrm{Gal}(E/L)$.

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

f) Calcula todas las subextensiones de E/L de grado 4 sobre L.

15. Sea $f(x) = x^4 - 3x^2 + 4 \in \mathbb{Q}[x]$. Calcula el grupo de Galois de f sobre $\mathbb{Q}$ y los cuerpos fijos por sus subgrupos.

16. 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 $\mathbb{Q}$.

17. Sea $x^4 + ax^2 + b$ un polinomio irreducible sobre K, un cuerpo de característica distinta de 2. Sea G su grupo de Galois. Demuestra que:

a) Si b es el cuadrado de un elemento de K, entonces $G \cong C_2 \times C_2$.

b) Si b no es el cuadrado de ningún elemento de K pero $b(a^2 - 4b)$ sí lo es, entonces G es cíclico de orden 4.

18. Sea $f = (x^2 - p)(x^2 - q) \in \mathbb{Q}[x]$ donde $p \neq q$ son primos. Determina la clase de isomorfía de $\mathrm{Gal}(f)$.

19. Sea E/K una extensión de Galois con $\mathrm{Gal}(E/K) \cong \mathsf{C}_2 \times \mathsf{C}_2$. Supongamos que la característica de K no es 2. Demuestra que existen $a, b \in E$ tales que $E = K(a, b)$ con $a^2, b^2 \in K$. ¿Qué sucede si la característica de K es 2 y suponemos cierta la conclusión?

20. Sea f un polinomio irreducible sobre $\mathbb{Q}$ con el grupo de Galois 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 $\mathbb{Q}(u)$.

21. 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 descomposición de $x^6 - 3x^3 + 2$ es $\mathbb{Q}(\sqrt[3]{2} + 2\sqrt{-3})$.