Teoría de Galois

Hoja 4. Teoría de Galois: Teorema Fundamental.

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. 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.

3. Demuestra que la extensión $\mathbb{F}_3(t)/\mathbb{F}_3(t^3)$ no es de Galois y que, en cambio, la extensión $\mathbb{C}(t)/\mathbb{C}(t^3)$ 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. 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 $\mathbb{Q}$:

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

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 $G/\mathrm{Gal}(E/M) \cong \mathsf{S}_3$

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 $\mathbb{Q}$.

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 $\mathbb{Q}$.

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 u1 impar entonces,

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

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.

Para el último apartado, usa el Ejercicio 4 de esta hoja de problemas.

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 $\mathrm{Gal}(E/\mathbb{Q})$.

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 $L = \mathbb{Q}(i) \subseteq E$ 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 $\mathrm{Gal}(E/L)$ tiene una presentación de la forma

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

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

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 $\mathbb{Q}$.

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 $\mathrm{Gal}(f)$.

16. 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 $a^2, b^2 \in K$.

17. Sea f un polinomio irreducible sobre $\mathbb{Q}$ con el grupo de Galois abeliano y u una raíz de f en $\mathbb{C}$. Demostrar que el grado de f es primo si, y solo si, no hay extensiones intermedias entre $\mathbb{Q}$ y $\mathbb{Q}(u)$.

18. 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 $\mathbb{Q}(\sqrt[3]{2} + 2\sqrt{-3})$.