Teoría de Galois

Hoja 2. Extensiones de cuerpos.

Escribiremos E/K para denotar que E es una extensión del cuerpo K. El grado $|E : K|$ de la extensión E/K es la dimensión de E como K-espacio vectorial. Si $a \in E$ es algebraico sobre K, denotaremos por $\mathrm{Irr}(K, a) \in K[x]$ al polinomio mínimo (o irreducible) de a sobre K.

1. Demuestra la igualdad $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, y halla un polinomio irreducible de $\mathbb{Q}[x]$ de grado 4 que tenga una raíz en $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

2. Calcula el polinomio mínimo de $\alpha = \sqrt[3]{9} + \sqrt[3]{3} - 1$ sobre $\mathbb{Q}$.

3. Estudia cuáles de los siguientes subcuerpos de $\mathbb{C}$ coinciden: $\mathbb{Q}(i, \sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{2}+i)$, $\mathbb{Q}\left(\sqrt{2}, \sqrt{1+\sqrt{2}}\right)$ y $\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$.

4. Halla el grado y una base de las siguientes extensiones de cuerpos.

(i)	$\mathbb{Q}(\sqrt[6]{3})/\mathbb{Q}$	(ii)	$\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$	(iii)	$\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)/\mathbb{Q}$
(iv)	$\mathbb{Q}(\sqrt{2}i)/\mathbb{Q}$	(v)	$\mathbb{Q}(\sqrt[5]{2}, \sqrt[3]{7})/\mathbb{Q}(\sqrt[5]{2})$	(vi)	$\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$
(vii)	$\mathbb{Q}(\sqrt{1+\sqrt{3}})/\mathbb{Q}$	$(viii)$	$\mathbb{Q}(e^{2\pi i/5})/\mathbb{Q}$	(ix)	$\mathbb{R}(\sqrt[4]{-3})/\mathbb{R}$.

5. Halla el grado y una base de la extensión $\mathbb{F}_7(t)/\mathbb{F}_7(t^2)$. Calcula t^{-1} y $(t+1)^{-1}$ como combinación lineal de los elementos de la base que has encontrado.

6. Considera las siguientes cuestiones sobre las raíces de la unidad:

a) Sea p un número primo y sea $1 \neq \xi \in \mathbb{C}$ tal que $\xi^p = 1$. Demuestra que $|\mathbb{Q}(\xi) : \mathbb{Q}| = p - 1$.

b) Sea $\omega = \cos\frac{\pi}{6} + i \sin\frac{\pi}{6} = \mathrm{e}^{\frac{\pi}{6}i}$. Observa que $\omega^{12} = 1$ pero que $\omega^r \neq 1$ si $1 \leq r < 12$. Demuestra que $|\mathbb{Q}(\omega) : \mathbb{Q}| = 4$ y calcula el polinomio mínimo de ω sobre $\mathbb{Q}$.

c) Sea $p2$ un número primo, si $p > 2$ calcula el grado del polinomio mínimo de $\cos\frac{2\pi}{p}$ sobre $\mathbb{Q}$. Deduce que $\cos\frac{2\pi}{p} \in \mathbb{Q}$ si, y solo si, $p \in \{2, 3\}$.

7. Dada E/K una extensión, prueba que el conjunto de elementos de E que son algebraicos sobre K forma un subcuerpo de E. Si $\mathbb{A}$ es el conjunto de elementos de $\mathbb{C}$ que son algebraicos sobre $\mathbb{Q}$, prueba que $\mathbb{A}/\mathbb{Q}$ es una extensión de grado infinito.
Sugerencia: para la segunda parte, usa el criterio de Einsestein.

8. Sea E/K una extensión de cuerpos y $\alpha \in E$. Prueba que $K[\alpha]$ es un cuerpo si, y solo si, $K(\alpha)/K$ es una extensión algebraica.

9. Considera E/K una extensión de cuerpos y un polinomio $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in E[x]$ de modo que los coeficientes a_i de p son algebraicos sobre K. Demuestra que si $u \in E$ es una raíz de p, entonces u es algebraico sobre K.
Sugerencia: considera el subcuerpo $L = K(a_0, \ldots, a_n) \subseteq E$.

10. Sea E/K una extensión y $\alpha \in E$ algebraico sobre K. Si L es un cuerpo intermedio, demuestra que el polinomio mínimo de α sobre L divide al polinomio mínimo de α sobre K. Concluye que $|L(\alpha) : L| \leq |K(\alpha) : K|$.

11. Considera una extensión de cuerpos E/K.

a) Demuestra que si es una extensión de grado primo, entonces los únicos subcuerpos intermedios $K \subseteq L \subseteq E$ son $L = K$ y $L = E$.

b) Demuestra que una extensión de grado primo es simple.

c) Suponiendo que el polinomio mínimo de un elemento α sobre un cuerpo K es $x^3 + x - 1$, halla el polinomio mínimo de α^2 sobre K.

d) Si $\alpha \in E$ es tal que $K(\alpha)/K$ es una extensión de grado impar, calcula $K(\alpha^2)/K$.

e) Si L_1 y L_2 son cuerpos intermedios tales que L_1/K y L_2/K son extensiones finitas de grados primos entre sí, demuestra que $L_1 \cap L_2 = K$.

12. Sea E/K una extensión y sean $a, b \in E$ algebraicos sobre K con $|K(a) : K| = n$ y $|K(b) : K| = m$.

a) Prueba que $|K(a, b) : K(b)| \leq n$.

b) Si n y m son coprimos, prueba que $K(a) \cap K(b) = K$ y $|K(a, b) : K| = nm$. Deduce que $\mathrm{Irr}(K, a) = \mathrm{Irr}(K(b), a)$.

c) Calcula $\mathrm{Irr}(\mathbb{Q}, a)$ donde $a = \sqrt{3} + \sqrt[3]{2}$.

13. Sea $K = \mathbb{F}_2[x]/(x^2 + x + 1)$.

a) Demuestra que K es un cuerpo con cuatro elementos, y escribe la tabla del producto de K.

b) Determina todos los automorfismos de K.

c) Demuestra que cualquier otro cuerpo con 4 elementos es isomorfo a K.

14. Considera E/K una extensión de cuerpos, y sean $\alpha_1, \ldots, \alpha_n$ elementos de E. Sea $\sigma\colon E \to L$ un isomorfismo de cuerpos. Prueba la igualdad:

$$\sigma(K(\alpha_1, \ldots, \alpha_n)) = \sigma(K)(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) \,.$$

15. Supongamos que E_1/K_1 es una extensión finita y que E_2/K_2 es otra extensión tal que existe un isomorfismo de cuerpos

$$\sigma : E_1 \to E_2.$$

Demuestra que si $\sigma(K_1) = K_2$, entonces $|E_1 : K_1| = |E_2 : K_2|$.

16. Decide justificadamente si cada una de las siguientes afirmaciones es verdadera o falsa:

a) Sea E/K una extensión finita y $p(x) \in K[x]$ irreducible. Si el grado de p y el grado de E/K son coprimos, entonces p no tiene raíces en E.

b) Sea E/K una extensión finita y $p \in K[x]$ un polinomio irreducible. Si p tiene una raíz en E, entonces el grado de p es igual a $|E : K|$.

c) Sea E/K una extensión finita y $p \in K[x]$ un polinomio irreducible. Si p tiene una raíz en E, entonces el grado de p divide a $|E : K|$.

d) Sea E/K una extensión y supongamos que $\alpha, \beta \in E$ son algebraicos sobre K. Si existe un isomorfismo de cuerpos $\theta\colon K(\alpha) \to K(\beta)$ tal que $\theta(\alpha) = \beta$ y $\theta(k) = k$ para todo $k \in K$, entonces existe un polinomio irreducible $p(x) \in K[x]$ tal que $p(\alpha) = p(\beta) = 0$.

e) Sea E/K una extensión y supongamos que $\alpha, \beta \in E$ son algebraicos sobre K. Si existe un isomorfismo de cuerpos $\theta\colon K(\alpha) \to K(\beta)$ tal que $\theta(\alpha) = \beta$, entonces existe un polinomio irreducible $p(x) \in K[x]$ tal que $p(\alpha) = p(\beta) = 0$.