TEORÍA DE GALOIS

Hoja 2. Extensiones de cuerpos.

Usamos E/K para indicar que el cuerpo E es una extensión del cuerpo K. El grado $|E:K|$ de la extensión es la dimensión de E como K-espacio vectorial. Si $\alpha \in E$ es algebraico sobre K, denotamos por $P_{\alpha,K}(x) \in K[x]$ al polinomio mínimo de α sobre K.

1. Estudia cuáles de los siguientes subcuerpos de $\mathbb{C}$ coinciden:

$$K_1 = \mathbb{Q}(i, \sqrt{2}),\ K_2 = \mathbb{Q}(\sqrt{-2}),\ K_3 = \mathbb{Q}(\sqrt{2}+i),$$

$$K_4 = \mathbb{Q}\left(\sqrt{2}, \sqrt{1+\sqrt{2}}\right),\ K_5 = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right).$$

2. 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)	$\mathbb{Q}(i\sqrt{2})/\mathbb{Q}$	(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)	$\mathbb{F}_7(t)/\mathbb{F}_7(t^2)$	$(viii)$	$\mathbb{Q}(e^{2\pi i/5})/\mathbb{Q}$	(ix)	$\mathbb{R}(\sqrt[4]{-3})/\mathbb{R}$
(x)	$\mathbb{F}_5(t)/\mathbb{F}_5(t^5)$	(xi)	$\mathbb{F}_5(\rho)/\mathbb{F}_5$ con $\rho^3+\rho+1=0$	(xii)	$\mathbb{F}_5(t,\rho)/\mathbb{F}_5(t^5)$ con $\rho^3+\rho+1=0$.

3. 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 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

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

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

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

b) Sea $\omega = \cos\frac{\pi}{6} + i\mathrm{sen}\frac{\pi}{6}$. 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) Calcula el polinomio mínimo de $\cos\frac{2\pi}{7}$ sobre $\mathbb{Q}$.

6. Sea F/K una extensión de cuerpos y sea $P(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ donde los coeficientes a_i se suponene algebraicos sobre K. Demuestra que si $u \in F$ es una raíz de $P(x)$, entonces u es algebraico sobre K. *Sugerencia: Considera el subcuerpo intermedio $E = K(a_0, \cdots, a_n)$.*

7. Consideramos tres cuerpos: $K \subset E \subset L$. Prueba que si $\alpha \in L$ es algebraico sobre K entonces $P_{\alpha,E} \mid P_{\alpha,K}$.

8. Sea $K \subset F$ una extensión finita de cuerpos y sea E un subcuerpo intermedio. Demuestra que si $u \in F$, entonces $|E(u):E| \leq |K(u):K|$.

9. Considera una extensión de cuerpos F/K.

a) Demuestra que si $|F:K|$ es primo, entonces no hay cuerpos intermedios entre F y K (si $K \subseteq E \subseteq F$ entonces $K = E$ ó $E = F$).

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

c) Sea $\alpha \in F$. Suponiendo que el polinomio mínimo de α sobre K es $x^3 + x - 1$, halla el polinomio mínimo de α^2 sobre K.

d) Si $\alpha \in F$ es tal que $|K(\alpha) : K|$ es impar, calcula $K(\alpha^2)/K$.

e) Si E_1 y E_2 son subcuerpos intermedios tales que $|E_1 : K|$ y $|E_2 : K|$ son coprimos, demuestra que $E_1 \cap E_2 = K$.

f) Considera $u, v \in F$ con $|K(u) : K| = n$ y $|K(v) : K| = m$. Demuestra que $|K(u,v) : K| \leq nm$. Si n y m son coprimos demuestra que entonces $|K(u,v) : K| = nm$.

10. Sea $E = \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$.

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

b) Determina todos los automorfismos de E.

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

11. Considera E/K una extensión de cuerpos, y sean $a_1, \ldots, a_n$ elementos de E. Sea $\sigma : E \to L$ un isomorfismo de cuerpos. Prueba la igualdad:

$$\sigma(K(a_1, \ldots, a_n)) = \sigma(K)(\sigma(a_1), \ldots, \sigma(a_n))\,.$$

12. 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 $|E_1 : K_1| = |E_2 : K_2|$.

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

a) Sea K un cuerpo y sea P un polinomio sobre K. Entonces existe una extensión de K donde P tiene al menos una raíz.

b) Sea K un cuerpo y P un polinomio sobre K. Entonces existe una extensión de K donde P se descompone como un producto de polinomios de grado 1.

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

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

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

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