TEORÍA DE GALOIS	Grado en Matemáticas	Hoja
(3-10-2022)	Curso 2022–23	nº 2

Extensiones de cuerpos.

1. Calcula el polinomio mínimo sobre $\mathbb{Q}$ de:

$$\alpha = \sqrt{3} + \sqrt{5}, \qquad \beta = \sqrt[3]{9} + \sqrt[3]{3} - 1, \qquad \gamma = \sqrt{3} + \sqrt[3]{2}.$$

2. Sea $L = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ y $\alpha = \sqrt{3} + \sqrt{5}$.

a) Calcula el polinomio mínimo de α sobre $\mathbb{Q}(\sqrt{3})$ y sobre $\mathbb{Q}(\sqrt{5})$.

b) Calcula $[L : \mathbb{Q}]$, $[L : \mathbb{Q}(\sqrt{3})]$ y $[L : \mathbb{Q}(\sqrt{5})]$.

c) Demuestra la igualdad $L = \mathbb{Q}(\alpha)$.

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

$$K_1 = \mathbb{Q}(i, \sqrt{2}), \qquad K_2 = \mathbb{Q}(\sqrt{-2}), \qquad K_3 = \mathbb{Q}(\sqrt{2} + i),$$
$$K_4 = \mathbb{Q}\left(\sqrt{2}, \sqrt{1+\sqrt{2}}\right), \qquad K_5 = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right), \qquad K_6 = \mathbb{Q}\left(\sqrt{2}, i, \sqrt{1+\sqrt{2}}\right)$$

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

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

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

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 q un número primo impar. Calcula el grado del polinomio mínimo de $\cos\frac{2\pi}{q}$ sobre $\mathbb{Q}$. Deduce que $\cos\frac{2\pi}{q} \in \mathbb{Q}$ si, y solo si, $q \in \{2, 3\}$.

7. 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.

8. Considera E/K una extensión de cuerpos y un polinomio $f(x) = a_0 + a_1x + \cdots + a_nx^n \in E[x]$ tal que $a_0, \ldots, a_n$ son algebraicos sobre K. Demuestra que si $u \in E$ es una raíz de $f(x)$, entonces u es algebraico sobre K.

9. Considera una extensión de cuerpos E/K.

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

b) 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.

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

d) 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 $L_1 \cap L_2 = K$.

10. Sea E/K una extensión y sean $\alpha, \beta \in E$ algebraicos sobre K con

$$[K(\alpha) : K] = n \qquad \text{y} \qquad [K(\beta) : K] = m.$$

a) Prueba que $[K(\alpha, \beta) : K(\beta)] \leq n$.

b) Si n y m son coprimos, prueba que $K(\alpha) \cap K(\beta) = K$ y $[K(\alpha, \beta) : K] = nm$. Demuestra que $p_{\alpha/K}(x) = p_{a/K(\beta)}(x)$.

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

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.

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

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

13. 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 $[E_1 : K_1] = [E_2 : K_2]$.

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

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

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

c) Sea E/K una extensión finita y $f(x) \in K[x]$ un polinomio irreducible. Si $f(x)$ tiene una raíz en E, entonces el grado de $f(x)$ 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 $f(x) \in K[x]$ tal que $f(\alpha) = f(\beta) = 0$.

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 $f(x) \in K[x]$ tal que $f(\alpha) = f(\beta) = 0$.

15. Sea p un número primo. Demuestra que una condición necesaria para poder dibujar *con regla y compas* el polígono regular de p-lados es que p sea un *primo de Fermat* (i.e. $p = 2^{2^n} + 1$ para algún $n \in \mathbb{N}$). Obsérvese que los únicos primos de Fermat que se conocen son $3, 5, 17, 257, 65537$.