# TEORÍA DE GALOIS

Hoja 3. Extensiones Galois

**1.** Sean $f(x) = (x^2 - 3)(x^3 + 1) \in \mathbb{Q}[x]$ y $g(x) = (x^2 - 2x - 2)(x^2 + 1) \in \mathbb{Q}[x]$. Demuestra que $\mathbb{Q}(\sqrt{3}, i)$ es cuerpo de descomposición de $f$ y $g$ sobre $\mathbb{Q}$.

**2.** Demuestra que $\mathbb{Q}(\sqrt{2}, i)$ es un cuerpo de descomposición de $x^2 - 2\sqrt{2}x + 3$ sobre $\mathbb{Q}(\sqrt{2})$.

**3.** Construye cuerpos de descomposición sobre $\mathbb{Q}$ de los polinomios $x^3 - 1$, $x^4 + 5x^2 + 5$ y $x^6 - 8$ y calcula el grado de la extensión correspondiente.

**4.** Demuestra que $K = \mathbb{F}_2[y]/(y^3 + y + 1)$ es el cuerpo de descomposición de $x^3 + x + 1$ y $x^3 + x^2 + 1$ sobre $\mathbb{F}_2$.

**5.** Decide si las siguientes extensiones son normales

$$\mathbb{Q}(\sqrt{5}i)/\mathbb{Q}, \ \mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}.$$

**6.** Demuestra que $\mathbb{Q}(\sqrt[3]{2})$ no es una extensión normal de $\mathbb{Q}$. Encuentra una extensión normal de $\mathbb{Q}$ que contenga a $\mathbb{Q}(\sqrt[3]{2})$ como un subcuerpo.

**7.** Demuestra que $\mathbb{Q}(\xi)$, donde $\xi = e^{\frac{2\pi i}{5}}$, es una extensión normal de $\mathbb{Q}$.

**8.** Decide razonadamente si las siguientes afirmaciones son verdaderas o falsas.

**a)** Supongamos que $f \in K[x]$ se descompone en $K[x]$, supongamos que $p \in K[x]$ no es constante y que $p \,|\, f$. Entonces $p$ se descompone en $K[x]$.

**b)** Supongamos que $K \subseteq L \subseteq E$ son extensiones de cuerpos. Sea $f \in K[x]$ no constante. Si $E$ es cuerpo de descomposición de $f$ sobre $K$, entonces $E$ es cuerpo de descomposición de $f$ sobre $L$.

**c)** Si $E = K(a_1, \ldots, a_n)$ y $\sigma$ es un $K$-automorfismo de $E$ tal que $\sigma(a_i) = a_i$ para todo $i$, entonces $\sigma = 1_E$.

**d)** Toda extensión de grado 2 es normal.

**e)** Si $E/L$ y $L/K$ son normales, entonces $E/K$ es normal.

**f)** Sea $K \subset L \subset M$ una cadena de extensiones de cuerpos tal que las extensiones $K \subset L$ y $L \subset M$ son finitas, normales y separables. Si todo automorfismo de $\mathcal{G}(L/K)$ puede extenderse a un automorfismo de $M$, entonces $M$ es normal sobre $K$.

**9.** Sea $F = \mathbb{F}_2[x]/(x^2 + x + 1)$. Demuestra que $F/\mathbb{F}_2$ es separable.

**10. a)** Demuestra que $\mathbb{F}_2(x)/\mathbb{F}_2(x^2)$ no es separable.

**14.** Encuentra el grupo de Galois de los siguientes polinomios sobre $\mathbb{Q}$ (el grupo de Galois de un polinomio $P \in K[x]$ es el grupo de Galois del cuerpo de descomposición de $P$ sobre $K$):

$$x^{12}-1,\ x^4-2,\ x^4+x^2-6,\ (x^3-2)(x^2-2).$$

**15.** Si $p$ es un primo. Halla el grupo de Galois del polinomio $f(x)=x^p-1 \in \mathbb{Q}[x]$.

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

**17.** Supongamos que $K$ es un cuerpo de característica $p$ y sea $a \in K$. Demuestra que el polinomio $p(x) = x^p - x - a$ o bien se descompone en factores lineales en $K[x]$ o bien es irreducible.

**18.** Sea $P(x) = x^q - x \in \mathbb{F}_p[x]$ con $q = p^n$ para $n \in \mathbb{N}$.

**a)** Demuestra que cualquier polinomio irreducible en $\mathbb{F}_p[x]$ de grado $n$ divide a $P(x)$.

**b)** Demuestra que todos los factores irreducibles de $P(x)$ son de grado un divisor de $n$.

**19.** Sea $P(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$. Halla:

**a)** el cuerpo de descomposición $L$ de $P$ sobre $\mathbb{Q}$;

**b)** el grupo de Galois de $P$ (esto es, $\mathrm{Gal}(L/\mathbb{Q})$);

**c)** el retículo de subgrupos de $\mathrm{Gal}(L/\mathbb{Q})$;

**d)** los cuerpos intermedios entre $\mathbb{Q}$ y $L$, marcando los que sean extensiones normales.

**20.** **a)** Factoriza el polinomio $x^2+ax+b \in K[x]$ si $K$ es un cuerpo de característica distinta de 2. Encuentra el retículo de subgrupos del grupo de Galois, y los subcuerpos intermedios.

**b)** Si $x^2 + ax + b \in \mathbb{F}_2[x]$, encuentra el retículo de subgrupos del grupo de Galois, y los subcuerpos intermedios entre $\mathbb{F}_2$ y el cuerpo de descomposición. Decide razonadamente si el cuerpo de descomposición se obtiene adjuntando una raíz cuadrada de un elemento de $\mathbb{F}_2$.

**21.** Responde, de manera razonada, a las siguientes preguntas:

**a)** Sea $P = x^3 + x + 1 \in \mathbb{F}_2[x]$. Demuestra que $F = \mathbb{F}_2[x]/(P)$ es un cuerpo finito y enumera sus elementos. Halla el inverso en $F$ del elemento $x^2 + x + 1 + (P)$. Comprueba que el grupo multiplicativo de $F$ es cíclico.

**b)** Halla un generador del grupo multiplicativo $K^*$ del cuerpo $K = \mathbb{F}_3[x]/(x^2 + 1)$ y expresa todo elemento de $K^*$ como potencia de dicho generador.

**c)** Construye cuerpos finitos con 8, 9, 25 y 27 elementos.

**22.** Demuestra que el grupo multiplicativo $\mathbb{F}_{p^n}^*$ es cíclico.