

Aplicaciones del Teorema Fundamental de la Teoría de Galois.

1. Sea K un cuerpo y $f(x) \in K[x]$ mónico. Sea L un cuerpo de descomposición de $f(x)$ y $\alpha_1, \dots, \alpha_n \in L$ las raíces de $f(x)$. Se define el *discriminante* de f como

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Supongamos $\text{char}(K) = 0$ y $f(x)$ irreducible. Demostrar:

a) $\Delta(f) \in K$.

b) $\Delta(f)$ es un cuadrado en $K \iff \text{Gal}(L/K)$ isomorfo a un subgrupo de A_n .

2. Sea K un cuerpo.

a) Demostrar que si $f(x) = x^2 + bx + c \in K[x]$, entonces $\Delta(f) = b^2 - 4c$.

b) Demostrar que si $f(x) = x^3 + bx^2 + cx + d \in K[x]$, entonces

$$\Delta(f) = b^2c^2 - 4b^3d + 18bcd - 4c^3 - 27d^2.$$

Para ello demostrar que $\Delta(f) = s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 18s_1s_2s_3 - 27s_3^2$, donde

$$s_1 = \alpha_1 + \alpha_2 + \alpha_3,$$

$$s_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3,$$

$$s_3 = \alpha_1\alpha_2\alpha_3.$$

3. Sea p un primo impar.

a) Demostrar $\Delta(x^p - 1) = (-1)^{\binom{p-1}{2}} p^p$.

b) Demostrar que la única subextensión cuadrática de $\mathbb{Q}(\zeta_p)$ es

$$\mathbb{Q}(\sqrt{p}) \quad \text{si } p \equiv 1 \pmod{4},$$

$$\mathbb{Q}(\sqrt{-p}) \quad \text{si } p \equiv 3 \pmod{4}.$$

4. Sean K un cuerpo de característica cero y $f \in K[x]$ un polinomio irreducible de grado 3. Sea L un cuerpo de descomposición de f sobre K . Demostrar:

a) $L = K(\alpha, \sqrt{\Delta(f)})$ donde $f(\alpha) = 0$.

b)

$$\text{Gal}(L/K) \simeq \begin{cases} C_3 & \text{si } \Delta(f) \text{ es un cuadrado en } K, \\ S_3 & \text{si } \Delta(f) \text{ no es un cuadrado en } K. \end{cases}$$

5. Sea $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$ y $\alpha, \beta, \gamma \in \mathbb{C}$ las raíces de $f(x)$. Sean $u = \alpha^2\beta^2$, $v = \alpha^2\gamma^2$, $w = \beta^2\gamma^2$ y $g(x) = (x - u)(x - v)(x - w)$.

a) Demostrar que $g(x) \in \mathbb{Q}[x]$. ¿Es g irreducible en $\mathbb{Q}[x]$?

b) Calcular $\text{Gal}(\mathbb{Q}(u, v, w)/\mathbb{Q})$.

6. Encontrar infinitas ternas $(x, y, z) \in \mathbb{Z}^3$ que satisfagan la igualdad $x^2 - 3y^2 = z^2$.
7. Consideramos el polinomio $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ y $K = \mathbb{F}_2[x]/\langle f(x) \rangle$.
- Demuestra que K es cuerpo de descomposición de $x^4 + x^3 + 1$ sobre \mathbb{F}_2 .
 - Demuestra que K contiene un cuerpo de descomposición de $x^2 + x + 1$ sobre \mathbb{F}_2 .
 - Determina $\text{Gal}(K/\mathbb{F}_2)$.
8. Sean p un número primo impar y $a \in \mathbb{F}_p$ un elemento que no es el cuadrado de otro elemento de \mathbb{F}_p . Sea $n \in \mathbb{N}$. Demostrar que a es el cuadrado de un elemento de \mathbb{F}_{p^n} si y sólo si n es par.
9. Sea $f(x) = x^3 + 2x + 2 \in \mathbb{F}_3[x]$.
- Demstrar que $f(x)$ es irreducible.
 - Sea α una raíz de $f(x)$ en un cuerpo de descomposición de $f(x)$. Calcular las raíces cúbicas de $\alpha + 2$ en $\mathbb{F}_3(\alpha)$.
10. Sea $f(x) = x^3 + x + 1 \in \mathbb{F}_{256}[x]$ ¿Es $f(x)$ irreducible?
11. Sean K un cuerpo con 2^{10} elementos y $\alpha \in K^*$ un generador del grupo multiplicativo K^* . Encontrar un elemento primitivo de cada subextensión de K/\mathbb{F}_2 .