Teoría de Galois

Hoja 3. Extensiones de Galois.

Escribiremos E/K para denotar que E es una extensión del cuerpo K. Decimos que E/K es normal si E es el cuerpo de escisión (descomposición) de algún polinomio $f \in K[x]$, y escribimos $E = K(f)$.

1. Construye cuerpos de escisión 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.

2. 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 escisión de f y g sobre $\mathbb{Q}$.

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

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

5. Decide si las siguientes extensiones son normales: $\mathbb{Q}(\sqrt{5}i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$.

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 $\xi \in \mathbb{C}$ es una raíz primitiva quinta de la unidad, es una extensión normal de $\mathbb{Q}$.

8. Prueba que toda extensión de grado 2 es normal.

9. Si E/L y L/K son extensiones normales, demuestra E/K no es necesariamente normal.
Sugerencia: considera $E = \mathbb{Q}(\sqrt[4]{2})$ *y* $L = \mathbb{Q}(\sqrt{2})$.

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

a) Sea K un cuerpo y sea $p(x) \in K[x]$. Entonces existe una extensión de K donde $p(x)$ tiene una raíz.

b) Sea K un cuerpo y $p(x) \in K[x]$. Entonces existe una extensión de K donde $p(x)$ se descompone como producto de polinomios de grado 1.

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

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

e) Si $E = K(a_1, \ldots, a_n)$ y $\sigma \in \mathrm{Gal}(E/K)$ tal que $\sigma(a_i) = a_i$ para todo i, entonces $\sigma = 1_E$.

f) Sean E/L y L/K extensiones normales. Si todo $\sigma \in \mathrm{Gal}(L/K)$ se puede extender a un automorfismo de E, entonces E es normal sobre K.

11. Calcula los siguientes grupos de Galois.

a) Prueba que $\mathrm{Aut}(\mathbb{Q}) = 1$ y $\mathrm{Aut}(\mathbb{R}) = \mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = 1$.

b) Definimos $\sigma\colon \mathbb{C} \to \mathbb{C}$ como $\sigma(a + bi) = a - bi$. Prueba que $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$.
Sugerencia: para el primer apartado, si $f \in \mathrm{Aut}(\mathbb{R})$ *y* $0 < x \in \mathbb{R}$, *entonces* $x = y^2$ *luego* $f(x) > 0$. *Deduce que* $x < y$ *implica que* $f(x) < f(y)$ *y usa que entre dos números reales siempre hay un racional.*

12. Indica cuáles de los siguientes polinomios son separables sobre $\mathbb{Q}$, $\mathbb{F}_2$, $\mathbb{F}_3$ y $\mathbb{F}_5$: x^3+1, x^2+x+1, $x^4+x^3+x^2+x+1$.

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

14. Demuestra que $\mathbb{F}_2(t)/\mathbb{F}_2(t^2)$ no es separable.

15. ¿Cuántas raíces distintas tiene $x^{12}+2x^6+1\in\mathbb{F}_3[x]$ en su cuerpo de escisión?

16. Construye cuerpos finitos con 8, 9, 25 y 27 elementos.

17. Prueba que para cada primo p y para cada entero positivo n, existe al menos un polinomio irreducible $f\in\mathbb{F}_p[x]$ de grado n.

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

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

b) Demuestra que el grado de todos los factores irreducibles de f divide a n.

19. Responde, de manera razonada, a las siguientes preguntas:

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

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

20. Sea E/K una extensión de grado 2. Si la característica de K no es 2, prueba que existe un $u\in E$ de modo que $E=K(u)$ y $u^2\in K$. Muestra que la hipótesis sobre la característica es necesaria.
Sugerencia: para la segunda parte, considera el cuerpo de 4 elementos.

21. Sea K es un cuerpo de característica p y $a\in K$. Demuestra que el polinomio $p(x)=x^p-x+a$ o bien se se escinde en $K[x]$ o bien es irreducible.

22. Demuestra que los polinomios de Artin-Schreier x^p-x+a donde p no divide a $a\in\mathbb{Z}$ son irreducibles.
Sugerencia: usa reducción de coeficientes módulo p, considera un cuerpo de escisión sobre $\mathbb{F}_p$ y aplica el pequeño teorema de Fermat para obtener todas las raíces.