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. Demuestra que toda extensión de grado 2 es normal.

9. Encuentra la menor extensión normal de $\mathbb{Q}$ que contiene a $\sqrt{2} + \sqrt[3]{2}$.

10. 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 $p \mid f$. 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 σ es un K-automorfismo de E tal que $\sigma(a_i) = a_i$ para todo i, entonces $\sigma = 1_E$.

d) Si E/L y L/K son normales, entonces E/K es normal. *Sugerencia: considera* $E = \mathbb{Q}(\sqrt[4]{2})$ *y* $L = \mathbb{Q}(\sqrt{2})$.

e) 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 L que fije K se puede extender a un automorfismo de M, entonces M es normal sobre K.

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

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

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

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

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

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

b) Demuestra que todos los factores irreducibles de $x^q - x \in \mathbb{F}_p[x]$ con $q = p^n$, son de grado menor o

igual que n.

c) Decide de manera razonada si el grado de cada divisor irreducible de $P(x)$ debe dividir a n.

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

a) Si en $\mathbb{F}_2[x]$ consideramos $f(x) = x^3+x+1$, entonces ¿es f irreducible? Demuestra que $F = \mathbb{F}_2[x]/(f)$ es un cuerpo finito y enumera sus elementos. Halla el inverso en F del elemento $x^2+x+1+(f)$. Comprueba que el grupo multiplicativo de F 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^* como potencia de dicho generador.

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

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

18. 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.*

19. 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.

20. 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 descomposición sobre $\mathbb{F}_p$ y aplica el pequeño teorema de Fermat para obtener todas las raíces.*