ECUACIONES ALGEBRAICAS, CURSO 2025-2026

José F. Fernando y José Manuel Gamboa

Polinomios en varias variables

1. Sean p un número primo impar y $\mathtt{s}_1, \ldots, \mathtt{s}_{p-1}$ las formas simétricas elementales en las indeterminadas $\mathtt{x}_1, \ldots, \mathtt{x}_{p-1}$. Denotamos $S_i := \mathtt{s}_i(1, \ldots, p-1) \in \mathbb{Z}$. Demostrar que los valores $S_1, \ldots, S_{p-2}$, $S_{p-1}+1$ son múltiplos de p.

2. Sea $g \in \mathbb{R}[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$ un polinomio no nulo tal que $g(x) \geq 0$ para cada $x \in \mathbb{R}^{n-1}$. Demostrar que el polinomio $f := \mathtt{x}_n^2 + g \in \mathbb{R}[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ es irreducible.

3. Probar que tres números no nulos $x, y, z \in \mathbb{C}$, convenientemente ordenados, son términos consecutivos de una progresión geométrica si y sólo si

$$(xy + xz + yz)^3 = xyz(x + y + z)^3.$$

4. Consideremos la aplicación

$$\varphi : \mathbb{C}^3 \to \mathbb{C}^3,\ (x, y, z) \mapsto (x + y + z, xy + xz + yz, xyz)$$

y el conjunto $M := \{(x, y, z) \in \mathbb{C}^3 :\ f(x, y, z) = 0\}$, donde f es el polinomio

$$f(\mathtt{x}, \mathtt{y}, \mathtt{z}) := \mathtt{x}^2(\mathtt{y} - \mathtt{z}) + \mathtt{x}(\mathtt{z}^2 - \mathtt{y}^2) + \mathtt{y}\mathtt{z}(\mathtt{y} - \mathtt{z}).$$

(1) Demostrar que φ es sobreyectiva y calcular la fibra del punto $p := (1, 1, 1)$. ¿Qué grado tiene la aplicación φ, esto es, cuántos elementos tiene la fibra que más elementos tiene? Encontrar un punto $q \in \mathbb{C}^3$ cuya fibra conste de menos puntos que el grado de φ.

(2) Factorizar f en producto de polinomios irreducibles en $\mathbb{C}[\mathtt{x}, \mathtt{y}, \mathtt{z}]$.

(3) Encontrar un polinomio $\Delta \in \mathbb{Z}[\mathtt{u}, \mathtt{v}, \mathtt{w}]$ tal que

$$\varphi(\mathbb{C}^3 \setminus M) = \{(u, v, w) \in \mathbb{C}^3 :\ \Delta(u, v, w) \neq 0\}.$$

¿Contiene $\varphi(\mathbb{C}^3 \setminus M)$ al punto $(0, -3, 2)$?

5. Se consideran los polinomios

$$f(\mathtt{x}, \mathtt{y}) := \mathtt{x}^2 - 5\mathtt{y}^2 - 2\mathtt{x}\mathtt{y} - 3\mathtt{x} + 3\mathtt{y} + 2 \quad \& \quad g(\mathtt{x}, \mathtt{y}) := \mathtt{x}^2 - 7\mathtt{y}^2 - 3\mathtt{x} - 5\mathtt{y} + 2.$$

Encontrar todos los puntos de corte de las cónicas afines

$$C_1 := \{(x, y) \in \mathbb{C}^2 :\ f(x, y) = 0\} \quad \& \quad C_2 := \{(x, y) \in \mathbb{C}^2 :\ g(x, y) = 0\}.$$

Generalidades sobre cuerpos

6. Sea $\mathfrak{a}$ el ideal de $\mathbb{Q}[\mathtt{t}]$ generado por los polinomios

$$f(\mathtt{t}) := \mathtt{t}^4 + \mathtt{t}^3 + 2\mathtt{t}^2 + \mathtt{t} + 1 \quad \& \quad g(\mathtt{t}) := \mathtt{t}^3 + 4\mathtt{t}^2 + 4\mathtt{t} + 3.$$

Probar que el cociente $K := \mathbb{Q}[\mathtt{t}]/\mathfrak{a}$ es un cuerpo extensión de $\mathbb{Q}$. Hallar el grado y un elemento primitivo de la extensión $K|\mathbb{Q}$.

7. Calcular el polinomio mínimo de $\alpha := \beta^2 + \beta$ sobre $\mathbb{Q}$, donde $\beta \in \mathbb{C}$ es una raíz del polinomio $f := \mathtt{t}^3 + 3\mathtt{t}^2 - 3$.

8. (i) Sean $L|K$ una extensión finita y $f \in K[\mathtt{t}]$ un polinomio irreducible. Probar que si f tiene alguna raíz en L entonces el grado de f divide al grado $[L : K]$ de la extensión.

(ii) Supongamos que $[L : K]$ es un número primo. Demostrar que cada elemento $\alpha \in L \setminus K$ cumple que $L = K(\alpha)$.

9. Sean K un cuerpo, $a \in K$ y m y n enteros positivos primos entre sí. Demostrar que el polinomio $f(\mathtt{t}) := \mathtt{t}^{mn} - a$ es irreducible en $K[\mathtt{t}]$ si y sólo si los polinomios $g(\mathtt{t}) := \mathtt{t}^m - a$ y $h(\mathtt{t}) := \mathtt{t}^n - a$ son irreducibles en $K[\mathtt{t}]$.

10. Sean K un cuerpo y $f(\mathtt{t}) := \mathtt{t}^n - a \in K[\mathtt{t}]$. Supongamos que f es irreducible en $K[\mathtt{t}]$. Dados un divisor m de n y una raíz α de f, calcular el polinomio mínimo de α^m sobre K.

11. Sean $E|K$ una extensión algebraica y $\sigma : E \to E$ un homomorfismo de cuerpos cuya restricción a K es la identidad. Demostrar que σ es sobreyectivo.

12. Hallar los polinomios mínimos de $\alpha := \sqrt[3]{5}$ sobre los cuerpos $\mathbb{Q}$ y $K := \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

13. Sea $L|K$ una extensión de cuerpos de característica 0. Supongamos que existe un entero positivo n tal que $[K(u) : K] \leq n$ para cada $u \in L$. Demostrar que la extensión $L|K$ es finita, de grado menor o igual que n.

14. Dados $k \in \mathbb{Z} \setminus 7\mathbb{Z}$ y $\alpha_k := 2k\pi/7$ calcular el polinomio mínimo de $u := 2\cos\alpha_k$ sobre $\mathbb{Q}$.

15. Sean $E|K$ una extensión de cuerpos y $u \in E$ un elemento no nulo algebraico sobre K.

    (1) Demostrar que la aplicación $f_u : K(u) \to K(u)$, $x \mapsto ux$ es un isomorfismo de K-espacios vectoriales

    (2) Demostrar que el polinomio mínimo de u sobre K es, salvo tal vez el signo, el polinomio característico del endomorfismo f_u.

    (3) Sean $\mathtt{i} := \sqrt{-1}$, $r := \sqrt[3]{2}$ y $u := r + \mathtt{i}$. Demostrar que $\mathbb{Q}(u) = \mathbb{Q}(r, \mathtt{i})$.

    (4) Calcular el polinomio mínimo de u sobre $\mathbb{Q}$.

    (5) Calcular el polinomio mínimo sobre $\mathbb{Q}$ de $v := 1 + r + r^2$.

Cuerpo de descomposición de un polinomio

16. Sean $p \in \mathbb{Z}$ un número primo y L un cuerpo de descomposición del polinomio $f(\mathtt{t}) := \mathtt{t}^p - 3$ sobre $\mathbb{Q}$. Calcular el grado $[L : \mathbb{Q}]$.

17. Sea α una raíz del polinomio $f := \mathtt{t}^3 + \mathtt{t}^2 + 1 \in \mathbb{Z}_2[\mathtt{t}]$ en un cuerpo de descomposición de f sobre $\mathbb{Z}_2$. Demostrar que $\mathbb{Z}_2(\alpha)$ es un cuerpo de descomposición de f sobre $\mathbb{Z}_2$.

18. Sean $E|K$ una extensión algebraica y $\sigma : E \to E$ un homomorfismo de cuerpos cuya restricción a K es la identidad. Demostrar que σ es sobreyectivo.

19. Probar que $u := \mathrm{tg}(2\pi/5)$ es un número algebraico sobre $\mathbb{Q}$ y hallar su polinomio mínimo. ¿Es $\mathbb{Q}(u)$ un cuerpo de descomposición sobre $\mathbb{Q}$ de algún polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$?

20. Encontrar conjuntos finitos de generadores de las subextensiones $\mathbb{Q}_f|\mathbb{Q}$ de $\mathbb{C}|\mathbb{Q}$, donde $\mathbb{Q}_f$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$, en los siguientes casos:

    $$f(\mathtt{t}) := \mathtt{t}^9 - 1, \quad f(\mathtt{t}) := \mathtt{t}^4 + 5\mathtt{t}^2 + 6 \quad \& \quad f(\mathtt{t}) := \mathtt{t}^6 - 8.$$

    Encontrar los grados de las extensiones $\mathbb{Q}_f|\mathbb{Q}$.

21. Sean K un cuerpo en el que el polinomio $f(\mathtt{t}) := \mathtt{t}^2+1$ no tiene ninguna raíz, y denotemos $\mathtt{i}$ una raíz de f en un cuerpo de descomposición de f sobre K. Supongamos que todo elemento de $K(\mathtt{i})$ es el cuadrado de un elemento de $K(\mathtt{i})$. Probar que toda suma de cuadrados en K es un cuadrado en K y calcular la característica de K.

22. Hallar un elemento primitivo u de la extensión $L|\mathbb{Q}$, donde L es un cuerpo de descomposición sobre $\mathbb{Q}$ de $f(\mathtt{t}) := \mathtt{t}^3 - 7$. Hallar el polinomio mínimo de u sobre $\mathbb{Q}$.

23. Sean K un cuerpo, $a \in K \setminus \{0\}$, p un número primo, $f(\mathtt{t}) := \mathtt{t}^p - a$, $h(\mathtt{t}) := \mathtt{t}^p - 1$ y L un cuerpo de descomposición de $f \cdot h$ sobre K.

    (1) Demostrar que si u es una raíz de f en L toda raíz de f en L es de la forma ζu para cierta raíz $\zeta \in L$ del polinomio h.

    (2) Demostrar que si f es reducible en $K[\mathtt{t}]$, entonces f tiene alguna raíz en K.

Grupo de automorfismos de una extensión

24. (1) Dado un primo $p \in \mathbb{Z}$, ¿cuál es el polinomio mínimo de $\sqrt[3]{p}$ sobre $\mathbb{Q}$?

    (2) Demostrar que $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$.

    (3) Calcular el grado de la extensión $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})|\mathbb{Q}$.

    (4) Calcular el polinomio mínimo de $\sqrt[3]{2} + \sqrt[3]{3}$ sobre $\mathbb{Q}$.

25. Sean $L|K$ una extensión de Galois y $\alpha \in L$ tal que el único automorfismo de L que deja fijo α es la identidad. Demostrar que $L = K(\alpha)$.

26. Sea α la raíz séptima real de 5. ¿Cuáles de las siguientes extensiones son de Galois?

$$\mathbb{Q}(\alpha)|\mathbb{Q}, \quad \mathbb{Q}(\sqrt{5}, \alpha)|\mathbb{Q}(\alpha), \quad \mathbb{Q}(\sqrt{-5})|\mathbb{Q} \quad \& \quad \mathbb{R}(\sqrt{-7})|\mathbb{R}.$$

27. Sean K un cuerpo de característica 0 tal que todo polinomio de $K[\mathtt{t}]$ de grado impar tiene alguna raíz en K y $L|K$ una extensión de Galois. Demostrar que el orden del grupo de Galois $G(L:K)$ es potencia de 2.

28. Sean $L|\mathbb{Q}$ una subextensión de Galois de $\mathbb{C}|\mathbb{Q}$ y denotemos $\mathtt{i} := \sqrt{-1}$ y

$$\sigma : \mathbb{C} \to \mathbb{C},\ a + \mathtt{i}b \mapsto a - \mathtt{i}b \quad \text{para todo } a, b \in \mathbb{R}.$$

    (1) Demostrar que $\sigma(L) = L$.

    (2) Probar que $\tau := \sigma|_L$ es un elemento del grupo de Galois $G(L:\mathbb{Q})$ cuyo cuerpo fijo es $L \cap \mathbb{R}$.

    (3) Probar que τ es la identidad si $L \subset \mathbb{R}$ y tiene orden 2 en caso contrario.

    (4) Sean $f \in \mathbb{Q}[\mathtt{t}]$ y $\mathbb{Q}_f \subset \mathbb{C}$ un cuerpo de descomposición de f sobre $\mathbb{Q}$. Supongamos que $[\mathbb{Q}_f : \mathbb{Q}]$ es impar. Probar que todas las raíces de f en $\mathbb{C}$ son números reales.

29. Sean $\alpha := e^{\pi \mathtt{i}/3}$ y β una raíz del polinomio $f(\mathtt{t}) := \mathtt{t}^4 - 6\mathtt{t}^2 + 6$. Encontrar conjuntos finitos de generadores de la clausura de Galois $L|\mathbb{Q}$ de las siguientes extensiones y calcular en cada caso el grado de la extensión $L|\mathbb{Q}$:

$$\mathbb{Q}(\sqrt[4]{3})|\mathbb{Q}, \quad \mathbb{Q}(\alpha)|\mathbb{Q}, \quad \mathbb{Q}(\beta)|\mathbb{Q} \quad \& \quad \mathbb{Q}(\sqrt[5]{2})|\mathbb{Q}.$$

30. (1) Probar que los polinomios $g(\mathtt{t}) := \mathtt{t}^2+4$, $h(\mathtt{t}) := \mathtt{t}^3+4$ y $f(\mathtt{t}) := \mathtt{t}^6+4$ son irreducibles en $\mathbb{Q}[\mathtt{t}]$.

    (2) Demostrar que $L := \mathbb{Q}(\sqrt{3}, \mathtt{i}, \sqrt[3]{2})$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$.

    (3) Calcular el grado de la extensión $L|\mathbb{Q}$.

    (4) ¿Cuál es el orden del grupo de Galois $G(L:\mathbb{Q})$? Probar que es un grupo diédrico.

    (5) Encontrar conjuntos finitos de generadores de todas las subextensiones no triviales de $L|\mathbb{Q}$ y determinar cuáles son de Galois.

31. Sean K un cuerpo de característica 0 y $f \in K[\mathtt{t}]$ un polinomio irreducible. Sea K_f un cuerpo de descomposición de f sobre K y supongamos que el grupo de Galois $G(K_f : K)$ es cíclico. Probar que el discriminante $\Delta(f)$ es el cuadrado de un elemento de K si y sólo si el orden del grupo $G(K_f : K)$ es impar.

32. Sean K un cuerpo de característica cero y $f \in K[\mathtt{t}]$ un polinomio irreducible de grado 3. Sea K_f un cuerpo de descomposición de f sobre K. Demostrar que $G(K_f : K) \simeq \mathbb{Z}_3$ si el discriminante $\Delta(f)$ de f es el cuadrado de un elemento de K mientras que $G(K_f : K) \simeq \mathcal{S}_3$ si $\Delta(f)$ no es el cuadrado de un elemento de K.

33. (1) Probar que $h(\mathtt{t}) := \mathtt{t}^4 + 1$ es un polinomio irreducible en $\mathbb{Q}[\mathtt{t}]$.

    (2) Sea L un cuerpo de descomposición de h sobre $\mathbb{Q}$. Encontrar un elemento primitivo de la extensión $L|\mathbb{Q}$.

    (3) ¿Cuál es el orden del grupo de Galois $G(L:\mathbb{Q})$? Demostrar que es abeliano y calcular sus coeficientes de torsión.

    (4) Encontrar elementos primitivos de todas las subextensiones no triviales de $L|\mathbb{Q}$ y determinar cuáles son de Galois.

Grupo de Galois de algunos polinomios

34. (1) Hallar el polinomio ciclotómico Φ_9 y su grupo de Galois $G_{\mathbb{Q}}(\Phi_9)$.

    (2) Sea $L \subset \mathbb{C}$ un cuerpo de descomposición de Φ_9 sobre $\mathbb{Q}$. Expresar como extensiones simples las subextensiones de $L|\mathbb{Q}$ y en cada caso encontrar el polinomio mínimo sobre $\mathbb{Q}$ de un elemento primitivo.

35. Sean n y k dos números enteros positivos tales que, o bien n es impar o bien tanto n como k son pares. Utilizar, si se desea, el Teorema del número primo de Dirichlet para demostrar que existen números enteros u, v tales que

$$\operatorname{mcd}(u, n) = \operatorname{mcd}(v, n) = 1 \quad \& \quad k = u + v.$$

36. Sean K un cuerpo de característica 0 y $f \in K[\mathtt{t}]$ un polinomio irreducible de grado 3. Sea L un cuerpo de descomposición de f sobre K. ¿Qué se puede decir acerca del número de extensiones $L|E$ de grado 2, donde $K \subset E \subset L$?

37. Sean u, v y w las raíces en $\mathbb{C}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^3 - 3\mathtt{t} + 1$. Sean $a := u^2v^2$, $b := u^2w^2$ y $c := v^2w^2$.

    (1) Calcular los coeficientes del polinomio $g(\mathtt{t}) := (\mathtt{t} - a)(\mathtt{t} - b)(\mathtt{t} - c)$. ¿Es g irreducible en $\mathbb{Q}[\mathtt{t}]$?

    (2) Calcular el discriminante de g y el grupo de Galois $G_{\mathbb{Q}}(g)$.

38. Encontrar infinitas ternas $(x, y, z) \in \mathbb{Z}^3$ que satisfagan la igualdad $x^2 - 3y^2 = z^2$.

39. Sean $p > 5$ un número primo y $f_p(\mathtt{t}) := \mathtt{t}^4 + p\mathtt{t} + p \in \mathbb{Q}[\mathtt{t}]$. Determinar el grupo de Galois $G_{\mathbb{Q}}(f_p)$.

40. Sean p un número primo y supongamos que el grupo de Galois $G_{\mathbb{Q}}(f)$ es cíclico, donde $f(\mathtt{t}) := \mathtt{t}^3 - p\mathtt{t} + p$. Demostrar que $p \equiv 1 \bmod 3$.

41. Sean K un cuerpo de característica 0 y $a, b \in K$ tales que el polinomio $f(\mathtt{t}) := \mathtt{t}^4 + a\mathtt{t}^2 + b$ es irreducible en $K[\mathtt{t}]$. Hallar, en función de los valores de a y b, el grupo de Galois de f sobre K.

42. Sean $f_1(\mathtt{t}) := \mathtt{t}^4 - 2\mathtt{t}^2 + 2, f_2(\mathtt{t}) := \mathtt{t}^3 + 9\mathtt{t} + 18$, L_i el cuerpo de descomposición de f_i sobre $\mathbb{Q}$ y L el menor subcuerpo de $\mathbb{C}$ que contiene a L_1 y L_2.

    (i) Probar que el grupo de Galois $G_{\mathbb{Q}}(f_1)$ es isomorfo al grupo diedral $\mathcal{D}_4$ de orden 8.

    (ii) Sean v y w dos raíces de f_1 en L_1 que no son opuestas. Calcular el polinomio mínimo de w sobre $\mathbb{Q}(v)$.

    (iii) Probar que f_2 tiene tres raíces distintas u_1, u_2 y u_3 en L_2, que el grupo de Galois $G_{\mathbb{Q}}(f_2) \cong \mathcal{S}_3$ y que $G_{L_1}(f_2)$ es isomorfo a $\mathbb{Z}_3$.

    (iv) Demostrar que $[L : \mathbb{Q}] = 24$.

    (v) Probar que $L_1|\mathbb{Q}$ es la única subextensión de $L|\mathbb{Q}$ de grado 8.

    (vi) Demostrar que $\mathbb{Q}(u_i)|\mathbb{Q}$, con $i = 1, 2, 3$ son todas las subextensiones de grado 3 de la extensión $L|\mathbb{Q}$.

    (vii) Demostrar que existe un único automorfismo $\rho \in G(L : \mathbb{Q})$ tal que $\rho(v) = w$, $\rho(w) = -v$ y $\rho(u_1) = u_2$. Calcular el grado $[F : \mathbb{Q}]$, donde $F = \operatorname{Fix}(\rho)$ es el cuerpo fijo de ρ.

    (viii) Hallar un elemento primitivo θ de la extensión $F|\mathbb{Q}$ y el polinomio mínimo $P_{\mathbb{Q},\theta}$ de θ sobre $\mathbb{Q}$.

Resolubilidad por radicales

43. Sean K un cuerpo y los polinomios de $K[\mathtt{t}]$ de grado n

$$f(\mathtt{t}) := \sum_{i=0}^{n} a_i \mathtt{t}^i \quad \& \quad g(\mathtt{t}) := \sum_{i=0}^{n} a_{n-i} \mathtt{t}^i.$$

Demostrar que f es resoluble por radicales sobre K si y sólo si g lo es.

44. (1) Estudiar si el polinomio $f(\mathtt{t}) := \mathtt{t}^6 - 3\mathtt{t}^4 + 6\mathtt{t}^2 - 3$ es resoluble por radicales sobre $\mathbb{Q}$.

(2) Sea $\alpha \in \mathbb{C}$ una raíz de f. Calcular el polinomio mínimo de $\alpha^2 - 1$ sobre $\mathbb{Q}$.

45. Sean $f, g \in \mathbb{Q}[\mathtt{t}]$ dos polinomios resolubles por radicales.

(1) ¿Se puede asegurar que también $f + g$ es resoluble por radicales?

(2) ¿Se puede asegurar que fg es resoluble por radicales?

46. ¿Es resoluble por radicales sobre $\mathbb{Q}$ el polinomio

$$h(\mathtt{t}) := \mathtt{t}^6 - \mathtt{t}^5 + \mathtt{t}^4 - \mathtt{t}^3 + \mathtt{t}^2 - \mathtt{t} + 1?$$

47. ¿Es $f := \mathtt{t}^5 - 5\mathtt{t}^4 + 5 \in \mathbb{Q}[\mathtt{t}]$ resoluble por radicales sobre $\mathbb{Q}$?

48. Sean K un cuerpo de característica 0 y $a, b, c, d \in K$. ¿Es resoluble por radicales sobre K el polinomio

$$f(\mathtt{t}) := \mathtt{t}^8 + a\mathtt{t}^7 + b\mathtt{t}^6 + c\mathtt{t}^5 + d\mathtt{t}^4 + c\mathtt{t}^3 + b\mathtt{t}^2 + a\mathtt{t} + 1?$$

49. Sean $\xi := e^{2\pi i/7}$ y $L := \mathbb{Q}(\xi)$.

(i) ¿Cuántas subextensiones de grado dos posee la extensión $L|\mathbb{Q}$? Obtener elementos primitivos de dichas subextensiones y los polinomios mínimos sobre $\mathbb{Q}$ de dichos elementos.

(ii) ¿Contiene L a $i := \sqrt{-1}$? Sea $\gamma := e^{\pi i/7}$. Demostrar que $\mathbb{Q}(\xi) = \mathbb{Q}(\gamma)$.

(iii) ¿Es resoluble por radicales sobre $\mathbb{Q}$ el polinomio

$$h(\mathtt{t}) := \mathtt{t}^6 - \mathtt{t}^5 + \mathtt{t}^4 - \mathtt{t}^3 + \mathtt{t}^2 - \mathtt{t} + 1?$$

50. Sean $f := \mathtt{t}^7 - 7$ y L un cuerpo de descomposición de f sobre $\mathbb{Q}$.

(i) Calcular el grado de la extensión $L|\mathbb{Q}$ y encontrar generadores suyos.

(ii) Describir los $\mathbb{Q}$-automorfismos de L.

(iii) ¿Es abeliano el grupo de Galois $G := G(L : \mathbb{Q})$? ¿Es resoluble?

(iv) ¿Qué números enteros son órdenes de elementos de G. ¿Cuántos elementos tiene G de cada orden?

(v) Demostrar que todos los subgrupos de G cuyo orden divide a 6 son cíclicos.

(vi) Encontrar un sistema generador de G formado por dos elementos. Exhibir una torre normal con factores cíclicos para el grupo G y una torre de resolución para la extensión $L|\mathbb{Q}$.

(vii) Para cada divisor positivo d del orden de G calcular el número de subgrupos de G de orden d.

(viii) ¿Cuántos subgrupos normales tiene G? ¿De qué órdenes?

(ix) Para cada divisor positivo d del grado $[L : \mathbb{Q}]$ calcular cuántas subextensiones tiene $L|\mathbb{Q}$ de grado d. ¿Cuántas de estas subextensiones son de Galois?

(x) Encontrar generadores de cada subextensión de $L|\mathbb{Q}$.

51. Sean K un cuerpo de característica 0 y $\mathtt{t}, \mathtt{x}_1, \ldots, \mathtt{x}_n$ indeterminadas sobre K. Denotamos $\mathtt{s}_1, \ldots, \mathtt{s}_n$ las formas simétricas elementales en las indeterminadas $\mathtt{x}_1, \ldots, \mathtt{x}_n$ y consideramos el polinomio

$$f(\mathtt{t}) := \mathtt{t}^n + \sum_{j=0}^{n-1} (-1)^{n-j} \mathtt{s}_{n-j} \mathtt{t}^j = \prod_{k=1}^{n} (\mathtt{t} - \mathtt{x}_k)$$

y el cuerpo $L := K(\mathtt{s}_1, \ldots, \mathtt{s}_n)$. Demostrar que si $c_1, \ldots, c_n$ son elementos de K distintos dos a dos y $E := K(\mathtt{x}_1, \ldots, \mathtt{x}_n)$, entonces $u := \sum_{k=1}^n c_k \mathtt{x}_k$ es un elemento primitivo de la extensión $E|L$.

52. **(Ternas pitagóricas)** Emplear el Teorema 90 de Hilbert para demostrar que una terna (x, y, z) de números enteros no nulos primos dos a dos cumple $x^2 + y^2 = z^2$ si y sólo si existen $s, m, n \in \mathbb{Z}$ tales que $s \neq 0$ y

$$(sx, sy, sz) = (m^2 - n^2, 2mn, m^2 + n^2).$$

53. **(Forma aditiva del Teorema 90 de Hilbert)** (i) Sean $L|K$ una extensión de Galois y $x \in L$. Se llama *traza* de x a

$$\mathsf{T}(x) := \sum_{\sigma \in G(L:K)} \sigma(x).$$

Demostrar que $\mathsf{T}(x) \in K$.

(ii) Supongamos que K tiene característica 0 y que el grupo de Galois $G(L : K) := \langle \sigma \rangle$ es cíclico. Demostrar que la traza de un elemento $x \in L$ es nula si y sólo si existe $\alpha \in L$ tal que $x = \alpha - \sigma(\alpha)$.

Cuerpos finitos

54. Calcular el inverso de 8 en $\mathbb{F}_{29}$.

55. Sean $f \in \mathbb{F}_p[\mathtt{t}]$ un polinomio irreducible y θ una raíz de f en un cuerpo de descomposición E de f sobre $\mathbb{F}_p$. Sea n el orden de θ en el grupo multiplicativo $E^* = E \setminus \{0\}$. Demostrar que f divide a $\mathtt{t}^n - 1$ en $\mathbb{F}_p[\mathtt{t}]$.

56. Sea α un generador del grupo cíclico formado por los elementos no nulos del cuerpo $\mathbb{F}_{1024}$. Demostrar que $\mathbb{F}_{1024} = \mathbb{F}_2(\alpha^3)$.

57. 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 un entero positivo. Demostrar que a es el cuadrado de un elemento de $\mathbb{F}_{p^n}$ si y sólo si n es par.

58. (1) Probar que el polinomio $f(\mathtt{t}) := \mathtt{t}^3 + 2\mathtt{t} + 2 \in \mathbb{F}_3[\mathtt{t}]$ es irreducible.

    (2) Sea u una raíz de f en una extensión de $\mathbb{F}_3$. Hallar las raíces cúbicas de $u+2$ en $\mathbb{F}_3(u)$.

59. ¿Es irreducible en $\mathbb{F}_{256}[\mathtt{t}]$ el polinomio $f(\mathtt{t}) := \mathtt{t}^3 + \mathtt{t} + 1$?

60. (1) Sean $\mathtt{i} := \sqrt{-1}$ y $A := \mathbb{Z}[\mathtt{i}]$ el anillo de los enteros de Gauss. Demostrar que el cociente $E := A/7A$ es un cuerpo finito y calcular cuántos elementos tiene.

    (2) Determinar el cuerpo primo K de E y un elemento primitivo ξ de la extensión $E|K$. Calcular el polinomio mínimo de ξ sobre K.

    (3) ¿Cuántos elementos $\alpha \in E$ cumplen la igualdad $E = K(\alpha)$?

    (4) ¿Cuántos cuerpos isomorfos a K contiene E?

61. (1) Factorizar $\mathtt{t}^{16} - \mathtt{t}$ como producto de polinomios irreducibles en $\mathbb{F}_2[\mathtt{t}]$.

    (2) Factorizar $\mathtt{t}^9 - \mathtt{t}$ como producto de polinomios irreducibles en $\mathbb{F}_3[\mathtt{t}]$.

62. Escribir las tablas de sumar y multiplicar del cuerpo de 9 elementos.

63. Sean K un cuerpo con 2^{10} elementos y $\alpha \in K^*$ un generador del grupo multiplicativo $K^* := K \setminus \{0\}$. Encontrar un elemento primitivo de cada subextensión de $K|\mathbb{F}_2$.

64. ¿Tiene alguna raíz el polinomio $f(\mathtt{t}) := \mathtt{t}^2 - [7]_{23} \in \mathbb{F}_{23}[\mathtt{t}]$ en el cuerpo $\mathbb{F}_{23}$?

65. Sean $K := \mathbb{F}_{31}$ y $f(\mathtt{x}, \mathtt{y}) := 317\mathtt{x}^2 - 151\mathtt{xy} + 40\mathtt{y}^2$. Decidir si existe algún punto $(a, b) \in K^2$ con alguna coordenada no nula en el que se anula la forma cuadrática f.

66. (1) Sea p un primo tal que $q := 2p+1$ es primo y $p \equiv 3 \mod 4$. Demostrar que $2^p \equiv 1 \mod q$.

    (2) ¿Es primo el número $2^{59} - 1$?

Extensiones transcendentes

67. Sean $F := K(\mathtt{t})$ y $L := K\big(\mathtt{t}^2/(1 + \mathtt{t}^3)\big)$, donde K es un cuerpo y $\mathtt{t}$ es una indeterminada. Demostrar que la extensión $F|L$ es algebraica y simple y calcular su grado $[F : L]$.

68. Sean $E|K$ una extensión de cuerpos y $u \in E \setminus K$.

    (1) Demostrar que existe una subextensión $L|K$ de $E|K$ maximal entre las que no contienen a u.

    (2) Demostrar que u es algebraico sobre L y que la extensión $E|L$ es algebraica.

69. Sea $\{u, v\}$ una base de transcendencia de la extensión de cuerpos $L|K$. Calcular el grado de transcendencia de la extensión $K(u^2, uv)|K$.

70. Sean $E|K$ una extensión de cuerpos y $x, y \in E$. Determinar razonadamente la veracidad o falsedad de las siguientes afirmaciones.

    (1) Si x o y es transcendente sobre K entonces $x + y$ o xy es transcendente sobre K.

    (2) Si x es transcendente sobre K pero y es algebraico sobre K, entonces $x + y$ es transcendente sobre K.

    (3) Si x es transcendente sobre K mientras que y es algebraico sobre K, entonces xy es transcendente sobre el cuerpo K.

    (4) Si tanto x como y son elementos transcendentes sobre K entonces, x, y son algebraicamente independientes sobre K.

    (5) Si x es transcendente sobre K e y es transcendente sobre $K(x)$, entonces x, y son algebraicamente independientes sobre K.

71. Utilizar el Teorema de Lindemann-Weierstrass para demostrar que para cada número algebraico $\alpha \in \mathbb{R} \setminus \{0\}$ los números $\operatorname{senh} \alpha$, $\cosh \alpha$ y $\operatorname{tgh} \alpha$ son transcendentes.

72. Emplear el Teorema de Gelfond-Schneider para probar que $e^{-\pi/2}$ es un número transcendente. ¿Es transcendente e^{π}?