ECUACIONES ALGEBRAICAS, CURSO 2016-2017

José F. Fernando y José Manuel Gamboa

Polinomios en varias variables

1. Calcular la suma de los cubos de las raíces en $\mathbb{C}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^3 - 2\mathtt{t}^2 + 3\mathtt{t} - 4$?

2. Sean $r \in \mathbb{C}$ y $f(\mathtt{t}) := 3\mathtt{t}^2 + 3r\mathtt{t} + r^2 - 1 \in \mathbb{C}[\mathtt{t}]$ cuyas raíces $u, v \in \mathbb{C}$ no son necesariamente distintas. Probar que $f(u^3) = f(v^3)$.

3. Encontrar las soluciones reales del sistema de ecuaciones

$$\begin{cases} \mathtt{xyz} & = & 8 \\ \mathtt{xz}^2 + \mathtt{yx}^2 + \mathtt{zy}^2 & = & 73 \\ \mathtt{x}(\mathtt{y}-\mathtt{z})^2 + \mathtt{y}(\mathtt{x}-\mathtt{z})^2 + \mathtt{z}(\mathtt{x}-\mathtt{y})^2 & = & 98 \end{cases}$$

4. Se consideran los polinomios

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

Encontrar todos los puntos de corte de las cónicas afines

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

5. 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

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

(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 $(0,-3,2)$?

Generalidades sobre cuerpos

6. Para los siguientes valores de $\alpha \in \mathbb{C}$ encontrar el polinomio mínimo de α sobre $\mathbb{Q}$ y el grado de la extensión $\mathbb{Q}(\alpha)|\mathbb{Q}$:

$$\alpha := (\sqrt{3}-1)/2, \quad \alpha := (i+2)\sqrt{3}/5 \quad \& \quad \alpha := \sqrt{1-\sqrt{11}}.$$

7. (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 $L = K(\alpha)$.

8. Sean $a := \sqrt{5} + \sqrt{-5}$ y $b := \sqrt[4]{5}$. Calcular el grado de la extensión $\mathbb{Q}(a,b)|\mathbb{Q}(b)$.

9. 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.

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

11. 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 $\mathbb{Q}$.

12. Sean K un cuerpo, $E := K(\mathtt{t})$ y $L := K\big(\mathtt{t}^3(1+\mathtt{t})^{-1}\big)$, donde $\mathtt{t}$ es una indeterminada. Probar que $E|L$ es una extensión algebraica simple y calcular $[E : L]$.

13. (i) Demostrar que el polinomio $f(\mathtt{t}) := \mathtt{t}^5 - \mathtt{t} - 1$ es irreducible en $\mathbb{Q}[\mathtt{t}]$.

    (ii) Sean $a, b \in \mathbb{Q}$. ¿Tienen los polinomios $\mathtt{t}^5 - \mathtt{t} - 1$ y $\mathtt{t}^3 + a\mathtt{t} + b$ alguna raíz compleja común?

    (iii) Sea $\alpha := [\mathtt{t}]$ la clase de $\mathtt{t}$ en $\mathbb{Q}[\mathtt{t}]/(\mathtt{t}^5 - \mathtt{t} - 1)$. Escribir el elemento $1/(1+\alpha+\alpha^3)$ como expresión polinómica en α con coeficientes en $\mathbb{Q}$.

Cuerpo de descomposición de un polinomio

14. 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 $K[\mathtt{t}]$.

15. Sean $f(\mathtt{t}) := \mathtt{t}^6 - 1$, $i := \sqrt{-1}$ y $\omega \neq 1$ tal que $\omega^3 = 1$. Hallar el grado de la extensión $L_f|L$, donde L_f denota un cuerpo de descomposición de f sobre cada uno de los siguientes cuerpos L: $\mathbb{Q}$, $\mathbb{Q}(i)$ y $\mathbb{Q}(\omega)$.

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. Probar que $u := \operatorname{tg}(2\pi/5)$ 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 $\mathbb{Q}[\mathtt{t}]$?

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

19. 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 $\mathbb{Q}$.

20. 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.

21. 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.

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

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

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

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

Grupo de automorfismos de una extensión

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

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

24. Sea $E := \mathbb{Q}(r)$, donde $r := \sqrt[4]{2}$ es el único número real positivo cuya potencia cuarta vale 2. ¿Existen números reales α y β tales que

$$\mathbb{Q}(\alpha) \neq E \neq \mathbb{Q}(\beta) \quad \& \quad E = \mathbb{Q}(\alpha,\beta)?$$

25. Sean $L|K$ una extensión algebraica y $\phi : L \to L$ un homomorfismo de cuerpos tal que $\phi|_K = \mathrm{id}_K$. Demostrar que $\phi \in G(L:K)$, esto es, que ϕ es un automorfismo.

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

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

27. Sean K un cuerpo, $f \in K[\mathtt{t}]$ un polinomio de grado n y E un cuerpo de descomposición de f sobre K en el que f posee n raíces distintas $\xi_1,\dots,\xi_n$. Probar que para cada polinomio $p \in K[\mathtt{t}]$ existe otro $g \in K[\mathtt{t}]$ de grado n del que son raíces $\{p(\xi_i) : 1 \leq i \leq n\}$.

28. (i) 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 $\mathbb{Q}[\mathtt{t}]$.

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

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

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

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

29. (i) Sea G un grupo abeliano de orden ocho tal que el orden máximo de los elementos de G es cuatro. Demostrar que G es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_4$ y calcular cuántos subgrupos tiene de cada orden.

    (ii) Sean $\xi := e^{\pi i/10}$, $\eta := \xi^4$, $i := \sqrt{-1}$ y $u := \eta + \eta^{-1}$. Calcular el polinomio mínimo de u sobre $\mathbb{Q}$ y decidir si el cuerpo $\mathbb{Q}(u)$ contiene a i.

    (iii) Demostrar que $\mathbb{Q}(\xi) = \mathbb{Q}(i,\eta)$, que $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{5})$ y que $[\mathbb{Q}(\xi):\mathbb{Q}] = 8$. Calcular el polinomio mínimo de ξ sobre $\mathbb{Q}$.

    (iv) Probar que el grupo de Galois $G(\mathbb{Q}(\xi):\mathbb{Q})$ es abeliano y encontrar generadores sobre $\mathbb{Q}$ de las subextensiones de $\mathbb{Q}(\xi)|\mathbb{Q}$.

    (v) Sea E el cuerpo de descomposición sobre $\mathbb{Q}(\xi)$ del polinomio $f(\mathtt{t}) := \mathtt{t}^4 - 5$. Probar que la extensión $E|\mathbb{Q}$ es de Galois, calcular su grado y decidir si $G(E:\mathbb{Q})$ es o no abeliano.

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

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

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

    (iv) 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

31. Sean $K := \mathbb{Q}(\sqrt{-3})$ y $f(\mathtt{t}) := (\mathtt{t}^3 - 2)(\mathtt{t}^2 - 5)$. Hallar el grupo de Galois $G_K(f)$.

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

    (ii) 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.

33. Sea $L \subset \mathbb{C}$ un cuerpo de descomposición sobre $\mathbb{Q}$ de un polinomio irreducible $f \in \mathbb{Q}[\mathtt{t}]$. Demostrar que si $[L : \mathbb{Q}]$ es impar entonces $L \subset \mathbb{R}$.

34. 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 $c := v^2w^2$.

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

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

35. 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 $p \equiv 1 \bmod 3$.

36. Sean $K \subset \mathbb{R}$ un cuerpo y $f \in K[\mathtt{t}]$ un polinomio irreducible de grado 4 que tiene, exactamente, dos raíces reales. Demostrar que su grupo de Galois $G_K(f)$ es $\mathcal{D}_4$ o $\mathcal{S}_4$.

37. 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.

38. Calcular el grupo de Galois $G_{\mathbb{Q}}(f_i)$ para $i = 1, 2$, donde

$$f_1(\mathtt{t}) := \mathtt{t}^4 + 3\mathtt{t}^3 - 3\mathtt{t} - 2 \quad \& \quad f_2(\mathtt{t}) := \mathtt{t}^4 + \mathtt{t}^2 - 2\mathtt{t} + 1.$$

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. Sea $E|K$ una extensión de cuerpos de grado 4. Demostrar que las siguientes afirmaciones son equivalentes:

    (i) $E|K$ es de Galois y $G(E : K) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

    (ii) Existen un elemento primitivo α de la extensión $E|K$ y $s, u \in K$ tales que

$$P_{K,\alpha}(\mathtt{t}) = \mathtt{t}^4 - 2(s + u)\mathtt{t}^2 + (s - u)^2.$$

41. 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 $F = \mathrm{Fix}(\rho)$ 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 $\mathbb{Q}$.

Aplicaciones de la teoría de Galois

42. 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.

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

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

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

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

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

45. 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

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

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

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

47. (i) Sea $f \in \mathbb{Q}[\mathtt{t}]$ un polinomio irreducible cuyo grado es un número primo. Supongamos que f posee al menos dos raíces reales y alguna raíz en $\mathbb{C} \setminus \mathbb{R}$. ¿Es f resoluble por radicales sobre $\mathbb{Q}$?

(ii) Sean $p \equiv 1 \,\mathsf{mod}\, 4$ un número primo y $f \in \mathbb{Q}[\mathtt{t}]$ un polinomio irreducible de grado p cuyo discriminante es negativo. Probar que f no es resoluble por radicales sobre $\mathbb{Q}$.

48. Sean K un cuerpo de característica 0 y $\mathtt{t}, \mathtt{x}_1, \dots, \mathtt{x}_n$ indeterminadas sobre K. Denotamos $\mathtt{s}_1, \dots, \mathtt{s}_n$ las formas simétricas elementales en las indeterminadas $\mathtt{x}_1, \dots, \mathtt{x}_n$ 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 $L := K(\mathtt{s}_1, \dots, \mathtt{s}_n)$. Demostrar que si $c_1, \dots, c_n$ son elementos de K distintos dos a dos y $E := K(\mathtt{x}_1, \dots, \mathtt{x}_n)$, entonces $u := \sum_{k=1}^{n} c_k \mathtt{x}_k$ es un elemento primitivo de la extensión $E|L$.

49. 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 $L|\mathbb{Q}$.

50. Sean G un grupo y K un cuerpo. Un *carácter* de G a valores en K es un homomorfismo de grupos $\chi : G \to K^*$.

(i) Probar que cualesquiera caracteres $\chi_1, \dots, \chi_n$ de G a valores en K distintos dos a dos son linealmente independientes sobre K, o sea, para cada n-upla $(a_1, \dots, a_n) \in K^n$ donde algún $a_i \neq 0$ existe $g \in G$ tal que

$$\sum_{k=1}^{n} a_k \chi_k(g) \neq 0.$$

(ii) Sean $\alpha_1, \dots, \alpha_\ell \in K$ no nulos y distintos dos a dos y $a_1, \dots, a_\ell \in K$ tales que

$$\sum_{k=1}^{\ell} a_k \alpha_k^n = 0 \quad \forall\, n \in \mathbb{Z}.$$

Demostrar que $a_k = 0$ para $1 \leq k \leq \ell$.

51. **(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

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

52. **(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 $x = \alpha - \sigma(\alpha)$.

53. **(Teorema de la base normal)** Sean K un cuerpo de característica 0 y $L|K$ una extensión de Galois cuyo grupo de Galois es $G(L:K) := \{\sigma_1, \dots, \sigma_n\}$.

(i) Probar que existe $u \in L$ tal que la matriz $A := (a_{ij}) \in \mathcal{M}_n(L)$ cuyos coeficientes son $a_{ij} := \sigma_i(\sigma_j^{-1}(u))$ tiene determinante no nulo.

(ii) Demostrar que el conjunto $\mathcal{B} := \{\sigma_j(u) : 1 \leq j \leq n\}$ es una base de L como K-espacio vectorial.

Cuerpos finitos

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

(ii) 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.

55. Sea K un cuerpo finito con q elementos. Determinar el número de polinomios mónicos e irreducibles de grado 3 en $K[\mathtt{t}]$. Deducir que para cada número primo p y cada entero positivo n existe un cuerpo con p^{3^n} elementos.

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

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

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

58. 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 $K|\mathbb{F}_2$.

59. Demostrar que $f(\mathtt{t}) := \mathtt{t}^4 + 1$ es irreducible como polinomio en $\mathbb{Z}[\mathtt{t}]$ pero es reducible en $\mathbb{F}_p[\mathtt{t}]$ para cada primo p.

60. ¿Tiene el polinomio $f(\mathtt{t}) := \mathtt{t}^2 - [2002]_{97} \in \mathbb{F}_{97}[\mathtt{t}]$ alguna raíz en el cuerpo $\mathbb{F}_{97}$?

61. ¿Existe algún número entero x tal que $x^2 + 4x + 3 \equiv 7 \bmod 11$?

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

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

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

Extensiones transcendentes

64. 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 $[F : L]$.

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

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

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

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

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

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

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

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

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

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

68. Sean p un número primo, $\mathtt{x}$ e $\mathtt{y}$ indeterminadas sobre $\mathbb{Z}_p$ y consideremos los cuerpos $E = \mathbb{Z}_p(\mathtt{x}, \mathtt{y})$ y $K = \mathbb{Z}_p(\mathtt{x}^p, \mathtt{y}^p)$. Demostrar que la extensión $E|K$ es finita y calcular su grado. ¿Cuál es el grado de transcendencia de la extensión $K|\mathbb{Z}_p$? Demostrar que $E|K$ no es una extensión simple.

69. 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.

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