ECUACIONES ALGEBRAICAS, CURSO 2015-2016

José F. Fernando

Generalidades sobre cuerpos

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

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

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

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

4. Sean $E|K$ una extensión y $\alpha \in E$ un elemento algebraico sobre K. Demostrar que si el grado de la extensión $K(\alpha)|K$ es impar entonces $K(\alpha^2) = K(\alpha)$.

5. Sean $L|K$ una extensión de cuerpos, $f \in K[\mathtt{t}] \setminus K$ y $\alpha \in L$ transcendente sobre K.

   (i) Demostrar que $f(\alpha)$ es transcendente sobre K.

   (ii) Demostrar que si $\beta \in L$ satisface $f(\beta) = \alpha$ entonces β es transcendente sobre K.

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

7. 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 $\mathbb{Q}$.

8. 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 $K|\mathbb{Q}$.

9. (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

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

11. 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 $\mathbb{Q}(\omega)$.

12. Sean K un cuerpo de característica distinta de 2 y $u,v \in K$ dos elementos que no son un cuadrado en K. Sean $\sqrt{u}$ y $\sqrt{v}$ raíces del polinomio $f(\mathtt{t}) := (\mathtt{t}^2-u)(\mathtt{t}^2-v)$ en un cuerpo de descomposición L de f sobre K tales que $K(\sqrt{u}) \neq K(\sqrt{v})$. Probar que

$$[K(\sqrt{u},\sqrt{v}):K] = 4 \quad \& \quad K(\sqrt{u},\sqrt{v}) = K(\sqrt{u}+\sqrt{v}).$$

13. 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 $[L : \mathbb{Q}]$.

14. 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 $\mathbb{Q}[\mathtt{t}]$?

15. Encontrar elementos primitivos 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 $\mathbb{Q}_f|\mathbb{Q}$.

16. Sea $\alpha := 1/(\sqrt{2} + \sqrt[3]{3})$. Encontrar el polinomio mínimo de α sobre $\mathbb{Q}$. Escribir α como expresión polinómica en $\sqrt{2}$ y $\sqrt[3]{3}$ con coeficientes racionales.

17. 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.

Extensiones transcendentes

18. 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 $[F : L]$.

19. 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.

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

21. 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.

22. 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.

23. 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.

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

Grupo de automorfismos de una extensión

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

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

26. 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

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

27. Sean $E \subset \mathbb{R}$ un cuerpo que contiene a $\mathbb{Q}$ de modo que la extensión $E|\mathbb{Q}$ es de Galois, y $F := E(\sqrt{-1})$. ¿Se puede asegurar que la extensión $F|\mathbb{Q}$ es también de Galois?

28. 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 $L|\mathbb{Q}$:

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

29. (*) Sean $A := \mathbb{Z}[\sqrt{2}]$, $\xi := e^{\pi i/5}$, donde $i := \sqrt{-1} \in \mathbb{C}$, y $L \subset \mathbb{C}$ un cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^{10} - 2$. Se pide:

    (i) Hallar el polinomio mínimo de ξ sobre $\mathbb{Q}$ y estudiar si es irreducible en $A[\mathtt{t}]$.

    (ii) Encontrar el polinomio mínimo de $\sqrt[10]{2}$ sobre $\mathbb{Q}$ y factorizarlo en producto de polinomios irreducibles en el anillo $A[\mathtt{t}]$.

    (iii) Calcular el grado $n := [L : \mathbb{Q}]$ de la extensión $L|\mathbb{Q}$.

    (iv) Demostrar que para cada divisor positivo d de n la extensión $L|\mathbb{Q}$ admite alguna subextensión de grado d.

    (v) ¿Cuántas subextensiones $E|\mathbb{Q}$ de $L|\mathbb{Q}$ tienen grado 8? ¿Cuántas tienen grado 5?

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

30. (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.

31. 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.

32. Sean E_1 y E_2 dos subcuerpos de $\mathbb{C}$ tales que las extensiones $E_1|\mathbb{Q}$ y $E_2|\mathbb{Q}$ son de Galois y $G(E_1 : \mathbb{Q}) \cong \mathbb{Z}_6 \cong G(E_2 : \mathbb{Q})$. Supongamos además que $[E_1 \cap E_2 : \mathbb{Q}] = 2$.

    (i) Sea F el menor subcuerpo de $\mathbb{C}$ que contiene a E_1 y E_2. ¿Es de Galois la extensión $F|\mathbb{Q}$? ¿Cuál es su grado?

    (ii) Demostrar que el grupo de Galois $G(F : \mathbb{Q})$ es abeliano. Calcular sus coeficientes de torsión. ¿Cuántas subextensiones propias y no triviales tiene $F|\mathbb{Q}$?

Grupo de Galois de algunos polinomios

33. (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.

34. ¿Es finito el conjunto formado por los números primos p para los que existe algún entero n tal que $p|(n^2+1)$?

35. 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 $L \subset \mathbb{R}$.

36. Consideremos los números reales

$$a := \sqrt[5]{2} \quad \& \quad b := \sqrt[3]{-7/2 - \sqrt{3981}/18} + \sqrt[3]{-7/2 + \sqrt{3981}/18}.$$

    Calcular el polinomio mínimo de $a+b$ sobre $\mathbb{Q}$.

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

    (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 $G_{\mathbb{Q}}(g)$.

38. Encontrar una extensión $K|\mathbb{Q}$ de grado 2 y un polinomio $f \in \mathbb{Q}[\mathtt{t}]$ de grado 3 tales que f es irreducible en $K[\mathtt{t}]$ y los grupos de Galois $G_{\mathbb{Q}}(f)$ y $G_K(f)$ no sean isomorfos.

39. Sean K un cuerpo de característica 0 y $f \in K[\mathtt{t}]$ un polinomio de grado 4 cuyo grupo de Galois $G_K(f)$ es el grupo alternado $\mathcal{A}_4$. ¿Cuál es el grupo de Galois sobre K de la resolvente cúbica g del polinomio f?

40. 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 $\mathcal{S}_4$.

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

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

Aplicacions de la teoría de Galois

44. 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?

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 $p \equiv 1 \bmod 4$ 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 $\mathtt{t}, \mathtt{x}_1, \ldots, \mathtt{x}_n$ 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 $E|L$.

49. 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 $\chi_1, \ldots, \chi_n$ de G a valores en K distintos dos a dos son linealmente independientes sobre K, o sea, para cada n-upla $(a_1, \ldots, a_n) \in K^n$ 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 $\alpha_1, \ldots, \alpha_\ell \in K$ no nulos y distintos dos a dos y $a_1, \ldots, a_\ell \in K$ tales que

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

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

50. **(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

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

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

52. Sean m y n enteros positivos y $M := \operatorname{mcm}(m, n)$ su mínimo común múltiplo. Supongamos que los polígonos regulares de m y n lados son constructibles con regla y compás. Demostrar que también es constructible con regla y compás el polígono con M lados.

53. Demostrar que si n es un divisor de $2^{32} - 1$, el polígono regular de n lados es constructible con regla y compás.

54. ¿Para qué valores del entero positivo n es trisecable con regla y compás el ángulo $2\pi/n$?

Cuerpos finitos

55. (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.

56. 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.

57. (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 $\mathtt{t}^9 - \mathtt{t}$.

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

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

60. 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.

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

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

63. 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.

64. (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 $2^{59} - 1$?

Polinomios en varias variables

65. Sean K un cuerpo y $f_1, f_2 \in K[\mathtt{x}, \mathtt{y}]$ polinomios homogéneos primos entre sí de grados $d \geq 1$ y $d + 1$, respectivamente. Probar que $f := f_1 + f_2$ es irreducible en $K[\mathtt{x}, \mathtt{y}]$.

66. Estudiar la irreducibilidad en $\mathbb{C}[\mathtt{x}, \mathtt{y}]$ de los siguientes polinomios:
$$f_1 := \mathtt{x}^2\mathtt{y}^5 + \mathtt{x}^3 + \mathtt{xy}^2 + \mathtt{y}^2 + \mathtt{x} - 1, \quad f_2 := \mathtt{x}^2\mathtt{y}^5 + \mathtt{yx}^3 - \mathtt{x}^2\mathtt{y}^2 + \mathtt{y} - 1,$$
$$f_3 := \mathtt{x}^3 + \mathtt{x}^2\mathtt{y} - 2\mathtt{xy}^2 + 3\mathtt{xy}^3 + 3\mathtt{y}^4.$$

67. ¿Es irreducible en $\mathbb{R}[\mathtt{x},\mathtt{y}]$ el polinomio

$$f := -\mathtt{x} + \mathtt{y} + \mathtt{x}^2 + \mathtt{xy} + \mathtt{x}^2\mathtt{y} + \mathtt{x}^2\mathtt{y}^2 + \mathtt{x}^2\mathtt{y}^3 + \mathtt{x}^2\mathtt{y}^4?$$

68. Consideremos los ideales $\mathfrak{a} := (2, \mathtt{x}^2 + 1, \mathtt{y})$, $\mathfrak{b} := (3, \mathtt{x}^2 + 1, \mathtt{y}^2 + 1)$ y $\mathfrak{m} := (3, \mathtt{x}^2 + 1, \mathtt{y})$ del anillo $\mathbb{Z}[\mathtt{x},\mathtt{y}]$. ¿Es alguno de ellos primo? ¿Y maximal?

69. Demostrar que el único polinomio $f \in \mathbb{C}[\mathtt{x},\mathtt{y}]$ que se anula en todos los puntos del producto $\mathbb{Z}^+ \times \mathbb{Z}^+$ es el polinomio nulo.

70. Calcular la suma de los inversos de las raíces en $\mathbb{C}$ de $f(\mathtt{t}) := \mathtt{t}^3 - 2\mathtt{t}^2 + 3\mathtt{t} - 4$. Calcular la suma de los cuadrados de dichas raíces.

71. Determinar todos los polinomios mónicos de $\mathbb{C}[\mathtt{t}]$ de grado 3 cuyas raíces, no necesariamente distintas, cumplen que dos de sus medias aritméticas son raíces de su derivada.

72. Probar que tres números complejos no nulos x, y y z, convenientemente ordenados, son términos consecutivos de una progresión geométrica si y sólo si

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

73. Encontrar las soluciones reales del sistema de ecuaciones

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

74. 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

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

75. 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

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

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

76. Sean $f, g \in \mathbb{C}[\mathtt{t}]$ dos polinomios no constantes, $\mathfrak{a}$ el ideal generado por f y el cociente $V := \mathbb{C}[\mathtt{t}]/\mathfrak{a}$.

(1) Comprobar que V tiene estructura de espacio vectorial sobre el cuerpo $\mathbb{C}$ con las operaciones definidas mediante: dados $h_1, h_2 \in \mathbb{C}[\mathtt{t}]$ y $\lambda \in \mathbb{C}$,

$$(h_1 + \mathfrak{a}) + (h_2 + \mathfrak{a}) := (h_1 + h_2) + \mathfrak{a} \quad \& \quad \lambda \cdot (h_1 + \mathfrak{a}) := \lambda h_1 + \mathfrak{a}.$$

Calcular la dimensión de V.

(2) Supongamos que el discriminante $\Delta(f)$ de f es no nulo. Demostrar que entonces la aplicación definida por $g_* : V \to V$, $h + \mathfrak{a} \mapsto gh + \mathfrak{a}$ es un endomorfismo de V y expresar sus autovalores en función de lo que vale g en las raíces de f.

(3) Probar que g_* es isomorfismo de $\mathbb{C}$-espacios vectoriales si y sólo si $\mathrm{Res}(f, g) \neq 0$.

(4) Demostrar que g_* es diagonalizable y expresar la traza de g_* en función de los valores que toma g en las raíces de f.

(5) Calcular la suma de los cubos de las raíces del polinomio $f(\mathtt{t}) := \mathtt{t}^5 - 2\mathtt{t}^2 - 2$.