PROBLEMAS DE EXAMEN DE CALIFICACIÓN DE ÁLGEBRA
TEORÍA DE CAMPOS

Universidad Estatal de Kent
Departamento de Ciencias Matemáticas

Compilado y mantenido por

Donald L. White

Versión: 7 de septiembre de 2023

CONTENIDO

TEORÍA DE CAMPOS

Teoría general de campos

1. Demuestre o refute cada una de las siguientes afirmaciones. (a) Si K es un subcuerpo de F y F es isomorfo a K, entonces F = K. (b) El cuerpo C de los números complejos es una clausura algebraica del cuerpo Q de los números racionales. (c) Si K es una extensión finitamente generada de F, entonces [K : F] es finito. (d) Si K es una extensión algebraica finitamente generada de F, entonces [K : F] es finito. (e) Si F E K es una torre de cuerpos y K es normal sobre F, entonces E es normal sobre F. (f) Si F E K es una torre de cuerpos y K es normal sobre F, entonces K es normal sobre E. (g) Si F E K es una torre de cuerpos, E es normal sobre F y K es normal sobre E, entonces K es normal sobre F.

   (h) Si F E K es una torre de campos y K es separable sobre F, entonces E es separable sobre F. (i) Si F E K es una torre de campos y K es separable sobre F, entonces K es separable sobre E. (j) Si F E K es una torre de campos, E es separable sobre F y K es separable sobre E, entonces K es separable sobre F.

2. Dé un ejemplo de una cadena infinita Ω1 Ω2 Ω3 · · · de campos algebraicamente cerrados.

3. Sea E un campo de extensión de un campo F y f(x), g(x) F[x]. Demuestre que un máximo común divisor de f y g en F[x] es también un máximo común divisor de f y g en E[x].

4. Sea F un campo y F^* Su grupo multiplicativo. Demuestre que los grupos abelianos (F, +) y (F^*, ·) no son isomorfos.

5. Demuestre que un subgrupo finito del grupo multiplicativo de un campo debe ser cíclico.

6. (a) Demuestre que un dominio integral finito es un campo. (b) Demuestre que si R es un dominio integral de dimensión finita sobre un subcampo F R, entonces R es un campo.

7. Demuestre que si F es una extensión finita de Q, entonces el subgrupo de torsión de F^* es finito. [Pista: El El subgrupo de torsión consta de raíces de la unidad.]

8. Suponga que F E K es cualquier torre de campos y [K : F] es finito. Demuestre que [K : F] = [K : E][E : F].

9. Sea K una extensión de campo de F de grado n y sea f(x) F[x] un polinomio irreducible de grado m > 1. Demuestre que si m es relativamente primo a n, entonces f no tiene raíz en K.

10. Sea f(x) = anx en la norte +· · ·+a1x+a0 Q[x] sea un polinomio irreducible de grado mayor que 1 que todas las raíces se encuentran en el círculo unitario de C. Demuestre que ai = an−i para todo i.

11. Sea F una extensión de campo de los números racionales.

    (a) Demuestre que {a + b $\sqrt{2}$ | a, b F} es un campo. (b) Dé las condiciones necesarias y suficientes para que {a + b $\sqrt[3]{2}$ | a, b F} sea un campo.

12. Sea K una extensión de campo de un campo F y sea α un elemento de K. Dé los valores necesarios y condiciones suficientes para que {a + bα | a, b F} sea un cuerpo.

13. Sea K un campo de extensión de F con a, b K. Sea [F(a) : F] = m y [F(b) : F] = n y Suponga que (m, n) = 1. Demuestre que F(a) ∩ F(b) = F y [F(a, b) : F] = mn.

14. Sean F, L y K subcampos de un campo M, con F K y F L. Sea [K : F] = k y [L : F] = .

(a) Demuestre que [KL : F] k. (b)

Demuestre que si (k,) = 1 entonces [KL : F] = k. (c) Dé

un ejemplo donde [KL : F] < k.

15. Sea K un campo de extensión de dimensión finita de un campo F y sea G un grupo de F-automorfismos de K. Demuestre que |G| [K : F].

16. Sea E una extensión de dimensión finita de un campo F y sea G un grupo de F-automorfismos de E tal que [E : F] = |G|. Demuestre que F es el campo fijo de G.

17. Sea E una extensión de dimensión finita de un campo F y sea G un grupo de F-automorfismos de E. Demuestre que si F es el campo fijo de G, entonces [E : F] = |G|.

18. Sea F un campo con la propiedad = 0,

(*) Si a, b F y a ^{2} +b ^{2} entonces a = 0 y b = 0.

(a) Demuestre que ^{2} + 1 es irreducible en F[x].

x (b) ¿Cuál de los campos Z3, Z5 satisface (*)?

19. Demuestre que p(x) = x ^{3} + x − 6 es irreducible sobre Q[i].

20. En cada caso a continuación se dan un cuerpo F y un polinomio f(x) F[x]. Demuestre que f es irreducible sobre f o factorice f(x) en polinomios irreducibles en F[x]. Encuentre [K : F], donde K es un cuerpo de descomposición para f sobre F.

(a) F = Q, f(x) = x (b) F = ^{4} − 5.

Q(√ −3), f(x) = x ^{3} − 3.

(c) F = Q, f(x) = x ^{3} $^{2 − x}$ − 5x + 5.

21. Sea Q el cuerpo de los números racionales. Demuestre que el grupo de automorfismos de Q es trivial.

22. Sea R el cuerpo de números reales. Demuestre que el grupo de automorfismos de R es trivial.

23. Sea R el cuerpo de los números reales. Demuestre que si f(x) es un polinomio irreducible sobre R, entonces f es de grado 1 o 2.

24. Sea F un cuerpo y p a primo. Sea G = {c F | c ^{norte} $_{pag}$ = 1 para algún entero positivo n}.

(a) Demuestre que G es un subgrupo del grupo multiplicativo de F. (b)

Demuestre que G es un grupo cíclico o que G es isomorfo a Z(p∞), el grupo de Prèufer para el primer p.

25. Sea E una extensión de dimensión finita de un cuerpo F y sea G un grupo de F-automorfismos de E. Muestre lo siguiente. (a) Si e E entonces
Ge = {σ G | σ(e) = e} es un subgrupo de G. (b) [G : Ge] [F(e) : F]. (c) Si F
es el cuerpo fijo de G y e1,
e2, . . . , en son las imágenes distintas de e bajo G, entonces f(x) = (x − e1)(x − e2)· · ·(x − en) es el polinomio minimal de e sobre F.

26. Demuestre que $Q(\sqrt{2}, \sqrt{3})$ es una extensión simple de Q.

27. Encuentra el polinomio mínimo de $\alpha = 3 + \sqrt{7}$ sobre el cuerpo Q de números racionales y demuestra es el polinomio mínimo.

28. Encuentra el polinomio mínimo de $\alpha = 5 + \sqrt{3}$ sobre el cuerpo Q de números racionales y demuestra es el polinomio mínimo.

29. Encuentra el polinomio mínimo de $\alpha = 11 + \sqrt{3}$ sobre el cuerpo Q de números racionales, y Demuestra que es el polinomio mínimo.

30. Encuentra el polinomio mínimo de $\alpha = 3 + 2\sqrt{2}$ sobre el cuerpo Q de números racionales, y Demuestra que es el polinomio mínimo.

31. Encuentra el polinomio mínimo de α = es el $\sqrt[3]{2 + \sqrt{2}}$ sobre el cuerpo Q de números racionales, y demuestra polinomio mínimo.

32. Sea F un cuerpo. Demuestre que F es algebraicamente cerrado si y solo si todo ideal máximo de F[x] tiene codimensión 1.

Extensiones algebraicas

33. Sea α perteneciente a alguna extensión de campo del campo F. Demuestre que F(α) = F[α] si y sólo si α es algebraico sobre F.

34. Demuestre que $p(x) = {}^{3} + 2x + 1$ es irreducible sobre Q. Sea θ una raíz de p(x) en una extensión campo x y encuentre el inverso multiplicativo de 1 + θ en Q[θ].

35. Sean F K cuerpos y sea α K algebraico sobre F con polinomio minimal f(x) F[x] de grado n. Demuestre que {1, α, . . . , αn−1} es una base para F(α) sobre F.

36. Demuestre que si K es una extensión de campo de dimensión finita de F, entonces K es algebraico sobre F.

37. Sea F un campo, sea E = F(α) un campo de extensión simple de F, y sea β E − F. Demuestre que α es algebraico sobre F(β).

38. Demuestre que si |F : Q| = 2, entonces existe un entero libre al cuadrado m distinto de 1 tal que F = $Q(\sqrt{m})$.

39. Sea K un cuerpo de extensión del cuerpo F tal que [K : F] es impar. Demuestre que si u K entonces F(u) = $F(u^{2})$.

40. (a) Sea α algebraico sobre un cuerpo F y haga E = F(α). Demuestre que si |E : F| es impar, entonces E = $F(\alpha^{2})$.
(b) Dé un ejemplo de una extensión algebraica simple E = F(α) donde |E : F| no es divisible) está estrictamente por 3 pero $F(\alpha^{3})$ contenido en E.

41. Sea K una extensión de grado finito del campo F tal que [K : F] es relativamente primo a 6.
Demuestre que si u K entonces F(u) = F(u ^{3}).

42. Sea F un cuerpo, f(x) un polinomio irreducible en F[x], y α una raíz de f en alguna extensión de F. Demuestre que si algún término de grado impar de f(x) tiene un coeficiente distinto de cero, entonces F(α) = F(α ^{2}).

43. Sean f(x) y g(x) polinomios irreducibles en F[x] de grados m y n, respectivamente, donde (m, n) = 1. Demuestre que si α es una raíz de f(x) en alguna extensión de cuerpo de F, entonces g(x) es irreducible en F(α)[x].

44. Sea K un campo de extensión de F y sea α un elemento de K. Demuestre que si F(α) = F(α entonces α es algebraico ^{2}), sobre F.

45. Sea K un campo de extensión de F y sea α un elemento de K. Demuestre que los siguientes son equivalente:
(i) α es algebraico sobre F, (ii)
F(α) es una extensión de dimensión finita de F, (iii) α está
contenido en una extensión de dimensión finita de F.

46. Sea α algebraico sobre Q con [Q(α) : Q] = 2 y F = Q(α). Demuestre que si f(x) Q[x] es irreducible sobre Q, entonces ocurre una de las siguientes situaciones:
(i) f(x) sigue siendo irreducible en F[x]; (ii) f(x)
es un producto de dos polinomios irreducibles en F[x] de igual grado.

47. Sea F E K una torre de campos tal que K = F(α) con α algebraico sobre F. Demuestre que si f(x) F[x] es el polinomio minimal de α sobre F y F = E, entonces f(x) no es irreducible en E[x].

48. Sea E un campo de extensión de F y A = {e E | e es algebraico sobre F}.
(a) Demuestre que A es un subcuerpo de E que contiene a F.
(b) Demuestre que si σ : E → E es un F-homomorfismo biunívoco, entonces σ(A) = A.

49. Sean p y q primos distintos. Demuestre que $\sqrt{q}$ no es un elemento de $Q(\sqrt{p})$.

50. Demuestre que si p1, . . . , pn, pn+1 son números primos distintos, entonces $\sqrt{pn+1}$ no es un elemento del campo $Q(\sqrt{p1}, \ldots, \sqrt{pn})$.

51. Sean α1, α2 y α3 números reales tales que (αi) ^{2} Q para cada i, y sea K = Q(α1, α2, α3).
Demuestre que $\sqrt{3}$ 2 no está en K.

52. (a) Demuestre que si E es una extensión de campo de dimensión finita de F que se genera sobre F por F para todo un subconjunto S de E que satisface ^{2} a S, entonces |E : F| es una potencia de 2.
a (b) Dé un ejemplo que muestre que 2 no puede reemplazarse por 3 en la parte (a).

53. Sea F L K con [L : F] finito, y sea α un elemento de K. Demuestre que α es algebraico sobre L si y sólo si α es algebraico sobre F.

54. Demuestre que si K es algebraico sobre F y σ : K → K es un F-monomorfismo, entonces σ es sobrexpositivo.

55. Supóngase que K es un campo de extensión algebraica de un campo F tal que sólo hay un número finito de campos intermedios entre F y K. Demuestre que K es una extensión simple de F.

56. Sea K una extensión algebraica simple de un campo F. Demuestre que solo hay un número finito de campos intermedios entre F y K.

57. Supóngase que E es una extensión algebraica de F y $\bar{E}$ es un cierre algebraico de E. Demuestre que $\bar{E}$ es un cierre algebraico de F.

58. Sea α algebraico sobre el cuerpo F con polinomio minimal f(x) F[x] y sea K = F[α]. Demuestre que si σ : F → L es un monomorfismo de campo y β L es una raíz de f σ (x) L[x], entonces σ tiene una extensión única ˆσ : K → L que satisface ˆσ(α) = β.

59. Supóngase que E1 y E2 son cierres algebraicos de un campo F. Demuestre que existe un F-isomorfismo. σ : E1 → E2.

60. (a) Demuestre que para cada primo p y cada entero positivo n existe un polinomio irreducible. mial de grado n sobre el cuerpo Fp de p elementos.

(b) Demuestre que para cada entero positivo n existe un polinomio irreducible de grado n sobre el campo Q de los números racionales.

Normalidad y campos de división

61. Sea K un campo de extensión de F. Demuestre que los siguientes son equivalentes. (i) Cada polinomio irreducible en F[x] con una raíz en K tiene todas sus raíces en K. (ii) K se obtiene de F mediante la unión de todas las raíces de un conjunto de polinomios en F[x]. (iii) Cada F-isomorfismo de K en un cierre algebraico fijo es un F-automorfismo.

62. Sea K el campo de descomposición de $x^2 + 2$ sobre Q. Demuestre o refute que $i = \sqrt{-1}$ es un elemento de K.

63. Sea K el campo de descomposición de $x^3 - 5$ sobre Q. Demuestre o refute que $i = \sqrt{-1}$ es un elemento de K.

64. Sea Ω una clausura algebraica fija de F y K Ω una extensión algebraica de F. Demuestre que K es una extensión normal de F si y solo si todo F-isomorfismo : K → K Ω es un F-automorfismo.

65. Sea F un cuerpo y E un cuerpo de desdoblamiento del polinomio irreducible f(x) F[x]. Demuestre que si c, d F y c = 0, entonces el polinomio f(cx + d) se divide en E[x].

Posibilidad de separación

66. Demuestre que si K es una extensión separable de F y L es un campo con F L K, entonces L es un La extensión separable de F y K es una extensión separable de L.

67. Sea f(x) F[x] un polinomio, y sea f (x) su derivada formal en F[x]. Demuestre que f(x) tiene raíces distintas en cualquier cuerpo de extensión de F si y solo si mcd(f(x), f (x)) = 1.

68. Demuestre que si K es una extensión separable de dimensión finita de F, entonces K = F(u) para algún u tinta.

69. Sea F un campo y sea f(x) = xpn − 1, norte − x F[x]. Demuestre que si char F = 0 o si char F = p y entonces f no tiene raíz múltiple en ninguna extensión de F.

70. Demuestre que si F es un campo de característica 0 entonces toda extensión algebraica de F es separable. (Proporcione un argumento; no se limite a afirmar que todo campo de característica 0 es perfecto y que toda extensión algebraica de un campo perfecto es separable).

71. Demuestre que si F es un campo finito, entonces toda extensión algebraica de F es separable.

72. Sea F un cuerpo de característica p y sea x una indeterminada sobre F.
(a) Demuestre que F(x p) es un subcuerpo propio de F(x). (b)
Demuestre que F(x) es un cuerpo de descomposición para algún polinomio sobre F(x p).
(c) Demuestre que el único automorfismo de F(x) que fija F(x p) es el automorfismo identidad.

73. Sea F un cuerpo y f(x) F[x] un polinomio irreducible. Demuestre que existe un primo p, un entero a ≤ 0 y un polinomio separable g(x) F[x] tal que f(x) = g(x p a).

74. Sea K una extensión separable arbitraria de F. Demuestre que si cada elemento de K es raíz de un polinomio en F[x] de grado menor o igual a n, entonces K es una extensión simple de F de grado menor o igual a n.

75. Sea F un cuerpo y sea f(x) F[x] con cuerpo de desdoblamiento K. Demuestre que si el grado de f es un primo p y [K : F] = tp para algún entero t, entonces (a) f(x) es
irreducible sobre F y (b) si t > 1 entonces
K es una extensión separable de F.

76. Sean x e y indeterminadas independientes sobre Zp, K = Zp(x, y), y F = Zp(x p , yp).
(a) Demuestre que [K : F] = p (b) 2
Demuestre que K no es una extensión simple de F.

77. Un cuerpo F se llama perfecto si cada elemento de una clausura algebraica de F es separable sobre F.
Sea F un campo de característica p. Demuestre que los siguientes son equivalentes.
(i) El campo F es perfecto. (ii)
Para cada F existe un δ F tal que δ p (iii) La función a → a p = .
es un automorfismo de F.

78. Demuestre que todo campo de característica 0 es perfecto.

79. Demuestra que todo campo finito es perfecto.

80. Sean F K campos que tienen característica p y supóngase que K es una extensión algebraica normal de F.
Demuestre que existe un campo E con F E K, E/F puramente inseparables y K/E separables.

81. Sea E un cuerpo y sea G un grupo finito de automorfismos de E. Sea F el cuerpo fijo de G. Demuestre que E es una extensión algebraica separable de F.

82. Sea G un grupo finito de automorfismos del cuerpo K y del conjunto

$$F = \{\alpha \in K \mid \alpha^{\sigma} = \alpha \text{ para todo } \sigma \in G\}.$$

Demuestre que cada elemento de K es separablemente algebraico sobre F de grado como máximo |G|.

83. Sea p un primo y sea F = Zp(x) el cuerpo de fracciones de Zp[x]. Sea E el cuerpo de descomposición de f(y) = y p − x sobre F. (a) Demuestre que [E : F] = p. (b) Demuestre que |AutF (E)| = 1. (c) ¿Qué conclusión puede extraer de (a) y (b)?

84. Sea K = F(u) una extensión separable de F con u metro F para algún entero positivo m. Muestre r, que si la característica de F es p y m = p el luego u o F.

85. Si K es una extensión de un campo F de característica p = 0, entonces un elemento u de K se llama puramente inseparable sobre F si u p t F para algún t. Demuestre que los siguientes son equivalentes.
(i) u es puramente inseparable sobre F.
(ii) u es algebraica sobre F con el polinomio mínimo x. (iii) u es pag nota − a para algún a F y entero n.
algebraica sobre F y sus factores polinomiales mínimos como (x − u) m.

86. Demuestre que toda extensión de campo puramente inseparable es una extensión normal.

87. Sea K una extensión de un campo F de característica p = 0. Demuestre que un elemento u de K es a la vez separable y puramente inseparable si y sólo si u F.

88. Sea Z2(x) el campo de fracciones del anillo polinomial Z2[x]. Construya una extensión de Z2(x) que no es ni separable ni puramente inseparable.

Teoría de Galois

89. Enuncie el teorema fundamental de la teoría de Galois.

90. Sea K una extensión de Galois finita de F con grupo de Galois G. Supóngase que E1 y E2 son extensiones intermedias que satisfacen E1 E2, y sean H1 H2 los subgrupos correspondientes de G. Demuestre que E2 es una extensión normal de E1 si y solo si H2 es un subgrupo normal de H1, y cuando esto sucede, el grupo de Galois de E2 sobre E1 es isomorfo a H1/H2.

91. Sea K una extensión finita de Galois de F con grupo de Galois G = Gal(K/F). Sea E un cuerpo intermedio normal a F. Demuestre que Gal(K/E) G y G/Gal(K/E) = Gal(E/F).

92. Sea K una extensión algebraica finita de F y sea G el grupo de todos los F-automorfismos de K. Sea F(G) = {u K | σ(u) = u para todo σ G}. Demuestre que K es separable y normal (es decir, Galois) sobre F si y solo si F(G) = F.

93. Sea K una extensión de Galois del cuerpo F con grupo de Galois G. Sea g(x) un polinomio mónico sobre F que se descompone sobre K (es decir, K contiene un cuerpo de descomposición para g(x) sobre F) y sea ∆ K el conjunto de raíces de g(x). Demuestre que g(x) es una potencia de un polinomio irreducible sobre F si y solo si G es transitivo sobre ∆.

94. Sea K un campo de extensión de dimensión finita de L y sea σ : L → F una incrustación de L en un campo F. Demuestre que hay como máximo [K : L] extensiones de σ a incrustaciones de K en F.

95. Si S es cualquier semigrupo (escrito multiplicativamente) y F cualquier cuerpo, un homomorfismo de S en el grupo multiplicativo de elementos distintos de cero de F se llama un F-carácter de S.

Demuestre que cualquier conjunto {σ1, σ2, . . . , σn} de F-caracteres de S es linealmente independiente en el espacio vectorial sobre F de funciones S → F.

96. Sea K un campo de extensión de F y sea F el campo fijo del grupo de F-automorfismos. de K. Demuestre que K es una extensión de Galois de F .

97. Sea K una extensión normal finita de F y sea E el cuerpo fijo del grupo de todos los F-automorfismos de K. Demuestre que el polinomio mínimo sobre F de cada elemento de E tiene sólo una raíz distinta.

98. Sea E un campo de desdoblamiento sobre F de un polinomio separable f(x) en F[x] y G = Gal(E/F). Demuestre que {e E | σ(e) = e para todo σ G} = F.

99. [NUEVO]
Sea F un cuerpo, f(x) F[x] irreducible y separable sobre F, y K el cuerpo de desdoblamiento de f(x) sobre F. Demuestre que si el grupo de Galois de K sobre F es abeliano, entonces K = F(α), donde α es una raíz de f(x).

100. Sea K una extensión de Galois de F con |Gal(K/F)| = 12. Demuestre que existe un subcuerpo E de K que contiene a F con [E : F] = 3. ¿Existe necesariamente una subextensión L que satisfaga [L : F] = 2? Explique.

101. Supóngase que K = F(α) es una extensión de Galois propia de F y supóngase que existe un elemento σ) : F] = de Gal(K/F) que satisface σ(α) = α $^{-1}$. Demuestre que [K : F] es par y que [F(α + α $^{-1}$ $\frac{}{12}$[K : F].

102. Sea K una extensión de Galois finita de F de característica 0. Demuestre que si Gal(K/F) es un 2-grupo no trivial, entonces existe una extensión cuadrática de F contenida en K.

103. Sea G un grupo finito. Demuestre que existe una extensión algebraica F del cuerpo Q de números racionales. números y una extensión de Galois K de F tal que G = Gal(K/F).

104. (a) Halla el grupo de Galois de x entre los ^{3} − 2 sobre Q y demostrar la correspondencia de Galois subgrupos del grupo de Galois y los subcuerpos del cuerpo descomponedor. (b) Halla todos los automorfismos de Q(√3 2). ¿Existe una f(x) $\overline{\ }$Q[x] con cuerpo descomponedor Q(√3 2)? $\overline{\ }$ Explicar.

105. Sea F cualquier cuerpo y sea f(x) = x $^{\text{nonu}}$ − 1 F[x]. Demuestre que si K es el campo de desdoblamiento de f(x) sobre F, entonces K es separable sobre F (de ahí Galois) y que Gal(K/F) es abeliano.

106. Sea η7 una raíz 7.ª primitiva compleja de la unidad y sea K = Q(η7). Halle Gal(K/Q) y exprese cada cuerpo intermedio F entre Q y K como F = Q(β) para algún β K.

107. Sea η una raíz 7.ª primitiva compleja de la unidad y sea K = Q(η), donde Q es el cuerpo de los números racionales. Demuestre que existe una extensión única F de grado 2 de Q contenida en K y halle q Q tal que F = Q(√q).

108. Sea Q el cuerpo de los números racionales y η una raíz octava primitiva compleja de la unidad. Determine Gal(Q(η)/Q) y todos los campos intermedios entre Q y Q(η).

109. (a) Determine el grupo de Galois de $x^4 - 4$ sobre el cuerpo Q de números racionales.

(b) ¿Cuántos campos intermedios hay entre Q y el campo de división de $x^4 - 4$?

110. Sea $f(x) = (x^2 - 2)(x^2 - 3)$ y sea K el campo de desdoblamiento de f(x) sobre Q. Halla, con prueba, todos los elementos de Gal(K/Q) y todos los subcampos intermedios de K.

111. Determine el grupo de Galois de $x^4 - 4$ sobre el campo Q de números racionales e identificar todos de los campos intermedios entre Q y el campo de división de $x^4 - 4$. Utilice los fundamentos Teorema.

112. Determine el grupo de Galois de $x^4 - 3$ sobre el cuerpo Q de números racionales.

113. Determine el grupo de Galois de $x^4 + 2$ sobre el cuerpo Q de números racionales.

114. Determine el grupo de Galois de $x^3 + 3x^2 - 1$ sobre Q.

115. Demuestre que el grupo de Galois de $x^3 - 5$ sobre Q es S3 y demuestra la correspondencia de Galois entre los subgrupos de S3 y los subcampos del campo de división. ¿Qué subcampos son? ¿normal sobre Q?

116. Sea K el campo de descomposición de $x^3 - 3$ sobre Q. Utilice la teoría de Galois para identificar Gal(K/Q) y encontrar explícitamente todos los subcampos intermedios.

117. Sea K un campo de descomposición para $x^5 - 2$ sobre Q.

(a) Determine [K : Q].

(b) Demuestre que Gal(K/Q) no es abeliano.

(c) Encuentre todas las extensiones intermedias normales F y expréselas como F = Q(α) para α apropiado.

118. Sea Q el cuerpo de los números racionales y E el cuerpo de descomposición (en el cuerpo de los números complejos). números) de $x^4 - 2$.

(a) Encuentra |Gal(E/Q)|.

(b) Sea $\sigma \in Gal(E/Q)$ tal que $\sigma(\alpha) = \bar{\alpha}$ para todo $\alpha \in E$ (donde $\bar{\alpha}$ es el conjugado complejo de α). Encuentre $Inv(\sigma) = \{\alpha \in E \mid \sigma(\alpha) = \alpha\}$.

(c) ¿Es σ un subgrupo normal de Gal(E/Q)?

119. Sea $f(x) = x^4 + 4x^2 + 2$ y sea K el campo de desdoblamiento de f sobre Q. Demuestre que la función de Galois El grupo de K sobre Q es cíclico de orden 4.

120. [NUEVO]
Hallar, con demostración, el grupo de Galois del campo de descomposición sobre los números racionales de la polinomio f(x) donde

(a) $f(x) = x^6 + 3$,

(b) $f(x) = x^6 - 3$,

(c) $f(x) = x^8 + 2$,

(d) $f(x) = x^8 - 2$.

121. Sea p un número primo y sea K el campo de descomposición de $f(x) = x^6 - p$ sobre Q, el campo de Números racionales. Determine el grupo de Galois de K sobre Q, así como todos los intermedios. campos E que satisfacen |E : Q| = 2.

122. Sea F el cuerpo de 2 elementos y K un cuerpo de descomposición de f(x) = x (a) $^{6\,3\,+\,1}$ sobre F. + x
Demuestre que si r es una raíz de f, entonces r ^{9} 3 = 1 pero r = 1.
(b) Demuestre que f es irreducible sobre F. (c)
Encuentre Gal(K/F) y exprese cada cuerpo intermedio entre F y K como F(b) para ap-
b apropiado en K.

123. Sea K una extensión de Galois de Q cuyo grupo de Galois es isomorfo a S5. Demuestre que K es el cuerpo de desdoblamiento de algún polinomio de grado 5 sobre Q.

124. Sea f(x) Q[x] un polinomio irreducible de grado n con raíces α1, . . . , αn. Demuestre que
$\sum_{i=1}^{n} \frac{1}{\alpha i}$ es un número racional.

125. Sea $\alpha = \sqrt{2} + \sqrt{3}$ y sea E = Q(α). (a) Encuentre
el polinomio minimal m(x) de α sobre Q y |E : Q|. (b) Encuentre el cuerpo de
descomposición de m(x) sobre Q y todos los cuerpos intermedios, y encuentre su grupo de Galois sobre Q y todos sus subgrupos.

126. Sea $\alpha = 3 + \sqrt{5}$. (a)
Encuentre el polinomio mínimo m(x) de α sobre Q. (b) Encuentre,
con prueba, el grupo de Galois del campo de descomposición de m(x) sobre Q.

127. (a) Encuentre el polinomio mínimo f(x) de $\alpha = 8 + \sqrt{15}$ sobre Q y demuestre que su respuesta es correcto
(b) Encuentre el grupo de Galois del campo de división de f(x) sobre Q.

128. Sea $u = 2 + \sqrt{2}$, $v = 2 - \sqrt{2}$, y E = Q(u), donde Q es el campo de los números racionales.
(a) Halla el polinomio mínimo f(x) de u sobre Q. (b) Muestra que
v E. Por lo tanto, concluye que E es un campo de descomposición de f(x) sobre Q. (c)
Determine el grupo de Galois de E sobre Q.

129. Sea F un cuerpo de característica 0 y sea a F. Demuestre que si $f(x) = x^4 + ax^2 + 1$ es irreducible sobre F y K es un cuerpo de desdoblamiento para f(x) sobre F, entonces Gal(K/F) tiene orden 4 y no es cíclico. [Pista: Si α es una raíz de f(x), entonces también lo son −α y 1/α].

130. Sea $\alpha = 5 + 2\sqrt{5}$. Demuestre que Q(α) es una extensión cíclica de Galois de Q de grado 4. Encuentre todos los campos F con Q F Q(α).
[Pista: Demuestre que $f(x) = x^4 - 10x^2 + 5$ es el polinomio mínimo de α sobre Q y que el de f son ±α, ± raíces alfa]

131. Sea p un primo tal que existe un entero positivo d con $p = 1+d^2$ y sea $\alpha = p + d\sqrt{p}$.
Demuestre que Q(α) es una extensión de Galois cíclica de Q de grado 4. Encuentre todos los campos F con Q F Q(α).
[Pista: Demuestre que $f(x) = x^4 - 2px2 + p$ es el polinomio mínimo de α sobre Q y que de f son ±α, ± raíces alfa]

132. Sea f(x) Q[x] un polinomio irreducible de grado 4 con exactamente dos raíces reales. Demuestre que el grupo de Galois de f sobre Q es de orden 8 o 24.

133. Sea f(x) Q[x] un polinomio irreducible de grado 4 con exactamente 2 raíces reales. Demuestre que el grupo de Galois de f sobre Q es S4 o el grupo diedro de orden 8.

134. Sea f(x) Q[x] un polinomio irreducible de grado 5. Supóngase que f(x) tiene exactamente 3 raíces reales distintas y un par complejo conjugado de raíces. Demuestre que si K es el cuerpo de descomposición de f(x) sobre Q, entonces Gal(K/Q) es S5.

135. Sea f(x) Q[x] un polinomio irreducible de grado n > 2 con n − 2 raíces reales y exactamente un par de raíces conjugadas complejas. Demuestre que el grupo de Galois de f(x) sobre Q no es un grupo simple.

136. Sea f(x) = x si α^4 + ax3 + bx2 + ax + 1 Q[x] y sea F un campo de desdoblamiento sobre Q. Demuestre que es una raíz de f, entonces 1/α también es una raíz, y |Gal(F/Q)| 8.

137. Sea F un cuerpo y sea f(x) F[x] un polinomio irreducible de grado 4 con raíces distintas α1, α2, α3 y α4. Sea K un cuerpo de desdoblamiento para f sobre F y supóngase Gal(K/F) = S4.
Encuentre Gal(K/F(β)), donde β = α1α2 + α3α4.

138. Sea E una extensión de Galois de dimensión finita de un cuerpo F y sea G = Gal(E/F). Supóngase que G es un grupo abeliano. Demuestre que si K es cualquier cuerpo entre E y F, entonces K es una extensión de Galois de F.

139. Sea K una extensión finita de Galois de F y sea E un cuerpo intermedio normal sobre F. Para un elemento σ de Gal(K/F) y g(x) = e0 + e1x + · · · + emx en E[x], denote σg(x) = σ(e0) + σ(e1)x + · · · + σ(em)x m. Para un[metro] elemento fijo α de K, sea f(x) E[x] el polinomio minimal de α sobre E. Demuestre lo siguiente. (a) σ(α) es una raíz de σf(x). (b) Si f1(x), f2(x), . . . , fn(x) son todos los elementos distintos de {σf(x) | σ Gal(K/F)}, entonces h(x) = f1(x)f2(x)· · · fn(x) está en F[x]. (c) h(x) es el polinomio mínimo de α sobre F.

140. Sea K una extensión de Galois de k y sea k F K y k L K.
(a) Demuestre que Gal(K/LF) = Gal(K/L) ∩ Gal(K/F). (b) Demuestre que Gal(K/L ∩ F) = Gal(K/L), Gal(K/F).

141. Sea $\overline{Q}$ la clausura algebraica de Q y sea α un elemento de $\overline{Q}$ no en Q.
(a) Demuestre que existe un campo M Q que es máximo con respecto a la propiedad que α M.
(b) Demuestre que cualquier extensión de Galois finita de M tiene un grupo de Galois cíclico.
(c) Demuestre que cualquier extensión finita de M es una extensión de Galois.

142. Sea E una extensión de Galois de dimensión finita de un cuerpo F y sea G = Gal(E/F). Para e E, sea G(e) = {σ(e) | σ G}. Sean e1, e2, ..., en todos los elementos distintos de G(e). (a) Demuestre que f(x) = (x − e1)(x − e2)· · ·(x − en) está en F[x]. (b) Demuestre que f(x) es irreducible en F[x].

143. Sea E una extensión de Galois de dimensión finita de F de característica distinta de 2. Supóngase que Gal(E/F) es un grupo no cíclico de orden 4. Demuestre que E = F(α, β) para algún α, β E con α^2 F y β^2 F.

144. Sea E = Q[α, β], donde α ^{2}, β2 Q y |E : Q| = 4. Demuestre que si γ E − Q y γ ^{2} Q, entonces γ es un múltiplo racional de uno de α, β o αβ.

Extensiones ciclotómicas

145. Encuentra los polinomios ciclotómicos 6º, 8º y 12º sobre Q.

146. Sea α una raíz 43ª primitiva compleja de 1. Demuestre que existe un campo de extensión F de los números racionales tal que [F(α) : F] = 14.

147. Sea m un entero impar y ηm, η2m una raíz primitiva compleja m-ésima y 2m-ésima de la unidad, respectivamente. Demuestre que Q(ηm) = Q(η2m).

148. Sea (m, n) = 1, y si i es cualquier entero positivo, sea ηi una raíz primitiva compleja i-ésima de unidad. Demuestre que Q(ηmn) = Q(ηm)Q(ηn) y Q(ηm) ∩ Q(ηn) = Q.

149. Sea el número complejo cos((a) es $\frac{2\pi}{\text{norte}}$) + está en($\frac{2\pi}{\text{norte}}$), donde n es un entero positivo. Mostrar algebraico sobre el cuerpo Q de números racionales, (b) si Φn(x)

es el polinomio mínimo de sobre Q, entonces Q() es un cuerpo de descomposición de Φn(x) sobre Q,

(c) el grupo de Galois de Q() sobre Q es isomorfo al grupo de unidades de Zn.

150. Sea una raíz n-ésima primitiva de la unidad sobre Q, donde n > 2, y sea α = + $^{-1}$. Demuestre que α es algebraica sobre Q de grado (n)/2.

Campos finitos

151. Demuestre que el grupo multiplicativo de un campo finito debe ser cíclico.

152. Demuestre que cualquier extensión finita de un campo finito debe ser una extensión simple.

153. Demuestre que dos campos finitos cualesquiera del mismo orden son isomorfos.

154. Sea F una extensión de Zp de grado n. Demuestre que F es una extensión de Galois y Gal(F/Zp) es cíclico de orden n.

155. Demuestre que toda extensión finita de un campo finito es una extensión de Galois.

156. Demuestre que toda extensión algebraica de un campo finito es separable.

157. Demuestre que todo cuerpo finito es perfecto. (Recuerde que un cuerpo F de característica p se llama perfecto, p F). Si la función α → αs una sobreyección sobre

158. Sea f(x) Zp[x] irreducible de grado m. Demuestre que f(x) | (x p $^{\text{norte}}$ − x) si y sólo si m | n.

159. Sea p un primo. Demuestre que el cuerpo de p elementos es un subcuerpo del cuerpo de p si y solo ^{b} elementos si a | b.

160. Sea p un primo y Fp el cuerpo de p elementos. Demuestre que para cada entero positivo n, hay es un polinomio irreducible de grado n sobre Fp.

161. Sea F un cuerpo finito. Demuestre que el anillo de polinomios F[x] contiene polinomios irreducibles de grado arbitrario.

162. Sea F un cuerpo finito. Demuestre que el producto de todos los elementos no nulos de F es −1.

163. Sea Fq el cuerpo de q elementos y sea f(x) un polinomio en Fq[x]. Demuestre que si α es una raíz de f(x), entonces α q también es una raíz de f(x).

164. Sean E y F subcampos de un campo finito K. Demuestre que si E es isomorfo a F entonces E = F.

165. Sean E y F subcuerpos finitos de un cuerpo K. Demuestre que si E y F tienen el mismo número de elementos, entonces E = F.

166. Sea Fp el cuerpo de p elementos y sea K una extensión de Fp de grado n. Demuestre que el conjunto de subcuerpos de K está ordenado linealmente (es decir, para cada par de subcuerpos L1 , L2, L1 L2 o L2 L1) si y solo si n es una potencia prima.

167. Sea f(x) = x un ^{2} − 2 Fp[x], donde p > 2 es primo y Fp es el cuerpo de p elementos. Dar un ejemplo de un primo p para el cual f es irreducible y otro ejemplo donde f se reduce.

168. Sea α una raíz de x 2+1 en una extensión de Z3, K = Z3(α), y sea f(x) = x 4+x 3+x+2 Z3[x].

(a) Demuestre que f se divide entre K.

(b) Encuentre un generador α del grupo multiplicativo de K y exprese las raíces de f en términos de α.

169. Sea α una raíz de x ^{2} + 1 en una extensión de Z3, K = Z3(α), y sea f(x) = x ^{4} + 1 Z3[x].

(a) Demuestre que f se divide entre K.

(b) Encuentre un generador β del grupo multiplicativo K de K. (c) Exprese las raíces de f en términos de β.

170. Sea K = Z3($\sqrt{2}$) y sea f(x) = x $^{4\,3}$ + x + 2 Z3[x]. (a) Demuestre que f se divide en K. (b) Encuentre un generador α del grupo multiplicativo K de K. (c) Exprese las raíces de f en términos de α.

171. Sea F = F81 el cuerpo de 81 elementos. (a) Halla todos los subcuerpos de F. (b) Determina el número de elementos primitivos para F sobre el cuerpo F3 de 3 elementos (es decir, elementos α de F tales que F = F3(α)). (c) Halla el número de generadores para el grupo multiplicativo F de F (es decir, elementos β de F tal que β = F).

172. Sea f(x) = x $^{4\,3}$ + 4x − 1 Z5[x]. Encuentra el grupo de Galois del campo de descomposición de f sobre Z5.

Extensiones cíclicas

173. Sea K un cuerpo de característica p = 0 y sea Kp = {u p − u : u K}. Demuestre que K tiene una extensión cíclica de grado p si y sólo si K = Kp.

174. Sea p un primo y F el cuerpo de fracciones de Zp[x]. Si E es el cuerpo de descomposición de y p − y − x sobre F, determinar el grupo de Galois de E sobre F.

175. Sea n un entero positivo y sea F un cuerpo de característica 0 que contiene una raíz n-ésima primitiva de la unidad. Sea a un elemento de F tal que a no es una potencia m-ésima de un elemento de F para cualquier 1 = m | n. Demuestre que si α es cualquier raíz de x − a, entonces F(α) es una extensión cíclica de F de grado n.

176. Sea F un cuerpo que contiene una raíz n-ésima primitiva de la unidad y sea K = F(t), el cuerpo de fracciones del anillo de polinomios F[t]. Sea L = F(t n) K. Demuestre que K es una extensión de Galois de L y que el grupo de Galois es cíclico de orden n.

177. Sea F un cuerpo de característica p. Fijemos c F y sea f(x) = x p − x + c F[x]. Demuestre que si α es raíz de f(x) en algún cuerpo de extensión, entonces también lo es α + 1. Use esto para demostrar que si K es el cuerpo de desdoblamiento de f(x) sobre F, entonces o bien K = F y f(x) se desdobla completamente sobre F, o bien [K : F] = p y f(x) es irreducible sobre F. (Use grupos de Galois).

Extensiones radicales y solubilidad por radicales

178. Una extensión K de F se llama extensión radical si hay una torre de campos

$$F \quad F(u1) \quad F(u1, u2) \quad \cdots \quad F(u1, \ldots, un) = K$$

tal que para i = 1, . . . , n, u_i^{mi} F(u1, . . . , ui−1) para algún entero positivo mi . (a) Dé un ejemplo de una extensión radical que no sea separable. (b) Dé un ejemplo de una extensión radical que no sea normal.

179. Sea F una extensión radical de K. Demuestre que existe una extensión radical N de K con N F K y N normal sobre K.

180. Sea F un cuerpo finito de característica p. Demuestre que si f F[x] es un polinomio irreducible y el grado de f es menor que p, entonces f(x) = 0 es resoluble mediante radicales.

181. Sean x1, . . . ,xn indeterminadas sobre un cuerpo F y sean s1, . . . , sn las funciones simétricas elementales de xi . Demuestre que [F(x1, . . . , xn) : F(s1, . . . , sn)] = n!.

Extensiones trascendentales

182. Sea x una indeterminada sobre el cuerpo F. Demuestre que un elemento de F(x) es algebraico sobre F. si y sólo si es un elemento de F.

183. Sean F E campos con E = F(α), donde α es trascendental sobre F. Demuestre que si β E−F, entonces [E : F(β)] es finito.

184. Sea F un cuerpo, F[x] el anillo de polinomios sobre F en la indeterminada x, y E = F(x) el campo de fracciones de F[x]. (a)

Demuestre que si σ es un automorfismo de E tal que σ(u) = u para todo u F, entonces $\sigma(x) = \frac{ax + b}{cx + d}$ para algunos a, b, c, d F con ad − bc = 0. (b)

Determine el grupo AutF (E) de F-automorfismos de E.

185. Sea K un cuerpo de extensión de F y sea α K trascendental sobre F. Demuestre que si β K es algebraico sobre F(α), entonces existe un polinomio distinto de cero p(x, y) F[x, y] tal que P(α, β) = 0.